Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Index to Volume 14

Thus 2 Sept 1993

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Cellular misinformation (Barry C. Nelson)
- Re: Key Registration (Alec Isaacson, Peter Wayner [2], Andrew Klossner)
- Re: Interesting/obscure interaction between users (Rich Kulawiec)

● Volume 14 Issue 04 (11 November 1992)

- Abuse of federal computer access (Barry C. Nelson)
- Therac-25 (Nancy Leveson)
- When "yes" means "no" (More voting screwups) (Ted Shapin)
- Re: Voting Machine Horror Story (David Conrad)
- Voicemail problems (C Martin)
- FBI digital telephony article in IEEE Institute (M. Granger Morgan via Lance Hoffman)
- Key registration risks (Phil Karn, Otto Tennant, Robert Philhower, PGN)
- Re: Risks Of Cellular Speech (Robert Gezelter)
- Re: Persistent resources and hypertext (David A. Honig)

● Volume 14 Issue 05 (16 November 1992)

- Voting fraud (is it an accident?) (Ray Todd Stevens)
- Safe Conduct (Jonathan Bowen)
- Retirement award trips up a crook (Ray Todd Stevens)
- PINs and Needles (Dik Winter)
- Re: "End-Running" Key Registration (Bob Frankston)
- Re: Cellular Phones in Aircraft (Berry Kercheval)
- Re: Voice mail systems (Jim Purtilo)
- Radio to remote computer protocol design (Edward J. Huff)
- Re: RISKS of technical people disengaging brain (Daniel Lance Herrick)
- Re: Credit Thieves (and learning from mistakes) (Michael J. Zehr)
- Re: Accountant's error catches thief! (D King)
- Re: Caller-ID (yet again) (Greg Rose)
- UNIX security Tutorials (7 Dec, San Jose) (Sun User Group Conference) (Nancy Frishberg)
- Papers accepted for AUSCRYPT'92 (Yuliang Zheng)

● Volume 14 Issue 06 (17 November 1992)

- "Computer programming error" reverses election (Nathan K. Meyers)
- Detecting Voting Problems (Fred Baube)
- Inaccurate stock system believed to cause British Air large losses (John Jones)
- England fights on against system failures: LAS, aging systems (James H. Paul)
- Stock price too high? (David Wittenberg)
- $Million per second -- CHIPS (John Sullivan)
- Re: Tandem's clocks (Don Stokes)
- Photography from orbit (Daniel Burstein)
- Smart cars? (Steve Mestad)
- Warrants without notification (Steve Mestad)
- Re: Two hackers caught tapping into Boeing, federal computers (Graham Toal)
- Registering your color copier/printer (Carl M. Kadie)
- Self-configuring devices (David A. Honig)
- November Scientific American Article on Risks (Greg Phillips)

● Volume 14 Issue 07 (18 November 1992 [misdated 17 Nov])

- Re: Recommended POLL FAULTING by RISKS folks (Rebecca Mercuri)
- Cordless phone users gain some privacy rights (Jerry Leichter)
- How to tell people about risks? (Xavier Xantico)
- Risks of DYI Home movies (Alex Heatley)

  - Re: A320 descent anomalies -- reported in French press (Pete Mellor)
  - Redressing the record on English system maintenance (James H. Paul)
  - Re: Safe Conduct (Ken Tindell)
  - Re: Risks of cellular phones in aircraft (James Olsen, Dan Sorenson, Bob Rahe)
  - Re: Key registration: a naive thought about encryption (Martyn Thomas)
  - Re: RISKS of technical people disengaging brain, encryption, outlaws ... (Mike Dixon, Dan Swartzendruber, Ken Arromdee, John Sullivan, Robert Hartman)

- Volume 14 Issue 08 (21 November 1992)
  - Installer Programs (Macintosh) (Mark Thorson)
  - Election hardware and software problems (A Urken)
  - How to talk about risks (Alan Wexelblat, Stuart Wray, Rob Cameron, Mike Coleman, Pete Mellor, L. Bootland,
  - Re: Software Reliability - how to calculate? (Pete Mellor to Janet Figueroa)
  - Re: POLL FAULTING recommended for RISKS folks (Pete Mellor)
  - Advanced technologies for automotive collision avoidance (Pete Mellor)
  - Wanted: GRADUATE PROGRAM in RISKS (Simson L. Garfinkel)
  - "The Information Society" (Bob Anderson)
  - An airline software-safety database? (Dave Ratner)

- Volume 14 Issue 09 (24 November 1992)
  - BNFL Sellafield nuclear incident (Peter Ilieve)
  - Privacy Risks of Computerized Medical Billing (Paul Kleeberg via John Bonine)
  - Teller machine networks (Steve Holzworth)
  - Re: Election HW/SW problems (Rebecca Mercuri)
  - The ultimate in anti-virus, anti-invasion security (Lee S. Ridgway)
  - Technophones (David Honig)
  - Re: London Ambulance Service (Trevor Jenkins)
  - Mathematics of Dependable Systems (conference announcement, Vicky Stavridou)

- Volume 14 Issue 10 (25 November 1992)
  - Police and Database [another name confusion] (Stanley (S.T.H.) Chow)
  - Nuclear-plant risks in the US (Alan Wexelblat)
  - Re: Election HW/SW Problems (Bill Murray)
  - Voting-machine humor (submitted by Joshua E. Muskovitz from rec.humor.funny)
  - Re: Smart cars? (Brinton Cooper)
  - Re: Installer problems (Richard Wexelblat)
  - Re: How to tell people about risks? (Richard Stead, John A. Palkovic, Arthur Delano, Phil Agre, George Buckner, Chaz Heritage)
  - Re: Stock price too high? (John R. Levine, Randall Davis)

- Volume 14 Issue 11 (27 November 1992)
  - Re: Computer Security Act and Computerized Voting Systems (Roy G. Saltman, Rebecca Mercuri)
  - How Is Technology Used for Crime in the Post-Hacker Era? (Sanford Sherizen)
  - Re: Nuclear plant risks (Brad Dolan)
  - Re: Installer Programs (John Bennett, Mathew)
  - Re: How to tell people about risks? (Sanford Sherizen, Mark Day)
  - Change in the Maximum Length of International Telephone Numbers (Nigel Allen)
  - Humorous submissions for a book (Andrew Davison)

- Volume 14 Issue 12 (30 November 1992)

  - Laser Printer Sucks up Cat (Douglas M. Kavner)
  - British Telecom find themselves being a phone pest (David Shepherd)
  - "The risk is not obvious" (Don Norman, Rex Black)
  - Re: Name confusions? (Don Norman, Jerry Leichter)
  - Electronic Banking Risks (Ross Anderson)
  - Re: How Is Technology Used for Crime ... (FoFP)
  - SNL accidentally informs people about risks of caller ID (Sean Eric Fagan)
  - Re: Nuclear plant risks (Victor Yodaiken)

- Volume 14 Issue 13 (2 December 1992)

  - Blackmail risk in thefts from general practitioners (Paul Leyland)
  - Computerized Voting (Doug Hardie)
  - Global Positioning System - Position Errors (Stuart Bell)
  - Re: Laser Printer Sucks up Cat (Dan Sorenson)
  - Smokey is not always a bear (Alan Dahl)
  - A310 Aerobatics (Karl Swartz)
  - New Distributed Systems Engineering Journal (Morris Sloman)

- Volume 14 Issue 14 (2 December 1992)

  - Akron BBS trial update! (David Lehrer)
  - Holiday reading on Risks (Phil Agre)
  - Re: Books on Probability (Pete Mellor)
  - FME'93 Call For Participation and Programme (Peter Gorm Larsen)

- Volume 14 Issue 15 (7 December 1992)

  - Similar But Different User Interfaces and Traces of Memory (Tom Swiss)
  - Name Confusion and Democratic Concept of Limited Government (Roy G. Saltman)
  - Re: Police and Database [name confusion with twist] (Alan (A.G.) Carter)
  - Toronto Stock Exchange Virus Scare (Shyamal Jajodia)
  - Re: Akron BBS trial update! (Phil Karn)
  - Risks of children using BBSes (Re: Akron BBS ..) (Michael P. Deignan)
  - Lost Technology (A. Padgett Peterson)
  - Re: Computer theft from GP's; encryption is not a cure-all (Julian Thomas)
  - Turn Signals (John Sullivan)
  - Estimating risks (Jerry Leichter)
  - Revenge via computer (Thomas Dzubin)
  - Re: Risk reduction: Human Factors (Chris Norloff)
  - Flood Stories (Lindsay F. Marshall)
  - Re: holiday reading on Risks (Gary McClelland)

- Volume 14 Issue 16 (8 December 1992)

  - Name confusion and its implications -- PART ONE (Don Norman, Guest Moderator, with contributions from Will Taber, George Buckner, Eric Johnson, Brian Hawthorne, Russell Aminzade, Bob Frankston, Chris Hibbert) [PART TWO IS IN RISKS-14.17.]

- Volume 14 Issue 17 (8 December 1992)

  - Name confusion and its implications -- PART TWO (Don Norman, Guest Moderator, with contributions from Amos Shapir, J. Brad Hicks, Tarl Neustaedter, Chris Hibbert, Will Taber, Andrew Shapiro, Olaf Titz, Wayne A. Christopher, Craig Hansen, Jim Morris, Simon Marshall, Gary McClelland, Craig Partridge) [PART ONE IS IN RISKS-14.16.]

- Volume 14 Issue 18 (10 December 1992)

- Released GSA Docs Slam FBI Wiretap Proposal (Dave Banisar)
- Four charged with theft of registration microfilms in Sapporo Japan (Hank)
- Nintendo and Epileptic attacks (Marvin Moskowitz, Robert A. Morris)

- Volume 14 Issue 29 (27 January 1993)
  - Synthesis report on DoD software problems (James H. Paul)
  - EM Radiation - is smoking safer? (Paul Menon)
  - Brazilian Banking Reserve Data Disappear (Sanford Sherizen)
  - Clinton Transition Team E-Mail (David Daniels)
  - Computer promises nothing (Conrad Bullock)
  - The FBI and Lotus cc:Mail (Dick Joltes)
  - A stopped clock never foils? (Paul Eggert)
  - Re: Racetrack goes to the dogs as computer fails (Conrad Bullock)
  - Request to Post Office on Selling of Personal Information (Dave Banisar)
  - TAPSOFT '93, APRIL 13-16, 1993, ORSAY, FRANCE (Cliff B Jones)

- Volume 14 Issue 30 (2 February 1993)
  - Clever Tactics Against Piracy (Jay Rolls)
  - Educational computer game banned in Milpitas CA (shaun)
  - "Two charged with computer fraud in credit scam" (Norm deCarteret)
  - Bible belt broadcast bungle (Peter J. Scott)
  - Phone Fraud numbers (John Mello)
  - Re: Clinton Transition Team E-Mail (James Barrett)
  - Re: EM Radiation (and cell phones) (Lauren Weinstein, Andrew Klossner)
  - Certification - Proposed Legislation (USA) (Alan Underwood)
  - Erratum: GAO ordering number (James H. Paul)
  - The Federal Criteria for Information Technology Security review (Nicki Lynch)
  - Preliminary Program for 1993 Security & Privacy (Dick Kemmerer)
  - Computers, Security and the Law (reply to Francoise Vassie)

- Volume 14 Issue 31 (5 February 1993)
  - "Computer Blamed For Phone Jam" [Ohio Bell] (Joe Brownlee)
  - BNFL prosecuted for unauthorised software changes (Martyn Thomas)
  - Residues in a surplus bank computer (Fred Cohen)
  - Re: Educational computer game banned (Guy K. Haas)
  - Re: Clever Tactics Against Piracy (Gerd Meissner)
  - Anecdotes Wanted on the Risks of Information Security (Dorothy Denning)
  - Re: The FBI and Lotus cc:Mail (Isaac Rabinovitch, Roger D Binns, Bill Stewart, Dorothy Denning [3x], Dick Joltes [2x], Ray Ozzie via Peter Wayner)
  - Anyone can get your U. of Illinois transcript (Carl M. Kadie)
  - Phone Company Cleverness (Jon Leech)

- Volume 14 Issue 32 (5 February 1993)
  - Programmer Licensing (Paul Robinson)
  - **** pointer-> Injured using Computer Pointing Device? (Pete W. Johnson)
  - Suggestions for a hi-tech crime-investigators' seminar ?? (Jim Warren)
  - Revised Computer Crime Sentencing Guidelines (Dave Banisar)

- Volume 14 Issue 33 (18 February 1993)
  - Cable freeloaders (Tony Scandora)
  - Esperanto from a computer error (Philip Brewer)

  - A "Handy" Risk for AirTravel? (Klaus Brunnstein)
  - Released GSA Docs Slam FBI Wiretap Proposal (A. Padgett Peterson)
  - Re: Tapping phones (Fred Cohen)
  - Re: Joltes Vs Denning (Gary Preckshot)
  - Mobile phones: "too secure"? (Marc Horowitz)
  - PLCs : Request for information (Pete Mellor)
  - User interface at the checkout stand (Rob Slade)
  - Where's the fire? (Jim Carroll)

- Volume 14 Issue 34 (22 February 1993)

  - And You thought Your Computer Chat Was Private (Marty Leisner)
  - _Friendly Spies_ (Peter Wayner)
  - The "Information America" service (Brian Randell)
  - "Telephone Service Cut Off" (Lin Zucconi)
  - Computer delays response to fatal fire (Lauren Wiener)
  - Tapping the new digital car phone systems (John W. Sinteur)
  - A quick request for opinions (Fred Cohen)
  - London Ambulance Service (Brian Randell)
  - DCCA-4 Call for Papers (Teresa Lunt)
  - Technology and Society, Call for Papers (William J. Kelly)
  - Privacy Digests (PGN)

- Volume 14 Issue 35 (23 February 1993)

  - Seeing red over valentine envelopes (Luis Fernandes)
  - KIO diskettes stolen from Spanish Government (Miguel Gallardo)
  - Citibank outage (Marty Leisner)
  - Japanese Bank Hit By Phone Fraud (John Mello)
  - Long Distance..Is the next best thing to praying there (Paul Robinson)
  - Re: _Friendly Spies_ (Sean Matthews)
  - Re: The "Information America" service (John Pettitt)
  - MIT's on-line Student Information Services (SIS) (Jonathan I. Kamens)
  - Re: Tapping Phones (Mark W. Schumann)
  - 1st ACM Conference on Computer and Communications Security (Dorothy Denning)
  - Call for Papers: Computer Security Applications Conf (Marshall D. Abrams)

- Volume 14 Issue 36 (24 February 1993)

  - 3rd Conf. on Computers, Freedom, & Privacy, CFP 1993 (Bruce R. Koball)
  - 2nd Conf. on Computers, Freedom, & Privacy -- PROCEEDINGS (Lance J. Hoffman)
  - Educational Loan Services -- ELSI (Steve Hoffman)
  - Phone problems: Re: "...Phone Jam", and a new problem (Bill Warner)
  - MIT's on-line Student Information Services (Steve Bellovin)
  - Kerberos and password-guessing attacks (Jonathan Kamens)
  - Re: Tapping Phones (Fred Cohen)
  - Re: On-line services (lack of) security (Bill Seurer)
  - Re: request for opinions on Artificial Life (Bill Humphries)

- Volume 14 Issue 37 (4 March 1993)

  - Power Outage Locks Up Jail System (Jennifer Smith)
  - Hacker disables cancer database (Jonathan Bowen)
  - Smells like Green Spirit... (Jeffrey S. Sorensen)
  - Evacuation plan, generators fail in World Trade Center blast (Jay Elinsky)
  - Bank account problems (Jeremy Epstein)

● Volume 14 Issue 46 (6 April 1993)

- Sound of the Fury: Sub-liminal highway monitoring... (Peter Wayner)
- Computer company helps students with fake IDs (Phil Haase)
- Mangled zip code leads to collection agency (Ken Hoyme)
- NREN WRAP [Joe's Final Houston Chronicle NII Story] (Joe Abernathy)
- Danny Dunn, Automatic House, Automatic Electric Post Office (Jerry Bakin)
- Teenage Hackers (Jim Haynes)
- Re: If they mention flying saucers (Ian Phillipps, Olaf Titz, Robert VanCleef)
- Re: FORTRAN-hating gateway (Nick Andrew)
- Re: FORTRAN-hating gateway, Hayes Sequence Triggered (A. Padgett Peterson)
- Re: Correcting computer information ... (Roger D Binns)
- Re: Dutch hacker in jail for another month (Ralph Mooonen)
- Internic Registration Services Security Compromised (Mark Boolootian)
- Call for Papers, PSAM II (System-Based Models) (Charlie Lavine)

● Volume 14 Issue 47 (7 April 1993)

- Another Mystery for the San Francisco Muni Metro (PGN)
- Columbia and Discovery shuttle problems (PGN, Jim DePorter, Ken Hollis via Paul Robichaux)
- ``Organized Crime Gets into Phone Fraud'' (PGN)
- An interesting bug for users of "at" (Dave Parnas)
- RISKS of Complacency (DOS 6.0) (A. Padgett Peterson)
- Using your company's E-mail for private purposes (Omer Zak)
- Re: Personal letters (Paul Robinson)
- Re: Hayes Sequence Triggered (Ron Dippold)
- Groupware (non)security query (Rob Slade)
- Legal Net Monthly Newsletter (Paul Ferguson)
- Injured Using a Computer Pointing Device?: Read This (Pete W. Johnson)
- FTCS-23 ADVANCE PROGRAM (Mohamed Kaaniche)

● Volume 14 Issue 48 (7 April 1993)

- Shuttle Failure Blamed On Computer Glitch (Kriss A. Hougland)
- Safety-Critical Software, special issue of IEEE Software (John Knight)
- London Ambulance Service Inquiry Report (Brian Randell) [long/definitive]

● Volume 14 Issue 49 (9 April 1993)

- Re: Columbia and Discovery shuttle problems (Dan Sorenson)
- "Massive Tax Fraud found in Toronto" and EFILE security (Peter Yamamoto)
- Video Surveillance Tapes and TV Programs (Sanford Sherizen)
- Re: Using your company's E-mail for private ... (Pat Place)
- Re: Sound of the Fury: Sub-liminal highway monitoring... (Rob Horn)
- Lessons from the London Ambulance Service (Bill Murray)
- Re: Another Mystery for the San Francisco Muni Metro (Joe Brennan)
- Review of "Syslaw" by Rose/Wallace (Rob Slade)
- Availability of Berne Convention (Selden E. Ball, Jr., Mike Godwin, Jerry Leichter)

● Volume 14 Issue 50 (14 April 1993)

- Head-on train collision in Berlin (Debora Weber-Wulff [2])
- Discovery discovery of ozone data (PGN)
- ``Navy Calls Satellite a Total Loss'' (PGN)
- Police data misused to find home address (Arthur R. McGee)
- 36,000 dollar bug! (John Pettitt)

- Volume 14 Issue 57 (3 May 1993)
    - The risks of non-24-hour days (Debora Weber-Wulff)
    - Flaws in government computer bond auction (Mark Seecof)
    - Evading 1-900 blocking (John Carr)
    - `New Computer Virus Reported in Japan (David Fowler)
    - Stunning vending machines (Edward N Kittlitz)
    - Junk mail reduction request can add to your junk mail, too (Rich Rosenbaum)
    - Re: SSN for Health Identifier (John R. Levine)
    - Re: How to rob a bank the cashcard way (Anthony Naggs)
    - Humans NOT needed to save NASA (Don Norman)
    - Re: Human vs. computer in space (Craig Partridge, Espen Andersen, Scott Alexander, R. Mehlman)
    - Re: Clipper - A dumb idea (Brian Seborg)
    - Re: Worries over the Clipper Chip (Brinton Cooper)
    - Re: Too much electricity (DonB)
- Volume 14 Issue 58 (10 May 1993)
    - 2 Women Accused in Sale of Adoption Information (John C Slimick)
    - Caller-ID mistakes (John H. Dale)
    - A RISK of Mailing Lists? (James Garven, discussed by Cal Jewell)
    - Census imposters invading Cary (George Entenman)
    - Analog vs Digital Speedometers (Martin Minow)
    - Computer Problem reveals tax details (John Gray)
    - Videoconferencing Bridge Likes Muscular Lungs (Shyamal Jajodia)
    - AIS BBS Capture log (anonymous)
    - Re: Pyramids in space (Wayne Throop)
    - Re: Epilepsy and video games (Antonella Dalessandro)
    - Re: Humans NOT needed to save NASA (Flint Pellett)
    - Re: Junk mail reduction request can add to your junk mail, too (Steve Mick)
    - Re: China executes hacker (Jonathan Bowen)
    - Re: Evading 1-900 blocking (David A Willcox)
    - Re: Utility-derived information (Phil Agre)
- Volume 14 Issue 59 (11 May 1993)
    - Worst Computer Nightmare Contest (Shari Steele via Arthur R. McGee)
    - IFIP resolution on demeaning games (Richard Wexelblat)
    - Fake ATM Machine Steals PINs (Eric)
    - Teller Users Beware (Tapper)
    - More on Census imposters invading Cary (George Entenman)
    - NIST Advisory Board Seeks Comments on Crypto (Clipper-Capstone Chip Info)
    - New NIST/NSA Revelations (Dave Banisar)
- Volume 14 Issue 60 (12 May 1993)
    - IFIP resolution on demeaning games (Barbara B. Simons)
    - Thoreau on Pyramids and Space (Victor Yodaiken)
    - Re: Fake ATM Machine Steals PINs (K. M. Peterson, Al Donaldson)
    - Re: Epilepsy and video games (Larry Hunter, Mich Kabay)
    - Mobile ComSec in Europe (A5) (Klaus Brunnstein)
    - Security&Control of IT in Society (Klaus Brunnstein)
- Volume 14 Issue 61 (15 May 1993)
    - Opel Corsa Stops for Mobile Phones (O\ystein Gulbrandsen)

  - Remote Control Car Locks (David Plumpton)
  - Airline entertainment systems - a true captive audience (Jon Leech)
  - Re: Strasbourg A320 crash: "Pilot Error" (Flint Pellett)
  - Re: Medical Reimbursements (Dan Yurman, Amos Shapir, Bob Frankston)
  - ATM Fraud/Databases/Ouch! (Russ Smith [2])
  - CFP94 (George Trubow via Willis Ware)
  - Science and Technology Through Science Fiction Workshop (Miquel Barcelo)

- Volume 14 Issue 77 (21 July 1993)

  - Another "time bomb" -- MOSS (Dave Horsfall)
  - Flood forecast risks (Douglas W. Jones)
  - Re: Earthquake `early' warning system (Richard Stead)
  - Re: Strasbourg A320 crash: "Pilot Error" (Lars-Henrik Eriksson)
  - Re: ATM Fraud/Databases/Ouch! (Scott Schwartz)
  - Credit Cards on the Internet (Paul Robinson)
  - Re: Medical Reimbursements ... (Michael T. Palmer)
  - Re: DSS as Stamp Tax (A. Padgett Peterson, Steve Bellovin, Jim Bidzos)
  - CPSR Secrecy Statement (Dave Banisar)
  - Announcements of NIST documents (Dolores Wallace)

- Volume 14 Issue 78 (27 July 1993)

  - Computer-aided tax fraud (Mich Kabay)
  - Industrial Espionage (Mich Kabay)
  - Stingers (Bob Frankston)
  - Chinese Airline Crashed a British Aerospace-made 146 "Whisperjet" (Li Gong)
  - Biz Card Machine -- New Risk! (Dan Hartung)
  - Re: Earthquake "early warning" systems (Lauren Weinstein, Brian Herzog)
  - Re: Credit Cards on the Internet (Blake Sobiloff, Nandakumar Sankaran, Matt Crawford)
  - Re: Seecof's reading ability (Mark Seecof)
  - Dependability conference; call for participants (Jeremy Jacob)
  - High-assurance software courses (Nancy Leveson)
  - Centre for Software Reliability Workshop 1993 (Pete Mellor)

- Volume 14 Issue 79 (10 August 1993)

  - Industrial espionage (Mich Kabay)
  - Criminal record data leakage and tampering (Mich Kabay)
  - Billion-dollar tax bills (Mich Kabay)
  - More data remanence (Mich Kabay)
  - Pizza RISK (Dale Drew)
  - Yet another lottery screwup (Reva Freedman)
  - "Terminal Compromise" by Winn Schwartau, on the Net (A. Padgett Peterson)
  - ATM modem insecure? (Andrew Marchant-Shapiro)
  - Jurassic Park Networks (Mich Kabay)
  - Intrusion Detection workshop (Teresa Lunt)
  - Computers, Freedom and Privacy (cfp'94) announcement (George Trubow)

- Volume 14 Issue 80 (dated 11 August 1993 (but issued 10 August))

  - Article by Dorothy Denning on Clipper Chip (Al Stangenberger)
  - SKIPJACK Review (Dorothy Denning)
  - The Rule of Law and the Clipper Escrow Project (Peter Wayner)

- Volume 14 Issue 81 (11 August 1993)

- Colorado prison is escape-proof! (We'll see...) (Lance Gatrell)
- Surprise! contained in tar file (Olaf Titz)
- Exploiting Medco's database (David J. States)
- SAAB JAS 39 "Gripen" crashed (Lars-Henrik Eriksson)
- MD-11 slat extension (Robert Dorsett, Peter Ladkin)
- Call forwarding with "remote code" feature (Reva Freedman)
- Re: "Terminal Compromise" on the Net (Espen Andersen)
- Re: Jurassic Park Networks (rebooting through power reset) (Lauren Weinstein)
- Re: ATM modem insecure? (Lauren Weinstein)
- CfP, IEEE Symposium on Research in Security and Privacy (John Rushby)

● Volume 14 Issue 83 (16 August 1993)

- Dorney Park Hercules roller coaster injures 14 (Steve Walker)
- About 'Terminal Compression' (Paul Robinson)
- Ghost in the machine (Mich Kabay)
- Clusters and electromagnetism (Phil Agre)
- Re: SKIPJACK Review (Brandon S. Allbery)
- Clipper & French key escrow (Richard Schroeppel)
- Privacy Digests --- reminder (PGN)
- PDCS2: Predictably Dependable Computing Systems, Open Workshop (Louise Heery)

● Volume 14 Issue 82 (17 August 1993)

- RISKS-14.83!!! and RISKS-%&#@!! (PGN)
- Re: Dorney Park Hercules roller coaster injures 14 (Scott Walker)
- Re: Surprise! contained in tar file (David Wittenberg)
- Re: Terminal compression (csvcjld)
- Re: Terminal compromise (Mich Kabay)
- Re: Clusters and electromagnetic fields (Kenneth R Foster)
- Re: Gripen crash: pilot's view (Martyn Thomas)

● Volume 14 Issue 84 (17 August 1993)

- Re: BARFmail and other list headaches (Dennis G. Rears)
- Prototype voice-operated ATM (Malcolm Butler)
- Filling Station Ripoff (Matt Healy)
- President Clinton's Tax Plan (Richard Schroeppel)
- Terminal Consternation (A. Padgett Peterson)
- Preserving electronic memos -- a serious problem (Bob Frankston)
- Call for Clipper Comments (Dave Banisar) [FED REG in RISKS-14.84N]
- Call for papers -- 2nd Workshop on Feature Interactions (Nancy Griffeth)
- Call for papers IFIP SEC'94 Caribbean (F. Bertil Fortrie)

● Volume 14 Issue 85 (20 August 1993)

- Child-Prodigy or Prodigy-Child? 14-year-old triggers alarms (Jason Harrison)
- IRS accounting bugs (Mich Kabay)
- IRS & security (Mich Kabay)
- Re: Dorney Park Hercules roller coaster ... (Gary Wright)
- Accessible answering machines may grant too much access (Tsutomu Shimomura)
- Re: ATM Scam (Gene Spafford)
- High-speed password matching (Steve Stevenson)
- Re: Crash of JAS 39 Gripen (Derrick Everett)
- Risks of coming mass-communication capabilities (Jim Hiller)

    Re: Computers dialing 911 (Mark)
    - Good news from the front lines (Jeremy Grodberg)
    - Gideon Kunda, Engineering Culture (Phil Agre)
    - Virus Catalog: new edition (Klaus Brunnstein)
    - InfoWar announcement (Mich Kabay)

- Volume 14 Issue 86 (23 August 1993)

    - Everyone gets a 'A' for Welsh exam (Richard Clayton)
    - Medicare checks for $0.01 (Bear Giles)
    - E-mail privacy (Mich Kabay)
    - Re: Child-Prodigy (Ed Ravin, Jeffrey I. Schiller)
    - AT&T Security Authenticators (thomp962)
    - Re: Remotely accessible answering machines (Mark A Biggar)
    - Worrying about online education (Steve Talbott)
    - NCSC 16 Announcement (Louise Reiner)

- Volume 14 Issue 87 (25 August 1993)

    - Mars Observer (PGN)
    - Chronicle of a bug foretold (Paul Eggert)
    - Quote for the Day (Brinton Cooper)
    - RISKS of elaborating on exploitation of known RISKS (David P. Reed, PGN)
    - Cisco routers (Al Whaley)
    - Phone Number Gridlock Looms (Sanford Sherizen)
    - Digital markets (Phil Agre)
    - Re: Everyone gets a 'A' for Welsh exam (Lars-Henrik Eriksson)
    - InfoTech Security and Control, Conference Report (Klaus Brunnstein)

- Volume 14 Issue 88 (25 August 1993)

    - Re: Mars Observer (Lee Mellinger, Michael Stern)
    - Re: RISKS of elaborating on ... known RISKS (Bob Brown, Douglas W. Jones)
    - Re: Telephone verification (Tom Swiss)
    - Re: Digital Markets (A. Padgett Peterson)
    - Re: Child-Prodigy or Prodigy-Child? (Bob Frankston)
    - 911 & Call Privacy *67 problems (US West) (David Kovanen via Richard Jensen)
    - More Gripen Griping (Peter B Ladkin)

- Volume 14 Issue 89 (27 August 1993)

    - Re: The Mars Observer (Ron Baalke at JPL via Ted Lee and Sandy Murphy)
    - Re: More Gripen Griping (Mary Shafer)
    - Be careful with your test cases! (Kenneth Wood)
    - Re: Quote for the Day (Wes Plouff)
    - Dial 1 first (Fredrick B. Cohen)
    - Re: Cisco backdoor? (Paul Traina)
    - sendmail debug option? RISK or friend? (Eric Allman)
    - Re: RISKS of elaborating on exploitation of known RISKS (Jim Hudson)
    - Call Privacy *67 faults (Ed Ravin, Stuart Moore)
    - Re: Electronic Education (Shyamal Jajodia)
    - Use of PIN as authenticator to humans (Jim Horning, Joe Konstan)
    - Call for Papers: IEEE Computer Security Foundations Workshop VII (Li Gong)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Search RISKS using swish-e

The RISKS Forum is a moderated digest. Its USENET equivalent is comp.risks. (Google archive)

- Vol 26 Issue 47 (Monday 6 June 2011) <= Latest Issue
- Vol 26 Issue 46 (Saturday 4 June 2011)
- Vol 26 Issue 45 (Tuesday 24 May 2011)

- News about the RISKS web pages
- Subscriptions, contributions and archives

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

You can also monitor RISKS at Freshnews, Daily Rotation and probably other places too.

Please report any website or feed problems you find to the website maintainer. Report issues with the digest content to the moderator.

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

The dates and counts do not include the index issues for each volume.

Index to the RISKS Digest

Volume Number	Date Range	Number of Issues
Volume 1	*1 Aug 1985 - 31 Jan 1986*	*45 issues*
Volume 2	*1 Feb 1986 - 30 May 1986*	*56 issues*
Volume 3	*4 Jun 1986 - 30 Oct 1986*	*91 issues*
Volume 4	*2 Nov 1986 - 6 Jun 1987*	*96 issues*
Volume 5	*7 Jun 1987 - 31 Dec 1987*	*84 issues*

Volume 6	2 Jan 1988 - 31 May 1988	*94 issues*
Volume 7	1 Jun 1988 - 22 Dec 1988	*98 issues*
Volume 8	4 Jan 1989 - 29 Jun 1989	*87 issues*
Volume 9	6 Jul 1989 - 30 May 1990	*97 issues*
Volume 10	1 Jun 1990 - 31 Jan 1991	*85 issues*
Volume 11	4 Feb 1991 - 28 Jun 1991	*95 issues*
Volume 12	1 Jul 1991 - 24 Dec 1991	*71 issues*
Volume 13	6 Jan 1992 - 2 Nov 1992	*89 issues*
Volume 14	4 Nov 1992 - 27 Aug 1993	*89 issues*
Volume 15	2 Sep 1993 - 29 Apr 1994	*81 issues*
Volume 16	2 May 1994 - 22 Mar 1995	*96 issues*
Volume 17	27 Mar 1995 - 1 Apr 1996	*96 issues*
Volume 18	5 Apr 1996 - 31 Mar 1997	*96 issues*
Volume 19	1 Apr 1997 - 23 Sep 1998	*97 issues*
Volume 20	1 Oct 1998 - 31 Jul 2000	*98 issues*
Volume 21	15 Aug 2000 - 29 Mar 2002	*98 issues*
Volume 22	1 Apr 2002 - 27 Oct 2003	*98 issues*
Volume 23	7 Nov 2003 - 2 Aug 2005	*96 issues*
Volume 24	10 Aug 2005 - 30 Dec 2007	*93 issues*
Volume 25	7 Jan 2008 - 1 Apr 2010	*98 issues*
Volume 26	8 Apr 2010 - 6 Jun 2011	*47 issues*

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 1

Weds 04 November 1992

Contents

Tandem Clock Outage (collated from various sources)

"Bruce Baker" <bruce_baker@qm.sri.com>
3 Nov 1992 15:27:25 -0800

[Bruce sent me a stack of messages. This (slightly edited) is the most coherent, from J. Lyngved and forwarded via Paul Hicks of RPS Ltd. PGN]

FROM: Lyngved.J

In case you have not yet heard, our TANDEM stopped last night. So did almost all TANDEMS around the world, I've heard.

We are currently trying to get it running again, helped by TANDEM people.

Worse yet, they inform us that unless we do some upgrading it will stop again on January 7, 1993.

This is not an April [fool's] joke.

Jesper

> [I hope the details surface in RISKS. It appears that at 15:00 on the 1st, all Tandem CLX machines abended, causing the BASE24 Nucleus to dump with a Trap 2 (arithmetic overflow) in the procedure age-timers. A cold reload would get the system going again. Stay tuned (or detuned). PGN]

Re: Air Inter A320 descent

Pete Mellor <pm@cs.city.ac.uk>
Tue, 3 Nov 92 21:48:50 GMT

It just *so* happened that I was in France last week (on something completely unrelated: an ISO meeting). I dropped into the office of a certain lawyer in Paris on my way out and back.

On the way out, he gave me a photocopy of an article in "Le Canard Echaine", about Michel Asseline's book about the Habsheim crash. On the way back, he gave me two photocopies of articles in "L'Alsace" (regional newspaper serving Habsheim and surroundings), and "Le Monde", which had appeared that very day (Friday 30th Oct.) or the day before.

The last two articles are detailed accounts of the "descente intempestive" which has been reported recently. If what the articles say is true, then it looks as though all bets are off regarding Bangalore, Strasbourg, AND the A300 and A310 crashes in Kathmandu.

To summarise: When "rate of descent" mode is selected, (as opposed to "flight path angle"), a fault in the FMGS software occasionally causes the aircraft to descend at **2 or 3 times** the rate selected by the pilots.

They don't even NEED to confuse "rate of descent" and "flight path angle"!!!

This was reported by several crews who were able to recover the situation because they weren't flying over mountains at the time.

The FMGS software (I *think*) is NOT regarded as SAFETY-CRITICAL!!!!

If this is so, then it is NOT certified to RTCA/DO-178A level 1.

The SAME FMGS is in use on A300, A310, and A320 (at least, *basically* the same)!!

The French pilots' unions are up in arms about it, and in France generally, all hell seems to be breaking loose.

Typically, in the UK press, the silence is deafening. (Presumably none of their French correspondents can speak French! :-)

The other thing that my French lawyer colleague gave me was a signed copy of Michel Asseline's book about Habsheim: "Le Pilote - Est-il Coupable?"
(You've guessed! He's Asseline's solicitor! :-)

Since I read French even more agonisingly slowly than I read English, you'll have to wait a while for my detailed review. In the meantime, I will try to find time in the next few days to translate the three newspaper articles.

If anyone sees anything in the media (French, UK, US and all points between), let us all know.

Pete

PS: If anyone knows of a publisher willing to handle the forthcoming English translation of Asseline's book, let me know about that, too.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: Leaving greasy marks on monitors may be dangerous (RISKS-13.89)

Pete Mellor <pm@cs.city.ac.uk>
Tue, 3 Nov 92 20:27:00 GMT

> Apparently, so I am told, CFCs have been replaced in these aerosols by
> flammable propellants.

Come back CFCs, all is forgiven!

Actually, I suspect that most of the CFCs that hit the ozone layer come from decommissioned refrigerators or industrial waste, and not from you or I spraying our hair or computer screens. (Prince Charles is reported to have banned the use of CFC aerosols in the Palace. "Every little helps!", as the wren said when she pee'd in the ocean! :-)

Why not go for the "Pump and Spray" approach adopted by a certain manufacturer of hair laquer? The lid of the can activates a pump. You push it up and down a few times to pressurise the can, and then spray out the contents with a propellant no more polluting (or inflammable) than compressed air.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: Risks of Cellular Speech (RISKS-13.89)

Phil Karn <karn@qualcomm.com>
Tue, 3 Nov 1992 02:29:38 GMT

> In a three-month study of the Metro Toronto area earlier this summer, Bell
> found that 80 percent of all cellular telephone traffic is monitored by third
> parties. Even more eye-opening is the fact that 60 percent of monitored calls
> are taped for closer scrutiny and culling of marketable information.

I would very much like know how Bell Canada obtained these figures, given that the monitoring of cellular telephone calls from the privacy of one's home is essentially undetectable.

> After discussing privacy laws, legalities, and realities, Flinn notes that at
> Scanners Unlimited in San Carlos, CA, "about a quarter of the customers are
> interested in telephone eavesdropping."

This problem will soon be stopped cold, as Congress recently passed a law to outlaw the manufacture of scanners capable of receiving cellular telephone calls. A truly inspired solution to the problem, comparable to the "B-Ark" people in "The Hitchhiker's Guide to the Galaxy" burning down the forests to solve the inflation problem caused by making leaves legal tender.

Phil

Risks Of Cellular Speech

Dave King <71270.450@compuserve.com>
03 Nov 92 16:47:58 EST

I must apologize to the list. I have been informed that we cannot confirm the percentage figures that were mentioned in the note that I quoted in the item that I posted yesterday concerning a study of the monitoring of cellular traffic in Toronto, Canada.

David L. King, IBM Southeast Region I&TSS, Mail Drop D072, 10401 Fernwood Road
Bethesda, Maryland 20817, (301) 571-4349

Re: Cash dispenser fraud (RISKS-13.89)

Pete Mellor <pm@cs.city.ac.uk>
Tue, 3 Nov 92 20:39:33 GMT

Erling Kristiansen writes (concerning cash dispenser fraud):

> If you do not take your money within a given time, the machine will swallow
> it back, and undo the transaction on your account.

Not in my experience. (See RISKS about a year ago.) I simply forgot to take the money, and the machine swallowed it. To get the amount credited to my account, I had to 'phone the bank personally, and the amount was only repaid after the till had been (manually) balanced, and the excess cash in stock verified.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: Caller-ID and Modems (Slade, RISKS-14.01)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Tue, 3 Nov 92 10:33:50 -0500

I realize that this may be a bit out of the ordinary for a RISKS posting but since Rob Slade raised the issue in RISKS yesterday, I have gotten quite a few questions.

First, it is my belief that much of the RISKS of dial-up access points is increased by the ease of discovering such points. War Dialer and Exchange Hacker programs are plentiful and have contributed to a number of notorious cases recently (the MOD is said to have used this method of discovering such lines).

The problem is that with all current systems that I am aware of, it is first necessary for the modem to answer the telephone before any authentication can take place. By doing so, the line may be positively identified as having a modem even if call-back or other rigorous identification means are in use. Once such line have been identified, serious penetration attempts can take place.

When announced, it was realized that Caller-ID provided an answer to this dilemma that was much better than the "ATS0=7" which I previously advised. (This command instructs a modem responding to the "AT" command set not to answer the phone until the seventh ring - typically about 40 seconds after connection starts. Since most War Diallers allocate only 30 seconds to each number, this is an effective, if annoying, answer).

Caller-ID places a 1200 baud digital signal on the telephone line between the first and second ring signal. The important factor is that the phone does not have to be answered to received this information. Some modems are able to pick up this signal and present it to the host computer.

What I did last weekend was to create a PROCOMM PLUS script file using their ASPECT language to do the following:

1) When the telephone rings the calling number is captured.

2) The number is recorded into a "LOG" file and then a scan of a database
of "approved" numbers (flat ASCII) is done.

3a)If the number is found in the "approved" file, PROCOMM is instructed to
enter its "HOST" mode - an effective single line BBS emulation that

supports uploads/downloads/mail/and "chat" and the phone is answered.

or

3b)If the number is not found, the line is not answered

4) After the caller hangs up, the system resets.

Given this, even if the "bad guys" know the number, they will still have to find a way to induce the modem to answer the line. Certainly if this were in widespread use, much of the plot of "Sneakers" would have had to be re-written.

Yes, I know that there are problems, particularly with "roving" people. If however 80-90% of all access could be handled in this manner (e.g. for telecommuters), the balance could use extraordinary means.

Right now the capability is limited to a PC running PROCOMM Plus 2.01 and equipped with a Supra Corp. SupraFAXmodem having the Caller-ID ROM upgrade. I haven't tried any others.

Why did I choose this combination ? - because I had them (both were privately purchased) and they would do what was necessary - this is all a hobby to me. In theory any Caller-ID unit with an RS-232 output could be used as could any scripting BBS software. What was desired was a "proof-of-principle" not a commercial product.

The PRIVACY concern is easily handled: you can block your number from Caller-ID (star-6-7 in most places) but I reserve the right not to have my computer answer the phone if you do.

IMHO this capability is still in its infancy but is important and easily implemented, we are just seeing the tip of the iceberg now.

Right now the biggest drawback is the limited availability of Caller-ID though IMHO again it will be nationwide in two years (law enforcement agencies already have a wider coverage so the holdup is political, not technical).

RISKS ? To me the most important is the question "Could an individual use star-6-7 to block the telco's ID and send their own 'approved' 1200 baud stream ?" The consensus so far is "NO" and I have some friends at GTE experimenting.

In any event, the script is FreeWare for anyone who might be interested, just be aware that I do not have any distribution means (might be able to send as E-Mail) and negative free time.

The importantance of this is that it is no longer theory, it is now fact, CHEAP fact.
Padgett <padgett@tccslr.dnet.mmc.com>

ps: Just to avoid the inevitable, Supra Corp. can be reached in Oregon
at (800)727-8647 (do not think Caller-ID is available outside the US
yet). I bought mine from a mail-order house for about 3/4 list price.

PROCOMM is a product of Datastorm Inc. (800)326-4999 (plugs)

Re: Privacy of e-mail (Symantec/Borland suit)

<HORN%athena@leia.polaroid.com>
Tue, 27 Oct 1992 08:08 EST

For further commentary on this issue, see the recent Forbes magazine article by Mitch Kapor. It raises the issues of how the ECPA Act and similar California privacy legislation might apply to this case. It will probably make a number of lawyers rich and drag on for years, but there are some very complex legal issues involved. The issue involves MCI's responsibility as an e-mail provider under ECPA and whether Borland was or was not authorized to have access to Wang's mail. I doubt that all the relevant facts are yet public.

Rob Horn horn%hydra@polaroid.com

Symantec/Borland and Brazilian President

<[anonymous]>
Sun, 1 Nov 92 15:19 PST

There are two topics in RISKS-13.87 that are actually related. Someone asked about software that could have been used to get the deleted files from the Brazilian president's disks. There was also a mention of the Symantec/Borland suit over theft of trade secrets. The Wall Street Journal had the most complete article about the latter (I don't have the date handy) and mentioned that Borland used a copy of a Symantec product, Norton Utilities, to recover erased files that are being used as evidence in the case against Symantec. Apparently Norton Utilities is widely used by law enforcement agencies for gathering evidence in cases involving PCs. The product also includes a utility for ensuring that deleted data cannot be recovered, but many people seem to think that if they "delete" a file and it seems to be gone, then that's what really happened to it. There's always a risk when a user's model of what the computer is doing behind the scenes is a simplified one which is adequate for doing their work, but not for predicting the outcome of unusual circumstances.

re: Interesting/obscure interaction between users (Honig, RISKS-13.88)

Jerry Leichter <leichter@lrw.com>
Sat, 31 Oct 92 13:51:06 EDT

David Honig remarks on his discovery that users of SunOS can allocate shared memory resources and fail to delete them properly, thus effectively rendering them unavailable to later programs, which fail. Only a reboot will resolve the situation.

A couple of remarks:

a) All the Unix System V IPC objects have this property. Allocating
and failing to free shared memory segments, semaphores, or
message queues, all of which exist in limited numbers and
cannot be replenished, can also cause later numbers to fail.

Mr. Honig remarks that there are typically 100 memory
segments. There are typically considerably fewer semaphores
or message queues.

b) This is not a SunOS problem; it's inherent in System V, which
defines a set of IPC facilities which allow objects to persist
even though no one is using them. Programs probably exist
which rely on this, so I doubt it can be changed.

c) It IS possible to recover from this without rebooting, since root
can attach to the "lost" objects and delete them. Of course,
you have to find them first. At least on Ultrix, and probably
on most other systems, there is a program (ipcstat, I think)
which displays a list of all IPC objects in the system. It
would remain up to a human being to decide which ones can
be deleted safely, however.

d) Given (c), the situation is, in a way, analogous to running out
of disk space because the disk is full of old junk. This
similarity, however, is tenuous, for several reasons: Disks
are much larger than the sets of IPC resources available;
the names of files being created are generally known, except
for temporary files - which as a matter of policy are treated
as expendable after a short time, and automatically cleaned
up; and people regularly see directory lists, but they rarely
if ever have reason to run ipcstat.

-- Jerry

Re: 15th NCSC (Denning, RISKS-13.87)

Brinton Cooper <abc@BRL.MIL>
Mon, 2 Nov 92 23:38:32 EST

First, I should hate to think that my right to safety from illegal search and seizure and/or illegal eavesdropping on my telephone conversations rested on the good will and integrity of a phone company!

Second, it's difficult to envision a non-governmental agency, created by the government but not really government. The Post Office purports to be a non-governmental agency but isn't. It's employees still look and act like US Civil Servants, and the P.O. can easily conduct a "mail cover" for a governmental agency without a court order.

You must remember that court orders, search warrants, and the like are useful only when the information or evidence gathered under their aegis is to be used in court against a suspect. If information is being gathered for political purposes, to blackmail someone, or to subvert the law (Watergate, Iran-Contra, the Italian bank, etc), the information will never see a public forum. Thus, the constraints of court orders are obviated.

The FBI needs to fund its own R&D out of its budgetary resources, just as the rest of the government at all levels must do. There is talent that can "red team" modern telecommunications and find trapdoors when necessary.

You must never forget that the gravest threat to our freedom is, and always has been, government itself.
_Brinton Cooper

Re: Key registration (Denning)

Carl Ellison <cme@ellisun.sw.stratus.com>
30 Oct 92 21:42:12 GMT

In the exchange over Dr. Denning's proposed key registration agency, I have learned that there are civilized countries out there (eg., Finland) where it is illegal for the government to do a wiretap. Even getting phone records in Finland (for traffic analysis) apparently results in the target's being told.

Sadly, we're not that civilized, it seems.

I can imagine some large company (one of the Baby Bells, perhaps) making a line of scrambled, digital phones -- perhaps cellular -- perhaps just wireless, but with digitization and end-to-end encryption done in the handset. I could see this line of phones using RSA (1000 bit) to pass triple-DES keys around (DES with 3x56 bit keys and 3x64 bits of random IV for CBC mode).

I can imagine that large company offering to register keys for the FBI -- just to keep from being hassled by the Gov't.

Were that to happen, I might even buy such a phone -- knowing that it's insecure but also knowing that my neighbor won't be listening in on her wireless phone.

However, it's important that the agency which releases keys not release the RSA keys (in this case) but rather the session key (360 bits of DES key and IV) of a particular conversation. Releasing the RSA key makes the phone in question insecure for all time, past and future.

(No, I don't advocate key registry -- but if it looks like we end up having it, let's have it limited. Meanwhile, it's perfectly reasonable to have an audit trail of all such taps made available to major news organizations immediately and eventually to the person targetted -- so that any Nixon-like abuses would get caught and prevented.)

Carl Ellison, Stratus Computer Inc., M3-2-BKW, 55 Fairbanks Boulevard,
Marlborough MA 01752-1298 cme@sw.stratus.com (508)460-2783 FAX: (508)624-7488

Re: New risk reports (Bowen, RISKS-13.87)

Pete Mellor <pm@cs.city.ac.uk>
Mon, 2 Nov 92 20:30:01 GMT

Please see also:

"Living with Risk", The British Medical Association Guide, John Wiley & Sons, 1987, ISBN 0 471 91598 X, 16.45 sterling. (Winner of the 1988 Science Book Prize.)

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

ASEE '93 EPPD Call for Papers

"Ken Sollows" <SOLLOWS@acad1.csd.unbsj.ca>
3 Nov 92 09:56:12 ADT

CALL FOR PAPERS

ENGINEERING AND PUBLIC POLICY DIVISION
1993 ASEE ANNUAL CONFERENCE
UNIVERSITY OF ILLINOIS, URBANA, IL
JUNE 20 - 24, 1993

Presentations and papers are invited on educational aspects of Engineering and Public Policy. Any related topic will receive consideration, however, suggested topics for sessions are the following:

* Energy and Environmental Policy
* The Role of Colleges of Engineering in Shaping Public Policy
* Public Policy in the Undergraduate Engineering Curriculum
* Governmental Initiatives in Engineering Education
* Educational Policy and Economic Growth

Deadline: 500 word abstracts due December 1, 1992

Presentations will be selected by the EPPD program staff based on abstracts only. Authors who also wish to submit their papers for publication in the conference Proceedings must submit a draft for peer review by January 15, 1993. There will be a page charge for publication. Include title, author's name, work address, and telephone number. Abstracts and papers should be submitted to the EPPD Program Chair:

Dr. P. Paxton Marshall, Department of Electrical Engineering
University of Virginia, Thornton Hall, Charlottesville, VA 22903-2442
Tel: (804) 924-6076 Fax: (804) 924-8818 e-mail: marshall@virginia.edu

Ken Sollows, Dept. of Engineering, UNBSJ
Email: sollows@unbsj.ca   Ph: (506) 648-5583   FAX: (506) 648-5528

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 2

Monday 9 November 1992

Contents

Voting Machine Horror Story

Al Stangenberger <forags@insect.berkeley.edu>
Fri, 6 Nov 92 09:20:45 PST

>From Daily Californian 6 November 1992

A misaligned Votomatic machine may have caused hundreds of Berkeley voters to cast their ballots for candidates and propositions they never intended to support, according to Alameda County Registrar of Voters Emmie Hill.

Votomatic machines align a pre-scored data card with numbers on a printed picture of the ballot. Voters make their choices by punching a stylus through designated holes, thereby punching a data card. In this case, the holes were still within the printed squares on the ballot, but were actually causing holes to be punched in other locations on the card.

An alert voter reviewed her completed ballot and noticed the discrepancy, but precinct workers did nothing until late afternoon, when a troubleshooter from the Registrar's office, acting on the voter's complaint, checked the unit and confirmed the voter's complaint.

I had never thought of this type of error being possible - the ballots look so neat when they come out of the machine. Should we add a second definition to GIGO, namely Goodness In, Garbage Out, to cover such cases?

Al Stangenberger   Dept. of Forestry & Resource Mgt.
145 Mulford Hall - Univ. of Calif. Berkeley, CA 94720

phone voting in NM

Gary McClelland <mcclella@yertle.Colorado.EDU>
Mon, 9 Nov 1992 08:17:04 -0700

A group of Boulder residents has been actively campaigning for phone voting. As a consequence, the Boulder media has followed phone voting efforts elsewhere. Below is a summary and excerpts from an article by Carol Chorey in the Boulder Daily Camera on 9 Nov 92 about phone voting developments in New Mexico.

"New Mexico was spurred to develop a phone voting system by `lots of voter frustration in getting to the polls,' said Russell Barnes, director for information systems with the New Mexico secretary of state's office. Members of his office started talking to the security experts at Sandia [National Labs in Albuquerque] last March because `we thought we had the expertise with Sandia Labs' so close at hand." Scientists at Sandia took on the work as a commercial project rather than a federal one. The labs...are converting from federal to commercial work because they have lost much of their funding."

The goal is to have phone voting as an option to voting at the polls in the same way that voting absentee by mail is currently an option. Thus, one would have to apply to vote by phone and the presumption is that not everyone would do so. Just like absentee voters, phone voters would have two to three weeks to call in their votes before election day so phone lines won't be overloaded.

Security? " `Voting by phone is not really the issue--it's a simple technology,' Barnes said. `The problem is people feel it is very unsafe because it's so easy to tap into the phone system." "With the help of computer security experts at Sandia...,the secretary of state's office is developing a system officials say will be uncrackable." :-) As a test, the prototype system was used in a mock election involving 2,300 high school students and their parents on a facsimile of this year's NM ballot. During the week-long mock election, "Sandia `black-hatters'--experts at breaking into telephone systems--were unable to crack the identification system and could not create duplicate votes." The article includes this cryptic comment: "An encoding system still needs to be developed to make sure the system will be safe from mass fraud."

New Mexico is spending about $2 million on the system. They hope to recover these costs by selling the system to other states.

gary mcclelland, univ of colorado, mcclella@yertle.colorado.edu

Salvage Association vs CAP Financial Services

Les Hatton, Programming Research Ltd., U.K. <lesh@prl0.uucp>
Mon Nov 9 17:57:00 1992

> The legal side catches up on the (lack of) quality ...
> CAP loses legal battle: Computer weekly, Thursday, 29 October, 1992
>
> The Salvage Association has won its year-long battle with CAP Financial Services over a botched computerised accounting system. The Salvage Association, which processes marine insurance claims, commissioned CAP to develop a bespoke accounts system based on software from relational database supplier Oracle in 1988. But the finished system was riddled with over 600 errors and had to be scrapped in 1989 after repeated attempts to modify it failed to produce a usable version.
>
> Last week Judge Thayne Forbes ordered CAP, now part of Anglo-French services group Sema, to pay the Salvage Association 662,926 UK pounds in damages. Further damages will be awarded next month when interest charges and legal costs will be taken into consideration ...

I wouldn't be surprised here if the damages exceeded the development costs! Really bad code probably has an error about every 50-100 lines suggesting that the package might be around 30,000-60,000 lines. At around 5000 lines per programmer year for this kind of stuff and say 50,000 pounds per year for a programmer all in, the development costs would be around 360,000-600,000 pounds. I guess that this kind of thing will get much more frequent.

Dr Les Hatton, Director of Research, Programming Research Ltd, England
esh@prl0.co.uk (44) 372-462130

Computer system blamed for lack of official trade figures

John Jones <jgj@cs.hull.ac.uk>

Thu, 5 Nov 92 13:50:15 GMT

An article that appeared in the Guardian (7th October, 1992) suggests that the British Government is unable to monitor trade sanctions imposed on Serbia because there are no official trade figures:

> Computer flaw lets Serb sanction-busting slip
>
> David Hencke, Westminster Correspondent, The Guardian, 7th October, 1992
>
> Details of Serbian sanctions busting are being wiped out every month by the erase button of a Whitehall computer, undermining Britain's pledge to the United Nations to root out and record the illicit trade. Embarrassed Customs and Excise officials admitted to the Guardian yesterday that they keep only one month's illegal trade figures for Serbia and Montenegro because they have no back-up system to hold the information for longer than 28 days.
>
> ``We weren't prepared for Yugoslavia to break up. We did not have a programme for separate republics,'' an official explained. ``We don't keep the information because our principal client, the Central Statistical Office, which records overseas trade figures, intends to keep Yugoslavia as a single country until next year.'' [...]

I do not think it was clear in the article exactly what was going on, but my interpretation is that the people who normally receive trade figures, the Central Statistical Office, do not want them. The people who generate the figures, Customs and Excise, are unable to save them because of an inadequate computer system. This is convenient, because the article went on to state that what trade figures are known show that trade has increased dramatically in a number of areas, including the export of telecommunications equipment and petrol (no specific figures quoted, so we could still be talking small numbers).

This article caught my attention for several reasons:

- the standard of reporting (lack of firm detail, choice of language)
- people hiding behind inadequacy of computer systems (as usual)
- political capital out of the inadequacy of software

John Jones, Department of Computer Science, University of Hull, UK

Privacy Digests

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 9 Nov 92 176:30:03 PDT

Periodically I will remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry higher-level discussions in which risks to privacy are a concern.

* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@cv.vortex.com"; you will receive a response from an automated listserv system.

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Dennis G. Rears. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to comp-privacy@pica.army.mil and administrative requests to comp-privacy-request@pica.army.mil.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

Another TV show showing computer `hackers'

Matthew D. Goldman <goldman@orac.cray.com>
Fri, 6 Nov 92 09:08:13 CST

You might want to turn into next week's Beverly Hills 90210 to catch the hacker subplot. Last week on 90210, One of the main characters obtained a password to the high school computer grade system via social engineering. Later he and a freshman computer dude (this is California after all) broke into the school and attempted to adjust school records. The password "JESTER" seemed to work at first; however, the system locked up and shutdown after a few minutes. The two kids fled. It will be interesting to see if there is an audit trail...

Matt Goldman goldman@orac.cray.com

Re: Encryption Keys (RISKS-13.85)

<STORY_GLENN@tandem.com>
9 Nov 92 09:44:00 -0800

In reference to Dorothy Denning's five-step sceme to protect the government holding encryption keys:

The Justice Department (and FBI) could dispense with steps 1-3 by the simple expedient of disregarding the use of due process. (It wouldn't be the first time.)

Step four can be eliminated with standard well-known intercept techniques.

This leaves only step five:

"Listen in and decrypt the communications."

Doesn't sound too tight to me.

Regards,
Glenn

"When cryptography is outlawed, only outlaws will use cryptography."

Can encryption be defined precisely?

Steven Tepper <greep@speech.sri.com>
Wed, 4 Nov 92 13:47:01 PST

> Dorothy Denning suggested that anyone using high-level encryption over a public
> network be required to register their encryption keys with some agency.

(I assume this is supposed to mean decryption keys, not encryption keys.) The discussion of requiring the registration of decryption keys raises the question of whether "encryption" can be defined precisely enough to make this proposal workable. Can translating a message in a different language be called "encryption"? We would not normally use the word in this way. But if a bad guy wants to send a message to a crony without having the government be able to understand it, he can send it in some extremely obscure language (suitably transliterated into a standard character code if necessary) that they happen to know (or take the trouble to learn a little of). Will the government decide to outlaw all communications in foreign languages? Or publish a list of approved languages?

Take this a step further. What's to stop the bad guys from creating their own language? (Say something like Esperanto but based on Navajo instead of Italian.) Let's say that the language is given a greatly simplified syntax, to make it easy to learn and remember. Can translating messages into this language be defined as encryption? If so, what is the appropriate decryption key? If the language changes fast enough, translation into it resembles the use of a one-time pad. Will the law attempt to distinguish between "real" and "artificial" languages and allow only the former? If so, would real languages that are now extinct be allowed? Would a language be allowed only if a written dictionary and description of its grammar exist in some more widely known language?

To summarize, is it possible to define a precise distinction between

encrypting a message and translating it into a different language? Is
it possible to outlaw the former while permitting the latter? Remember
that there will always be people pushing the limits of the law.

Steven Tepper <greep@speech.sri.com>
SRI International Menlo Park, California

FBI Registration

CA29F200CE9F204D17@qut.edu.au ?? <D.LONGLEY@qut.edu.au>
Tue, 10 Nov 92 09:07 +1000

Dennis Longley, Information Security Research Centre, Queensland University of Technology.

HOW TEFLON JOHN COPED WITH KEY REGISTRATION.

1. Teflon John registers DES key K1 with the FBI and announces that he is using 4-bit cipher feedback, IV to be a preamble to message.

2. Teflon John gives MAC the KNIFE a second DES key K2 and a software package.

3. Teflon John wants to tell MAC the KNIFE to make an offer that LOUIE can't refuse, but he doesn't want to spoil the surprise to LOUIE or the FBI. Moreover he does not want to involve near MAC the KNIFE, who can read easy words but can't write real good, in complex codebook systems. The scheme must be virtually transparent to both sender and receiver.

4. Teflon John produces plaintext " Give Louie a nice present at 6 pm on Monday' encrypts it with K2 giving ciphertext C1.

5. Teflon John's problem is that although the FBI can't decipher C1, they will get suspicious if they tap a message that cannot be decrypted with K1. He has to find a mechanism of transmitting C1 so that it appears to be an innocent message when decrypted with K1, but a true message when decrypted with K2.

6. Teflon John breaks C1 up into 4 bit messages and produces a host, about 30-40, of innocent messages I1 - In.

7. The messages I1 to In are encrypted with 4 bit cipher feedback using K1. The first 4 bits of each message are scanned until one is found with the same first 4 bits as C1. Since there is a 1:16 probability that two four-bit messages are identical then with 32 messages there is an 87% probability that a match can be found. Just keep generating messages if necessary until match message Im is found. The encrypted message eK1(Im) is transmitted. The FBI decrypt a harmless message, MAC the KNIFE uses the software package to retain the first 4 bits of the ciphertext eK1(Im).

8. Next get the second nibble from C1 and search through the ciphertexts eK1(Ip) for the second innocent message to be transmitted i.e., the one whose second nibble is identical with the second nibble of C1. MAC the KNIFE's software package retains the second nibble of this message.

9. Proceed in this manner until MAC the KNIFE has C1 which is then decrypted with K2, and goodbye Louie.

10. Now the same innocent messages can be used over and over again, they will be simply sent in a different order. If the FBI are getting suspicious then variants of the message can be made, any variation after the 4 bits used will not affect the process.

I guess that the FBI cryptanalysts could get suspicious about the burst of similar innocent messages preceding expensive funerals, but their prosecuting attorneys would not have an easy job, particularly if Teflon John had a good key management scheme for K2. The only prosecution evidence would be a set of ciphertexts that they claimed represented evil intent, but they could not produce the corresponding plaintext messages.

11. Everybody is happy with the system, Teflon John is getting his messages through securely, the FBI assures itself that it is doing a good job keeping Teflon John on the straight and narrow, and AT$T is getting a much larger telephone income from Teflon John. Louie is not so keen but nobody liked him anyway.

12. The 4 bit cipher feedback allows Teflon John to reduce his phone bill with more sophisticated approaches where more than 1 nibble is used per message. With 4 bit cipher feedback there is more control over the ciphertext so that the messages can be modified easily to produce the requisite nibbles corresponding to the ciphertext used by MAC the knife.

Re: Risks Of Cellular Speech (RISKS-13.89)

Johnathan Vail <vail@tegra.com>
Wed, 4 Nov 92 17:40:57 EST

Dave King <71270.450@compuserve.com> and Peter G. Neumann talk about the "Privacy" issues of cellular phones. They point out that cellular phones are not private and mention many incidents where this is illustrated.

[Technical note: the Dan Quayle call was probably not cellular phone but a dedicated or airphone frequency. Cellular from aircraft is illegal because the aircraft can "see" too many cells at once. JV]

It should be obvious to anyone that using radio to communicate over distances of many miles is never private. The real RISK involved is why people think it can be private in the first place. In the US we have laws specifically outlawing listening to cellular phone calls and they recently passed a law banning the sale of scanners that can receive cellular phone. But even banning new scanners will not eliminate the millions already sold or even older UHF TVs that can tune those frequencies.

These laws can not change the laws of physics but they will promote the *myth* of privacy. People using cell phones are led to believe that it is just like a wire phone. Cell phone vendors fought for a law that cannot be enforced rather than a law that requires them to warn their customers that there is no privacy. It is cheaper for them to bury their head in the sand then to invest in digital technology that will offer privacy.

And for conspiracy theorists: remember the discussion where the FBI and NSA are trying to delay and weaken digital techniques for cell phones. Who do you think is doing a lot of listening now?

Johnathan Vail vail@tegra.com jv@n1dxg.ampr.org (league@prep.ai.mit.edu)
MEMBER: League for Programming Freedom N1DXG@448.625-(WorldNet) 508-663-7435

London Ambulance Service computer fails again

Tony Lezard <tony@mantis.co.uk>
Thu, 05 Nov 92 10:47:30 GMT

The Times of 5 November 1992 reports that Britain's biggest ambulance service, the London Ambulance Service, yesterday reverted to full manual control after another failure in its computer management system forced senior management to concede it could not cope with its task.

It reports that the health secretary Virginia Bottomly was studying a letter from a York-based computer consultancy claiming that tenders for the contract from experienced providers of command and control systems were ignored in favour of the lowest bid.

Control room staff had noticed early yesterday that system response was slowing and computer back up procedures had failed to solve the problem. Because of the faults, there was a 25 minute delay in dispatching an ambulance.

Ten days earlier, the service's chief executive, John Wilby, resigned following allegations by the public sector union NUPE that a similar failure could have contributed to the loss of 20 lives. The LAS has challenged NUPE to substantiate its claim.

Martin Gorham, acting chief executive of the LAS said that yesterday's problems occurred when demand was low, and not as a result of system congestion as had been the case previously. In a statement he said "Since the problems with the computer system at the beginning of last week, the LAS has been operating extra back-up systems, including paper duplicates and voice confirmation to crews. In addition, the staffing of the control room has been significantly increased. As a result of these measures, call answering times have substantially improved, leading to greater efficiency in allocating ambulances."

Tony Lezard: tony@mantis.co.uk Mantis Consultants Limited, Cambridge, UK.
Alternative email: tony%mantis.co.uk@pipex.net or arl10@phx.cam.ac.uk

London Ambulance Dispatch Computer

paj <paj@gec-mrc.co.uk>

5 Nov 1992 09:22:48-GMT

The London Ambulance Service computer fiasco rumbles on.

According to "Computing" (5 Nov 92) the senior officials of LAS were warned that the system would be an "expensive disaster" by Michael Page. Page's company submitted a competing bid which was rejected last year, and he wrote a series of memoranda to LAS in June and July 1991 warning that the mapping subsystem (which tracks ambulances and dispatches the nearest to an incident) was not up to the requirements. "The rule-based, analytical approach used by the LAS cannot deal as well as an experienced operator with the small minority of difficult cases. The system wrongly reduces the influence of operators".

Meanwhile Mike Smith, systems manager at LAS stated "One thing that did not fail was the computer. What seems to have gone wrong is that the people working on the system were flooded with exception messages - we don't yet know why. We may have lost local knowledge by breaking up sector desks at the weekend."

LAS have now gone back to a hybrid system using human expertise to dispatch ambulances rather than a computer. The two days of chaos last week may have cost up to 20 lives, although exact figures are of course impossible to obtain.

Paul Johnson (paj@gec-mrc.co.uk). | Tel: +44 245 73331 ext 3245

> [Also reported by Chris Welch <me_s420@ceres.king.ac.uk>, with more from Brian Randell (Brian.Randell@newcastle.ac.uk) and Lord Wodehouse <w0400@ggr.co.uk>. Complete articles from Computer Weekly, The Guardian, The Independent, and Computing can be FTPed from the file risks-14.02LAS in the RISKS: directory. PGN]

Re: Cash dispenser fraud (Kristiansen, RISKS-13.89)

Thor Lancelot Simon <tls@panix.com>
Mon, 9 Nov 92 00:23:31 EST

I had an experience earlier this week that indicates that banks hereabouts (Connecticut -- but probably at least the Northeastern US in general) are aware of this problem, and have realized a `solution'. I believe the ATM machines with the `jaws' are Diebold TABS machines, but I might be wrong. In any case, I ran into one of these machines with a rather shorter than usual timeout period, grabbed for my money just as it was pulled back, and didn't get it in time. I then found that my account had _not_ been credited for the money I hadn't received, and had a fair bit of difficulty getting the bank in question to credit me for it when I showed up the next day to complain. I suppose that since one doesn't get credit for the money the machine takes back in, it's impossible to take part of the money and run. On the other hand, why is it even necessary for the machine to pull the money back at all, if it's not going to give credit for it? This `fix' seems to me to be blatant opportunism on the part of the banks. I know that among the readers of this list are some ATM programmers; any comment?

[REPLY TO tls@panix.com on this one, please. Cc: risks if you wish. PGN]

Re: Cash dispenser fraud (Mellor on Kristiansen, RISKS-14.01)

Antoon Pardon <apardon@vub.ac.be>
Thu, 5 Nov 92 8:50:47 MET

I don't know the legal situation in other countries. But if I understand it correctly in Belgium the bank can't refuse to give you your money when you state that you didn't receive it. This is because you don't sign a note when getting money from a cash dispenser. So the bank has no prove that it handed the money out to you. Counting the remaining money in the till and checking with the balance does no good since the money could have been taken by the following client.

Antoon Pardon <apardon@vub.ac.be>

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 3

Tuesday 10 November 1992

Contents

"To ensure the continuing access of law enforcement" [Re: Denning...]

Jyrki Kuoppala, Helsinki University of Technology <jkp@cs.hut.fi>
Tue, 10 Nov 1992 13:29:31 +0200

The Russian government is going to pass a law requiring furniture manufacturers to build microphones and radio transmitters inside every sofa, chair, and table manufactured. A high official from the Russian government was reported to say:

> We just aren't able to function any more without a law like this. After the Soviet Union ceased to exist, the United States government has hired over 50 percent of the KGB staff and we are losing the ability to watch criminals. They have the need, and they have the money, and they value experience you couldn't have gotten anywhere else. Thus, our law enforcement has suffered.

> When this law passes, we can catch all criminals even before they have time to commit the crimes.

It is planned that at a later stage when Russia has the technology to do it, a similar law will be passed for dentists to install the same hardware in tooth fillings.

For people who have doubts that this would be a return to the former Soviet Union policies of watching for political dissidents, the official says:

> Absolutely not. We have learned from our past mistakes. It is only natural that we want to maintain our ability to catch criminals in the changing times -- the changes in the job market are taking all our KGB men for a country where there's money and where there's a flourishing job market, and it's only fair we should keep our law enforcement at the high level we have managed to get it. Thus we are not even increasing our resources, we are just keeping them the same. The tapes will be used only to catch criminals, and a court order will be required before we will listen to the tapes. Trust us, we're the Government and we are here to help our citizens.

The law also requires that if anyone sitting on a sofa or a chair, or at a table, speaks any other language than Russian, she or he must be able to provide an interpreter who will translate his talk to Russian if the law enforcement decides there's a legitimate need to listen to the tape of the conversation. To make this possible, the name and address of the interpreter must be clearly said aloud in Russian near the table/sofa/chair before each conversation in any language other than Russian.

//Jyrki

[Although April Fools' Day is still far away, Guy Fawkes'
Day was last week. Mayhaps this is appropriate? PGN]

Credit Thieves [also submitted to the privacy digests...]

"Message Center" <FZC@CU.NIH.GOV>
Mon, 09 Nov 1992 22:23:37 EST

(Really Paul Robinson -- TDARCOS@MCIMAIL.COM)

Article Summary, "The Credit Thieves" (Washington Post, Nov. 9, Page D5), "They Take Your Identity, Then Your Good Name."

In "The Credit Thieves" article author Stephen J. Shaw asks if you have checked your credit rating lately; some thieves have been known to find people's personal information, then create new identities - and new credit histories - for some people. Apparently name and address is enough to be able to "borrow" someone else's credit information. Some so-called "credit doctors" charge $500 to find someone else with the same or similar name and a clean record, and give the buyer that person's credit record.

Shaw declares personal exposure to credit fraud: his credit rating showed "almost $100,000" in credit, services and merchandise ("loans, credit cards, personal bank loans, plane tickets, home-entertainment systems, computers, clothes, furniture, cellular telephones and a slew of other consumer goodies") granted to "him" even though he lives in Washington DC, and the credit granted to "him" was to someone in Orlando Florida, and he's never heard of the things claimed to be charged to him.

He only found out about the incident when he applied for credit with an organization and they asked him why he didn't declare all the OTHER credit cards and such that he has.

Apparently almost anyone with access to a computer terminal with access to a regular credit reporting agency can probably find out your credit history.

His "Credit Double" was only caught because he tried to buy a house using Shaw's name. The Secret Service is the agency that handles trying to catch people who do this. The "credit mugger" is in jail awaiting trial for four counts of bank and credit fraud.

Happy ending, eh? NOT. Now getting rid of the inaccurate and fraudulent credit requests is a job in and of itself.

"Equifax had deleted five of the bogus accounts, kept another four on my report and added three new ones. TRW told me that most of the disputed accounts had been deleted because the creditor had not replied to TRW's inquiry, but added that the 'creditor may re-report item.' stating , in effect, that the accounts could reappear in future editions." Trans Union did not have the incorrect accounts, but still had the Florida address. TRW also has his address listed as Florida.

A New York State agency found six out of 17 credit reporting agencies which advertised would sell credit histories without any attempt to verify the purpose of the request. An executive at TRW told a 1991 Congressional hearing that "if someone is willing to lie to get a consumer report on another individual, there is nothing in the present law to act as a deterrent."

Apparently it's not all that hard even to get someone's credit report legally. The Fair Credit Reporting Act (FCRA) allows anyone with "a legitimate business need for the information" can get your report; this includes prospective creditors and employers. "This loophole covers anything from renting an apartment to paying for something by check to joining a health club or a dating service. Reports can be ordered legitimately by employers checking on employees, insurance companies writing policies, someone trying to collect a debt, and government agencies deciding to grant any form of assistance or licenses."

The article notes one can request not to be put in the list of "pre-screened" or "targeted" people that credit reporting agencies sell to companies that sometimes offer credit. You can also ask to be taken off mailing lists by writing the Direct Marketing Association, Mail Preference Services, 11 West 42nd St, Box 3961, New York, NY 10163-3861. They can also take requests just to remove your telephone number from some lists.

The article recommends contacting each of the three major agencies twice yearly, and at least 6 months before a major purchase, because some of them don't get what the others have. If something is wrong, contact the creditor directly as well as the reporting agency. If you can't get something corrected, ask to have a statement inserted in your record.

If you're not satisfied, you can write the Federal Trade Commission at
Correspondence Dept, Room 692, Washington DC 20580.

The major credit reporting agencies are:
 - Equifax, Box 740241, Atlanta GA 30374   1-800-685-1111
 - Trans Union, Box 7000, North Olmsted, OH 44070
   Regional Offices:
   - Box 360, Philadelphia, PA, 19105   215-569-4582
   - 222 South First St., Suite 201,
     Louisville KY 40202   502-584-0121
   - Box 3110, Fullerton, CA 92634   714-870-5191
 - TRW National Consumer Relations Center,
   12606 Greenville Ave., Box 749029,
   Dallas TX 75374-9029   214-235-1200
   (TRW allows one free report a year by mail from)
   - TRW, Box 2350, Chatsworth CA, 91313-2350

Paul Robinson -- TDARCOS@MCIMAIL.COM   [Disclaimer omitted...]

Concerns about quality in products of modern technology

<rmoonen@ihlpl.att.com>
Tue, 10 Nov 92 06:39 CST

I have been a regular reader of the RISKS forum for quite a while now, and the situation seems to be that more and more people are becoming aware of the risks associated with modern technology. However, also increasing is the amount of life-threatening accidents/near-accident/malfunctions/errors in computers and related other electronics. Some people have proposed measures to make sure certain quality standards are met. I can still remember the proposition for having software professionals register themselves as such. Much was said at that time, and the proposal got bombed. ISO has a set of standards (the 9000 series) for quality, which we adhere to within the company I work for. Others have proposed plans, but none really seem to get the attention they deserve, and if they do, they die a certain death after a while. After having read 'Zen and the Art of Motorcycle Maintainance' (highly recommended) and the ideas about quality described in that book, I think technology desperately needs to get in touch with reality again. I have thought about this, and have come up with a set of situations that can adversely influence the quality of a project or new technology. Furthermore, I would like to hear your views on the countermeasures I propose. Just to be clear, I am in no way a quality-expert, just a programmer who tries to keep in touch with reality, and reports as such. The way I see it, the following are major contributors to bad quality of a project/product:

Before implementation:

1) Concessions during design w.r.t. costs, politics, human factors.

I realise some consessions must be made sometimes, but I have seen a lot of projects go down because of too many concessions.

2) Too rigid a view of what is possible/impossible.
As seen often here, some systems think it's impossible for people to have 1-letter names, resulting in chaos. Others think it is possible to positively identify people by just a subset of their personal data available. Many more examples are to be found, but basically they all boil down to the fact that the input/output requirements are context-sensitive. Don't forget the Fringe-Factor (TM)!!

3) Future needs are disregarded too often.
"Works as designed" is a standard way of getting out of this, but isn't a solution. Some thought *must* be given to future needs when designing a project

4) Compatibility needs.
If a product is intended to work together with a different product, it should be clear during design exactly how the other product operates.

During implementation:

1) On the fly changes to the design, usually a result of too high a cost or implementors just not being up to their task. If you have a good design, stick too it, or change it only when it *adds* quality.

2) The tools to do the job turn out to be defective. In stead of replacing the tools, too often implementors are forced to use the old ones, thereby reducing quality of the end-product.

3) Mis-communication between implementors and supervisors of a project. Things are heard like "You want it next *week*?? I thought you said next *month*!!" Several variations on this theme come to mind :-(

4) Loss of oversight over project. Every implementor must have a general view of the totality of the project. The final quality is *his* responsibility. Details are OK, but don't loose the "feeling".

After implementation:

1) Incomplete testing of the product before delivery. Too little time is taken to test the product, and a product will be under-developed when it reaches the marketplace. Combined with point 2 this leads to extremely counterproductive results.

2) Rigidity of supplier.
After the product has been delivered and installed, a provider should support the project with a total commitment to quality. Usually this is done by means of a maintenance-contract or an update-contract, but I think it shouldn't stop at that. Too often a product is only then corrected, if the customer reports the failure, even if supplier knew about it long ago. A supplier should do everything in its power to ensure the

integrity of the product. Alas, usually the supplier won't do
anything, even if told frequently.

3) Untrained personnel handling the new product/project.
After said product has been delivered, unknowledgeable personnel
often get thrown in at the deep end, sometimes with disastrous results.

While all these points are pretty straight-forward, when seen as a list, it immediately becomes clear where most manufacturers fail. While they don't cover all points, I believe the following countermeasures could increase overall quality.

1) Start design from specifications which are as context-insensitive
as possible.
2) As I said before, don't forget the Fringe-Factor (TM).
3) Survey possible future needs *before* design.
4) Make sure you stick to the design, once it is accepted. If it costs
more, you have failed in the initial estimate, and you should ensure
that you can continue the project. It will pay off.
5) Check methodology and tools before implementation.
6) Make it exactly clear which secondary requirements there are to
a project. Both the implementors and supervisors should have the
best communication about this.
7) Make sure every developer of a product is aware of what part
of the project he is working on, and why. Ensure he has at least
a good working knowledge of the other parts of the project.
8) If the product is complex, then supplier should provide the
client with an opportunity to give the clients employees and future
users of it's product a training in the use of this product.

If these points are taken well, I think we would see better products, which are not necessarily more expensive. Note that I haven't touched the subject of user interaction, but that's because I think it's a completely different field, and is more subject to psychology than technology. Maybe some net.psychologist can shed his/her light on this? Oh, BTW, if you plan on sending me email replies on this, do so to:

accucx.cc.ruu.nl!hairy%knoware.ruu.nl

It is my private email account, so my email won't clog up AT&T's machines.

--Ralph Moonen

New emphasis for SDIO

Diego Latella <latella@cs.utwente.nl>
Tue, 10 Nov 92 10:30:15 +0100

>From "Disarmament Newsletter - Newsletter of World Disarmament Campaign"
United Nations Vol. 10, No.3 - June 1992

New emphasis for SDIO

The US Strategic Defense Initiative Organization (SDIO) has moved
to cut its funding for space-based systems in order to increase
its ability to deploy a ground-based system in conformity to the United
States Missile Defense Act of 1991.
The system proposed by this Act would be in compliance with the Treaty
on anti-ballistic missiles and would have the goal of providing
a ground-based SDI system by 1996 with the capacity to defend most
of the continental United States. This has lead to reductions in
funding the "brilliant pebbles" space-based intercepter programme.

This on my opinion seems extremely dangerous since

1) It speaks explicitly of a *deployment* program.

2) It is in *compliance with ABM Treaty*.

3) It speaks again of *defending most of the US*.

4) Being ground-based and after the (supposed) "success" of patriots
in the Gulf War it may claim for *more credibility* than space-based SDI.

It is my feeling the Scientific Community should once again mobilize as it did against SDI, being also conscious that its task will probably be harder this time (see points 2 and 4).

Diego Latella, Univ. of Twente - Faculty of Computer Science, TeleInformatics
and Open Systems (TIOS) Group, P.O. Box 217, 7500 AE Enschede - The Netherlands
phone: +31 53 893755 email: latella@cs.utwente.nl

Accountant's error catches thief!

<jgrace@tetrasoft.com>
Tue, 10 Nov 92 12:21:14 PST

I am taking an introductory Accounting course (enough groaning! :-) and actually its quite a bit of fun --- since accounting is basically an exercise in managing the risks of having and not having accurate information to run a business.

Of course, the accountants try to be as exact and consistent as possible to uncover any inconsistencies (e.g., theft, loss, mistakes). However, only so much can be done before the costs outweigh the gains, so only so much is *really* done --- with the hope that that's enough and that everything will be alright. (This "constraint" principle is that of "Cost-benefit --- the value of a financial item reported should be higher for the decision makers than the cost of reporting it" [Fundamentals of Financial Accounting, 6th E., Short and Welsch, page 159].) Of course, this seemingly cut and dry principle is *really* a matter of judgment --- what may *appear* as diminishing returns may actually be very valuable information. To sum up, accountants *try* to walk the line between valuable information (on one side) and diminishing returns (on the other side) with as accurate, relevant information as possible.

Unfortunately, accounting systems are easily abused by crooks. So, accounting also covers "Internal Controls" (this week's lecture :-), especially of cash handling (but other stuff too, e.g., inventory, supplies). The main approach to avoiding misappropriation of cash is the division of responsibility for cash collection and accounting (and other responsibilities too). A commonly observed example of this separation of duties:

> At most movie theaters, one employee sells tickets and another employee collects the tickets. It would be less expensive to have one employee do
>
> both jobs, but it would be easier for an employee to steal cash.
> [FoFA, p. 356]

As you can see, these measures are very important and, unfortunately, can be very expensive to implement.

So this week, our instructor (who is full of great anecdotes from his banking/loaning experience) related the story of a merchandise business where, despite separation of duties, the delivery person found a way to defraud the company. The scenario follows:

The delivery person delivered goods to customers in return for checks and cash which he was supposed to hand over to the bookkeeper to record (separation of duties :-). Then the bookkeeper gave him the checks and cash to deposit at the bank --- with a slip from the accountant for the amount of the deposit (separation of duties). Instead, the delivery person withheld a check from the accountant and picked up a deposit slip for the reduced amount. Then, on the way to the bank to make the deposit, he "cashed" his pocketed check in via the deposit cash --- thereby maintaining the validity of the bookkeeper's deposit slip (but coming away with the cash equivalent of the "cashed" in check from the company's payments). The only inconsistency left by the scheme is that customers who have paid for goods, are recorded by the company as having an unpaid balance (when they have actually already paid). I don't know how long this scheme had gone on, but I imagine small discrepancies are overlooked by larger companies (cost-benefit constraint again :-).

Ironically, as long as everything goes well, the thief gets away with his scheme. Of course, the error here is believing the "Internal Control" system is not flawed --- but practically speaking, cost-benefit constraint kicks in and keeps apparently working systems from being scrutinized (or the old, simplistic maxim "If it ain't broke, don't fix it").

However, eventually, our ever vigilant but imperfect bookkeeper made a mistake on the deposit slip (where an even number was odd or somesuch). I don't know the details (at all) but apparently the thief didn't catch the error (or it didn't matter whether he did or not) and eventually the bank and company had to do research to resolve the problem. Of course, the research led to discovering how customers thought they had paid but were recorded as not paying, etc., and the fraud and thief were discovered.

I found the case amusing and apropos to RISKS since Accounting is a formal attempt at reducing risk through cost-effective, relevant information (trade-off flag immediately waving :-), "Internal Control" systems which are subtly subject to abuse, and the ironic *value* of making a mistake once in a awhile (perhaps even on purpose) to highlight areas taken for granted. In this case, "If it ain't broke, break it" [to make sure it *really* isn't busted] seems a propos!

Of course, technology may help address these issues (while creating fresh ones of course :-), e.g., electronic verification of paid and unpaid balances between the company and its customers or even electronic payment (e.g., CheckFree), etc..

Joe

Cellular misinformation

"Barry C. Nelson" <bnelson@ccb.bbn.com>
Tue, 10 Nov 92 14:58:48 EST

The Boston Globe, 9 Nov 1992, had a human interest story illustrating some good uses for the ubiquitous cellular phones. In many places you can dial *SP for the State Police, and this had been credited with getting rapid assistance to accident and crime victims, as well as apprehending a dangerous escapee. They mentioned problems with routing 911 calls.

What I found more interesting was a discussion about the Coast Guard preparing to adopt *CG as a maritime cellular distress number. A local official was quoted as saying that the existing broadcast channels will remain in operation because anyone nearby will hear you and the CG operates Direction Finding stations to pinpoint your location. Okay...

But then he went on to say that cellular calls "only give you a point to point channel", leading one to the wrong belief that they couldn't DF a cellular user, and that nobody else could listen if they wanted to.

-BCNelson

P.S.: After a PGN talk at MIT recently, someone in the audience claimed that
the FBI has multiple "trunks" attached to the local cellular hub in
Boston and they can monitor both sides of a conversation by just typing
in your number. Thank goodness that this is a democracy. :-^

"End-Running" Key Registration

Alec Isaacson <AI4CPHYW@MIAMIU.ACS.MUOHIO.EDU>
Tue, 10 Nov 92 10:07:36 EST

Recently D.LONGLEY@qut.edu.au wrote about "How Teflon John Coped with Key Registration" which got me to thinking about _other_ ways to beat key registration, namely a cipher group method. (i.e. an "innocent" word has some other word or sentence associated with it).

In that case, our criminal could send to his associate, "How is your dear Uncle Joe." The associate, or his computer, looks in the code table and sees that "your" = liquidate "dear" = soonest and the intended victim is (by

pre-arrangement) the next name mentioned. The FBI could crawl all over a
message like that with a microscope and not discover a thing.

I can't see why this wouldn't work (unless it becomes illegal to write about
non-existent relatives :).

I welcome comments, since the sum total of my crypto experience comes from
reading the spy novels on occasion.

Alec D. Isaacson, Miami University, Oxford, OH
AI4CPHYW@miamiu.acs.muohio.edu isaacson@rogue.acs.muohio.edu (NeXt Mail)

... on a way to foil the fbi...

Peter Wayner <pcw@access.digex.com>
Tue, 10 Nov 92 10:08:43 -0500

Actually, the FBI is very technically proficient. James Bamford tells
a story about their cryptographic prowess in _The Puzzle Palace._ Apparently,
the agents determined that the _only_ way communication could be
leaving the criminals is through the shirts they sent out to be laundered.
The FBI kept track of the shipments with great patience and finally
figured out that the number of shirts of each color encrypted the message.

12. The 4 bit cipher feedback allows Teflon John to reduce his phone bill with
more sophisticated approaches where more than 1 nibble is used per message.
With 4 bit cipher feedback there is more control over the ciphertext so that
the messages can be modified easily to produce the requisite nibbles
corresponding to the ciphertext used by MAC the knife.

And by logical extension...

Peter Wayner <pcw@access.digex.com>
Tue, 10 Nov 92 10:00:05 -0500

> Dorothy Denning suggested that anyone using high-level encryption over a
> public network be required to register their encryption keys with some
> agency.

Steve Tepper writes:

> Take this a step further. What's to stop the bad guys from creating their
> own language? (Say something like Esperanto but based on Navajo instead of
> Italian.)

And what about puns, double entendres, and anagrams? Will metaphor, simile,
metonymy, and synecdoche be the next to go?
Peter Wayner

[Don't forget the anecdoche and its antidoche, the cynicure.
Actually, there are all sorts of cryptic messages hidden in

RISKS, but few people seem to notice them. PGN]

Re: FBI Registration

Andrew Klossner <andrew@frip.wv.tek.com>
Tue, 10 Nov 92 13:30:49 PST

The clever ruse that Dennis Longley discusses doesn't differ substantially from simply using a code within the cipher. If you're going to load encrypted information into the first few bits of innocent messages, you might as well just redefine the innocent messages. For example, "buy soybeans" might be code for "kill tough tony".

Andrew Klossner andrew@frip.wv.tek.com uunet!tektronix!frip.WV.TEK!andrew

Re: Interesting/obscure interaction between users

Rich Kulawiec <rsk@gynko.circ.upenn.edu>
Tue, 10 Nov 92 08:57:16 EST

(Honig, RISKS-13.88, Leichter, RISKS-14.01)

Jerry Leichter follows up on David Honig's discussion of the SunOS shared memory resources by noting that it is possible to recover from resource exhaustion by using various programs to locate shared memory segments which are (a) were not properly deleted and (b) are not in use. In particular, he mentions Ultrix's "ipcstat", which displays a list of known IPC objects. (The corresponding SunOS program is called "ipcs"; I believe that it's functionally equivalent.)

The problem is, though, that the situation is worse than either David or Jerry mention. It is not only possible to create shared memory segments which persist when they should not, but it is also possible to do so in a way that is *invisible* to ipcs--but visible to programs like top and pstat, which can measure available memory. We discovered this by accident when attempting to diagnose a resource exhaustion problem that our principal in-house application appeared to trigger.

The scenario works like this: the basic operations permitted on shared memory segments are creation, deletion, attachment, and detachment. In normal use, a master program would create a shared memory segment, and various subprograms might attach to and detach from it as they needed to. Eventually, the master program would delete the shared memory segment before exiting.

However, if one process creates a shared memory segment, and a second process attaches to it and then deletes it *while still attached*, the segment is not freed, even though it is marked as such and is thus invisible to ipcs. (It's not freed when the processes exit, either.) It's possible to start another process which can still locate and attach to this ostensibly non-existent segment, which is surprising. It can be deleted without a reboot by running a program which iterates through all possible shared memory segment identifiers and attempts to delete each one, regardless of whether or not it appears to exist, but this is a rather drastic solution. (We've also discovered some additional scenarios which lead to roughly the same problem; all of this was under SunOS 4.1.1.)

Rich Kulawiec

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 4

Weds 11 November 1992

Contents

Abuse of federal computer access

"Barry C. Nelson" <bnelson@ccb.bbn.com>
Wed, 11 Nov 92 14:48:14 EST

At the September 92 Seminar of the American Society for Industrial Security (ASIS), I attended a lecture by the office of the Inspector General of Health and Human Services (HHS-IG). They are normally tasked with tracking down people who cheat on Medicare and other assistance programs. Last year they cited $15 million in penalties in over 2500 cases.

The lecture was about "Operation Private Trust" -- catching people who abused their official computer access. In mid-1990 HHS noticed that a company in Florida was offering personal information which could probably not be legally obtained as fast as they were providing it. They called themselves "Nationwide Electronic Tracking" service, NET.

NET offered everything from credit checks in an hour ($10) to a 10-year employment history ($175) in five days. A scale of prices included $7.50 to get someone's home address based on their Social Security Number in under two hours. They also offered info on a variety of topics including your official criminal records, employers, neighbors, post office box, driver's license and car registration, workmen's compensation claims, etc.

There are normally 200,000 legitimate external IRS queries every year, but processing them normally takes 2-4 weeks, providing a niche for a criminal entrepreneur. How do you identify the illegal queries?

To make a long story short: They laid a trap wherein a NET "customer" requested information based on a certain SSN. HHS then asked the IRS to quietly monitor their system for a query. It popped up two hours later in Phoenix. (The IRS had to modify their system to trace the identity of the person requesting the information.) Investigators then did other types of queries and soon discovered a large nationwide network of middlemen with sources working at various government agencies. Dozens of government employees were selling information to which they had online access. Systems included IRS tax returns, and the FBI's NCIC.

In some cases the "customers" were drug dealers who were trying to check out backgrounds in order to find undercover investigators. Some of the "middlemen" also turned out to be former IG and other HHS agents who were aware of the records' accessibility and lack of system security. The middlemen made huge tax-free profits. Where NET customers paid $100 for a report, the clerk who did the access might receive only $5 for the effort.

As a result of the investigation, the US Attorney in Tampa issued ten indictments against fourteen people, and 11 of them pleaded guilty. They were charged with over 30 counts of conspiracy, unauthorized disclosure of tax return information, theft/conversion of government property (records), aiding and abetting a crime, bribery of public officials, making false official statements, and fraudulent access to Federal computers (18 USC 1030(a)(4)). There were details of literally hundreds of illegal overt acts (some of which were probably recorded on wiretaps). Additional indictments were filed in New Jersey with more to follow soon.

The IRS systems have now been tightened up so that fewer clerks have valid access rights. Audit records are now scrutinized monthly and clerk transaction profiles monitored. The FBI is said to be "examining the problem" of user authentication on their systems.

The moral of the story was: If you're given special access to online federal information and you abuse it, you may have to pay the consequences which include ten years in federal prison and a $10,000 fine. No end-users of the illegally obtained files were indicted and there continues to be a large market

for private information held in government computer systems.
-BCNelson

Therac-25

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Wed, 11 Nov 92 12:00:15 -0800

A paper describing the details of what really happened with the Therac-25, including detailed descriptions of the software bugs and the response by users, government agencies, the manufacturer, etc. is now in review for publication and available as a technical report. This is the result of three years of detective work by myself and Clark Turner (my student) and the collection and distillation of several large boxes of documents. Many of the previous media accounts and papers have been incomplete, misleading, or plain wrong.

To order, call or write to UCI (Info. and Computer Science Dept., University of California, Irvine, CA 92717) or to UW (Computer Science and Engineering, FR-35, University of Washington, Seattle, WA 98195) and ask for:

"An Investigation of the Therac-25 Accidents," by Nancy Leveson and Clark Turner. UCI TR #92-108 or UW TR #92-11-05

[Nancy gave a preview of this paper in New Orleans at SIGSOFT '91 last December. It has been long awaited, and I expect it will be a best-selling technothriller, even if it is completely NONfiction. (Truth is often stranger than fiction, anyway!) However, I hope RISKS readers do not deluge Nancy with TOO MANY requests that she decides never again to make such a generous offer! But I am absolutely delighted that she is giving RISKS readers an early chance to review this report. PGN]

When "yes" means "no" (More voting screwups)

Ted Shapin <TSHAPIN@biivax.dp.BECKMAN.COM>
11 Nov 1992 09:04:39 -0800 (PST)

From an article by Daryl Kelley, Los Angeles Times Staff Writer, Nov. 11, 1992:

Chagrined Ventura County [CA] election officials confirmed Tuesday [Nov 10?] that they had fed inaccurate vote tabulations on 13 state ballot propositions to the secretary of state's office last week. The foul-up, which reversed Ventura County's YES and NO votes for each proposition, did not involve enough votes to change the outcome for any of the statewide measures, state officials said.

"I don't know of any other county that screwed up, but I did," Ventura County elections chief Bruce Bradley said Tuesday. "I linked their YES [computer line] to my NO, and vice versa. So on Thursday when we found out, we corrected it." The error was made only on the ballot measures, Bradley said. Ventura County tabulations in other state and federal races, such as the two for U.S. Senate,

were fed accurately to Sacramento by computer lines identified with the names
of the candidates, he said. All the results for local ballot measures and
races were accurate, Bradley said.

Melissa Warren, spokeswoman for the secretary of state, said the error did not
affect the outcome of any proposition because Ventura County's voting trends
generally jibed with the rest of the state and because Ventura County voters
are a small part of the state total.

The closest ballot measure was Proposition 162, which shifts control of funds
in the public employees' retirement systems. The measure won by 187,101 votes
statewide, according to semiofficial results, It lost by 5,528 votes in Ventura
County.

Such mistakes are not rare, Warren said.
==== ======== === === ===== ====== ==== [emphasis added!]

Over the next three weeks, California counties will count late arriving
absentee ballots and provisional and damaged ballots, Warren said. Then they
will file a final count with the state by Dec. 1. An official count is expected
to be released Dec. 14.

John Flynn, chairman of the Ventura County Board of Supervisors, said he had
just congratulated Bradley on a particularly smooth election when he learned of
the mistake Tuesday. "It's regrettable," Flynn said. "But these are human
beings who run these things."

Ted Shapin, Beckman Instruments, Inc., 2500 Harbor, M/S X-11
Fullerton, CA 92634-3100 714/961-3393 tshapin@beckman.com

Re: Voting Machine Horror Story (Stangenberger, RISKS-14.02)

David Conrad <dave@tygra.Michigan.COM>
Wed Nov 11 06:53:00 1992

[tygra!dave@destroyer.rs.itd.umich.edu]

This sounds quite like the system used here in Detroit, MI. I always
spot-check a few important items to a) make sure that they are correct and b)
give me confidence that the rest of the ballot is punched correctly. This is
possible because the correct box numbers are printed on the ballot.

So, for instance, in the recent election I verified the holes on the card with
the numbers on the ballot for: President, Congressional Representative, and the
four major ballot proposals here in Michigan; but not for all the minor and
judicial offices. I also looked at the ballot before I put it in the machine
to make sure no holes had been accidentally punched.

Some may consider this excessive, paranoid, or simply inconsiderate of
others who were waiting for my voting booth (we had a record turnout,
and I had to do it in the booth since I needed to be looking at the
ballot to compare the numbers), but considering how quick and easy it

was and that no perfect voting machine will ever be built, I think that double-checking by the voter is the only prudent course.

Note also that checking would be impossible if the correct numbers were not given on the ballot, as they are here in Detroit and apparently were in Berkeley.

David R. Conrad dave@michigan.com

Voicemail problems

"PGE" <CMARTIN@unode2.nswc.navy.mil>
11 Nov 92 14:56:00 EST

When I went to college (University of Maryland at College Park) our school got a new voice mail system to keep up with the times. This system offered a message area for each user accessible from any phone so long as you knew the passcode for that particular number. The problem was that all the passwords were set to 12345 at the beginning of the semester, so the people who first got to campus started having a ball changing friends, enemies and strangers passcodes. By the time I got to campus, I had several messages that I could not get to because the passcode had been changed(remember this was before classes began so students had lots of time on their hands). I had no way to figure out my code except to go to the phone building on campus (though it never came to that because a friend confessed to doing it and gave me the number).

Another risk was the students were never explicitly told that all the numbers were the same, so some students left their number the same and as a result people would "fish" for numbers to listen to the messages of. If any sort of security was there to protect the information (logs or the like) no one I knew who did this ever got caught, and castigated.

The final problem was the message append function. What people could do is the same as E-MAIL reply, except with the original message appended. People would send these messages back and forth until they filled your mailbox, then they would send the message to every number they could think of(if you knew someone in a dormitory, all the hallmates numbers clustered around their number and so all of them might get the message).

During my final year there, when the system was installed these problems were never noticeably addressed, including at the end of the semester being asked to change the passcode back to 12345.

Well, this is just a warning to system engineers to better recognize the users of a system to better handle these shortcomings.

Re: FBI digital telephony article in IEEE Institute (fwd)

"Lance J. Hoffman" <hoffman@seas.gwu.edu>
Wed, 11 Nov 92 13:54:05 EST

Reprinted with permission ("do with it as you wish. Granger")
[and forwarded by Professor Lance J. Hoffman, EECS, The George Washington University, Washington, D. C. 20052, (202) 994-4955 hoffman@seas.gwu.edu]

A "Viewpoint " piece in The Institute, November 1992

Balancing National Interests

The September/October issue of The Institute carried a front page story reporting that the Federal Bureau of Investigation is promoting legislation that would require all telephone systems to be designed in such a way that they can be wiretapped by law enforcement officials. The argument is that wiretapping is a key tool in much of law enforcement, particularly in fields such as drugs, racketeering, conspiracy and white collar crime, and that unless care is taken in the design of future telecommunications systems, this tool may become difficult or impossible to exercise. To solve this problem the FBI is promoting legislation that would establish design requirements on future telephone systems. Not surprisingly, civil liberties groups and telephone companies are reported to be less than enthusiastic.

While interesting and important in its own right, this controversy is perhaps even more important as a symbol of a broader set of conflicts between a number of important national interests. As a country, we want to promote:

* Individual privacy (including the right of citizens and other residents of the U.S. to keep personal records private, hold private communications with others, and move about without being "tracked".)

* Security for organizations (including protection of financial transactions, and the ability to keep corporate data, plans, and communications confidential.)

* Effective domestic law enforcement (including the ability to perform surveillance of legitimately identified suspects, and the ability to audit and reconstruct fraudulent activities.)

* Effective international intelligence gathering (including the ability to monitor the plans and activities of organizations abroad that may pose a threat to the U.S. or to other peaceful states and peoples.)

* Secure world-wide reliable communications for U.S. diplomats and the military, for U.S. business, and for U.S. citizens in their activities all around the world (including the ability to maintain and gain access to secure, reliable, communications channels.)

Just as with most of our society's other fundamental objectives, these objectives are in conflict. You can not maximize them all because getting more of some involves giving up some of others. A dynamic tension must be created that keeps the various objectives properly balanced. That socially optimal point of balance may change gradually over time as world conditions and our society's values evolve.

An electrical engineer who thinks for a moment about the problem of achieving any particular specified balance among the various objectives I have listed will quickly conclude that communications and information technology design choices lie at the heart of the way in which many of the necessary tradeoffs will be made. We would like easy portable communications for all, but doing that in a way that allows people to keep their legitimate travels private poses significant design challenges. Banks and other businesses would like secure encrypted communications world-wide, but promoting the general availability of such technologies all around the world severely complicates the signal intelligence operations of intelligence organizations.

The troubling thing about the FBI's legislative proposals is not that they are being made, but that we lack a broader institutional context within which to evaluate them. In making such choices, we need to look systematically at all the legitimate interests that are at stake in telecommunications and information technology design choices, consider the ways in which technology and the world are evolving, and integrate all these considerations to arrive at a reasoned balance. In the old days, if things got too far out of line in some balance (for example, between freedom of the press and protection against liable), the courts simply readjusted things and we went on. Today, and increasingly in the future, with many of these balances hard wired into the basic design of our information and communication systems, it may be much harder to readjust the balance after the fact.

There are several organizations that should be working harder on these issues. On the government side the Telecommunication and Computing Technologies Program in the Office of Technology Assessment should be doing more systematic studies of these tradeoffs to help inform the Congress; The National Telecommunications and Information Administration in the Department of Commerce (or some appropriate interagency committee) should be doing similar studies to develop more coherent and comprehensive executive branch policy; and the Office of Policy and Plans in the Federal Communications Commission (which is an independent regulatory agency not directly subject to executive branch policy) should be giving these issues more attention so it can better support the Commissioners when they confront such tradeoffs. On the non-government side, the Office of Computer and Information Technology at the National Research Council might appropriately mount a comprehensive study. There is an ideal opportunity here for a private foundation to fund an independent blue-ribbon commission. Finally, the computer and telecommunications industries, both individually and collectively through their industry associations, should be taking more interest in how the country will strike these all important balances.

M. Granger Morgan

M. Granger Morgan (F) is head of the Department of Engineering and Public Policy at Carnegie Mellon University where he is also a Professor in the Department of Electrical and Computer Engineering and in the H. John Heinz III School of Public Policy and Management. He teaches and performs research on a variety of problems in technology and public policy in which technical issues are of central importance.

Encryption key registration risks

Phil Karn <karn@qualcomm.com>
Mon, 26 Oct 92 20:29:17 -0800

David Willcox spoke of the obvious risks of registering encryption keys with some agency. Dorothy Denning responded in RISKS-13.86 that the "risk can be reduced to about zero" and described a mechanism. Yet neither elaborated on just what specific risks are to be protected against.

Denning chooses to ignore one obvious class of risks: defective warrants, incompetence and/or outright corruption in the government and the key registration agency. The government has abused its wiretap facilities in the past (e.g., Operation Shamrock) and will do so again until the widespread use of strong cryptography stops it.

Anyone who thinks that the warrant is a meaningful safeguard ought to consider what happened recently in Poway, California (just northeast of San Diego). Customs and DEA agents broke into an innocent man's house at midnight and exchanged gunfire with the owner, who quite reasonably thought his home was being invaded (the agents did not identify themselves). Last I heard, the owner was in critical condition in the hospital. After the shooting, neighbors overheard the leader telling his troops "Now get this straight. He shot first!"

The sole basis of the warrant? A "tip" from an informer, already known by Customs to be unreliable. He admitted the next day that he had merely picked a house at random when the agents pressed him to "produce".

The judge who approved this particular warrant obviously didn't scrutinize it very closely despite the clear potential for serious injury to an innocent person. It's not hard to imagine a judge being even less critical of an application for a wiretap warrant. "After all", he'll reason, "what harm can to you really do to an innocent person by just listening to his phone calls? It's not like the agents are asking for permission to break his door down."

That's the whole problem with government wiretaps. They're easy and (from law enforcement's perspective) almost risk-free. Break down the wrong guy's door, and there's no way to keep it out of the papers. But tap the wrong guy's phone and he may never know. Warrants? Don't bother -- they leave paper trails, and are unnecessary unless you want to produce the recordings in court. There are many other uses for wiretaps that need not reveal one's "sources and methods".

This is especially tempting with radio. ECPA or no ECPA, the fact is that it's incredibly easy to intercept analog cell phones and very hard to get caught doing it. Indeed, the government successfully opposed meaningful encryption in digital cellular, even though it would only protect the air link -- the land side of the call could still be tapped with the phone company's assistance. I wonder why.

Okay, so maybe I'm paranoid. But I don't think so. A healthy distrust of government, particularly of those functions that are not always open to public scrutiny, is essential to a free society. Or so the authors of the Constitution seemed to think, even if the average person wouldn't mind repealing the Bill of Rights to help fight the drug war.

But let's assume that we've found some saints to populate the entire Executive branch, so we can safely pass a law requiring crypto key registration. Exactly how would it be enforced? Routinely scan all private telephone conversations looking for bit streams that cannot be easily decoded? What about certain rare natural languages - ban them too? (Recall that the US military used Navajo radio operators in the Pacific during WWII as "human crypto machines" against the Japanese). So much for the First Amendment.

Suppose you find an undecodable conversation that you actually have good reason to believe conceals criminal activity. How would you compel the users to reveal the key, if indeed they used a protocol that could be compromised in this way? According to several lawyers I've asked, including a law professor at the University of Wisconsin who specializes in the Fifth Amendment, a memorized crypto key would clearly be considered "testimonial" evidence that could not be compelled without a grant of immunity. So what do we do -- repeal the Fifth Amendment too?

It is absolutely obvious to me that any attempt to control the private use of cryptography could not help but impinge on some very basic Constitutional guarantees. And yet it probably still wouldn't have the desired effect. It's already a cliche, but it's still true: when cryptography is outlawed, only outlaws will use cryptography. (And no, I *don't* believe the same is true for guns.)

Phil

Evading registration of cryptography keys

Otto Tennant <jot@teak.cray.com>
Tue, 10 Nov 92 22:43:16 CST

Suppose both parties ("Joe Teflon" and "Louie") have a ".gif" picture of something, say Yellowstone Falls, exchanged by disk. An encrypted message could be overlayed as "noise" on the video image, recovered easily on the other end, while appearing innocuous to anyone intercepting the image.

(To tease, one could use politically incorrect images.)

Attempts to defeat encryption will defeat only the stupid. Maybe that is worthwhile.

Cryptic messages in RISKS (RISKS-14.03)

<philhowr@unix.cie.rpi.edu>
Wed, 11 Nov 92 09:51:32 -0500

Our moderator writes:

> [...Actually, there are all sorts of cryptic messages hidden in
> RISKS, but few people seem to notice them. PGN]

It is not surprising that few people notice the cryptic messages hidden in RISKS. The longevity of the Forum itself attests to the fact that few people notice even the obvious messages of RISKS.

Robert Philhower, Rensselaer Center for Integrated Electronics, CII 6111
Rensselaer Polytechnic Institute / Troy, NY 12180 philhowr@unix.cie.rpi.edu

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 11 Nov 92 18:15:12 PDT

Thanks, Robert. By the way, I think we have about mined this one out for the time being, so let's see if I can end it without opening up more discussion! Thanks to Dorothy Denning for having opened up a difficult debate at the National Computer Security Conference, Rebecca Mercuri for having brought it up in RISKS-13.84, and all the rest of you who contributed. The problems are very deep, and the risks of simplistic solutions are extensive. This is probably one of those cases in which "there are no easy answers." However, just because a supposedly "easy answer" got included in RISKS, don't assume it was correct, or reasonable, or realistic -- even if it went unchallenged. I did not include ALL of the messages on this subject. There were simply too many. PGN

Re: Risks Of Cellular Speech (Johnathan Vail, RISKS-14.02)

Robert Gezelter <gezelter@rlgsc.com>
Wed, 11 Nov 92 00:51:41 EST

There is a comment in "Risks of Cellular Speech" in RISKS-14.02 which, I suspect, is not correct.

While I believe that it is true that the use of Cellular phones is prohibited in aircraft (at least those operating under Instrument Flight Rules), I seem to remember that the rationale is aviation related, not Cellular Phone related. To be exact, my recollection is that the frequencies used by Cellular are fairly close to some of the frequencies used by the avionics.

In any event, the prohibition is, I believe, a blanket one, not based on, for example, altitude. If the problem were caused by cell overlap, then there would need to be a ban on the use of Cell phones at any altitude where more than one cell site would be over the horizon.

I seem to remember a discussion on this subject a couple of months ago in rec.aviation, but I don't have easy access to an archive.

Bob   Robert Gezelter Software Consultant   5-20 167th Street, Suite 215
Flushing, New York 11358-1731   +1 718 463 1079   gezelter@rlgsc.com

Re: (was persistent resources; risks of thinking hypertext complete)

"David A. Honig" <honig@ruffles.ICS.UCI.EDU>
Tue, 10 Nov 92 16:26:31 -0800

In RISKS-14.03 I saw mention of an earlier post in which I described my discovery that BSD shared memory segments persist; people who know better will be reassured to find out that I have since understood 1) that this persistence can be a feature, not a bug and 2) the SysV libraries allow one to use mmap()

calls to implement shared memory, without the 100 segments of 1MB each limitation (*).

But I discovered along the way two interesting things: first, you can't trust the man pages' SEE ALSO section to give you complete cross-referencing on all related topics, especially between the BSD and SysV camps. Second, the Net and Local Smart People (who turned me on to the mmap() calls) are really great resources.

(*) It was pointed out to me that the BSD segments can be made contiguous, which is helpful; but I also might conceivably need more than that (yes, seriously.)

David Honig

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 5

Monday 16 November 1992

Contents

Voting fraud (is it an accident?)

"Ray Todd Stevens" <RAY@safety.nwscc.sea06.navy.mil>
12 Nov 92 12:39:21 EST

Our voting machines are a series of buttons on the outside of a continuous sheet of paper. You can go page to page with buttons. each button is supposed to point at a candidate/proposal. It didn't work that way.

When I went through the ballot I found several pages that pointed at the lines between the selections, and not at a selection. I found that it was not possible to push the button for Clinton, but was possible to push the button above Bush. I also found that went I paged forward, and back that the lit buttons didn't point at the people I had voted for.

I pointed this out to the election judges and was told that "They only deal with the totals, and therefore it would all average out"

Ray Todd Stevens, Contractor, Resource Protection Dept NSWC Crane Div.
Ray@safety.nwscc.sea06.navy.mil (812) 854-3292 854-3294 854-3289

Safe Conduct

<Jonathan.Bowen@prg.ox.ac.uk>
Fri, 13 Nov 92 12:40:01 GMT

The 12 November 1992 issue of the weekly UK newspaper "Computing" has a three page spread (pp18-21) on safety-critical systems entitled "Safe Conduct" by Clair Neesham. In particular, new piece of EC legislatation, the Machine Safety Directive, comes into effect in the UK on 1 January 1993. This encompasses software and if there is an error in the machine's logic that results in injury then a claim can be made under civil law against the supplier. If negligence can be proved during the product's design or manufacture then criminal proceedings may be taken against the director or manager in charge. There will be a maximum penalty of three months in jail or a large fine. (This actually sounds rather low to me.) Suppliers will have to demonstrate that they are using best working practice including, for example, risk analysis and project planning. The DTI-funded (Department of Trade and Industry) Safety-Critical Systems Club is helping to raise awareness of the issues in the UK with regular meetings and a newsletter. A knowledge of relevant standards is important (e.g., ISO9001, 00-55 & 00-56, DO-178, ...). Formal methods (e.g., Z, VDM and B) are cited as one way of improving matters, but judging from the "site study" boxes in the article, there is still considerable scepticism in industry about their applicability at the moment, due to lack of trained personnel, problems of scaling up, worries about extra cost, etc. However, they are seen as promising for the future.

Jonathan Bowen, Oxford University

Retirement award trips up a crook

"Ray Todd Stevens" <RAY@safety.nwscc.sea06.navy.mil>
12 Nov 92 12:39:21 EST

I number of years ago I was called in as a consultant to look into a suspected case of fraud. The reason for the belief that there was fraud involved was that one of their low paid clerks had retired, and at the end of the year they give out attendance awards. They wanted this person to pick up his "20 years without a sick day" award at the awards banquet, and attempted to invite him. They found out that this guy had been living it up as a jet setter. Someone decided to find out how he could afford it. It was not hard to figure out.

This guy was in charge of all office supplies for the Corp (a large multinational). This meant that he was in charge of ordering and then confirming receipt of supplies. He was supposed to keep an inventory on hand, (central management to the max) and ship out supplies as needed. The supposed control was the the office managers were supposed to confirm that they received what he said he sent them. He was able to set up a phony company and order goods from it he then receipted in the goods, and include these in shipments. If he had missed just one day he would never have been caught.

By the way he basically got a way with it. I return for keeping his mouth shut about where he got the money he got to keep all of the interest, and way not prosecuted.

Ray Todd Stevens, Contractor, Resource Protection Dept NSWC Crane Div.
Ray@safety.nwscc.sea06.navy.mil (812) 854-3292 854-3294 854-3289

PINs and Needles

<Dik.Winter@cwi.nl>
Wed, 11 Nov 1992 02:28:13 +0100

(Based on an article in Vrij Nederland of 31 October, 1992.)

For years the Dutch banks have stated that they do not store the PIN code required for many transactions using cards. They imply that if somebody reports illegal use of the card plus PIN code this is only because the owner of the card has not been careful enough with his code. They also told us that there is no way to calculate the code given an account number only. And they also imply that a 4-digit PIN code is sufficient for security (as many know, this is not true).

It has now been revealed that some banks routinely tell customers their PIN code if they did forget it. There is one case on record where during a criminal investigation the police wondered whether a particular number written down by the person under investigation was the PIN code connected to a particular account. They just asked the bank for the PIN code for the account and received it back, the number as written down was just the code in reverse.

More interesting is here that even though the banks do not store actual PIN codes (and as such are technically correct in some of their statements), some have the data available to calculate the code even if the card is not available.

They still maintain the system is safe.

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland home: bovenover 215, 1025 jn amsterdam, nederland; e-mail: dik@cwi.nl

Re: "End-Running" Key Registration

<Bob_Frankston@frankston.com>
Thu 12 Nov 1992 10:08 -0400

When I talk on cellular phones, I already take precautions by making allusions to other events and taking full advantage of the shared context so that the message is innocuous the the casual listeners. This is the norm for aware people in any case where there is a concern about the possibility of being overheard. Teflon John wouldn't be caught dead (or would be dead if caught?) being too direct over a potentially public (i.e. tappable) channel. This technique works even without intent to be secret -- just listen to two MIT students planning their courses for the following semester.

The real issue is exchanging large amounts of data or regular transmissions such as financial transactions among a large community of users so that all the information about the techniques is public and all that is hidden are the keys.

BTW, it has long been the case that encryping over Telex by using code words, or even nonEnglish words, has been illegal in many countries.

Cellular Phones in Aircraft

Berry Kercheval <berry@athos.pei.com>
Thu, 12 Nov 92 15:30:46 PST

Mr. Robert Gezelter writes in RISKS-14.04 about cellular phones being used "in aircraft (at least those operating under Instrument Flight Rules)".

First of all, the FAA (Federal Aviation Administration) leaves the decision of the use of electronic equipment in aircraft up to the operator of the aircraft. This means, essentially, the aircraft's owner: either me, in the case of my own plane, or the company operating the aircraft: American Airlines, for instance.

The frequencies that cellular phones operate on do not directly conflict with aviation frequencies, but some poorly designed phones could emit RFI (harmonics of the carrier, or IF frequencies for example) in frequencies that could interfere with navigation equipment. Usually this is not a problem, though, as most avionics gear is tolerably well shielded.

Secondly, the FCC (Federal Communications Commission) is the one that bans cellular phone use in aircraft, whether under Instrument Flight rules or not. It turns out that when a cellular phone at, say, 20,000 feet tries to make a call it will wake up cells for hundreds of miles around and badly confuse the system, which is expecting to get a signal from only a few cells at once.

The blanket ban *is* due to cell overlap, then, and my guess is the reason there is not an altitude restriction is that it's too hard to figure out; the number of cells reached is a complex function of altitude, position of the

aircraft and cells, and the topography of the surrounding landscape. I can
just picture the FCC bureaucrat saying ``Hell, that's too hard. Let's just ban
'em all.''.
--berry

voice mail systems

Jim Purtilo <purtilo@cs.UMD.EDU>
Thu, 12 Nov 92 09:33:57 -0500

CMARTIN@nswc.navy.mil wrote about the then-new voice mail system installed at Maryland, and the problems which ensued when students discovered that all the pass codes were set the same. One lesson he suggested from this was to the engineers, who should either make the codes different, or make a better attempt to warn users about the situation.

The education needs to be given regularly to new employees and also visitors, else they can become special targets of locals who already "know the system". As case in point, I cite one of my own (many) experiences with the UM voice mail system that CMARTIN mentions. A few months ago I was given a new office, whose previous occupant had been a prestigious visitor. My own phone number lagged behind the move by a few days, so I temporarily got use of phone account of our visitor, Nancy Leveson. Guess who didn't get the word to change the default passcode!

Don't worry, Nancy, none of the messages sounded urgent. :-)

I discovered you can learn a lot about someone by playing with their intelligent phone system. The "redial" button suggested a last user might have ordered a carry out meal from Cluck-U-Chicken, a popular campus town eatery at the time. (If the place had used caller-ID like so many carry-out businesses these days, then I suppose I could have just ordered the "usual" and found out the previous user's tastes too.) I thought it best not to see where the "speed dialing" buttons got me. But does anyone know of stock brokers or doctors offices use caller-ID as a check for letting callers request a transaction or access info?

CMARTIN did not report the most fun aspect of the voice mail system, which was not generally open to students. It was (notice past tense) "call pickup".... intended, I presume, as convenience in a large office, it lets you answer a call to your number from someone else's phone. After hearing a distinctive ring, say while you are down the hall, you can hit one button and get the next incoming call, picking it up. Well .... as we know so much in this business, "programming in the small" is not the same as "programming in the large". The call pickup feature does not scale, as we demonstrated empirically. Some thoughtful soul had spec'd call pickup in our new system, but, to save money set up the entire CS department on the same "group". (We were told this was to save money... one paid per group, where "group" was a set of numbers within which the pickup feature would work.) The net result of this was that whenever a professor got bored, he or she could play call-pickup-roulette ... that is, pick up the phone, punch the "pickup number" and see if anyone was calling *anyone* in the building. That is, you could intercept any incoming call with lucky timing. (I should note that John Gannon had demonstrated a keen proficiency in this technique.) The entertaining part of this was how you handled the call, which I leave to the reader's imagination.

John has a fertile imagination, especially when egged on by his office neighbor. The feature didn't last long.

Jim

Radio to remote computer protocol design

Edward J. Huff <huff@MCCLB0.MED.NYU.EDU>
12 Nov 1992 07:55:05 -0500

Here is a chance to help get some equipment which will be widely used by the public to work right from the start. A friend of mine in the communications industry is a member of a committee made of representatives of equipment manufacturers. They are not experts in designing or testing protocols, but are designing several which will be used to accept messages from the public, carry them between equipment made by the several companies, ending in a radio receiver interfaced to the end user's computer. If things go as they have in the past, the protocols may be far from robust. I am not identifying the parties involved, and I hope that none of them take offense. None is intended. Learning to design protocols is not so easy. Just being smart is not enough.

No doubt the "obviously difficult" parts, like the radio forward error correction, will be done properly. It is the "easy" parts involving asynchronous communications that are likely to be defective in nonobvious ways. One likely defect is that not every manufacturer's equipment will work properly with the others. This is a source of cost, and is the primary reason the question of validating the equipment and protocols came up. But of course, if that sort of defect can arise, probably others which cause the public harm might also arise.

Anyway, I will capture and forward any e-mail I receive on the subject to the committee. Maybe they can be persuaded to publish the protocols in a suitable Usenet newsgroup, or elsewhere, for comment. Maybe they can also be persuaded to make eavesdropping difficult. Recommendations of books, papers, testing software, or qualified experts, is solicited.

The correct reply address is "huff@mcclb0.med.nyu.edu"

RISKS of technical people disengaging brain

daniel lance herrick <ICCGCC.dnet!HERRICKD@cs.hh.ab.com>
Fri, 13 Nov 92 12:26:35 EST

>It's already a cliche, but it's still true: when cryptography is outlawed,
>only outlaws will use cryptography. (And no, I *don't* believe the same
>is true for guns.)

Realizing that anyone who wants it can recover it, I have excised the signature from this quotation because the author only made himself a representative of a large class of fuzzy thinkers when he wrote it.

Consider the proposition:

If X is outlawed, then only outlaws will {have|use} X.

The hypothesis of that proposition is merely a statement that some legislative body has declared the consequent to be true. The proposition is a tautology, true for all possible values of the variable X.

In particular, it is true for typewriters. I believe the samizdat caused at least one legislative body to substitute typewriter into the proposition for X. It is true for photocopiers. It is true for orange peels, though I don't know of any legislature that has outlawed orange peels.

Most of us are in professions where logic is of some importance. It hurts credibility to declare in public, "I *don't* believe" a tautology.

dan herrick   dlh%dlhpfm@NCoast.org

Re: Credit Thieves (and learning from mistakes)

<tada@Athena.MIT.EDU>
Wed, 11 Nov 92 14:13:08 -0500

Credit fraud is a particular concern of mine because I'm going through a similar situation. What I found interesting about the article posted by Mr. Robinson was a parallel to previous well known computer system failures.

In his October 20 talk at MIT, Mr. Neumann pointed out [some of the problems of] not learning from our mistakes. The 1980 ARAPANET failure and the 1990 AT&T failure were both caused by propagation of invalid packets across a network (conceptually speaking, at least). Cleaning up a corrupted credit record is a similar problem. Given the sharing of credit data, one has to remove the incorrect information from all credit database simultaneously, or it's likely to spread throughout the system again!

In addition, there's a security risk: the owner of any credit database can insert faulty information and it will then be propagated throughout the system.

michael j. zehr

Re: Accountant's error catches thief! (RISKS-14.03)

<king@ukulele.reasoning.com>
Wed, 11 Nov 92 13:24:30 GMT

<> ... Eventually a screw-up elsewhere in the system
<> forced a thorough enough audit to plug the hole for one set of
<> transactions, leading to the transgressor's arrest]

The error, of course, had no essential role in catching the embezzler. What had to happen is that occasionally the accounting thoroughness had to far exceed the bounds of cost-effectiveness.

The random process is all too often an error of some sort, but i understand that banks do an extreme audit on each branch every six months or so, at random times.

-dk

Re: Caller-ID (yet again)

"Greg Rose" <ggr@nareen.acci.com.au>
Wed, 11 Nov 92 14:01:26 +1100

I just thought that readers of RISKS might like to know that IBM Australia has a newly installed phone system that shows the calling number much of the time. There has been no public comment (that I have seen) about the availability of such information, or any way to turn it off. Most people I have talked to don't know that the feature is available.

I spoke to our Telecom representative. Both ACCI and IBM Australia are ISDN customers, and Caller-ID is a standard feature of ISDN. Individual customers get to enable or disable outgoing caller identification at the time they get the service. By default the outgoing information is the phone number, but the PABX can be programmed to send alphanumeric information, such as the caller's name! (According to the techie I talked to, most ISDN customers do allow their identification information to go out, although some don't. Either way, the customer has to specifically address the question. ACCI allows the Caller-ID information even though our own handsets don't have display capability.)

Caller-ID for non-ISDN customers is technically available on most newer exchanges, but AUSTEL, the regulatory authority now that Telecom has competition, has not yet allowed general access until they address the privacy issues.

I was impressed by this answer, both that it seems Australia is addressing the issues pro-actively rather than waiting for a hoo-haa to occur, and also because it was not particularly difficult to get the information.

Greg Rose Australian Computing and Communications Institute
ggr@acci.com.au +61 18 174 842

Tutorials (12/7, San Jose) - UNIX security (Sun User Group Conference)

Nancy Frishberg <nancyf@sug.org>
Thu, 12 Nov 1992 20:00:01 GMT

If you're concerned about UNIX security, you might plan to be at the Sun User Group Conference (San Jose Convention Center) on Monday, December 7, 1992. The Conference and Exhibition extends through Thursday.

In the all-day tutorial "Advanced Unix Security", Matt Bishop
(Dartmouth University) will examine four areas critical to the
functioning of secure Unix systems: user authentication, management of
privileges, defending against malicious logic, and networking.

Concurrently Brent Chapman (Great Circle Associates) will lead
a morning session on "Preparing for Disaster" and Bob Baldwin (Tandem
Computers) will answer the question "Why have Computer Security?" during
the afternoon.

Special offer: 5 full conference registrations (each includes a day of
tutorial) for the price of 4 when preregistering with a single payment.

Other full-day tutorials:
* Sun Network Debugging (Smoot Carl-Mitchell, Texas Internet Consulting)
* Topics in Perl (Tom Christiansen, Convex Computer Corporation)
* Programming in POSIX (Jeffrey S. Haemer, Canary Software)
* UNIX Programming Tools (Kenneth Ingham, consultant)
* The Internet and its Protocols (William LeFebvre, Northwestern University)
* Introduction to UNIX System Administration (Dinah McNutt, Tivoli Systems)
* Integrating C Code and Xt Widgets (Craig Rudlin, MD, Medical Software and
  Computer Systems)

If you just want to go to the exhibits, ask for a free show-only pass.

To get more information by email about these tutorials, the technical program,
or exhibits at the Sun User Group conference, send requests to sugshow@sug.org .

You will receive the full tutorials and program description with
registration information. Or call 1-800/727-EXPO. (Outside the U.S.,
use 512/331-7761 (voice) or 512/331-3950 (FAX).)

Nancy Frishberg, Sun User Group.

Papers accepted for AUSCRYPT'92 -- Schedule

Yuliang Zheng <yuliang@cs.uow.edu.au>
Fri, 13 Nov 1992 14:57:16 +1100

MONDAY, 14TH DECEMBER 1992

Session 1: AUTHENTICATION AND SECRET SHARING I

(9.00-9.50)
Threshold cryptography (invited talk)
Y. Desmedt (University of Wisconsin-Milwaukee, US),

(9.50-10.10)
Authentication codes with perfect protection,
L. Tombak, R. Safavi-Naini (University of Wollongong, Australia)

(10.10-10.30)
Practical proven secure authentication with arbitration
Y. Desmedt (University of Wisconsin-Milwaukee, US),
J. Seberry (university of Wollongong, Australia)

Session 2: AUTHENTICATION AND SECRET SHARING II

(11.00-11.20)
Authentication codes under impersonation attack,
R. Safavi-Naini, L. Tombak (University of Wollongong, Australia)

(11.20-11.40)
Cumulative arrays and geometric secret sharing schemes,
W.A. Jackson (Royal Holloway and Bedford New College, UK),
K.M. Martin (University of Adelaide, Australia)

(11.40-12.00)
Nonperfect secret sharing schemes,
W. Ogata, K. Kurosawa (Tokyo Institute of Technology, Japan)

(12.00-12.20)
A construction of practical secret sharing schemes
using linear block codes,
M. Bertilsson, I. Ingemarsson (Linkoping University, Sweden)

Session 3: SIGNATURES AND HASHING ALGORITHMS

(13.40-14.00)
HAVAL --- a one-way hashing algorithm with variable length of output,
Y. Zheng, J. Pieprzyk, J. Seberry (University of Wollongong, Australia)

(14.00-14.20)
On the power of memory in the design of collision
resistant hash functions,
B. Preneel, R. Govaerts, J. Vandewalle (Katholieke Univesiteit
Leuven, Belgium)

(14.20-14.40)
A practical digital multisignature scheme based on discrete logarithms,
T. Hardjono (ATR Communication Research, Japan),
Y. Zheng (University of Wollongong, Australia)

(14.40-15.00)
Group-oriented undeniable signature schemes without
the assistance of a mutually trusted party,
L. Harn (University of Missouri-Kansas City, US),
S. Yang (University of Science and Technology of China, PRC)

Session 4: THEORY OF S-BOXES

(15.30-15.50)
Highly nonlinear 0-1 balanced Boolean functions satisfying
strict avalanche criterion,
X.M. Zhang, J. Seberry (University of Wollongong, Australia)

(15.50-16.10)
Linear nonequivalence versus nonlinearity,
C. Charnes, J. Pieprzyk University of Wollongong, Australia)

(16.10-16.30)
Constructing large cryptographically strong S-boxes,
J. Detombe, S. Tavares (Queen's University, Canada)

TUESDAY, 15TH DECEMBER 1992

Session 5: CRYPTANALYSIS

(9.00-9.50)
Wire tape channel (invited talk)
V. Korjik (Bronch-Bruevitch Technical Communications University,
St Petersburg, Russia)

(9.50-10.10)
Cryptanalysis of LOKI91,
L.R. Knudsen (Aarhus University, Denmark)

(10.10-10.30)
Cryptanalysis of summation generator,
E. Dawson (Queensland University of Technology, Australia)

Session 6: PROTOCOLS I

(11.00-11.20)
Secure addition sequence and its application
on the server aided secret computation protocols,
C.S. Laih, S.M. Yen (National Cheng Kung University, Taiwan)

(11.20-11.40)
Subliminal channels for signature transfer and their
application to signature distribution schemes,
K. Sakurai (Mitsubishi Electric Co., Japan),
T. Itoh (Tokyo Institute of Technology, Japan)

(11.40-12.00)
A practical secret voting scheme for large scale elections,
A. Fujioka, T. Okamoto, K. Ohta (NTT, Japan)

(12.00-12.20)
Privacy for multi-party protocols,
T. Satoh, K. Kurosawa (Tokyo Institute of Technology, Japan)

Session 7: PROTOCOLS II

(13.30-13.50)
New protocols for electronic money,
J.C. Pailles (SEPT, France)

(13.50-14.10)
Modeling and analyzing cryptographic protocols using Petri nets,
B.B. Nieh, S.E. Tavares (Queen's University, Canada)

(14.10-14.30)
On verifiable implicit asking protocols for RSA computation,
T. Matsumoto, H. Imai (Yokohama National University, Japan),
C-S. Laih, S-M. Yen (National Cheng Kung University, Taiwan)

(14.30-14.50)
Modified Maurer-Yacobi's scheme and its applications,
C.H. Lim, P.J. Lee (Pohang Institute of Science and Technology, Korea)

Session 8: SEQUENCES

(15.20-15.40)
The vulnerability of geometric sequences based on
fields of odd characteristic,
A. Klapper (University of Manitoba, Canada)

(15.40-16.00)
A fast cryptographic checksum algorithm based on stream ciphers,
X. Lai, R.A. Rueppel, J. Woollven (R^3 Security Engineering,
Switzerland)

(16.00-16.20)
An approach to the initial state reconstruction of a clock-controlled
shift register based on a novel distance measure,
M. Mihaljevic (University of Belgrade, Yugoslavia)

(16.20-16.40)
Construction of m-ary de-Bruijn sequences,
J.H. Yang, Z.D. Dai (Academia Sinica, China)

WEDNESDAY, 16TH DECEMBER 1992

Session 9: PSEUDORANDOMNESS

(9.00-9.50)
Information technology security standards (invited talk)
J. Snare (Telecom Research Laboratories, Australia)

(9.50-10.10)
Non-interactive generation of shared pseudorandom sequences,
M. Cerecedo, T. Matsumoto, H. Imai (Yokohama National University, Japan)

(10.10-10.30)
A generalized description of DES-based and Benes-based
permutation generators,
M. Portz (RWTH Aachen, Germany)

Session 10: ODDS AND ENDS

(11.00-11.20)

Prime generation with the Demytko-Miller-Trbovich algorithm,
L. Condie (University of New England, Australia)

(11.20-11.40)
Construction of feebly-one-way families of permutations,
A.P. Hiltgen (Swiss Federal Institute of Technology, Switzerland)

(11.40-12.00)
On bit correlations among preimages of "many to one" one-way functions,
K. Sakurai (Mitsubishi Electric Co., Japan),
T. Itoh (Tokyo Institute of Technology, Japan)

(12.00-12.20)
A fast cascade exponentiation algorithm and its
application on cryptography,
S.M. Yen, C.S. Laih (National Cheng Kung University, Taiwan)

Session 11: PUBLIC KEY CRYPTOGRAPHY I

(13.30-14.20)
Public key generation --- state-of-the-art (invited talk)
P. Landrock (Aarhus University, Denmark)

(14.20-14.40)
The design of a conference key distribution system,
C.C. Chang (National Chung Cheng University, Taiwan),
T.C. Wu (National Chiao Tung University, Taiwan),
C.P. Chen (National Chung Cheng University, Taiwan)

(14.40-15.00)
Public-key cryptosystem based on the discrete logarithm problem,
L. Harn (University of Missouri-Kansas City, US),
S. Yang (University of Science and Technology of China, PRC)

Session 12: PUBLIC KEY CRYPTOGRAPHY II

(15.30-15.50)
Elliptic curves over Fp suitable for cryptosystems,
A. Miyaji (Matsushita Electric Industrial Co., Japan)

(15.50-16.10)
New public-key cryptosystems based on factorization of finite groups,
M. Qu, S.A. Vanstone (University of Waterloo, Canada)

(16.10-16.30)
The probability distribution of the Diffie-Hellman key,
C.P. Waldvogel, J.L. Massey
(Swiss Federal Institute of Technology, Switzerland)

(16.30-16.50)
A modular unit based on systolic arrays,
J. Sauerbrey (Technische Universitat Munchen, Germany)

(16.50-17.10)
A comparison of key distribution patterns
constructed from circle geometries,
C.M. O'Keefe (University of Adelaide, Australia)

For more information, please contact

Auscrypt'92 Secretary,   Office of Educational Services
Queensland University of Technology,   G.P.O. Box 2434
Brisbane, QLD 4001   Australia

Fax: +61-7-864 3529   Phone: +61-7-864 2822
Email: zsrcdawson@qut.edu.au (Ed Dawson) or
    w_caelli@qut.edu.au (Bill Caelli)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 6

Tuesday 17 November 1992

Contents

"Computer programming error" reverses election

Nathan K. Meyers <nathanm@hp-pcd.cv.hp.com>
Tue, 17 Nov 92 08:27:49 -0800

McMinnville, OR (AP, 17 Nov 1992) -- The Yamhill County clerk discovered a computer programming error that reverses the election results of the county's district attorney's race. Incumbent District Attorney John Mercer didn't lose in the November election -- he won by a landslide.

Clerk Charles Stern said the computer error occurred because the program failed to list the candidates in alphabetical order, as they were on the ballot. Mercer had supposedly lost to Bernt "Owl" Hansen, 16,539 votes to 8,519 votes. On Monday, the clerk's office told him Hansen's votes were actually his votes.

Mercer said he was astounded at the turn of events. "The feedback I was getting everywhere during the campaign was very positive. And that's why it was such an emotional extreme to see that I'd lost," Mercer said. "But this is really just as shocking the other way."

Nathan Meyers nathanm@cv.hp.com

[Stern Warning: Once Bernt, Twice Mercerized. (in the proper 2:1 ratio) PGN]

Re: Detecting Voting Problems (Stevens, RISKS-14.05)

F.Baube x554 <flb@flb.optiplan.fi>
Tue, 17 Nov 92 10:03:44 EET

In high school I campaigned for a Democrat in a town near Buffalo with a Republican "machine". He said the the single most important thing to do on election day is to get someone to EVERY voting machine at the very hour the polls open, to cast their own votes but also to *test* the machines. And if ANY problem is found, you demand the machine's closure, and telephone the Board of Elections just to make sure.

In our case every voting machine in town was set up to allow only straight party-line voting. Hurried calls to the county Board of Elections [run by the Democrats] got the machines closed until they were set right, later the same morning.

To keep this relevant, in the example RAY cited it was quite evident that the voting system was not working properly, but in general can *-electronic-* voting and tabulating systems be checked by users for correct operation ? If so, RISKS readers can offer their services for the morning of polling day, to the party of their choosing. If not, don't be surprised when "accidents" occur.

fred :: baube@optiplan.fi

[Better make it the WHOLE DAY, not just the morning. And keep your eyes open for those curiosities about which you should by now be aware, as well as others as yet unexposed. PGN]

Inaccurate stock system believed to cause British Air large losses

John Jones <jgj@cs.hull.ac.uk>

Mon, 16 Nov 92 17:35:30 GMT

Time-out costs BA dear

Its computer system may have cost the airline millions in lost earnings, missing spare parts and legal expenses. Chris Blackhurst, Independent on Sunday, 15th November, 1992

That was the headline over an article relating to a computer system called `Total Inventory Management Engineering' (Time) which British Airways (BA) introduced in July 1987, at a cost of 10M UK pounds. Time, designed in-house, governs BA's aircraft parts and stock control operation, handling 250,000 parts worth 400M pounds.

It is suggested that problems have arisen because when Time was installed it was initialised with inaccurate current stock levels taken from the original manual stock system (known to be as much as 45% out), and these have apparently never been corrected.

The article claims that this has affected BA in a number of ways:

a) General Electric took over servicing aircraft engines for BA in 1991. BA initially claimed the transfer of 53M pounds worth of spare parts. General Electric have nearly finished counting them, and have found only 30-35M pounds worth.

b) In October 1991, BA submitted an insurance claim for a fire at its Gatwick (London) warehouse. The claim included 50M pounds worth of spare parts. The loss adjuster's report hints that BA's figures are not entirely reliable, and valued the lost spares at 28M pounds.

c) The prosecution of 12 people on theft of aircraft parts and conspiracy was based substantially on evidence from Time. 9 were acquitted, some of whom are bringing legal proceedings against BA for wrongful arrest. During cross-examination, the person managing Time admitted that when it was installed in 1987 40,000 items, including 94 complete aircraft engines each valued at 250,000 pounds, were found to be missing. (The article is not too clear on this point, but I presume it means to imply that concern over accuracy of the data produced by Time contributed to the collapse of cases against some individuals.)

d) Lack of confidence in the reliability of Time has lead to it being ignored in some instances. In one particular case, an engineer did not consult it when refitting a cockpit windscreen. As a result, he used the wrong bolts, and the windscreen blew out in flight, almost sucking the pilot to his death (June 1990).

BA dispute the interpretation of events referred to in this article, suggesting that there is no disagreement with General Electric, and that in the case of the fire an initial `guesstimate' had later been revised.

John Jones, Department of Computer Science, University of Hull, UK.

England fights on against system failures

James H. Paul <PAUL@NOVA.HOUSE.GOV>
Tue, 17 Nov 1992 17:57:18 -0500 (EST)

The British magazine _New Scientist_ has in its issue of November 14, 1992, two articles of interest. The first relates to the recent discussion of the London Ambulance Service. The article states that the review began last week and a report is due in February. The article begins:

> "An overcomplicated system and incomplete training for control staff and ambulance crews are the likely causes of the collapse of London's computerised ambulance dispatch service two weeks ago. One software company says that the London Ambulance Service (LAS) underestimated the pressure placed on staff at the control center, and that it makes working there `like a wartime action room.'"

The article continues with general observations about system complexity and a description of the process of ambulance dispatching that the system was intending to automate. The computer consultant working on the review panel, Paul Williams ("from the City firm Binder Hamlyn"), is described as having 13 years experience but he has never reviewed a safety-critical system. He intends to compensate with "expert help from his firm and the computer industry."

[The Tied Typer of Hamlyn? PGN]

The second article is a four-page discussion entitled "Battling on with veteran computers." The major theme is the problems that are created by trying to keep aging software and hardware going. Examples discussed include the Patriot missile system, IBM's Customer Information Control System package, the recent upgrade to the Space Shuttle on-board computer system (we're up to a whole megabyte of memory now!), porting the software for power distribution in Britain from archaic Ferranti Argus 500 machines to modern equipment --

(I interject here a wonderful vignette:

> "The software for the initial system was written in a language called April, which disappeared long ago. But the problem was not the rarity or age of the language, it was the lack of documentation. Three years after the system was delivered [1969], the CEGB [Central Electricity Generating Board] decided to develop its own software. Today the system is maintained by a lone programmer who has been working on the system in assembler for 20 years. Ask Derek Roberts, the group head of control facilities at the national centre of the National Grid Company what would happen if that person fell under a bus, and he pauses. Then he replies: `we don't like to think about that.'"

We now return to our regularly scheduled programming.)

and the early flight control system for the Boeing 747-400. According to the article, so long as there are three copies of any aircraft type still flying in the US, the avionics manufacturer is required by law to continue support -- so

Honeywell (which bought Sperry Flight Systems some time ago) is still cranking
out gauges and regulators for DC-3s.

Something new to add to everyone's burgeoning files.

Stock price too high?

"David Wittenberg" <dkw@chaos.cs.brandeis.edu>
Tue, 17 Nov 92 15:07:49 EST

According to Marketplace on American Public Radio, a stock on the New York Stock Exchange (I don't remember the company) closed above 10000 on 16 Nov. This is the first time any stock has been above $10000, and as you might expect, the stock exchange's computers couldn't handle the 5 digit price.

The price rise wasn't incredibly fast, as the stock was up 400 for the day, so one hopes they saw this problem coming and dealt with it, but the report I heard had no further details.

There's nothing particularly surprising about this report, as we've seen lots of similar examples. After a while it's more depressing than surprising to see the same mistake over and over again.

--David Wittenberg

$Million per second -- CHIPS

<sullivan@geom.umn.edu>
Sun, 15 Nov 92 18:57:32 CST

The NewYorkTimes Magazine had an article on October 18 about CHIPS, the financial clearinghouse for major American banks, which handles one trillion dollars electronically every day. Although 85 percent of all transactions are still made in cash, and only 2% electronically, the electronic payments make up 85% by value.

The article examines some of the possible risks in this system. The hardware is run off of storage batteries, in a room with a Halon fire extinguishing system. But on Oct 1981, "a hardware breakdown took out both New York computers" and "processing was interrupted for five minutes" until backup systems (on an "independent communications grid") in New Jersey were brought up. Users "would never have known" if they hadn't been told.

Messages are verified/encrypted in such a way that someone intercepting a message couldn't just change a dollar amount. Once, in 1989, some criminals (with inside help at a Swiss bank) used CHIPS to help steal $20M(illion). They wired money from the Swiss bank (entering a fake deposit on the books) to Australia, and quickly spread it around. Though they have been caught, only $8M has been recovered. The electronic system merely helped them disperse the large amount quickly.

The bigger worry is a loss of confidence. Unlike in the similar European system, all debts are netted at the end of the day. Each bank either owes some amount to the center, or is owed money. If one bank fails to meet its obligations, all transactions involving it that day are supposed to be "unwound". This could, of course, lead some other bank to no longer be able to meet its own obligations for the day, causing a cascade. CHIPS does allow each bank to set a limit on how much it is willing to be owed by all other banks; this limit is monitored continuously, and so a cautious bank could avoid problems.

The Federal Reserve runs a similar system, and once had to make an overnight loan of $24 billion to the Bank of New York "in order to settle the day's accounts on transfers of Government securities that got fouled up in a software snafu." Of course, these days such securities are really just electronic entities stored with the Fed, so the overnight loan was well collateralized, and evidently the situation was fixed the next day. The article says this could not happen on CHIPS, because each transfer must be originated by the payer. [I don't know what this implies about the Fed system.]

The article concludes that "what all the experts fear is what they do not know."

-John Sullivan@geom.umn.edu

Re: Tandem's clocks (RISKS-14.01)

Don Stokes <Don.Stokes@vuw.ac.nz>
Thu, 12 Nov 1992 17:16:06 +1300

BANK SYSTEM IN CHAOS AS MICROCODE BUG STRIKES
By Randall Jackson

November 1, 3pm: a date and time users of Tandem's CLX systems around the world won't forget in a hurry. That's when a microcode bug struck, sending system timers incoherent and causing chaos in applications such as EFTPOS and automatic telling machines. The bug was discovered first in New Zealand, which is the first country to greet the new day.

"Literally, a bit seemed to fall off the field and the timers went incoherent and began talking to themselves," says Ken Hennessy, chief manager at Electronic Transfer Services (ETSL), which manages EFTPOS in New Zealand. "They took the date back to December 1983."

There are five CLX installations in New Zealand, including Westpac, whose ATM system crashed at the same time as EFTPOS.

Hennessy says Australia was the next affected, then Asia. "I believe Japan was a hell of a mess. "We had been in touch with Australia because ETSL operates contracts there, and they started to notice the problem. They contacted Tandem and the Americans became involved. "By midnight, Tandem had worked out a way of getting around the problem."

That was important, because Tandem was able to advise all its users in

America and Europe and prevent systems crashing there.

Hennessy says EFTPOS in Wellington was up and running again by 6.30pm. "We turned the clocks back two years to give us a clearance into 1990 at least. Then we had to raise each host and hope it didn't cause problems of irreconcilability. It didn't, because it was day-to-day, month-to-month. "Our Auckland node came up at 9:40pm and in the early hours of Monday morning we got back to 1992." Hennessy says that there were two fixes: rolling the clocks forward past 3pm then shifting them back so 3pm wasn't hit, or waiting until 3pm rolled around, and doing a cold start.

Typically, New Zealand businesses affected on a Sunday were supermarkets and petrol stations.

Foodstuffs Wellington retail systems manager Alistair Garvie syas the loss of EFTPOS was a major inconvenience. "One of out largest stores does 25% of its business through EFTPOS, and customers were complaining about having to pay cheque fees instead," he says.

BP spokesperson Beppie Holmes says there was some inconvenience but the company was able to revert to paper based transactions. "Where it did affect us was in our ability to provide cash to customers, which has an effect on residual business," she says.

Tandem New Zealand manager John Simms says it took about four hours to work out an answer to the problem, then communicate it to customers. "There was a microcode defect that caused the internal clock to be read incorrectly. It affected different applications in different ways," he says. "It was a field where at rollover the bug caused the data to be interpreted wrongly. "We got our customers to cold load and then reset correctly."

Simms says Tandem acted quickly to provide a fix. "It would happen again in 2001 if we hadn't fixed it," he says.

From Computerworld New Zealand, November 9, 1992:

Don Stokes, Network Manager, Computing Services Centre, Victoria University of Wellington, New Zealand +64-4-495-5052 don@vuw.ac.nz (wk) don@zl2tnm.gen.nz

Photography from orbit

Daniel Burstein <0001964967@mcimail.com>
Tue, 17 Nov 92 12:02 GMT

The following material is from "Space Digest" v15 #425,
distributed as "Space@ubvm.cc.buffalo.edu"

The article deals with the newly available, from the RUSSIANS, satellite photo imagery with resolutions of 1.5 meters. This is good enough, to pick out individual cars in parking lots (although not to read the apocryphal license plates).

They expect a bit more sharpness after some technical problems get resolved.

This is a curious "RISK." On the one hand, it makes all sorts of overhead photographic info available. On the other hand, it also makes it (almost) available to the general public.

Is it a "RISK" to find out how many Japanese fishing trawlers are out there? What about which cars are parked overnight at the take-a-buck hot sheets motel?

article follows:

4- RUSSIAN MILITARY SPACE OBSERVATION DATA ON THE MARKET

[Ran across a couple of interesting notes, with interesting ramifications.]

Central Trading Systems in Arlington, Texas has a new product. Digitized, very high resolution Russian "Earth Observations" data. This data showed up about a month ago when some demonstration data was circulated within the industry to see if there was some interest in buying it. Folks who've analyzed the data say it's in the 1.5-2 meter resolution range.

At that resolution, you can pick out the Christmas tree in front of the White House, or pick out individual cars in the Pentagon parking lot on the demo tapes data. Some rumors circulating in the industry claim the data could have even a higher resolution quality, but the data has been poorly digitized from photos. This data is obvious from a former "strategic asset" of the Soviet Union.

Central Trading systems, can't identify what satellite generated the photo data, but that the Russians call it a "DD5" system, for Digital Data 5. As a representative of the data seller Central Trading Systems is offering global coverage with an extensive data archive of digital images. If the scenes are in the archive, customers can have the images on data tapes within 2 weeks, delivered by Federal Express. If new scenes are required, they can be delivered with 45 days, weather permitting. Central Trading Systems thinks the data is delivered digitally in Russian, transferred to photos, and then re-digitized. His offers the possibility that resolution can improve as more advanced digitizing and image processing systems are applied.

Cost for the data is $3180 (including shipping and handling) for a 13 x 13 Km, 8-bit scene, of 40 mps at 1600 bpi. Demand is reportedly high.

As a side note, on 2 October, a top Russian space commander stated the Russian military space program will only survive by sharing its expertise and hardware. Col General Vladimir Ivanov was quoted in a Krasnaya Zvezda interview as recommending Russian military space systems be used for commercial and civilian purposes. In particular, he was reported to have stated "Reconnaissance satellites can be successfully used for long-distance probing of the Earth's surface and for ecological monitoring without impairing their main task."

[Commentary: New competition in the Earth Resources market area. There are reportedly warehouses of high-resolution Earth observation data on both sides of the ex-Iron curtain. Different organizations have been selling ex-Soviet observation data in the 10-meter resolution class, but the data availability and market response has been poor, partially because the data was only available sporadically or only in photographic form. (For obvious reasons, the preference is for data in digital format.)

But if true, a marketable archive of global 2 meter or better data could be a market gold mine. And the Krasnaya Zveda quote could indicate regular availability to high-resolution data from Russian military systems could become official policy and routine.

SPOT and Landsat data is about an order of magnitude more coarse, with some gaps in the digital data coverage available. The Russian data prices are also very competitive. I expect if the initial expectations are proven for this Russian data, then it will capture a large share of the market within a few years.

Again, there can be a substantial commercial market pact from an ex-Soviet system. Due to policy considerations, the US government has been reticent to release high-resolution Earth Observation data, and has encouraged the use of 100-meter resolution Landsat Data for commercial or non-critical government needs. It was only last month the US Department of Defense even officially revealed the existence of the office which controlled such space assets.

Similarly, SPOT, which has a very large ownership share by the French government, has not striven to achieve the maximum resolution in its system. A higher resolution has been expected in the French military HELIOS observation system under development.

Perhaps the sale of high-resolution Russian data will encourage the release of high resolution data by Western governments. But this will also decimate the existing SPOT or Landsat/EOSAT data markets, when they still have not reached a critical mass for full commercial viability. The best result would be the encouragement of the construction of commercial Western systems with equivalent capability, which is well within the capability of the industry.

As it stands now, there are still significant unknowns in the future of commercial Earth observations data. This new source of data, if it is proven as reliable and accurate, could substantially change some of the market assumptions for Earth resources data.]

Smart cars?

Steve Mestad <stevem@diehard.ssc.gov>
Tue, 17 Nov 92 14:27:14 -0600

>From the December issue of Popular Mechanics, Tech Update column

(paraphrased)

Workers are installing on all 2400 Greyhound buses an on-board radar system made by VORAD Safety Systems. One radar beam will scan ahead for obstacles while a second will probe the driver's blind spot. Steering, braking, speed and obstacle closing rates will be recorded by a 'black box'.

VORAD is already testing a system on passenger cars that links the radar and cruise control, enabling the car to maintain a constant distance away from the vehicle ahead. (no longer paraphrasing the magazine) "The next step, says VORAD, is to connect the radar directly with the brakes, to decelerate the car before the driver has time to react to an obstacle."

The RISKS seem obvious enough to me...

Steve Mestad, Physics Research Division, Superconducting Super Collider Lab
2550 Beckleymeade Ave., MS 2003 Dallas TX 75237   stevem@diehard.ssc.gov

Warrants without notification

Steve Mestad <stevem@diehard.ssc.gov>
Tue, 17 Nov 92 14:15:38 -0600

>From the Dallas Morning News Friday Nov 13 issue, in the Line One column
(an advocate column of sorts):

Person's problem: (paraphrasing salient points)

Person went to renew their driver's license during lunch; paid; was photographed and taken to the back. There they were informed of an outstanding warrant and told to either pay the fine or be arrested. Person admitted to old speeding ticket which was allegedly paid. Previous queries of driving record and traffic stops did not reveal anything about the warrant nor was any notification received by mail.

Response from Texas Dept of Public Safety: (again paraphrased)

Signature on citation is promise to contact/appear in court by date on citation. Failure results in issuing the warrant. Issuing trooper enters warrant into the Warrant Data Bank (WDB). Warrants are placed in WDB are for traffic citations issued only by the Dept. Anytime license record is checked, outstanding warrants will be indicated. Some police depts. do not serve warrants on license checks so a person may not be notified at a stop. Warrant information is not provided on driver's record checks. With the start of the WDB, the Dept. no longer sends mail to advise of issuing a warrant.

Steve Mestad, Physics Research Division, Superconducting Super Collider Lab
2550 Beckleymeade Ave., MS 2003 Dallas TX 75237   stevem@diehard.ssc.gov

Re: Two hackers caught tapping into Boeing, federal computers

Graham Toal <gtoal@ibmpcug.co.uk>
Mon, 16 Nov 92 0:09:48 GMT

I recently heard from someone who *works* on British Airway's flight booking system that it is only lack of access that keeps hackers out - the system it runs is completely unprotected - a multitasking system where every task can access the memory of other tasks. And they're scared to make major changes to it in case it falls over.

So he told me. Season with salt as desired.

Registering your color copier/printer

Carl M. Kadie <kadie@cs.uiuc.edu>
Sat, 14 Nov 1992 18:29:52 GMT

The coin collecting column in the Books section of the Chicago Tribune of Sunday, Nov 8th is about counterfeiting paper money. Among other things it says:

> Meanwhile, Canon USA has reported that it soon will add either one or two counterfeit deterrents to its new color copiers in an attempt to thwart would-be forgers.
>
> One technology places an invisible code on every copy made so that police could trace the machine that duplicated a dollar bill or other documents. The company also might produce machines that print black copies of greenbacks and other bank notes because of information programmed into the machine's computer memory.

I see a risk that these "invisible codes" will be used not only to track counterfeiters but also whistleblowers, government critics, and those who only want to be able to communicate privately. The risk increases if (when?) the authorities require that each color copier/printer's "invisible code" be registered.

I'm also unhappy with the idea that my printer will try to enforce laws about what I can and cannot put on paper. How accurate will it be? Also, the scheme creates the risk that more color copies of money will be produced. Who could resist trying to fool the censor-in-the-machine?

Carl Kadie -- kadie@cs.uiuc.edu -- University of Illinois at Urbana-Champaign

Self-configuring devices

"David A. Honig" <honig@ruffles.ICS.UCI.EDU>
Sun, 15 Nov 92 09:56:57 -0800

Just discovered a feature that will probably amuse other readers of RISKS.

A certain very-popular-workstation-tape-storage-device will reload its firmware upon finding a firmware-reconfiguration tape within its maw upon power-cycling. Presumably it reads whatevers loaded upon start up and upon finding the right code, interprets the data as destined for its EEPROMS. Totally convenient but amusing to a reader of RISKS.

David Honig

Scientific American Article on Risks

g 6367 Capt G Phillips <phillips@rmc.ca>
Tue, 17 Nov 92 9:48:30 EST

The November 92 issue of Scientific American has an interesting article on the risks of computers and proposes three different mechanisms to limit them. Nothing there that regular readers of this forum won't have seen before, but spelled out in clean language that anyone can understand.

Note that this is a case of circular reference, since the article ends by recommending this forum as a good place to learn more about risks.

Greg Captain W. Greg Phillips, Royal Military College of Canada 613-541-6367

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 7

Weds 17 November 1992

Contents

Re: POLL FAULTING recommended for RISKS folks (Baube, RISKS-14.07)

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>
Tue, 17 Nov 92 20:21:42 EST

I browsed some of the recent postings on RISKS regarding what appeared to be voting "anomalies" and had been keeping my typing fingers firmly clenched in my fists for fear of provoking another flame war (now that the Denning one seems to have abated). As I had published recently on the subject of electronic voting (CACM Nov 1992 Inside Risks; Virus & Security Conference, March 1992), have been involved in voting matters for close to a decade as an elected official (committeeperson), and have provided expert witness testimonies, your moderator requested that I comment on this subject. Here then, is my advice:

1. Read the state and local election codes (they may differ).
   You may find that in your municipality it is perfectly "legal" to have misaligned ballots and other more egregious problems, simply because the law does not specifically preclude such things. Copies of the laws should be available at your county or city courthouse.

2. Raise a LEGITIMATE protest.
   This might include:
   a) Lobbying to get the laws changed if you think they are inadequate.
   b) Petitioning the courts to have elections thrown out, or recounts, if you think that there has been a breach of the law.
   c) Getting press coverage.

3. Get involved at the grass roots level.
   Although many municipalities saw a > 80% turnout of _registered_ voters at the polls this November, the Spring primaries will likely see < 20% of those same voters returning. It is typically in the off-year races where people who will be appointing the members of your Boards of Elections (who oversee the process) will be getting elected. Vigilance is a year-round process. Although it is quite eye-opening to work at the polls THROUGHOUT election day (not just at the beginning or end of the day), what occurs during the other 363 days of the year often sets the stage for what happens at the polling places. If you have no idea how to get involved, start by perusing your telephone book for the numbers of local officials, and your newspapers for announcements of political or civic gatherings.

And while I am on the soap-box...

4. Spend considerably more time WORKING for the causes you care about than you do reading or writing about them (on bbs or email).
   The problems of elections and computer risks (as well as poverty, unemployment, hunger, discrimination, violence, ...) are not going to be solved if we sit here at our terminals relaying anecdotes around the world at NSF (and other government-funded) expense. If you are not ACTIVELY contributing to the solution, you are part of the problem. Many of the RISKS postings point to the inadequacy of software engineering methodologies and practices, yet few colleges and universities offer COMPREHENSIVE courses in SW Eng. and far fewer REQUIRE them as part of core curricula for the next generation of EE and CS professionals. Many of the problems with computerized vote-counting are directly related to failures in verification, validation and auditability (all familiar words to Software Engineers). If you are concerned about reducing risks, get out there and make it happen.

I regret, in advance, that I will not be able to reply to private emails relating to the above posting, as my bandwidth is severely impacted due to writing a dissertation. If you feel moved to comment, please relay such to RISKS and Neumann will filter them as appropriate. I hope that at least one person will write (in a few months, because that is how long it will take) that they did ALL of points 1, 2, 3, and 4 and report on their results.

Rebecca Mercuri.

Cordless phone users gain some privacy rights

Jerry Leichter <leichter@lrw.com>
Wed, 18 Nov 92 11:26:21 EDT

Cordless telephone users, whose conversations have been easy prey for electronic eavesdroppers, finally won a degree of privacy in a federal appeals-court ruling.

The Fifth U.S. Circuit Court of Appeals, in a criminal case, said that when such phone users reasonably expect their conversations to be private, the government can't listen in. But the court said the Fourth Amendment privacy right must be evaluated case by case, depending on such factors as whether the phone user had sought privacy by purchasing devices intended to foil eavesdroppers or by using phones known to be more difficult to tap.

The ruling is apparently the first in which a federal court has allowed cordless-phone users any privacy rights. Previously, other appeals courts have said the phones are so easy to eavesdrop on - with an AM/FM radio or even with another cordless phone - that any expectation of privacy was ridiculous.

The Eight U.S. Circuit Court of Appeals ruled in the late 1980s that eavesdropping was allowed, and the U.S. Supreme Court declined to review the decision.

The New Orleans court noted that the previous opinions are all several years old, and that the technology has since advanced in the $1.39 billion cordless-phone market. Some phones on store shelves now, for instance, come with scrambling devices made to combat high-tech eavesdroppers. Other phones work within shorter ranges, so their frequencies can't be as easily intercepted as they were in the past. More than 18 million cordless phones are expected to be sold this year....

"The reasonableness of expectations of privacy for a cordless phone conversation will depend, in large part, upon the specific telephone at issue," the court said. It declined to spell out the technological features it considered most relevant.

[The actual drug conviction, based on information recorded by a neighbor, was upheld since no evidence about the phone had been introduced.]

Privacy-rights lawyers applauded the broader ruling, which they said is a step toward preventing eavesdropping by private citizens as well as police. The lawyers noted that cellular-phone conversations already are protected [though technically they are as easy to intercept.] ...

[N]ow that cordless phones are more secure, they should be treated the same as cellular phones, Ms. [Janlori] Goldman [of the ACLU] said. "People who use these different kinds of phones do not make these kinds of distinctions," she said. "One circuit is willing to recognize that this might be an absurd distinction." ...

[For those interested, the case citation is U.S. vs. David Lee Smith, Fifth U.S. Circuit Court of Appeals, New Orleans, 91-5077.

Can we expect future Willie Horton's who beat the rap to get hired by the maker of their phone to tout it as "private - and a court agreed?"]

-- Jerry

How to tell people about risks?

"Xavier Xantico QZ (=J. P a l m e QZ)" <./S=J.P.SKHB/G=S.@heron.dafa.se>
18 Nov 92 18:06:12+0100

A problem with risks is that it is difficult to communicate information about risks to people. If, for example, a doctor says to a patient "there is a very small risk that this pill will cause liver problems" then many patients interpret this as if the doctor had said "there is a large risk that this pill will cause liver problems". So doctors usually do not tell the patients such information, because the patients so often misinterpret the information.

Any comment on how to communicate risk information so that people get a correct understanding, especially when you are informing people about very small risks?

Risks of DYI Home movies

Alex Heatley <Alex.Heatley@vuw.ac.nz>
Thu, 19 Nov 92 11:03:03 +1300

Recently in Auckland, Aotearoa (New Zealand) the police were involved in an unusual case. It seems that several people burgled a house and among the items taken was a set of videotapes. The tapes contained home-made pornographic movies involving the inhabitants of the burgled house. The burglars then attempted to use their possession of the tapes to blackmail the "actors" into paying for the return of the tapes. Unfortunately when the burglars arrived at the payment drop off point they were met by the NZ Police, who seized them and the tapes.

Any sighs of relief that the "actors" might have had were short-lived. The burglars counter-charged that the tapes contained scenes of child pornography and bestiality which made them indecent under NZ Law. The result was that several police "had" to view 40 hours of video recordings to verify whether these claims were or were not correct (it turned out that the recordings did not contain any child pornography or bestiality).

The tapes were returned to the, by now, extremely embarrassed "actors". With the increase in home computers capable of using frame grabbing software to create digitised pictures and the almost insatiable desire of the networks to spread any and all such pictures, the "actors" involved in this case were very lucky that their images didn't end up adding to the network traffic statistics for alt.sex.pictures.erotic.

Of course, if the original tapes had been encrypted, this embarrassment would never have occurred... or would it?

Alex Heatley Computing Services Centre, Victoria University of Wellington, P.O Box 600, New Zealand. Alex.Heatley@vuw.ac.nz

[The proof is done. KiWiD. PGN]

A320 descent anomalies reported in French press

Pete Mellor <pm@cs.city.ac.uk>
Tue, 17 Nov 92 17:33:30 GMT

---------------------------Le Monde------------------------

Translated from Le Monde, 10-30-92 from the "Faits Divers" column.
Translation by John Lupien (jrl@world.stdl.com)

Incident during the descent of an Airbus A-320 of Air Inter

The crew of an Airbus A320 who were making in September a flight between Clermont-Ferrand and Paris-Orly were surprised to witness an aberration in the vertical speed of descent of the equipment. Having chosen a mode of descent of 550 meters per minute, they noticed that the plane was losing 750 meters per minute, and that when they tried to correct that value to 450 meters per minute, the rate worsened to 850 meters per minute. The pilots at that point changed their procedure and chose an angle (rather than a rate) of descent and everything went back to normal.

The cause of the incident can be imputed to defective design in the interface between the flight controller and the auto-pilot, both developed by the French Sextant-Avionique and by the German BGT and with which other types of planes such as the Airbus A-300 and A-310 are equipped with. This kind of fault is not frequent, but it is one of the anomalies that the crew is trained to correct.

This incident would have passed unnoticed if certain pilots had not made it public to point out a relationship to the aerial catastrophe of Mount Saint-Odile which happened in January, when 87 persons were killed in the crash of an Airbus A-320 of Air Inter. The first findings of the commission of inquiry had perhaps made it appear that the crew was mistaken in the choice of descent mode towards the airport of Strasbourg and that they had not monitored their trajectory.

Translator's comment - The translation is as literal as I could manage...
Certain bits such as "esquisser un rapprochement" perhaps translate not
so well...

---------------------------End Le Monde-------------------------

-----------------------------Figaro-----------------------------

Translated from Le Figaro, 10-30-92 from the "En Bref" ("In Brief") column.
Translation by John Lupien (jrl@world.std.com)

AIRBUS

Electronics in question

Judge Francois Guichard, in charge of the investigation of the accident of Mount Saint-Odile, which killed 87 last January 20, indicated on Thursday evening in Toulouse that the recent incident in the descent mode of an A320 of Air Inter "Could a priori appear to be one of the reasons that caused the accident". The magistrate referred to the failure of the electronic control systems for the mode of descent of an A320 of Air Inter which, in September, took a much steeper descent than that chosen [by the pilots].

----------------------end Figaro-------------------------

My thanks to John for these two translations.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

---

Redressing the record on English system maintenance (RISKS-14.06)

James H. Paul <PAUL@NOVA.HOUSE.GOV>
Wed, 18 Nov 1992 12:25:16 -0500 (EST)

> From: Scott Dorsey <kludge@agcb.larc.nasa.gov>
> To: paul@nova.house.gov
> Subject: DC-3
>
> In a recent Risks digest, you mention that if more than three production
> aircraft are still flying, it's a requirement that avionics become available,
> and use the Honeywell equipment for the DC-3 as an example. This is not a
> good example at all, since there are almost two thousand DC-3 aircraft flying
> in the US alone, as well as many more abroad. The DC-3 remains a reliable
> workhorse of an aircraft; easy to fly and inexpensive to maintain. A large
> amount of current cargo lines still have DC-3s for use to smaller airports
> where larger jets cannot land, and in fact there are still turboprop retrofit
> kits available for the DC-3.
>
> Nonetheless, this is not as much of a problem as you might expect, both

> because most avionics are fairly standardized, and because the low production
> volume means that most of them are handmade on a one-off basis.
> --scott

After receiving the message above, I went back to my posting in RISKS-14.06. Those who aren't able to find the article could very well misinterpret the comment about avionics support requirements. My summary improperly tied actual system problems in various applications to a different concern about long-term support for aircraft avionics. The author cited the DC-3 (Dakota to Englishmen) as the example of how long the a company might find itself in harness to produce vintage equipment. Dorsey is, of course, correct about the treasured status of the venerable DC-3, and the profit to be made from the large number of planes left. The article's discussion focused more on the close fit between autopilot and aircraft necessary for certification and the likely difficulties this would pose as the more computer-literate aircraft of the jet age continue to carry us around the world and the avionics firms try to keep the control systems up-to-date. I did a poor job of setting the context.

Re: Safe Conduct (RISKS-14.05)

<ken@minster.york.ac.uk>
Wed, 18 Nov 92 12:26:20

This will have very important consequences for UK industry. For example, none of the UK motor industry considers computing in cars as safety critical, and hence do not use appropriate techniques for developing software ("a bunch of cowboy hackers" was one description of the software developers in one company). Of course, with this new law (which is EC wide) it won't be up to the industry to deign if something is safety critical or not, it will be up to the law courts. If I were an executive in the car industry I would be quaking in my shoes at the moment..

Ken Tindell Internet : ken@minster.york.ac.uk Computer Science Dept., York University, YO1 5DD, UK : +44-904-433244 Local FTP site: minster.york.ac.uk

Re: Risks Of Cellular Speech

James Olsen <olsen@hing.LCS.MIT.EDU>
Tue, 17 Nov 92 10:27:44 -0500

In RISKS-14.04, Robert Gezelter writes:

>While I believe that it is true that the use of Cellular phones is
>prohibited in aircraft ... I seem to remember that the rationale is
>aviation related, not Cellular Phone related.

There are, in fact, two separate risks involved here, and two separate regulations to control them. In-flight users can impose an excessive load on a a cellular phone system by accessing many cells at once; therefore the FCC has recently prohibited airborne use of cellular phones (see 57 FR 830).

There is also a more general risk of any portable electronic equipment used in aircraft, since it has not been tested for interference with the electronic systems in the aircraft. FAA regulation 91.21 therefore prohibits the use of portable electronic equipment (with minor exceptions) in an airliner unless the airline has determined that it will not cause interference. Many airlines have issued blanket permission for items such as tape players and laptop computers, but I am unaware of any that yet allow the use of cellular phones, even on the ground, where they would otherwise be legal.

Jim Olsen   olsen@cag.lcs.mit.edu   "Tache d'etre heureux."

Re: Risks Of Cellular Speech (Gezelter, RISKS-14.04)

Dan Sorenson <viking@iastate.edu>
Thu, 12 Nov 1992 05:11:25 GMT

> ... To be exact, my recollection is that the frequencies used by
>Cellular are fairly close to some of the frequencies used by the avionics.

This is my understanding too, but note that this was extended on some airlines to laptop computers and even some hand-held video games. Midwest Express, a rather expensive but high-quality business-oriented airline, has cellular phones in each seat. I suspect it's not the frequency of the cellular phone transmission that worries the airlines, but rather the electro-magnetic or RF interference it might play with the IFR systems or possibly the electronic controls on the aircraft.

The risk here would be allowing non-certified phones on board, whereas airline-supplied phones can be easily tested by the airline.

Dan Sorenson, DoD #1066 z1dan@exnet.iastate.edu viking@iastate.edu

---

Re: Cellular phones in aircraft

Bob Rahe <bob@hobbes.dtcc.edu>
Tue, 17 Nov 1992 13:13:27 -0500

In RISKS-14.05, berry@athos.pei.com (Berry Kercheval) writes:

|>The blanket ban *is* due to cell overlap, then, and my guess is the reason
|>there is not an altitude restriction is that it's too hard to figure out; the
|>number of cells reached is a complex function of altitude, position of the
|>aircraft and cells, and the topography of the surrounding landscape. I can
|>just picture the FCC bureaucrat saying ``Hell, that's too hard. Let's just ban
|>'em all.''.

Now I'm all for blasting bureaucrats but this shot seems a bit gratuitous. Just how might a regulation be written that would allow cellular use from aircraft given the complexity of deciding? Would I have to carry my (possibly banned) portable computer with a CD-ROM geographical database of cells in the US (or wherever I was travelling) along in order to calculate whether I could make a call? Actually, it sounds as tho the bureaucrat is correct. It is too hard to be reasonably done.

Bob Rahe, Delaware Tech&Comm College Internet: bob@hobbes.dtcc.edu
CompuServe: 72406,525 Genie:BOB.RAHE

a naive thought about encryption

Martyn Thomas <mct@praxis.co.uk>
Mon, 16 Nov 92 11:03:33 GMT

The security services are using a lot of very expensive resources to decrypt intercepted messages (Spycatcher revealed that all telephone traffic and all radio traffic was routinely monitored and recorded in the 1950s to 1970s - so this is probably still true, or close to true).

If you don't *need* your messages to be secure from the Government, why not give them a break and agree to a key registration scheme? Arguments that this will always be defeated by the criminals seem to ignore the help that the law-abiding can give by making the unco-operative easier to identify, and thereby freeing decryption effort.

Isn't there a balance between distrust of Government,(however justified) and a need to help the law-enforcers to enforce the laws that keep society civilised?

We are the experts in this technology. What can we propose that gives a proper balance between privacy and law-enforcement?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Re: RISKS of technical people disengaging brain

Mike Dixon <mdixon@parc.xerox.com>
Tue, 17 Nov 1992 13:26:16 PST

>Most of us are in professions where logic is of some importance. It hurts
>credibility to declare in public, "I *don't* believe" a tautology.

in a very aptly-titled Risks submissions, Dan Herrick purports to make a contribution to a serious social discussion (the effectiveness of gun control) with a trivial "logic" analysis. this is the kind of argument that gives technical people a bad name.

the statement "When guns are outlawed, only outlaws will have guns" isn't a tautology on anything but the shallowest reading (hint: people usually don't bother to assert tautologies). it's an assertion that dangerous, threatening, bad people will have guns and good, honest citizens won't be able to defend themselves. some people believe it, some don't; only extreme technical

blindness would allow someone to think the question could be dismissed with a
puff of logic. *that's* what hurts credibility (and that's perhaps the least
of its risks).
                                .mike.

Re: RISKS DIGEST 14.05

Dan Swartzendruber <dswartz@lectroid.sw.stratus.com>
17 Nov 1992 16:12:12 GMT

On the subject of "RISKS of technical people disengaging brains", I'm afraid Mr. Herrick has fallen victim to over-literalism. I've used this expression more than once, and I'm perfectly aware of the tautology. The point he is missing is that many natural languages contain grammatical constructs which if analyzed grammatically, are either tautologies or self-contradictory. This doesn't automatically make them nonsense or their users fuzzy-thinking fools. I think most native English speakers understand intuitively the implied clause which follows statements of the form "If/when they outlaw X, only outlaws will have X". If he doesn't, I'm sure he can find any number of people (possibly even without advanced degrees) who would be more than happy to explain it to him.

Dan S.

Re: RISKS DIGEST 14.05

Ken Arromdee <arromdee@jyusenkyou.cs.jhu.edu>
Tue, 17 Nov 1992 03:59:02 GMT

It's not a tautology. One reasonable interpretation of the statement is that "if X is outlawed, only people who are already outlaws of other types will use X".

I suppose this indicates a RISK of some sort, though I don't really feel like phrasing it fully.

Ken Arromdee (UUCP: ....!jhunix!arromdee; BITNET: arromdee@jhuvm;
    INTERNET: arromdee@jyusenkyou.cs.jhu.edu)

Re: RISKS of technical people disengaging brain

<sullivan@geom.umn.edu>
Tue, 17 Nov 92 17:46:13 -0600

Dan Herrick, dlh%dlhpfm@NCoast.org, misses the deeper meanings of the statement "if X is outlawed, only outlaws will use X". Of course, there is a tautologous interpretation, explained by Herrick. But when X is refers to guns, this statement has been used to imply many things that are not tautologies. Far-right lobbying groups have used this slogan to imply that any waiting period, or other reasonable restriction on the purchase of deadly weapons, would lead merely to difficulties for "law-abiding citizens" while having no effect on criminals.

I'm sure the original author (Phil Karn, karn@qualcomm.com) was merely trying to disassociate himself from such "fuzzy thinking", by pointing out that what might be true for cryptography might not be true for guns.

Statements in a language like English are very rarely tautologies: they always carry around extra baggage.

-John Sullivan, sullivan@geom.umn.edu

Re: RISKS-14.05: Logic vs. Clever Slogans

Robert Hartman <infmx!hartman@uunet.UU.NET>
Tue, 17 Nov 92 20:02:00 GMT

Actually, this statement is not, strictly speaking, a tautology. It isn't even, strictly speaking, a statement of logic. Why? Because its truth value depends not on its logical form, but on the meaning of its terms.

In particular, the meaning of the term "outlaw" is telling. It is one thing to break the law. It is quite another to "be an outlaw." Ordinary citizens break laws. Some even scoff at certain laws, and other still skirt the letter of the law while seeing its value and holding to its intent. But "being an outlaw" implies a habitual disdain or disregard for the law--which is why the clever originators of that slogan use that word in order to frighten ordinary citizens into opposing restrictions on their ability to purchase guns. It's funny how much less impact the slogan has when you replace "guns" with "encryption."

While it's true that if you make codes or guns more difficult to obtain, only those with stronger motivation will obtain them. Nevertheless, one need not be an outlaw to vehemently desire both protection and privacy.

-r

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 8

Saturday 21 November 1992

Contents

Installer Programs

<mmm@cup.portal.com>
Wed, 18 Nov 92 20:20:03 PST

I recently had a terrible experience (involving loss of several hours of work time and much swearing) with a print spooler program for the Macintosh. As with many such programs, you put it on the system by running an installer program. The installer performs all sorts of modifications to the system software, and basically you just gotta cross your fingers and hope the software works okay. This one didn't.

As soon as I attempted to print something, the system no longer saw my printer and the printer would go into an alarm condition every time I tried to print something. Calling the software company was no help, I probably spent 1/2 hour listening to an NPR station in Louisiana hoping they would pick up the phone.

I tried de-installing the software, by putting the old system up from backups and tracking down all the files the installer had inserted into my system. This was a lot of work, and had no effect on the problem. This is an important point I'd like to make: any installer program should also have the capacity to de-install, so that the user has at least one back-tracking path if something goes wrong.

A de-install feature probably wouldn't have helped me out, though. The problem turned out to be that the program accidentally changed one of my system defaults. Without asking, it activated Applelink (the networking system) which normally uses the line printer port. That caused my default printer port to switch to the modem port.

Mark Thorson mmm@cup.portal.com

Election hardware and software problems

<AURKEN@VAXC.STEVENS-TECH.EDU>
19 Nov 1992 21:23:13 -0500 (EST)

Recent discussion of problems with election equipment and software has not included any mention of the efforts of the Federal Election Commission and National Association of State Election Directors (NASED) to promote the development of standards and certification testing of election systems.

NASED just recently recognized the first national Independent Testing Authority (ITA) to conduct testing of election equipment and software. Election Technology Laboratories (ETL), a joint operation of Stevens Institute of Technology and U.S. Testing Company, is now ready to conduct hardware, electrical, environmental, package, software, and human factors testing of election systems.

We are very interested in learning about election system breakdowns. Since election officials do not typically advertise the breakdown of election systems, it would be good to hear from anyone in the RISKS FORUM about their experiences.

How to talk about risks (Xantico, RISKS-14.07)

Post-Postmodern Man <wex@MEDIA-LAB.MEDIA.MIT.EDU>
Wed, 18 Nov 92 23:49:48 -0500

There is a great body of literature about the way people make decisions and the systematic biases in their thinking. Just to cite one example, people tend to be risk-taking when a question is framed in terms of possible gain, but risk-aversive when the question is framed in terms of possible losses.

Perhaps the best single reference on this is the book "Judgement Under Uncertainty: Heuristics and Biases", edited by Kahneman, Slovic, and Tversky. (My copy is almost 10 years old, but it was published by Cambridge University Press, ISBN 0-521-28414-7). Kahneman and Tversky in particular have spent a long time analyzing the systematic biases in peoples' judgement and have published many papers on the topic.

I highly recommend studying their work if you are in a position either of having to present probabilistic risks to others or of having to evaluate such risks presented to you.

--Alan Wexelblat, Reality Hacker and Cyberspace Bard,, Media Lab - Advanced
Human Interface Group   wex@media.mit.edu 617-258-9168 wexelblat.chi@xerox.com

---

Re: How to tell people about risks?

Stuart Wray <scw@cam-orl.co.uk>
Thu, 19 Nov 92 14:31:14 +0000

> Any comment on how to communicate risk information so that people get a correct
> understanding, especially when you are informing people about very small risks?

Perhaps a good way to communicate information about risks is to tell people the odds and compare them with the odds of various every-day disasters. For example (off the top of my head):

```
  Odds of dying in a car accident in the next year: 1 in 10000
  Odds of a mother dying during childbirth:         1 in 10000
  Odds of middle-aged adult dying in the next year: 1 in 1000
  Odds of a young child dying in the next year:     1 in 100
  Odds of a baby dying during childbirth:           1 in 100
```

People are usually given insufficient credit for being able to compare risks themselves, perhaps because they are seldom handed straight numbers by experts.

Stuart Wray, Olivetti Research Limited, 24a Trumpington Street, Cambridge CB2
1QA ENGLAND   scw@cam-orl.co.uk +44 223 343204   fax: +44 223 313542

Re: How to tell people about risks?

Rob Cameron <cameron@cs.sfu.ca>
Thu, 19 Nov 1992 09:21:35 -0800

Xavier Xantico asks how to communicate risk information to the public in a meaningful manner.

Suggestion: it would be nice to see the "automobile accident" and the "cigarette smoking" standards.

Examples (purely fictional):
"The risk of your child seriously injuring himself in 3 hours of playing with this toy is about the same as that of being an automobile passenger for 4 minutes."

"The risk of long-term liver damage from this medication is approximately the same as the risk of cancer from smoking 2 packs of cigarettes."

I realize that there would be serious problems in accurately calibrating such "standards," but I think they would be very valuable in giving people a clear understanding of risks.

Robert D. Cameron, School of Computing Science, Simon Fraser University
Burnaby, B.C., V5A 1S6 cameron@cs.sfu.ca

Re: How to tell people about risks?

Mike Coleman <coleman@rocky.CS.UCLA.EDU>
Fri, 20 Nov 92 10:35:08 GMT

In a previous article, Xavier Xantico (?) writes about the difficulty of communicating statistical risks to ordinary people. The Richter scale seems to be successful in allowing people to think about and compare seismic events (earthquakes); perhaps we can develop a similar scale for statistical risks.

I suggest a logarithmic (base 10) scale based on the expected lifetime frequency of the event (and population) in question. To avoid confusion, a "lifetime" should be defined as a fixed duration, 80 years perhaps, since many interesting events will be fatal.

Thus, an event scoring 0 on this scale would be expected to happen once per lifetime (per person), an event scoring +1 ten times, etc. The event "dying in an airline crash" might score -6, "dying of cancer" -1, "hearing a campaign promise" +3, and so on.

The approximate useful range of the scale would be -14 (a 1 in 5000 chance of occurring once in the lifetimes of 5 billion people) to +11 (expected to happen tens of times per second for each individual).

One or two canonical events could be chosen for each integer on the scale to make the scale easily accessible to nonstatisticians (such as myself).

--Mike Coleman (coleman@cs.ucla.edu), Lord High Executioner of Anhedonia--

---

Re: How to tell people about risks? (Xavier Xantico, RISKS-14.07)

Pete Mellor <pm@cs.city.ac.uk>
Fri, 20 Nov 92 10:57:11 GMT

> Any comment on how to communicate risk information so that people get a

> correct understanding, especially when you are informing people about very
> small risks?

Well, what you *don't* do is say:

"Every time you do X, it knocks n days off your life!"

Such statements are hopelessly misleading to anyone not familiar with the concepts of "distribution of time to failure" and "mean time to failure". It is unfortunate that many government health education statements are couched in precisely those terms.

Other than that, you must get across a few of the basic ideas of probability theory. The "urn" model is quite intuitive: a 0.01 probability is the probability of pulling the black ball out of an urn containing 99 white balls and one black ball.

The best introduction to probability for the non-mathematical reader that I have read is "How to take a chance" by Darrel Huff (perhaps better known for his other popular book "How to lie with statistics").

Also try:

"Making Decisions", D.V. Lindley, John Wiley & Sons, 2nd Ed., 1985

Lindley is a bit more demanding than Huff. (Also Huff teaches you how to play good poker! :-)

To see if the ideas have been understood, ask the "student" what is wrong with the following:

A businessman, who needs to fly a lot in order to do his job, is terribly afraid that there will be a bomb on board one of his flights. He asks his friend (a probability theorist) what to do about it.

"Well!" says the friend, "What do you think are the chances that there will be a bomb aboard your flight?"

"Judging by recent statistics," says the worried flyer, "it could be about 1 in ten thousand."

"So what would be an acceptable risk?", says the friend. "How about 1 in 100 million, which is the probability of two separate bombs being on board?"

"Yes, that would be OK."

"Fine! So all you have to do is, every time you board a flight, make sure you carry a bomb!"

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: How to tell people about risks? (Xantico, RISKS-14.07)

<eang42@castle.edinburgh.ac.uk>
Sat, 21 Nov 92 13:58:58 WET

One thing you have to remember is that the risk of something happening isn't the only factor to be considered when deciding whether or not to accept that risk. The consequences of the event, its preventability, and the likely consequences of alternative actions also have to be considered. To return to your example, I have a fungal infection in the nail beds on one of my feet. The only cure is to take tablets that ensure there is a fungicide in your blood, and hence fungicide reaching the nailbed. Now this drug occasionally destroys the liver, and doesn't always work. Without a liver I would be dead. The risk is low but the benefits from the drug are minor, I can live with tickly toenails, especially as I can treat the itch. It isn't worth the risk in my opinion. If I had a mestasised cancer on the other hand and the drug of choice could destroy my liver I would take it.

I once went to a talk on people's assessments of the risk of having a handicapped baby, and how likely people were to risk amniocentesis/chorionic villi testing (which has a risk of inducing a miscarriage). The lecturer was startled that the willingness to be tested varied with whether or not people already had a handicapped child, how many normal children they had, and the severity of the handicap as well as the risk that the child was handicapped. He didn't see that the greater impact the care of a handicapped child would cause of the more important it was that it didn't happen and the less important the relatively fixed "cost" of a miscarriage became.

He was also horrified that people who didn't want an abortion would want to be tested. I think that makes sense. Knowing gives you time to prepare, and there may be a miscarriage (even if the latter option isn't admitted to themselves).

Basically what I am saying is that people aren't misjudging risks as often as is assumed by professionals, they are taking other factors into account as well.

L. Bootland, University of Edinburgh, Genetics   eang42@castle.ed.ac.uk

Re: Software Reliability - how to calculate?

Pete Mellor <pm@cs.city.ac.uk>
Fri, 20 Nov 92 18:00:23 GMT

To: figueroa@jimminy.serum.kodak.com

Janet,

I don't normally read comp.software-eng. (It takes up enough of my time reading comp.risks and a couple of others!) However, your message was passed on to me by Dave Bolton in the Computer Science Department here. (Thanks, Dave!)

I hope you don't mind, but I have sent this reply, including a copy of your
original message, to comp.risks also, since it is relevant to a recent
discussion there. Perhaps you could forward it to comp.software-eng as well,
since I am not sure of the distribution address for that list, and I'm too
lazy to look it up right now!

----- Begin Included Message -----

>Newsgroups: comp.software-eng
>From: figueroa@jimminy.serum.kodak.com (Janet Figueroa (x37973))
>Subject: Software Reliability - how to calculate?
>Summary: Require reference for software reliability calculation
>Keywords: software reliability reference calculation
>Organization: Clinical Diagnostics Division, Eastman Kodak Company
>Date: Tue, 17 Nov 1992 18:21:19 GMT

I just had an interesting discussion with a peer who is an electrical engineer. It was about our reliability budget in which we have set a goal of a certain number of service calls per year upon the introduction of the instrument. She asked if there was a methodology followed in calculating reliability for software. One of the examples we were discussing was code that resides in a PROM. If there was an error in the software and our service representative will have to replace the PROM, how would that be looked at?

I told her point blank that I was not aware of any process used to calculate software reliability. Is there one? I would be very interested to know how the reliability is measured in an application programming environment as compared to how it is determined for a device driver, for example.

Any insights would be appreciated. Thank you very much

Janet C. Figueroa, figueroa@serum.kodak.com

----- End Included Message -----

> She asked if there was a methodology followed in calculating relaibility for
> software.

There certainly is! Basically, you observe the software during its later test and trial phases, when it is reasonable to assume that it is being run under conditions which are a fair approximation to its eventual operational environment.

You record the execution time and the failures. You diagnose the cause of each failure, and strip out from your data set solely those failures which are due to activations of *new* faults (i.e., your final data set consists of instances of detecting new faults over execution time).

Unless something is wrong with the environment in which you are running your software, you will observe a decreasing rate of finding new faults over execution time. You can do a statistical analysis of the growth in reliability as you debug the software, and estimate such quantities as:-

- current rate of finding new faults,

- number of faults that will be found in a given period,

- median time to failure,

- extra testing time required to get to given target levels of any of the above.

To do the analysis, you can apply various software reliability models. The estimation process involves estimating the values of the model parameters from the observed history of finding faults.

Be warned! :-

1. Different reliability models sometimes give different predictions based on the same set of data. (However, there are statistical methods which can measure the bias in the predictions from each model, correct for this, and so reconcile the predictions.)

2. The whole procedure depends *crucially* upon the observations being made in the same operational environment as that in which the software will be used in service.

3. The measure of "execution time" employed must be a meaningful measure of the degree to which the software has been used, taking account of the type of software and its application.

4. Serious problems arise if very high reliability is required. (Basically, the statistical methods require a reasonably large data set of faults found in order to work with any degree of accuracy. For ultra-high levels of reliability, such as those required for safety-critical systems, the observation of even one failure during the trial period means that the software is not good enough!)

Apart from the restriction regarding ultra-high reliability requirements, the methods can be applied to any type of software, whether resident in a PROM or not. They have been applied "in anger" to all types of software where a modest failure-rate is acceptable, including operating systems and application software, and have given reasonably accurate predictions.

Given that you are envisaging a situation where support representatives *will* be deployed (i.e., this system *is* going to fail, isn't it? :-) these are exactly the sort of methods you should be employing.

Logistical calculations can be based on the reliability estimates.
For example: How do we decide when to issue a "bug-clearance" release on a new PROM, in order to achieve the maximum cost-effectiveness of our support operation?

There is a voluminous literature on all of these problems, and CSR has specialised in them for a number of years. If you require any further information, copies of papers, etc., do not hesitate to get in touch.

Regards,

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: POLL FAULTING recommended for RISKS folks (Mercuri, RISKS-14.07)

Pete Mellor <pm@cs.city.ac.uk>
Fri, 20 Nov 92 10:22:42 GMT

Rebecca Mercuri (mercuri@gradient.cis.upenn.edu) writes:

> Many of the RISKS postings point to the inadequacy of software
> engineering methodologies and practices, yet few colleges and
> universities offer COMPREHENSIVE courses in SW Eng. and far fewer
> REQUIRE them as part of core curricula for the next generation of EE
> and CS professionals.

City University now offers (starting this year, i.e., Oct. 92) a BEng in Software Engineering as a first degree. The BSc in Computer Science has for many years included both core and optional modules on Software Engineering, which are also taken by students on other degree programmes (Mathematics, Computer Engineering, Economics and Computing, etc.) Similar modules are also offered as options on several Master's courses.

Having been heavily involved in teaching many of these courses, and being part of the design team for the new BEng in SW Eng., I would be extremely interested to hear the views of other RISKS folk about what should go into a "COMPREHENSIVE" course in SW Eng.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Advanced technologies for automotive collision avoidance (seminar)

Pete Mellor <pm@cs.city.ac.uk>
Fri, 20 Nov 92 13:21:09 GMT

RISKS readers may be interested to in the following seminar. Some UK readers may even be able to come along. (All welcome!)

```
   *************************************************************
   *      City University Computer Science Seminar          *
   * Advanced technologies for automotive collision avoidance *
   *       Raglan Tribe, of Lucas Automotive Ltd.           *
   *    Wednesday 25th November, 2 - 3pm, room A230         *
   *************************************************************
```

Every year, in the 12 countries of the European Community, some 55,000 people are killed in road accidents. The European vehicle manufacturers have joined together with component suppliers to share research on improved safety and traffic efficiency.

A team at Lucas is collaborating with Jaguar to develop collision avoidance systems suitable for fitting to the majority of road vehicles. Basically, the system will use various sensing methods -- optical, infrared, and radar -- to detect where the road is, and the location of other objects (vehicles, people, stationary objects) that are likely to cross the path of the vehicle equipped with the system. The system then assess what threat these objects pose, and assists the driver in selecting the best course of action.

Enormous processing power is necessary to extract edges in the video image, before detecting vehicles and road or lane edges. Some 3000 million operations per second must be carried out for real-time working. The next stage of the project will investigate the fusion of microwave and infrared sensors to provide a more reliable view of the world around the vehicle.

All are welcome to come to this seminar on Wednesday the 25th November, from 2 - 3 pm in A230. We are very fortunate to be able to listen to Raglan Tribe, of Lucas Automotive Ltd., who will also be presenting a short video of the system. Please contact Geoff Dowling on 071 477 8442, or e-mail g.dowling@uk.ac.city.cs to confirm these arrangements in case of last minute changes.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Wanted: GRADUATE PROGRAM in RISKS

Simson L. Garfinkel <simsong@next.cambridge.ma.us>
Fri, 20 Nov 92 09:33:59 -0500

I am looking for a PhD program in Computer Science or in Technology and Public Policy programs in the US or Canada in which one could specialize in the topics familiar to RISKS readers.

So far, I have only heard of the Computing, Organization, Policy and Society at UC Irvine. Dr. Rob Kling heads a program on RISKS and related issues. It sounds good.

Any others out there?

"The Information Society"

Bob Anderson <anderson@iris.rand.org>
Wed, 18 Nov 92 15:55:50 PST

Dr. Stephen Lukasik has agreed to act as guest editor of a special issue of "The Information Society" journal addressing errors in large databases and their social implications. Attached is a brief prospectus for this special issue.

If you know of data or research reports relevant to the topics mentioned in this prospectus, or can suggest relevant authors or are interested in submitting a manuscript yourself, please contact one of us.

Also, I would appreciate your forwarding or posting this message to others that may have interest in this topic.

If anyone receiving this message is unfamiliar with the journal and its focus and interests, I would be happy to supply additional information. (For those on the RAND mailing list: It is available for routing or perusal in the RAND library.) Thanks for your assistance.

Bob Anderson

- -

ERRORS IN LARGE DATABASES AND THEIR
SOCIAL IMPLICATIONS

Prospectus for a special issue
of the Information Society Journal

With the growth of information technology over time, we are becoming increasingly affected by data in electronic databases. The social and business premise is that electronic databases improve productivity and quality of life. The dark side of all this is that these databases contain errors, most trivial but in some cases they contain errors that by their nature impose a penalty on society. The penalties can range from minor annoyance and modest administrative cost in having a record corrected, to more serious cases where more costly consequences ensue, to conceivably, loss of life or major loss of property.

The consequences to society of errors in electronic databases can be expected to increase, probably at an increasing rate. Some factors contributing to this expected increase are the increasing extent, in both size and coverage, of existing databases; increasing capture of data by automated transaction systems, from text and image scanners and the like; greater coupling of databases, either by administrative agreements or by more sophisticated search processes; more "amateur" database administration with increasingly widespread use of information technology; increasing use of heuristic search techniques that lack "common sense;" and probably other well-meaning but pernicious influences.

The purpose of the proposed issue is to accomplish the following: (a) increase recognition of, and awareness of the growing nature of the problem of errors in electronic databases that are increasingly becoming regulators of modern life; (b) encourage greater attention to the collection of error rate data and to quantitatively assessing the social and economic costs deriving from those errors; (c) foster theoretical and empirical studies of the propagation of errors through the coupling of, or joint search of, multiple databases; and (d) encourage the formulation of measures, in both technology and policy domains, designed to limit the costs accruing from the inherent growth in size and connectivity of electronic databases.

We seek papers for the issue that will focus on the following aspects of the problem addressed here: (1) an enumeration of socially relevant databases, whose errors can have important consequences, either from a large number of small unit cost consequences or a small number of high cost consequences; (2) quantitative data on errors in databases, classified by the nature of the errors and their derivative costs; (3) obstacles to a full and open discussion of the problem such as those deriving from concern over legal liability and loss of business from "owning up" to the problem; and (4) proposals for technical and policy measures that can limit the growth of the problems addressed.

The premises of the journal issue are: (1) that the problems of errors in databases can not be minimized until they are adequately recognized and fixes explored by the professionals in the field; and (2) that we must move from the anecdotal level, where horror stories abound, to a quantitative level where the economics of fixes, either in quality control at the point of data collection, or the quality control of the output of database searches, can be sensibly analyzed.

Your interest in contributing to this special issue is invited. Suggestions for possible topics, authors, or an interest in contributing should be communicated to one of:

guest editor:	editor-in-chief:
Dr. Stephen Lukasik	Dr. Robert H. Anderson
1714 Stone Canyon Road	RAND, P.O. Box 2138
Los Angeles CA 90077	Santa Monica CA 90407-2138
net: lukasik@rand.org	net: anderson@rand.org
tel: (310) 472-4387	tel: (310) 393-0411 x7597
fax: (310) 472-0019	fax: (310) 393-4818

Airline Software-safety database

Dave "Van Damme" Ratner <ratner@ficus.CS.UCLA.EDU>
20 Nov 92 19:08:47 GMT

I am posting this for Robert Ratner, Ratner Associates Inc, which does international consulting in air-traffic control and aviation safety issues. He is looking for a public-accessible data base on software-related incidents in this area. Email correspondence can be sent to me at ratner@cs.ucla.edu.
Thanks. Dave "Van Damme" Ratner ratner@cs.ucla.edu

[I suppose he should be reading RISKS! PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 9

Tuesday 24 November 1992

Contents

BNFL Sellafield nuclear incident (followup to RISKS-12.65)

Peter Ilieve <peter@memex.co.uk>
Tue, 24 Nov 92 13:43:16 GMT

RISKS readers with long memories or good archives may remember the piece I submitted about an incident at the British Nuclear Fuels plc plant at Sellafield (RISKS-12.65). I recently noticed that the official report by the Nuclear Installations Inspectorate (NII) had been published in July and I now have a copy. It is summarised below. As will be seen at the end, this is a real `text-book' incident.

First, the complete text of the Health and Safety Executive's quarterly Statement of Nuclear Incidents relating to this incident. This was dated 3 Jan 92. The NII are part of the HSE.

> In September maintenence work was taking place within a monitoring cell at British Nuclear Fuels (BNFL) Sellafield Waste Vitrification Plant, which is used to handle containers of highly active vitrified waste. To facilitate the maintenence two shield doors, normally closed during cell operations, had been opened to allow access.
>
> On 15 September, a container of the vitrified waste was raised into the cell remotely by a process worker who had been instructed to restart operations. The worker then observed on a TV monitor that both sets of shield doors were still open and took action to close them, reinstating the shielding. No workers were in the area at the time.
>
> The matter was reported to the HSE's Nuclear Installations Inspectorate (NII), which immediately started an investigation to determine the causes of the incident. A similar investigation was also set in train by BNFL. The plant will remain shut down until the results of these investigations are known and any necessary modifications to the equipment and changes to procedures have been completed to prevent a recurrence. The NII will monitor the implementation of these changes to both plant and procedures.

This is a very bland statement, just saying `two doors were open'. The incident was considered serious though. There are about 3 incidents reported via this mechanism every quarter but I can't remember another case where a full report was published.

To the report itself. Knowing that nobody was irradiated or otherwise hurt you can enjoy the comedy of errors that follows.

The cell involved was a room with a robot in it. Freshly cast blocks of vitrified waste were cooled and decontaminated on the level below the cell, then lifted by a crane through a hatch door in the floor, given a final scrub down by the robot, and then passed up trough another door, the gamma gate, in the ceiling. The two shield doors allow access into the cell for people to fix the robot, using the doors like an airlock.

When the plant was designed it was not expected that much fixing would be needed and it was though acceptable that only one door would be open at a time during maintenence. The system that ensured this was a Programmable Logic Controller (PLC) driven by a key exchange box. This is a partly mechanical thing that ensures that the key needed to open the outer door is trapped in a dummy lock until an external key from the Permit Foreman's office is inserted and the key to operate the inner door is put in a dummy lock and the inner door is closed. It would seem to be enough in itself to ensure that only one door is open at at time. There is also a hardwired interlock to prevent the outer door opening if a gamma monitor inside the cell detected high radiation.

During the initial commissioning of the plant it was discovered that the robot needed a lot more fixing than at first thought, and it was also decided that it would be better if people working inside the cell could get out quickly by having both doors open at once. An additional keyswitch was added to the key exchange box to bypass the existing arrangement, with another key which was normally held in the Permit Foreman's office.

In mid 1990, still during commissioning, more changes were made. Hardware changes were made to ensure that the doors could only open in the correct sequence and that the hatch door in the floor could not open if the new override key was in use. Software changes were also made to prevent the hatch door opening when the inner door was open `however, instead of being achieved directly, this was effected by a complicated set of conditional relationships intended to ensure that the inner door could only be opened if the in-cell crane was parked next to the inner door'. If the crane was parked there it could not be lifting anything through the hatch.

During commissioning of these mods. a further change was made to the PLC program. This was designed to prevent the hatch door opening when the inner door was open. `However it has since been shown to contain a coding error: a "+" sign had been missed out, which rendered it completely ineffective.' This did not cause the incident, but if it had been correct it would have prevented it.

There are procedures under the nuclear site licence from the NII that modifications should be categorised according to their safety importance and if they are significant they should be checked and the NII informed before proceeding. All of these mods. were categorised as minor, partly because they were designed to improve things and partly because no single mod. could have a serious effect as there were multiple protective systems. As a result, they were not comprehensively checked, nor was the NII informed.

The scene was set for the incident by the need to fix the robot and also to replace some hydraulic hoses in the cell. The Foreman's log shows that at 22:00 on Thursday 12 September 91 the outer door was in the closed position.

The conditions for entering the cell, laid down in the written cell entry procedure, included the isolation of the gamma gate in the ceiling and a mobile decontamination tank below the hatch door in the floor, first checking that the tank was not below the hatch. Isolating the gamma gate also isolated the supply to the switch indicating the gate was closed. This meant that the in-cell crane could not be moved, as the signal saying the gamma gate was closed was not present. This was not recognised at the time.

The cell entry procedure states that the inner door should be opened first. However, the Foreman's log at 06:30 on Friday showed that the outer door was open. The Foreman tried to open the inner door and failed, because:

a. The outer door was open and the software in the PLC would not allow
   the inner door to open in this condition
b. The in-cell crane was not parked just inside the inner door, which
   the PLC also required to see before opening the inner door.

The Foreman thought the inner door was actually faulty and got the maintenance department to look at it. They spent most of Friday morning trying to find a fault, before realising that the doors were being opened in the wrong sequence. They then shut the outer door. The inner door would still not open as the in-cell crane was parked above the hatch door, and it could not be moved without re-energising the gamma gate.

After thinking about this for a while the Shift Manager decided to place a temporary override on the PLC to fool it into thinking the crane was in the correct position just inside the inner door. `This course of action was quicker to implement. The decision was probably influenced by the fact that the engineer responsible for robot repairs worked on dayshift only: there might not have been time to complete the necessary repairs if the other systems had been re-energised to move the crane and then re-isolated in accordance with the checklist.'

He authorised a Temporary Plant Modification Proposal (TPMP) and got the door to open. The details of this TPMP were added to the shift log, the permit to work, and a TPMP book, but the entry in the shift log did not get carried forward to subsequent shifts.

The robot engineer fixed the robot. The doors were left open as the hoses still needed replacing. `During the night shift little work was done in the Control Cell as the replacement hoses were found to have the wrong end fittings.'

Work restarted about Saturday lunchtime and was probably finished by about 18:00 on Saturday. The cell could not be re-energised yet as there was no electrician on duty who could do this until the night shift. The Shift Manager's log noted that the doors were still open and the Foreman's log said that the outer door was open and the cell still needed re-energising. The TPMP was not mentioned at this handover to the Saturday night shift. Shortly before midnight the electrician was authorised to re-energise the cell. The TPMP remained in place.

The incident itself happened when an operator raised a container of waste through the hatch door into the cell. His written instructions had nothing about checking the state of the doors, his control panel had no indicators for the doors, and it was almost impossible to see the doors from his control position. He did have a TV monitor to provide another view of the cell and as he raised the container he noticed in the background that the doors were open. He went to another control panel about 5 metres away and managed to close the inner door. The TPMP gets an honourable mention here as without it the PLC would not have allowed the inner door to move.

Nobody was in the room outside the cell. Four people were in the next room and they were warned by an alarm in the room outside the cell. These people were not intending to enter this room at all. Nobody was found to have received any radiation exposure from the incident.

During the subsequent NII investigation it was discovered that:

- The changes to the key exchange box for the doors had resulted in its design becoming unsafe. The added override key was not held captive in the box so it could be removed at any time, and if it was removed it restored power to the hatch door. Also, once the outer door was open the keys could be removed from the box by reversing the normal sequence but with the outer door still open. These defects had not been discovered during any of the commissioning stages. It was not discovered when the keys had been removed and returned to the Permit Foreman's office.

- The permit to work was signed off based on the keys being returned without any physical check of the state of the doors.

- The logic controlling the crane did not care that the crane appeared to be in two places at once, where it really was and where the TPMP said it was. The logic still allowed the crane to lift the container of waste into the cell in this condition.

- The PLC modification to prevent the hatch door opening if the inner door was open, described above, had the coding error involving the + sign.

The NII made various technical recommendations, but their first recommendation bears repeating:

> The incident graphically illustrates the need for:
>
> (a) those who design and operate such plants to ensure that the protection systems provided are, so far as is reasonably practicable, independent of the control systems for the plants. The design and operation of such systems should be made as simple as possible.

The NII are also discussing with BNFL and the IAEA to get this incident included as one of the case-book examples on the International Nuclear Event Scale for Nuclear Reprocessing Plants.

Summarised from: HSE, Windscale Vitrification Plant Shield Door Incident
15 September 1991, HMSO, ISBN 0 11 886348 7.
Peter Ilieve peter@memex.co.uk

Privacy Risks of Computerized Medical Billing

John Bonine E-LAW US <ejohn@igc.apc.org>
Mon, 23 Nov 92 07:16:33 PST

I forward to you the following, which contains a good discussion, from a professor of medicine in Minnesota, of why doctors are resisting a drive for (seemingly innocuous) computerization of billing procedures. John Bonine

```
>From: Paul Kleeberg <PAUL@gacvx1.gac.edu>
>
>Last Thursday Gerald M. Phillips <GMP@PSUVM.BITNET> said:
>
<> I was working with AMANET when it collapsed because doctors wouldn't use it.
>Out of curiosity, did you aver ask the doctors why?  I used it and found the
>interface somewhat non-intuitive and was disappointed that there was never
>any type of gateway established with the Internet.  The current iteration of
>AMA/Net => U.S. HealthLink also is free standing though I am told they are
>looking into an internet gateway.  Same non-intuitive interface.  Many of us
>who would most wish to use the system (rural physicians) have to pay long
>distance phone charges on top of access charges.
>
<> Now the HCFA is mandating computerized recordkeeping, but doctors are
<> fighting it tooth and nail.
```

>
>The family doctors on my list (Fam-Med) are concerned about a number of
>things. Among them: confidentiality of patient records, who is going to pay
>for this change and has it ever been shown to improve outcome or patient
>care?
>
>Regarding the confidentiality of patient records, the paper chart assured
>confidentiality since it could never be found. An electronic chart can be
>accessed by several people at once from distant locations and since payors
>are one of the groups who are strongly supportive of an electronic record, I
>might be just a bit concerned as an individual. Given payors propensity to
>exclude preexisting conditions, a simple keyword search of an electronic
>chart could unearth all sorts of interesting data about an individual with
>little effort. It would further interfere with the physician-patient
>relationship causing patients to be even more cautious about the types of
>information that got into their chart.
>
>Who is going to pay for it? Gov't has told us in no uncertain terms that we
>physicians should. For those of us in struggling rural practices, that
>added burden will be all that it takes to cause some of us to close up shop
>and join a HMO in a metropolitan area (Better pay, less call, fewer
>administrative hassles and better cultural quality of life) or just retire.
>For those of you in urban areas that may not sound like much but out here in
>rural America, where communities and hospitals depend on having a physician,
>it can mean economic survival of the community as well as life or death for
>the individual.
>
>Has it ever been shown to improve outcome or patient care? We all believe
>it will but I do not believe it has ever been studied. Nothing like going
>full tilt investing megabucks in systems we *believe* should work without
>first evaluating the costs or measuring the benefits of implementation.
>Lets look at the systems in use today. What difference have they made?
>
>You can be sure that if a computer can be shown to help a physician see more
>patients in a day, reduce the cost of providing services or enable her to
>provide a higher quality of care to her patients, it will be quickly adapted.
>
>Paul Kleeberg, M.D., 604 North 3rd St, St. Peter, MN 56082   507-931-6721
>Family Practice, University of Minnesota Paul@GAC.Edu or Paul@GACVAX1.Bitnet

Teller machine networks

Steve Holzworth <sch@unx.sas.com>
Mon, 23 Nov 1992 15:12:14 -0500 (EST)

I experienced an interesting failure of an ATM network over the weekend. Using a Mastercard supplied by an out-of-state (OUS) bank, I accessed an ATM at my usual personal bank, NationsBank (NC). I was attempting to get my bank card balance. The ATM had me enter my PIN, then asked for the transaction type. I pressed "Acct. Balance" (actually, a series of buttons), and the ATM paused briefly, then dutifully spit out a receipt with a balance on it. The interesting thing was that the balance, to the best of my knowledge, was about

$1200 high, just over my credit limit. I was NOT amused. I assumed I might have been subjected to a fraudulent use of my card, so I went home and called the 800 number for OUS. I reached a call director, which among other things, allowed balance requests. I asked for my balance, and was given a number right in line with what I expected, about $2000. Further, the automated system stated that this WAS the current balance as of that day, Saturday.

Monday morning, I called OUS Customer Service and spoke with one of their representatives. I related the problem I had had over the weekend. She checked the balance herself, and indicated that the automated system gave the correct number, and the ATM gave an incorrect number. Her response was: 'it's an ATM failure, so you need to contact that bank about it...'.

I called the local branch of NationsBank, the same branch where the ATM is located. They had me call an 800 number for NationsBank. The person there looked at a few things, including my current CHECKING balance, just in case the ATM had printed THAT number by mistake (!). Nope, not even close. After leaving me on hold for awhile, she stated that her supervisor felt that I should speak to someone in their ATM division. I was transferred there to yet another front-line service rep. After I explained the circumstances again, she thought about, then said it was OUS's problem since they were the issuing bank for the card and I should take it up with them (of course).

Ignoring the customer service runaround, there are several interesting points here:

1) My ATM is getting (or giving me) an incorrect balance for a Mastercard, despite being part of the Mastercard ATM net. Note that the normal failure for a request not handled by the network, or the bank in question, is to say "Not a valid transaction type" (or something like that). I've had this happen when attempting a balance request for a card from yet another bank.

2) If my balance request is being mishandled, what about cash withdrawals? What number actually gets relayed between the banks?

3) The printed receipt has the correct Mastercard number on it, along with the text:

```
  CC INQUIRY
  FR CREDIT CARD
  BALANCE      $too.many
```

so it thought it was doing the correct transaction, with the correct account.

4) The only numbers I enter are for my PIN (4 digits).

5) Off the topic, but interesting, is the fact that my bank-supplied PIN is identical to the third group of digits in the account number. This may be a strange coincidence, or an example of gross stupidity.

Steve Holzworth sch@unx.sas.com SAS Institute, Open Systems R&D, Cary, N.C.

Re: Election HW/SW problems (Urken, RISKS-14.08)

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>
Sat, 21 Nov 92 19:39:39 EST

A. Urken posted some comments in RISKS-14.08 regarding the FEC's and NASED's joint efforts in "development of standards and certification testing" for election equipment and software. This is a somewhat misleading statement. The "standards" that have been issued to date are not standards, only suggested guidelines. They need to be adopted by the individual states before they are accepted as standards. This is a lengthy process, and some states have been lax in doing so. Furthermore, upon investigation of these documents, it will be revealed that the rigorous security standards work of NCSC, which takes the form of the rainbow series, seems to have been largely ignored by the FEC and NASED to date.

Note that election equipment does not come under the Computer Security Act, and hence it is not required to conform to any Orange Book standards. The question that concerned citizens have been asking for years is: WHY NOT?

Although Independent Testing Agencies are now becoming "certified," the purpose of ITAs is presently dubious. SRI [a consultant to N.Y.C. and the system evaluators] had its hands tied by two non-disclosure agreements (one 6 years, and one 30 years) by one manufacturer of election equipment, during an (ongoing) examination process. The policy of the FEC is to allow secrecy in the examinations, in order to preserve trade secrets claimed by the manufacturers. Perhaps someone can explain how an ITA can be "independent" while being prohibited from disclosing certain information they discover in the course of their testing process to the intended purchasers? Yes, the manufacturers know that they can protect their property with copyrights and patents, but some have claimed that such filings would "provide a road map to rigging elections" and so rely on and impose trade secrecy.

Regarding Peter Mellor's posting on City University's SW Engineering program: HAIL BRITTANIA! Let us ally forces and post some curricula to the forum!

Rebecca Mercuri.

The ultimate in anti-virus, anti-invasion security

"Lee S. Ridgway" <RIDGWAY@mitvma.mit.edu>
Tue, 24 Nov 92 09:35:56 EST

Found in rec.humor:

Here are The Three Laws of Secure Computing (TLSC)

1) Don't buy a computer

2) If you do buy a computer, don't plug it in.

And, finally,

3) If you do plug it in, sell it and return to step 1.

Technophones

David Honig <honig@ruffles.ICS.UCI.EDU>
Fri, 20 Nov 92 17:03:26 -0800

Just encountered yet another hazard of modern life. In a certain new office phone system, unplugging the phone from the wall jack disables it. It won't work after its plugged in again, though after a moment it does tell you the time.

Also, hidden in the manual is a line telling you not to reprogram certain keys. Of course, someone tried it, not having memorized the manual, and this disabled not only the phone but also the receptionist's master phone.

Pretty neat, huh?

Re: London Ambulance Service (RISKS-14.05)

Trevor Jenkins <tfj@apusapus.demon.co.uk>
Sat, 21 Nov 92 11:54:00 GMT

Some news related to the London Ambulance Service fiasco.

This week's edition of Computer Weekly had a small article from the chief executive of the British Computer Society. The implication was that had the programmers and analysts from the LAS project participated in the society's Professional Development Scheme then this fiasco would not have happened.

I doubt his conclusion very much because I've been a member of the BCS for the last 15 years and during that time I have received nothing substantial about the PDS. What I know about the scheme has been gleaned from Computer Weekly and Computing rather than from the BCS themselves. If those involved in the LAS fiasco would have benefitted from such a scheme it is unlikely that they would have discovered that the scheme existed.
Trevor

PS Computer Weekly and Computing are the ``free'' weekly trade press.

Trevor Jenkins, 134 Frankland Rd, Croxley Green, Rickmansworth, WD3 3AU,
England email: tfj@apusapus.demon.co.uk phone: +44 (0)923 776436

Conference announcement

Vicky Stavridou <victoria@dcs.rhbnc.ac.uk>
Mon, 23 Nov 92 18:03:25 GMT

THE INSTITUTE OF MATHEMATICS AND ITS APPLICATIONS
THE MATHEMATICS OF DEPENDABLE SYSTEMS
1st--3rd September 1993
Royal Holloway, University of London, Egham, Surrey, United Kingdom

PRELIMINARY ANNOUNCEMENT AND CALL FOR PAPERS

The construction of dependable systems, by which we mean systems providing high levels of reliability, availability, safety and/or security, is a problem of considerable concern to both providers and users of information processing systems of all types. Historically, different aspects of system dependability (e.g. reliability and security) have been studied quite independently, albeit that many of the goals are similar. For example, the notion of certifying functionality assurance levels applies equally to reliable systems and secure systems. In addition, users will often require some combination of security and fail-safe operation.

The purpose of this conference is to consider the mathematical aspects of the provision of dependable systems, one goal being a comparison and possible unification of mathematical techniques for providing safe, reliable and secure systems. A number of different mathematical approaches have been taken to the overall problem, including probabilistic/statistical reasoning, formal models of safe, secure and reliable systems and logics of authentication and access control/privilege delegation. Papers on all these areas are solicited, the unifying theme being the application of mathematical techniques to the overall dependability problem. Hence papers will be particularly welcome which cross-fertilise the application domains. The conference will consider dependability for both hardware and software systems.

Organising Committee
....

Dr. B. Chorley (National Physical Laboratory)
Dr. J. Jacob (Coventry University)
Prof. B. Littlewood (City University)
Prof. C. Mitchell FIMA (RHUL)
Dr. V. Stavridou (RHUL)
Dr. V. Varadharajan (Hewlett-Packard)

Call for papers
....

Extended abstracts of papers (of between 1000 and 1500 words) should be submitted to: Miss Pamela Irving, Conference Officer, IMA, 16 Nelson Street, Southend-on-Sea, Essex SS1 1EF, United Kingdom to arrive no later than 31st March 1993.

Authors will be notified of the decision of the programme committee regarding their paper by 31st May 1993. Accepted papers will have a 30 minute presentation time at the conference. The conference will be run under the normal IMA procedures.

Conference Proceedings
....

It is hoped that the proceedings of the conference will be published by Oxford University Press in the IMA Conference Proceedings Series. Full papers will be subjected to the normal refereeing procedure after the conference before being accepted for publication in the proceedings.

Location
....

The conference will be held at Royal Holloway, University of London (RHUL), Egham, Surrey, England where accommodation will be available for participants from the evening of August 31st 1993. RHUL combines an attractive parkland setting with easy transport access (5 minutes from the M25, 20 minutes from Heathrow airport, and 40 minutes by train from London Waterloo).

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 10

Weds 25 November 1992

Contents

Police and Database [another name confusion]

"Stanley (S.T.H.) Chow" <schow@bnr.ca>
Tue, 24 Nov 1992 13:18:00 +0000

In the Nov 23 (today) edition of "The Ottawa Citizen", there is a story attributed to the "SouthamStar net". The story talks about the problems of one Steven Reid - there appears to be two people by that name, with the same birthday, living in the same city (Montreal). The story talks about the usual identity mix-up and problems well know to the readers of this forum. The scary part is the quote attributed to Lt. Gerard Blouin of the Montreal Police:

"it's up to him to change his name somehow. If he can modify his name,
just by adding a middle initial or something, it would help him."

For those unfamiliar with Canada, Ottawa is the capital and Montreal along with Toronto are the two biggest cities in Canada, each with millions of people. One would have expected the computer system to be able to deal with this problem; but it would appear that in at least one public institution, the computer rules supreme.

Stanley Chow (613) 763-2831

BNR, PO Box 3511 Stn C schow%BNR.CA.bitnet@cunyvm.cuny.edu
Ottawa Ontario Canada K1Y 4H7 ..!uunet!bnrgate!bcarh185!schow

Nuclear-plant risks in the US (Re: Ilieve, RISKS-14.09)

Hip but Harried <wex@MEDIA-LAB.MEDIA.MIT.EDU>
Tue, 24 Nov 92 14:50:44 -0500

Peter Ilieve gives a wonderful summary of the implementation changes which led to a near-incident in Britain. In the US, we used to have a process which was supposed to avoid this. Hearings and design reviews were held before a plant was to be built and then a second set of hearings and reviews were held after the plant was built before licensing took place.

Unfortunately, and with very little fanfare, the Congress bowed this year to pressure from the Bush Administration and the nuke industry and passed a law which (among other measures) eliminates the post-construction hearings and reviews before licensing takes place. Thus we now have a system which is guaranteed to produce unknown flaws from implementation changes such as the door-interlock changes Ilieve reported on.

--Alan Wexelblat, Reality Hacker and Cyberspace Bard, Media Lab - Advanced
Human Interface Group wex@media.mit.edu 617-258-9168 wexelblat.chi@xerox.com

Re: Election HW/SW Problems (Mercuri, RISKS-14.09)

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 25 Nov 92 13:23 EST

>Note that election equipment does not come under the Computer Security Act,
>and hence it is not required to conform to any Orange Book standards. The
>question that concerned citizens have been asking for years is: WHY NOT?

The implication of Ms. Mercuri's rhetorical question it that the Computer Security Act should apply to computer-based machines for recording, tabulating, or reporting votes, that the Orange book would then apply to such systems and that all of that would be helpful. (Be careful what you ask for, you might get it.)

The explicit purpose of the Computer Security Act was to limit the influence of the Department of Defense over non-defense uses of computers. While assuming that NIST would not re-invent the wheel, it provided that standards for non-defense government and the private sector would be promulgated by NIST. However, control over voting procedures is reserved to the states.

The Orange book was developed almost two decades ago to respond to a Department of Defense problem. It deals with the protection of national security classified data in "shared resource" (i.e., multiuser) computing systems. It was intended to deal primarily with the operating system on the assumption that the policies of interest could be most effectively and efficiently enforced there. It was not intended to deal with problems, like those in vote recording, tabulating, and reporting, that are specific to the purpose for which the computer was being used.

While we have learned a great deal from the Orange Book about how to enhance the trust in computers, neither the Orange Book nor any of its progeny is directly applicable here. Any attempt to apply them would be, at best, misguided and inappropriate, perhaps, counter-productive or even mischievous.

To a great extent, the Orange Book has been overwhelmed by changes in computer economics and styles of use. It was based upon the implicit assumption that computers were expensive; it did not anticipate cheap computers. It assumed that operating systems were dear, limited in number, and practically free from non-management interference. It assumed that the operating system could be made trusted, at least for limited purposes. It did not anticipate operating systems of millions of lines of code that sell in the tens of millions of copies for tens of dollars and that are not under the control of management.

It assumed that the portions of the operating system that were responsible for controlling access to operating system resources could be separately identified, isolated, and so limited in scope and complexity that they could be made effective and reliable and demonstrated to the satisfaction of a third party (not user or vendor). It assumed that all of these things could be done cheaply enough to be covered by the reduction in risk that would result.

It assumed that control of access to the resources known to the operating system would be sufficient, i.e., that all of the resources of interest were identified to and known by the operating system. It assumed that applications could not be economically be made trusted and that uses that required that they be so were intractable.

It assumed that preserving the confidentiality of data was the problem of interest. While it dealt with the integrity of the operating system, it was essentially silent on the integrity of the data or of the results produced by the application. Of course, these are exactly the problems of interest in recording, tabulating, and reporting votes.

The requirement for trust in the use of computers for recording, tabulating, and reporting votes is very high. Such systems must be developed with extraordinary, not "standard," rigor and they must be developed in the light of independent scrutiny. While the operating system, if any, must protect the application controls, it is the controls specific to and implemented in the application that are of interest. The problem is much more analogous to the problem of ATMs than the class of systems dealt with in the Orange Book.

These systems should be enabled and adopted under law that is specific to them, not generalized across more generic problems. While the Computer Security Act and the Orange Book have much to teach, they are neither applicable to nor sufficient for this problem.

William Hugh Murray, Information System Security, 49 Locust Avenue, Suite 104;
New Canaan CT 06840   1-0-ATT-0-700-WMURRAY   WHMurray@DOCKMASTER.NCSC.MIL

A rec.humor.funny post about voting machines

"Joshua E. Muskovitz" <rocker@vnet.ibm.com>
Tue, 24 Nov 92 13:24:32 EST

A tale from my first experience as a poll worker last Tuesday:

> On Election Day the sash cord broke on one of the voting machines in the precinct where I was working as a poll worker. The curtain couldn't be closed to permit a secret ballot. The Judge of Elections took the machine out of service and sent for a technician who arrived an hour later and spent about 10 minutes working on the machine. As he came out of the polling station another poll worker asked: "Well, is the machine fixed?"
>
> The technician replied as he hurried on to his next assignment: "Now, now, we don't like to use the 'F-word' on Election Day. The word is 'repaired'."

Selected by Maddi Hausmann. MAIL your joke (jokes ONLY) to funny@clarinet.com
Attribute the joke's source if at all possible. A Daemon will auto-reply.

Re: Smart cars? (Mestad, RISKS-14.06)

Brinton Cooper <abc@BRL.MIL>
Wed, 25 Nov 92 14:56:35 EST

Steve quotes from the December issue of Popular Mechanics on the installation of on-board radar to identify obstacles in the path of a vehicle and to monitor steering, braking, speed, and closing rates. He reports on work to link the radar and cruise control, then the radar and the brakes. He comments:

> "The RISKS seem obvious enough to me..."

I grant the risk. Again, however, I make a plea for identifying the risk of NOT doing something like this. At present, there simply is no way for authorities in certain western and southwestern states to know of near zero-visibility (due to fog, sand, dust,...) on some portion of an interstate highway. This deficiency leads to multiple, telescoping collisions involving

dozens of vehicles and severe injury and death. The risk not doing something like this is the unabated continuation of such injury and death.
_Brint

Re: Installer problems (Thorson, RISKS-14.08)

Richard Wexelblat <rlw@ida.org>
Tue, 24 Nov 92 14:40:02 EST

This is one of those features/flaws that occur in user friendly (ha) systems. I installed the new MS Windows 3.1 and discovered that the drivers for my Brand-X video controller didn't work under 3.1. No problem, temporarily I can use the system in bigprint mode. So I call the Brand-X distributor. No problem, they'll send me the new drivers as soon as they come in. "I dunno, maybe a few months."

Who makes the chips on the Brand-X board? Trident. Aha! a reputable company. I call Trident. No problem, they'll ship the W/3.1 drivers immediately.

(A few days pass).

The drivers install easily, but guess what, the otherwise quite adequate documentation doesn't list Brand-X so which of the various options shall I select? I call Brand-X. "Oh, _those_ drivers? Yeah, we have them." Documentation? No problem, they'll ship it to me in a few months... Customer assistance? "Sorry, we don't make that model any more. Just try whatever resolution you want."

So I use the hyper-handy install-it-yourself function under Windows. No problem, the driver installs fine. Oops! It was an unsupported driver, the screen is 100% rectangular garbage. How do I back off? Easy, just delete all of Windows and install it all over again. Since I can't read the screen, that good old install-it-yourself utility is unusable.

Turn sharply left twice in France, Brand-X!

--Dick Wexelblat (rlw@ida.org) 703 845 6601 This message is not copyright.
Please feel free to use it in any context, at any time, with or without attribution. Quotes out of context and parodies are encouraged.

Re: How to tell people about risks?

Richard Stead <stead@seismo.CSS.GOV>
Mon, 23 Nov 92 11:30:14 EST

Mike Coleman recommends an analogy to the Richter scale as a means to relate risks to ordinary people

> communicating statistical risks to ordinary people. The Richter scale seems
> to be successful in allowing people to think about and compare seismic events

While his proposed risks scale may be useful in this respect, it would not reflect the success of the Richter scale. As a seismologist who has attempted to explain quake magnitude to laymen on countless ocassions, I can vouch for the fact that it does not communicate well to laymen. Few understand the concept of logarithms, and beyond that, they have a very hard time understanding what is being measured.

The Richter scale was developed as a device to aid in cataloging quakes, based on analogy to star magnitudes; it was not designed with the public in mind. It measures the "size" of a quake based on the amplitude of shaking it can induce (with many constraints). It does not measure energy, frequency, duration, etc., (although these can be related to magnitude). Yet I have met few layman that understand why uttering "That felt like a magnitude 6!" after feeling a quake makes no sense. The notation is difficult, too, without knowledge of logarithms "If a 6 is 10 times as big as a 5, then is a 5.5 5 times as big?" I find that it is the single most misunderstood aspect of seismology. I suspect that the problems (logs and what value is measured) would similarly be problems with risks reported this way.

Richard Stead   stead@seismo.css.gov

Re: How to tell people about risks?

John A. Palkovic <john@warped.phc.org>
Sat, 21 Nov 92 21:16:56 -0600

Mike Coleman writes:

>The Richter scale seems to be successful in allowing people to think
>about and compare seismic events (earthquakes); perhaps we can develop
>a similar scale for statistical risks.

It seems to be successful in demonstrating that newspeople are ignorant of logarithms. Many times I have heard a newsperson say knowingly that an increase of 1 on the Richter scale represents an increase of 10 in the strength of the quake. This is incorrect.

The equation defining the Richter scale is log E = 11.4 + 1.5M, where E is the energy released in ergs and M is the magnitude. Thus a delta M of 1 represents an increase of 10^(1.5) or about 32 in the amount of energy released. People who say otherwise do not really know what they are talking about.

John Palkovic   home: john@phc.org || work: jp@ssc.gov

Re: How to tell people about risks?

Arthur Delano <ajd@oit.itd.umich.edu>
Sun, 22 Nov 92 17:58:20 EST

In Risks 14.08, several contributors (Stuart Wray <scw@cam-orl.co.uk>), (Rob Cameron <cameron@cs.sfu.ca>), (coleman@rocky.CS.UCLA.EDU (Mike

Coleman)) suggest a standardized table of comparative risks.

The problem with presenting potential of risk by analogy is with the implications of the analogy.

Even though, statistically, one is as likely to be killed in an airplane collision as to identify a blade of grass and then hit it with a golf ball, one _seems_ more probable than the other. Airplane collisions are real tragedies many people are continuously working to avert, the silly golfing bet is trivial and may have never happened. Although these events suggest extreme differences in emotional content, almost any two events of similar possibility can carry different implications based as much on personal experience as on general significance of the event.

Citing the very small odds for an absurd situation (hitting the blade of grass) as being similar to those of failure for an item one is defending can make the chance of failure seem absurd. When the mathematics cannot be fudged, their relevance can be changed through the context in which they are presented. The audience could then determine the significance (to them) of the event regardless of the odds and decide if the risk is worth taking.

AjD

telling people about risks

Phil Agre <pagre@weber.ucsd.edu>
Mon, 23 Nov 92 15:42:57 -0800

RISKS-14.08 contains a number of suggestions about how to inform people about technological and other risks. Those interested in the professional literature about the subject should look at various books and manuals by Peter Sandman and his colleagues. The state of the art in implementing such "risk communication" schemes is (believe it or not) the "CAER" (Community Awareness and Emergency Response, pronounced "care") program of the Chemical Manufacturers Association. I personally have grave reservations about this entire field, but it's certainly much better than what it replaced.

Stuart Wray <scw@cam-orl.co.uk> suggests that we "tell people the odds and compare them with the odds of various every-day disasters". This is a very common approach, and something that Sandman (for example) tends to recommend against (though not as strongly as he recommends against comparing the odds of getting cancer from your local factory to getting cancer from eating a peanut butter sandwich, which tends to infuriate people). One of the many problems with numbers like Wray's (for example, "Odds of dying in a car accident in the next year: 1 in 10000"), is that they're not very meaningful. They don't reflect "my risk" of dying in a car, but rather the average across some large population (Wray doesn't say which one). If we computed the statistics for incrementally more closely defined groups (urban, light drinker, no previous accidents, and so forth), we would get a lot of different numbers, some of which would probably be more impressive than others.

My impression in talking to people who communicate risks professionally is that auto-accident statistics (and many others, especially drowning for some reason) are a form of urban myth. The numbers circulate among the community of people who, for one reason or another, tend to think of risks from industrial activities as minimal, and they serve largely as self-reassurance, since ordinary people have a strong tendency to reject such statistics as self-serving nonsense. (On this subject I strongly recommend the organizing materials of the Citizens' Clearinghouse on Hazardous Waste, which you can read about in William Greider's brilliant and highly relevant new book, "Who Will Tell the People?: The Betrayal of American Democracy", New York: Simon and Schuster, 1992.)

Phil Agre, UCSD

Re: Telling people about risks (RISKS-14.09)

"George Buckner" <GRB@nccibm1.bitnet>
Wed, 25 Nov 92 10:21 EST

On the subject of how to inform the public of risks:

ABC news had a story this week about work in progress to fit automobiles with computerized roadmaps and sensing/control systems which are intended to automate car driving -leave even the driving to the computer. They quoted one man involved (I didn't catch who it was or who he was with) as saying (paraphrased):

> .a certain. (high) percentage of auto accidents are caused by driver error. If we can replace the driver with a computer then we can reduce the accident rate accordingly.

Ah yes, the computer to the rescue -again -replacing us fallible humans with the perfectly functioning machine, and reducing the accident rate due to operator error (who or whatever that operator may be) to zero.

Perhaps this is best filed under "Risks of assuming non-sequiters". Regardless of which school of thought we subscribe to re: software quality measurement/safety assurance, this kind of simplistic and misleading language -and thinking -should never be heard coming from systems designers.

Risks of fashionable risk-metaphors

<chaz_heritage.wgc1@rx.xerox.com>
Wed, 25 Nov 1992 06:23:02 PST

In RISKS-14.08 Rob Cameron suggests the following risk-metaphors for "communicat[ing] risk information to the public in a meaningful manner":

>"The risk of your child seriously injuring himself in 3 hours of playing with this toy is about the same as that of being an automobile passenger for 4 minutes."<

>"The risk of long-term liver damage from this medication is approximately the same as the risk of cancer from smoking 2 packs of cigarettes."<

Despite this being essentially a good idea he could not have picked two worse metaphors. The perception, on the part of the majority of the general public, of these two activities - smoking and riding in cars - is about as slanted as it can possibly be by an endless barrage of moral homilies from the health & fitness weirdos and the environmentalist ban-it-all brigade, who have singled out the cigarette and the automobile, respectively, as Global Enemy No. 1.

Mr. Cameron seems to be idealistic enough to imagine that people will read the numbers and possibly even calculate with them. They will not. They *may* see that the risks of the toy can be compared in some way with those of cars - and leave the toyshop at once. They *may* see that the risks of the medication can be compared in some way with those of cigarettes - and sue the doctor (unless, of course, they are unregenerated and unrepentant smoking drivers like me!).

For myself I do not believe that there is any point in attempting to convey numerical, let alone statistical, information to a 'general public' increasingly deskilled, de-educated, aggressive and litigious.

An example of the perceptions of the general public: European food manufacturers, who are subject to labelling requirements, find it expensive to produce a different label for each country, translating the complex chemical names of food additives for each language group.

Solution: give each additive - they are more or less standardised - a European code number (e.g. "E123"). This can then be looked up in a language-specific list to provide the chemical name in the required language, if anyone is really that interested.

Result: the general public, egged on by extremely ill-informed and sensationalist 'consumer investigative journalists', boycott products that are now labelled as containing what they call 'E-numbers' - exactly the same additives as they placidly accepted previously. Indeed, the term 'E-numbers' is now used by the general public to describe universally vile, infallibly carcinogenic and, above all, *secret* additives with which mad-scientist food-technologists try covertly to poison their kiddies.

Consequence: the food manufacturers, shaking their collective heads in disbelief, are rapidly going back to printing complex chemical names in each of the European languages, and passing on the cost of this exercise to their few remaining customers.

Chaz

Re: Stock price too high?

John R. Levine <johnl@iecc.cambridge.ma.us>
19 Nov 92 00:09:17 EST (Thu)

The company with the $10,000 share price is Warren Buffett's Berkshire-Hathaway. He personally owns enough stock to control the company and doesn't want a lot of shareholders, so he refuses to split the stock. It's been trading in the thousands for years (shoulda bought a share or two at

$7K) so it's pretty stupid if the exchange didn't see a $10K price coming.

For quite a while, its price has been at least an order of magnitude greater than the next most expensive listed stock and its entry in newpaper stock price lists, which are invariably generated by computer from data sent by the Associated Press, is often mangled.

Share prices in the thousands of dollars are quite common in unlisted stocks and foreign companies. The Swiss drug company Hoffman-Laroche long ago had a share price in the $12,000 range.

John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

---

Re: Stock price too high? (Wittenberg, RISKS-14.06)

Randall Davis <davis@ai.mit.edu>
Thu, 19 Nov 92 18:13:42 est

[...] Then let's tell everyone the solution so they can avoid this mistake in the future. How many bits should the internal representation be?

Seems like all you have to do to answer is predict the future.

Some years ago the most expensive stock on the NY exchange was Superior Oil, which sold for around $800/share. Clearly an order of magnitude bigger than that should be plenty, right? And it would have, for about 20 or so years. Now, two decades later, you can point out how terribly nearsighted that design decision was.

OK, let's fix it once and for all: let's make it two orders of magnitude bigger than Berkshire is now; 7 digits should work.

Uh oh, what about the growing international market? What if the NY market starts providing quotes on Japanese stocks in yen and Italian stocks in lira (or quoting US stocks like Berkshire in lira)? So maybe we do need a few more orders of magnitude. Ok, let's use 11 digits; surely there won't be a currency with more than 10,000 units to the dollar.

Ooops, here comes Eastern Europe with 15,000 Polish Zloty to the dollar.

Ok, so maybe we can figure no currency will have more than 100,000 units to the dollar... and then someone gets hit with hyperinflation....

The point should be clear: hindsight provides perfect vision for criticizing design decisions. That's the easy part. The difficult part is making design decisions now, attempting to design a system for now and the future.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 11

Friday 27 November 1992

Contents

Re: Computer Security Act and Computerized Voting Systems

Roy G. Saltman <SALTMAN@ECF.NCSL.NIST.GOV>
Fri, 27 Nov 1992 15:39:01 -0500 (EST)

This is in response to Rebecca Mercuri [RISKS-14.09] and Bill Murray [RISKS-14.10] on the subject of the applicability of the Computer Security Act of 1987 (P.L. 100-235) to computerized voting systems.

The purpose of the Computer Security Act was to create, according to Section 2 (a) of that act, "a means for establishing minimum acceptable security practices" for "improving the security and privacy of sensitive information in Federal computer systems." Systems containing national security, i.e., classified, information are excluded from the purview of the act. In Section 2 (b), the act assigned to the National Bureau of Standards (now the National

Institute of Standards and Technology, NIST) "responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems..." By assigning primary responsibility to NIST for providing the necessary guidance, the act limited the influence of DoD, as Mr. Murray states, although that was only one of the purposes, not "the" explicit purpose.

The Computer Security Act of 1987 applies to "Federal computer systems," where such a system, in the language of the act "means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function."

Now, Mr. Murray is incorrect when he states that "control over voting procedures is reserved to the states." That is specifically untrue in the case of Federal elections. Federal elections are elections for President, Vice-President, U.S. Senators, and U.S. Representatives. The U.S. Constitution provides, in Article I, section 4 that the Congress may "at any time by law alter such regulations" that the State Legislatures impose for determining the time, places, and manner of holding [Federal] elections. In addition, in Article I, section 5, the Constitution states that "each House [of Congress] shall be the judge of the elections, returns and qualifications of its own members."

A number of Constitutional Amendments and Federal laws have changed (expanded) voting rights. In the most recent Congress, a bill was passed mandating very specific procedures for voter registration. The bill would have become law if not vetoed successfully by President Bush. While such laws affect only Federal elections, the states invariably apply them to their own state elections, because they cannot afford two sets of procedures. This was specifically true for the amendment granting voting rights to 18-year-olds, as well as for the Voting Rights Act of 1965.

As the President, Vice-President, and members of Congress are Federal officials remunerated through appropriations of the Federal budget, the votes cast for them on a state or local government computer system is a "system operated by ... [an] other organization that processes information ... on behalf of the Federal Government to accomplish a Federal function."

Clearly, votes in Federal elections are sensitive information, under the Computer Security Act. The reason that vote-tallying in Federal elections is not covered is that the act mandates actions by Federal agencies to implement the act. However, the definition given to "Federal agency" given in the act specifically omits the U.S. Senate and the U.S. House of Representatives. These are the agencies ultimately responsible for Federal election data, and they have excluded themselves from coverage of the act. Thus, the only sensitive Federal data omitted from coverage is the most important for continuation of our democratic government.

Re: Computer Security Act and Computerized Voting Systems

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>

Fri, 27 Nov 92 18:28:39 EST

In response to William Hugh Murray's posting in RISKS Forum 14.10:

First of all, let me state that I agree with much of what was said. Some of which has even appeared in my earlier writings on this subject, most notably the observation that DREs are similar to ATMs (which I comment on extensively in my March 1992 paper published in the Proceedings for the Fifth International Computer Virus & Security Conference), the statement that "control over voting procedures is reserved to the states" (which also appears in that same paper), and I had also alluded to the insufficiency of security standards and theory applicable to this problem in my recent (November 92 CACM) Inside Risks column. So it appears that we are in agreement here (with sufficient citations in evidence of this fact).

Readers should note that my use of the phrase "Orange Book" was intended more generically (as is common) than to the specific book itself. The primary intent of my posting was to make the public aware of the fact that the FEC and NASED have not made sufficient use of the ongoing work by NCSC in their establishment of guidelines and controls for voting equipment. I was not suggesting that the NCSC documents would BE SUFFICIENT for voting applications, only that they should be consulted as it is the largest body of standards work to date regarding computer security and MUCH (not all) of the rainbow series material IS applicable to the voting area (as well as in banking, where it is certainly considered), regardless of the original intention of the Act.

Where Murray and I are not in agreement is in his assertion that the shared resource problem is not applicable to vote recording, reporting and tallying. He may have conceived of computerized voting as taking place on independent, stand-alone systems, but in actuality this is often not the case. Many computer systems used for voting purposes are networked and time-shared. The RISKS implications of this should be obvious, now that I have pointed this out.

A recent voting machine security document that I was asked to review contained the following statement:

> "The proposed DEC computer operating system (VMS) is one
> of the most secure systems available today. Security
> features that comply with the National Computer Security
> System (NCSC) C2 classification have been built in as an
> integral part of the operating system."

I include these sentences not for their merit (with which I have considerable difficulty), but to point out that the operating system problem is ALSO highly applicable to the voting problem.

Both Peter Neumann and I are well aware of the ramifications of getting what is asked for. We have each publically called for greater care in developing voting systems with, as Murray said, "extraordinary, not standard, rigor and ... in the light of independent scrutiny." But I must bring to light the fact that this is not presently the case. I also agree that the laws which affect voting machines should be specific to their manufacture, and have personally lobbied to improve these laws, but as some states have failed to adopt even weak regulations, there must be some place to start, and an existing Computer Security Act might be a good place to at least look. Note that Congress IS responsible for overseeing FEDERAL (Presidential and Congressional) elections, and such SHOULD be considered a matter of national security. Congress did, though, exempt itself from the CSA and hence it does not apply to elections at present.

Due to time constraints I am not at liberty to iterate at length on this subject, but numerous documents and publications are available that will confirm the fact that electronic voting systems are not being administered with the care that should be given, that current laws are inadequate, standards are lacking, and rigorous theories are needed in this area. CPSR is a good place to contact if one would like to become more fully aware of this problem, and then I hope that more individuals will join the effort to ensure that accurate, anonymous voting is guaranteed.

Rebecca Mercuri.

How Is Technology Used for Crime in the Post-Hacker Era?

Sanford Sherizen <0003965782@mcimail.com>
Fri, 27 Nov 92 14:38 GMT

I am working on a research project and book involving the process by which some people have been able to "invent" computer and other high tech crimes. The issue that I am trying to understand is how people adopt new technologies for purposes other than those envisaged by the developers. Specifically, some people are very skilled in what I call thinking like a thief. They see technology from a particular perspective, based on how it can be used for anti-social, deviant, and/or criminal acts. A counterpart to this are those who come up with new applications for technology, which may also be viewed as negative by developers but can often lead to new applications (and even new industries).

It could be quite important to establish how other technologies have been used for "inventing" crimes. How do technologies get expanded and changed, especially by "non-official" people, i.e., they do not work for the original technology developers or owners? These "non-official people" see new possibilities, whether for a positive or negative use. I know that the terms positive and negative raise many definitional and value difficulties. Yet, I am interested in how people view technology, how they are able to frame questions about other uses, how this information gets spread to others, and the positive as well as negative consequences of this process.

Drawing on my background in criminology, sociology, and information security, I have collected examples on how other crimes have developed and been responded to by technologists and law enforcement. Some examples that come to mind include how the car was relatively quickly adopted by bank robbers to improve their chances of getting away from the crime scene. This led to police forces having to become motorized, which had many other consequences for command and control of police deployment and changes in how the police had involvements with citizens. The Xerox or photocopying machine certainly led to better protection of documents by allowing the making of file copies but was quickly understood by some that it could also be used to steal copies as well as to leak documents to unauthorized sources, e.g. the Pentagon Papers. The automatic dial system was invented to Strowger to prevent Kansas City telephone operators from depriving him of business by giving busy signals or wrong numbers to potential customers. Ithiel de Sola Pool, in his book on the telephone, discusses how the telephone was portrayed as both the promoter and the conquerer of crime. "Call girls" and obscene callers were at least two of the ways that telephones were viewed as contributing to moral decay while the first electric police-communication system of record was installed in 1867.

Answering these questions could help establish some clues as to how computer crime is developing and areas that require particular security attention. We have not been very prepared for the "Post-Hacker Era" and we have not been raising questions about the crime potential of new technologies.

Any ideas, reactions to these comments, and suggestions of any social historical studies about these issues are welcomed. I will post a summary of responses.

Sanford Sherizen, Data Security Systems, Inc., Natick, MA MCI Mail: 3965782

Re: Nuclear plant risks (RISKS-14.09, 14.10)

Brad Dolan <71431.2564@compuserve.com>
27 Nov 92 15:36:59 EST

Mr. Wexelblat points out that recent legislation (mostly) eliminates post-construction hearings from the nuclear plant licensing process.

I believe the second stage review was often used as a platform by intervenor groups to delay plant licensing; adding millions, even billions to plant costs. Utilities pass these costs along to ratepayers, who must either reduce their consumption of electrical energy or reduce spending on other things to pay increased electrical bills. In the southeastern U.S., many people have begun heating their homes with wood or (unvented!) kerosene heaters, which expose them to potentially substantial risks.

I would like to see a comparison of safety benefits (in terms of expected lives saved, property saved, or whatever) resulting from intervenors' interventions with the safety detriments which have resulted from increased electrical bills.

Brad Dolan 71431.2564@compuserve.com 10288-700-NUCLEAR N4VHH

Re: Installer Programs (Thorson alias mmm, RISKS-14.08)

John Bennett, Defence Science & Technology <BENNETT@dstos3.dsto.gov.au>
Thu, 26 Nov 1992 9:58:23 +1030 (CST)

Unfortunately, a de-installer is likely to introduce its own risks if it is
written by the writer of a buggy installer, e.g.,
 a. It might not deinstall everything which should be deinstalled
 b. It might deinstall something which should not be deinstalled
 c. Something else might go wrong.

Sometimes I think Macs are too smart, there are times when I would like some manual intervention in automatic processes such as Mak describes.

John Bennett, DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION PO Box 1500
Salisbury, South Australia 5108 Phone : +61 8 259 5292 FAX : +61 8 259 5537

Risks of Believing Install Programs

mathew <mathew@mantis.co.uk>
Thu, 26 Nov 92 12:33:59 GMT

I recently installed Microsoft Windows for Workgroups on a Toshiba T5200 "portable" computer. (I say "portable" because the machine is a few years old, and hence measures 37x10x40cm and weighs nearly 9kg.)

The machine is connected to our Novell Netware network, and so the process included installation of Netware and Ethernet drivers.

Windows for Workgroups detected the Ethernet card automatically, and presented a dialogue box suggesting that it was a Novell NE2000 Anthem card. This was absolutely correct, so I confirmed it. The installer then presented another dialogue, this time with the DMA address and IRQ interrupt number. The DMA address was correct, and I reasoned that since the machine had worked everything else out it probably had the IRQ number correct also. I hit the OK button.

A warning box appeared stating that the IRQ number on my Ethernet card would clash with the machine's second serial port, and would have to be changed if I wanted to use that port. I'd never used it before, but I did want to now. I abandoned the installation.

Twenty minutes, three technical reference manuals, twelve fixing screws and three removable covers later, I had the Ethernet card in my hands. I peered at the card. It was set to address 320, IRQ 2. Windows had reported this as address 320, IRQ 3. I left it exactly as it was, put the machine back together again, and went through the install once more.

The risk, of course, is that because the install program seemed to know exactly what sort of Ethernet card I had and what DMA address it used, I automatically assumed it knew what it was talking about when it told me the IRQ number. In my defence, I must say that Windows had been spot-on at working out the IRQ number for the card in my Elonex machine.

The message for authors of install programs is that perhaps they should avoid making their programs supply default values using guesswork if the software can't actually read the value. If the program makes a couple of lucky guesses, the user might be tempted to believe that the program knows something he doesn't.

The message for users is: even if an install program tells you exactly what hardware you have attached to your machine, never trust it to pick correct settings based on that information.

mathew

Re: How to tell people about risks?

Sanford Sherizen <0003965782@mcimail.com>
Fri, 27 Nov 92 14:24 GMT

Several years ago, public safety messages would appear prior to major holidays warning drivers in the U.S. about accidents. The messages said (paraphrase) "350 people will die this Thanksgiving holiday. Don't be one of these fatalities. Drive carefully." Researchers from the Safety Council found that these risk messages were not helpful at all. Drivers thought that an accident would not happen to them. The risks became someone else's problem.

The Safety Council then decided to personalize risk. They ran ads directed at kids suggesting that the kids ask their parents to drive safely and to use seatbelts. This approach to risk was much more successful and may have been one of the many reasons why traffic fatalities have declined over the years.

Sanford Sherizen, Data Security Systems, MCI MAIL: SSHERIZEN (396-5782)

Telling people about risks (ingredient labels)

Mark Day <mday@jukebox.lcs.mit.edu>
Fri, 27 Nov 92 11:40:25 -0500

One contributor to the discussion about describing risks made two alarming comments. I read both comments as arguing (basically) "since ingredient labels pose certain problems, we should eliminate them and thereby eliminate the problems". The comments struck me as a good example of creating a major risk to correct a minor one, perhaps because I'm more interested in this issue as a consumer of food than as a producer of food.

Here's the first comment:

> I do not believe that there is any point in attempting to convey numerical, let alone statistical, information to a 'general public' increasingly deskilled, de-educated, aggressive and litigious.

In essence, since the 'general public' can't be trusted to interpret facts properly, better not to tell them.

The writer would presumably not include himself in the 'general public' that he characterizes as so unpleasant; no doubt he could interpret the facts properly. But unless the information is on the carton of whatever he's buying, he won't have access to that information either. Realistically, the choice is between making the information available to everyone or making it available to no-one. The writer will not be able to go to a special store (reserved for those who pass a test of numerical skills) to buy goods with labels describing their contents.

On to the second alarming comment:

> An example of the perceptions of the general public: European food manufacturers, who are subject to labelling requirements, find it expensive to produce a different label for each country, translating the complex chemical names of food additives for each language group.
>
> Solution: give each additive - they are more or less standardised - a European code number (e.g. "E123"). This can then be looked up in a language-specific list to provide the chemical name in the required language, if anyone is really that interested.
>
> [goes on to describe that consumers didn't like this]

This is a dreadful solution, and I can understand why consumers would be less than thrilled about it. The purpose of ingredient labels on goods is to convey information to potential purchasers, and this code-word scheme definitely conveys less information in the real world.

An analogous argument would eliminate ingredient labels altogether, and require only that the manufacturers provide a telephone number to call for the ingredients. After all, the information is still "available", just much less convenient to check when you actually need it.

If I've learned that I must avoid products containing monosodium glutamate because of an allergy, I'm going to be unhappy when I need to learn a new code name for it. The convenience for the manufacturer is balanced by an inconvenience for me.

And frankly, the whole business seems like a fraud to me. It's not just chemicals that have different names in different European languages, it's also simple things like water, sugar, salt. Either all of those get code numbers (at which point the ingredient labels become utterly useless) or else the manufacturers still have to produce multiple labels for an identical product.

--Mark Day

Change in the Maximum Length of International Telephone Numbers

Nigel Allen <nigel.allen@canrem.com>
Wed, 25 Nov 1992 19:00:00 -0500

Any application that does not allow for fifteen-digit international telephone numbers is a potential risk today, and will become a real risk on January 1, 1997.

The following information from Stentor Canadian Network Management, the consortium of major Canadian telephone companies, was distributed through the Canadian Department of Communications' Terminal Attachment Program Advisory Committee as TAPAC bulletin 92-13.

Advance Notice of Change in the Maximum Length of International Telephone Numbers

Beginning midnight December 31, 1996, CCITT Recommendation E.164 will be implemented. This recommendation allows the expansion of international telephone numbers from 12 to 15 digits. Although the North American Numbering Plan will not change, some foreign administrations may assign numbers up to 15 digits long to subscribers. Therefore, terminal equipment originating calls to these subscribers must be able to handle the additional digits.

For more information on this change, please contact:
Marion Norman
Stentor Canadian Network Management
410 Laurier Ave. West, 8th Floor
P.O. Box 2410, Station D
Ottawa, Ontario
Canada K1P 6H5
telephone (613) 560-3420
fax (613) 560-3226

Note from NDA: I think the "international telephone number" in this context includes the country code but excludes the access prefix, such as 011 in Canada and the United States.

Readers in the United States should presumably contact the North American Numbering Plan Administration at Bellcore rather than Stentor.

Nigel Allen nigel.allen@canrem.com

Canada Remote Systems - Toronto, Ontario
World's Largest PCBOARD System - 416-629-7000/629-7044

[And so, dear RISKS readers, beginning 1 Jan 1997 we
can expect various strange reports to appear... PGN

Humorous Submissions

Andrew Davison <ad@munta.cs.mu.OZ.AU>
Fri, 27 Nov 1992 11:53:46 +1100

CALL FOR SUBMISSIONS FOR A NEW BOOK Tentatively titled:
"Humour the Computer:
Humorous Writings concerning Computing"

We seek contributions of a humorous nature for a new book called `Humour the Computer', an anthology of the comic, amusing and laughable aspects of Computing. It is scheduled to be published by MIT Press early in 1994.

Topics of interest include:

* computing experiences: e.g. `a day in the life',
computing jobs - industry, commerce, teaching, research, etc;
getting funded in the 90's, getting a job in the 90's,
home computing, how computer people relax, exam marking stories,
getting published, office politics

* the history of computing: e.g. the mistakes, the disasters, the egos
gone mad (with names changed to prevent law suits), folklore (not
necessarily true)

* the future of computing

* computing in the Real World: e.g. in the media, computer salesmen,
misconceptions about computing, the misuse (abuse) of computing, faulty
software/hardware, the `training' course

* fake journal articles: e.g. AI, expert systems, machine architectures
software engineering, new programming languages, semantics;
surveys of `important' fields: Virtual Reality, neural nets,
OO, what-ever, etcl

* jokes and cartoons (these will only occupy a small portion of
the book)

* suggestions for a better name for the collection

Contributions will be judged on clarity, insignificance, irrelevance, incorrectness, originality, but most of all for their ability to make the editor laugh. Authors should make their papers understandable to a broad audience - not too many `in-jokes' please.

Authors should submit three (3) copies (preferably double-sided) of the prospective article to the editor; people without access to a photocopier may submit a single copy. Electronic submissions are *not* encouraged.

Each manuscript should have a title page with the title of the essay, full name(s) and affiliation(s) of author(s), complete postal and electronic addresses, telephone number(s), and a 150 word summary.

Contributions must *not* exceed 4000 words (approximately 8 A4 pages typeset 10-point on 16-point spacing, or 12 pages if typewritten double-spaced). Shorter articles will be viewed more favourably than longer ones.

Previously unpublished material is preferred. Contributors of published material must have copyright to it. All contributors will be asked to sign a permission letter giving MIT Press the right to print the material but NOT transferring copyright.

Submissions must be received by April 3rd, 1993. Authors will
be notified of acceptance or rejection by July 1st, 1993. Full
versions of the accepted articles must be formatted according to MIT Press

conventions, and camera-ready copy must be received by the editor
by August 24th, 1993.

For further information, contact the editor:

Dr. Andrew Davison, Department of Computer Science
University of Melbourne, Parkville, Victoria 3052, Australia
Email: ad@cs.mu.oz.au Fax: +61 3 348 1184 Tel: +61 3 344 7207 / 5230
Telex: AA 35185

Summary of Important Dates:

April 3rd, 1993:   Due date for 3 copies of submission
July 1st, 1993:   Notification of acceptance
August 24th, 1993: Due date for final manuscript
Early 1994:   Publication

[If you submit something that you saw in RISKS, which even I shall
probably do, you might be very careful to indicate all of the
indicated sources -- including RISKS... Good luck! PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 12

Monday 30 November 1992

Contents

Laser Printer Sucks up Cat

Douglas M. Kavner <0028017@msgate.emis.hac.com>
Mon, 30 Nov 92 12:51:19 PST

Danger from personal computers? Most people think of electromagnetic fields or getting zapped while monkeying around inside the box. Nothing immediately threatening could happen while just printing a spreadsheet. Right?

That's what I thought until last week when my wife was severely bitten by our kitten as it was hanging in mid-air by the tip of its tail. It all started so innocently. Our 8-month-old kitten likes to lie on top of our Apple Personal LaserWriter LS. We have tried to get him off, but he keeps getting back up on it. He must like the hum. My wife was printing a few pages in the background. While she was talking on the phone, there suddenly was a shriek from the kitten. The printer was only about 2 feet away from her, luckily turned the opposite direction. The kitten was sprawled stiff on top of the printer, like he had been stuffed. We just had him declawed, but his teeth were grabbing at anything in sight, including my wife's arm as she tried to turn off the printer. The party on the other end of the phone thought that both the kitten and my wife were being murdered.

After a few deep bites, the printer was off, but the tail was still stuck in the top roller that ejects the paper from the printer. Apparently, the hair on the tip of his tail had gotten inside the roller and was sucked in as the paper was being fed out. While my wife was getting a towel to prevent further injury, the kitten jumped off the side of the printer. The top of the desk is slightly waxed and the printer nearly slid off. It would have landed on top of him. Can you imagine how hard it is to figure out how to open a printer under these conditions? Before she got the towel around him, the kitten took a few more deep bites out of my wife's leg through her bluejeans! After what must have seemed like an eternity, my wife got the printer open and freed the kitten.

A $27 trip to the vet informed us that we had a real lucky kitten. If he had been a little older and heavier, the tail would have separated and required amputation. If he still had claws, my wife would have had to have been stitched back together. What if it had been a child's long hair?

So Apple, how about a Kitty Guard? Unfortunately, Cats don't read the generic warnings that came with the printer. I really like the quality and value of the printer. How much extra would I pay for more safety? At least $27. I knew I was cutting corners when I bought the printer since it did not include PostScript, but I really didn't expect this.

Several other companies also use the same type of printer case. They all have a max speed of 4 pages/minute and a cut-out in the top for the paper to reverse stack or innocent kitties to take a nap. Some have different paper feed mechanisms, so the eject roller may also vary.

In case you were wondering, the kitten has been avoiding the printer the last few days, but was seen standing on it once while it was off.

Doug Kavner, Hughes Aircraft Company, P.O. Box 3310, Fullerton, CA 92634
0028017@msgate.emis.hac.com (714) 732-3682

[Also posted to comp.sys.mac.hardware . This version edited by PGN,
who notes that there is a risk for children's fingers as well.
Perhaps the sportier models should have scroll-bars.]

British Telecom find themselves being a phone pest

David Shepherd <des@inmos.co.uk>
Mon, 30 Nov 1992 11:10:37 +0000 (GMT)

A short news article in a weekend newspaper told how a woman was woken by a mysterious phone call at 4:30am every day. She reported it to British Telecom who monitored the line for several months to track down the phone pest ... and eventually discovered that the calls were due to a programming error in one of their own test computers!

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 625
inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

Editorial: "The risk is not obvious"

Don Norman <norman@cogsci.ucsd.edu>
Mon, 30 Nov 1992 10:12:24 -0800

This is an editorial comment against the tendency among Risks contributors to take a rather simplistic view of things.

I assume that Risks readers shudder when they read a description of some new technological advance that ends with the phrase "the benefits are obvious." You should. But you should shudder equally at the complimentary phrase "the risks are obvious." (Sometimes this seems to be said only in order to justify submission of an article and get it past the eagle eyes of our esteemed moderator. It is as if the person says, "I came across the following cute story I wish to share. Why Risks? Oh, well, umm, the risks are obvious." Not to me.)

Not only are the risks not always obvious to me, but I worry about the risk of believing that complex things can be judged along simple, uni-dimensional values. The risk of the alternatives, including that of not doing anything, must also be weighed (here I simply repeat Brint Cooper's plea that people who submit such claims should do a more thorough analysis)

Life is complex. Life presents us with a series of tradeoffs: each benefit comes along with some risks. And many risks come along with some benefits. We are doing society no favors if we simply emphasize the risks instead of a more careful -- and more difficult-- analysis of the tradeoffs, both good and bad. You might still conclude that the item in question is dangerous and immoral: the careful analysis will then strengthen the claim.

There was a similar over-simplistic view of things in the recent discussion of the inability of people to perceive the correct odds for low-probability risks. Readers rushed in with well-intended, but simplistic solutions. In fact, people -- most people, including you, very sophisticated risk readers, cannot properly judge these low probability events. This is well known in the professional field that deals with these events -- even those professionals have problems. Human psychology simply cannot match probabilities in the 10^-3 to 10^-6 range with everyday experiences. Not only that, but it is well known in cognitive science that human memory and decision making is biased toward particular events and does not do a good job of matching real probabilities. In fact, it is probably a counter-productive evolutionary strategy to do so.

Describing one unlikely event as being similar or more or less risk than some other low-probability event (that we similarly cannot understand the risks of) helps, but does not solve the difficulty.

Everyone is an expert in folk psychology, for everyone has observed themselves -- and others -- for their entire lifetime. Alas, folk psychology often has little to do with real psychology. Risks at times seems to degenerate into a field day for amateur psychologists, where professionals in one discipline -- who understand that it took years for them to reach that level of sophistication in their chosen field -- ignore that a similar level of commitment and level of expertise is required to make professional judgments in the human sciences.

Sorry for the editorial. I like Risks, but at times I wish it had a higher level of professional standards. [I make the above statements wearing several hats: professional debunker of technology; professional praiser of technology; Professor Psychology and former chair of a psych department; former member of a team doing of nuclear power plant probability risk assessments (I was the expert on human reliability -- the result of this exercise was to completely distrust all such exercises, while admitting that I couldn't think of any better method).]

Don Norman
 Cognitive Science; University of California, San Diego; La Jolla, CA 92093
  Internet: dnorman@ucsd.edu   Bitnet: dnorman@ucsd   AppleLink: dnorman
After January 1, 1993: Apple Computer, Cupertino, CA

Re: Obvious Risks? (Cooper in RISKS-14.10 on Mestad in RISKS-14.06)

Rex Black <rex@iqsc.com>
Mon, 30 Nov 92 11:41:34 CST

> "The RISKS seem obvious enough to me..."
>
> I grant the risk. Again, however, I make a plea for identifying the risk of
> NOT doing something like this...

I do not believe we should talk or think in terms of all-or-nothing propositions on this issue. First, a computerized driver-advisory system is a very different kettle of fish than a computer-driven car, since the advisory system is passive and can not through its actions kill anyone. Second, computer-driven cars would pose a number of risks to the public socially in terms of law enforcement and other Big Brother problems. I do not believe that a computer-driven car solves many problems that a computer advisory system could not, and it creates a whole slew of new problems that a passive system can't.

Rex

How can we deal with name confusions?

Don Norman <norman@cogsci.ucsd.edu>

Mon, 30 Nov 1992 10:12:47 -0800

This is a request for solutions. A recent Risks article pointed out the confusion in databases when people had the exact same names and birthdate. In this case, the contributor stated:

"The scary part is the quote attributed to Lt. Gerard Blouin of the Montreal Police:
'it's up to him to change his name somehow. If he can modify his name,
just by adding a middle initial or something, it would help him.' "

Well, in this case, I sympathize with the police. Let me ask all of you folks -- how should society deal with this? I believe myself to be one of the most fervent publicists of the notion that technology must adapt to people, but there are some real problems to be faced that technology cannot solve. Names are not just for the benefit of the individual: they are also to benefit society. Asking people to select unique names doesn't seem all that outrageous.

Names, you realize, are a technological invention to make it easy to identify people uniquely. At first, people only had single names. This didn't work beyond the village level: hence longer descriptions that eventually became standardized as last names (well, family names, which is some cultures are written first). Middle initials were part of the attempt to fully describe the lineage, and they also helped discriminate among otherwise similar names.

Today, with world-wide commerce, full names are not enough. So we now use longer descriptions to identify people: sometimes full name plus birthdate; or full name plus parents' full names plus birthdate and birthplace and ....? The problem with all these schemes is that they are arbitrary. Without standards, they simply lead to chaos. And without standards there are bound to be more confusions. But standards are easy to abuse, to turn into national identification numbers for evil purposes. Some countries use unique identification numbers, assigned at birth (in the US, the social security number is more and more serving this purpose, regardless of the legality of such usage). Many rebel against some universal identification number -- and for good reason -- but there are cases where they would really come in handy, cases where they are really essential. What are the alternatives?

In the case before us, asking each person to get a middle name is a temporary fix. It won't always work -- I happen to know of at least one other person with the same name as I have -- including middle name (although not the same birthdate). With billions of people in the world, amazing coincidences will happen, even ones that have a probability of "one chance in a billion."

Would a world-wide registry for names work? Supose that before I can assign a legal name to a newborn child (or change the name I already have), I must check it out with the registry. The risks of this are obvious (isn't that a wonderful phrase?), but so are some of the benefits. It can even work smoothly: In California: I can assign myself any license plate I want as long as it is less than 7 characters, not confusable with others, and not on the socially-prohibited list. I think of a possible name, the name gets typed into a computer, and I am told immediately whether or not I may have it. Several tries later, I have my choice. Suppose the database only contained names, no other personal information. Perhaps a successful database entry would give me a certificate or other authorization that I had permission to use that unique name, but suppose that was it -- the database wouldn't even know who had made the request -- just the fact that the request had been made (it would obviously know the location of the terminal as well). Would such a scheme work for names?

This is a serious request. how can we invent unique identifiers for people that:
1. Make it easy to select a name
2. Work for an entire country and potentially scale to the entire world
3. Do not violate civil liberties
4. Do not make it possible for others to misuse the system

In other words, how to we get the benefits and avoid the risks?

Don Norman
Cognitive Science; University of California, San Diego; La Jolla, CA 92093
Internet: dnorman@ucsd.edu   Bitnet: dnorman@ucsd   AppleLink: dnorman
After January 1, 1993: Apple Computer, Cupertino, CA

Name confusion is problem confusion

Jerry Leichter <leichter@lrw.com>
Mon, 30 Nov 92 17:20:58 EDT

In a recent RISKS, Stanley Chow reports on yet another case of "name confusion": One Steven Reid of Montreal has been repeatedly confused with another person of the same name, with the same birthday, living in the same city. He describes as "scary" a quote attributed to a police officer suggesting that it was up to Mr. Reid to "change his name somehow", say by adding a middle initial.

The problem of name confusion is neither new, nor related to computers, and I for one find nothing scary or in any way troubling in the police officer's suggestion. Any society has to have a way to identify individuals. At one time, when the scale of society was small, a single name, plus perhaps a city of origin, or a parent's name, or a job name, was enough identification. Even when it wasn't, most transactions were of a personal nature, and if I personally knew both "John of Dullville"'s, it really made no difference to me that they had the same name.

Later, as the scale of society grew larger, the ambiguities became more of a problem. We began to use two names, initially just as a conventional form of the older identifications by parent (in names like "Johnson") or by social role (names like "Baker" and "Smith"); later simply as link to a family within which one could probably assume that first names would not be re-used too often, at least within a locale and generation.

Today, the scale of society is global and "first and last name" has long become useless as a unique identification. There are not all THAT many additional natural identifying features we can use. Adding the full birth date is actually quite good; sometimes mother's maiden name is useful. But where can we go beyond that? Use the address, hearkening back to the old "John of Dullville"? In today's mobile society, that's not a very useful identification marker. Should Mr. Reid perhaps identify himself as "Steven Reid the taxi driver" (or whatever he is)? People change jobs much more than they once did, too.

Computer technology has helped us create and maintain a very large-scale society, in which we long ago stopped relying on personal contact as a reliable means of identification - we can't possibly personally know all the people we will have to interact with. The ambiguity of names is a result of that social change, not of computers; it would appear in exactly the same form in manual databases. Just let them be large enough so that their users have no personal knowledge of the people described, a threshold that was probably crossed a hundred or more years ago.

There's an easy solution to the name ambiguity problem: Just assign everyone a unique id number. This is a trivial thing to do, with or without computers. We could even make the id "number" be a pronounceable sequence of letters, or of words. Hell, we could even use first a last names, just requiring a check of the database to make sure they are unique.

Many organizations have used this solution for years, with great success, ranging from the military of any country you want to name to, say, any large health care system, private or government-run. In the US and Canada, we have for various cogent reasons chosen not to use this solution, at least not for a wide variety of interactions we have with government: When identifying ourselves to the police, we expect to be able to use our names, not our "national ID numbers".

Any choice has costs. The fact that one does not like the alternative of a national ID number does not make the costs of using our traditional naming system go away. At one time, there was a significant monetary cost in keeping and looking up records under alphabetic names. The power of today's computer systems makes that irrelevant - but the underlying ambiguity hasn't gone away, and WON'T go away. As long as it is there, as long as "Steven Reid, born on xx/yy/zzzz" is unrealistically expected to uniquely identify an individual, these problems will continue to arise. No solution can possibly exist without Mr. Reid's cooperation: If he stands by his insistence that "Steven Reid, born on xx/yy/zzzz" is all the identifying information he will give, he cannot expect to be distinguished from the other Mr. Reid who just as adamantly insists on his right to identify himself in the same way.

Living in a society has both benefits and costs. Since Mr. Reid, as a member of society, has chosen the benefits of a police record system that does not require us to provide our national ID number, or perhaps even a set of finger-prints, on demand, he will necessarily bear the cost of somehow distinguishing himself from his doppelganger. No one else can possibly do it for him.

Jerry

Electronic Banking Risks

Ross Anderson <rja14@cl.cam.ac.uk>
Mon, 30 Nov 92 14:46:31 GMT

The Sunday Times (London) yesterday printed a piece about how easy it was to get hold of people's bank and credit card statements.

They paid 200 pounds a time to private detectives for personal dossiers on cabinet ministers, including their addresses and private telephone numbers, and their last few months' transaction details.

This is highly security sensitive information: if you are an IRA sympathiser and want to blow up the UK minister of defence, it is quite useful to know what his favourite restaurant is.

With a bit of luck, the government will now take its own legislation seriously. I understand it is an offence for the various banks to make client information available to unauthorised persons in this way, and indeed the negligence of the UK banks about computer security is well known.

Essentially, by making account enquiry facilities available to tens of thousands of low-level staff, the banks make it virtually certain that there will be at least one bent staff member who has access and who is prepared to sell the information on to private detective agencies.

In France, on the other hand, at least one bank I know of has a system which rings a silent alarm whenever a staff member makes an enquiry about an account held at another branch. Anyone who started selling the database would be caught quickly.

In Britain, on the other hand, they even have the cheek to charge you if you draw funds at another branch.

Not everybody in government was unaware of this abuse: it was mentioned in the newspaper article that the head of MI6, Sir Colin McColl, and the head of MI5, Stella Rimington, had taken measures to ensure that their own bank accounts could not be read (maybe they bank in France).

The abuse was also well known here at Cambridge: a speaker described it at our fraud seminar about a month ago, before it was even a story in the press.

What odds will you give me on any of the bank directors going to jail? I'm sure that if I, rather than the banks, had leaked this sort of information, I'd have got ten years under the Prevention of Terrorism Act, and another stretch under the Data Protection Act. Still, there's one law for the rich, as they say, and another for us poor dogs.

May I suggest that next time you write to your bank manager, you demand that he gives you a list of all persons (by name) who have access to your account details? If enough people ask for this, it might make a difference,

Ross Anderson

Re: How Is Technology Used for Crime ... (Sherizen, RISKS-14.11)

<fofp@castle.edinburgh.ac.uk>
Mon, 30 Nov 92 14:39:44 WET

>"Call girls" and obscene callers ...

>Any ideas, reactions to these comments, and suggestions of any social
>historical studies about these issues are welcomed...

These two paragraphs conjoined have suggested a likely area of crime. Once comms bandwidths improve enough to start sending videophone around the world, it'll be pretty easy to ship any sort of information.

Now obviously a lot of governments don't want certain sorts of information to get around. There are the more obvious political sorts of information which totalitarian governments don't want spread around, but the same thing applies to more mundane sorts of info like pornography.

There's already been a few press scares about pornography and obscene gifs on usenet. In the uk it's illegal to import pornographic videos or magazines, where the government idea of pornography more or less amounts to having two naked people in the same picture.

Naturally, since this is illegal in the uk, and legal in continental europe, folks import these for the high prices you can obtain on illegal items.

At the moment though, importation amounts to actually carrying magazines, or video masters through customs with the consequent risk of being searched, caught, and arrested.

However, with higher bandwidth comms in the future, there's no real reason why they couldn't just mail the digitised files over and produce the videos (or magazines?) from the files. Since these files could also be encoded, it'd be damned difficult, if not impossible, to detect.

A mundane, though profitable, sort of crime, and not dissimilar to your "call girls" example above.

On the plus side, it's gonna be a lot harder for governments to control information.

FoFP

SNL accidentally informs people about risks of caller ID

Sean Eric Fagan <sef@kithrup.com>
Mon, 30 Nov 92 1:46:27 PST

For reasons I still don't fathom, I was watching Saturday Night Live this week. It was a repeat from a year or so ago.

One of the skits was a commercial spoof. A man in an obviously cheap hotel room dials a number from a phone book, and says, 'Mrs. so and so? At such-and-such address?' The other person, a woman, said yes, and the man replied, 'You have won a free trip to the Bahamas. We just need a credit card number to verify who you are.' Classic scam, right?

The woman then asks for his phone number, and the guy hesitates. She then says, not to worry, I already have it, and presses a button on a little thing next to her phone, and then reads the guy's phone number back to him.

He hangs up, and then says, "Hm. She knows my phone number. I guess I'll have to kill her now."

Fade to black, and a logo that says "U S FON -- Maybe we're the right choice," with a voice-over of something like, "We don't have it, so maybe we are the right choice."

All in all, I think it did a passable job, accidentally, of pointing out a risk of caller-id.

Sean Eric Fagan sef@kithrup.COM

Re: Nuclear plant risks (Dolan, RISKS-14.11)

Victor Yodaiken <yodaiken%chelm@cs.umass.edu>
Mon, 30 Nov 92 19:10:39 -0500

Brad Dolan <71431.2564@compuserve.com> repeats some commonplaces from nuclear industry advertising to the effect that the costs of nuclear power have been vastly inflated by the costs of citizen intervention in licensing. RISKS is not the place for a debate on nuclear power economics, but I don't want to let this dubious claim pass unchallenged. The book "Safety Second" by the Union of Concerned Scientists presents a strong case for the contrary opinion.

Mr. Dolan concludes as follows:

>I would like to see a comparison of safety benefits (in terms of expected
>lives saved, property saved, or whatever) resulting from intervenors'
>interventions with the safety detriments which have resulted from increased
>electrical bills.

This is a rather naive plea, in my humble opinion and technological innocence is a significant source of risk. Risk assessment is at best a very inexact science, and there are zero grounds for believing that such a comparison would illuminate anything more than the presuppositions of the assessor. For a survey of the complexities involved in risk assessment for nuclear power, see the Brookhaven/EPRI workshop on "Health and Environmental Risk Assessment" (Pergamon Press, 1985).

Victor Yodaiken yodaiken@chelm.cs.umass.edu

◀ ▲ ▶ ℹ ✎

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 13

Weds 2 December 1992

Contents

Blackmail risk in thefts from general practitioners

Paul Leyland <pcl@ox.ac.uk>
Wed, 2 Dec 92 10:50:43 GMT

Blackmail risk from GP thefts (The _Times_ (of London), 2 Dec 1992)

A sharp rise in the theft of computers from doctors' surgeries has led to increasing numbers of patients' medical records falling into the hands of burglars and potential blackmailers.

In the past six months, the number of general practitioners seeking advice from the office of the data protection registrar after the theft of a surgery computer has risen by nearly 700 per cent. Officials fear that files could include information about public figures that buyers of stolen computers might use maliciously.

The office, based in Wilmslow, Cheshire, has heard of 20 thefts during the past six months but believes there are many more as holders of personal, electronically held information are not legally required to report a theft. Previously there had been about six thefts a year.

The Data Protection Act's eighth principle does, however, require GPs to have tight security to protect patient records held on computers. Eric Howe, the data protection registrar, yesterday warned GPs to review their security.

PCL's comments:

There are a number of interesting observations to be made on this report. First is the classic scare-statistic fallacy. A 700% increase sounds dramatic, and is doubtless significant. However, an increase from three to twenty is much less startling.

More important, is the lack of any requirement to notify the authorities of the theft of equipment containing personal information. If this is really the case, it would appear to be a serious loophole in the Data Protection Act. As I understand it, the implication is that you are only responsible for the security of your data until your security measures are broken!

Finally, one must seriously ask: why was the data not encrypted? I strongly suspect that the thefts are for the equipment, not the data. If all data were DES-encrypted (for example), at the very least it would be protected from the prying eyes of amateur thieves. Let me re-phrase that: (possibly) professional thieves, but amateur cryptanalysts. I'm prepared to bet a small sum, at moderate odds, that the database systems that are in common use do not have easily used encryption, designed for reasonable security but for use by non-experts in cryptology.

Perhaps a requirement for databases to be used by GPs and the like is the automatic encryption of all records held on disk. Only government action could force such a requirement.

Computerized Voting

Doug Hardie <doug@kronos.nisd.cam.unisys.com>
Wed, 2 Dec 92 10:30:04 PST

During the entire 5 years of undergraduate work at San Jose State, I was a member of the marching band. Each year the Band-Aides, a group of 8 or so young ladies who danced with the band, sponsored one of their members for homecoming queen. Each year, that young lady won the election. I found that quite interesting since there were only 120 men in the band and a few additional hanger ons in a 20,000+ person student body.

I also ran the college computer center for the last 3 years and had the "honor"of opening up the computer center for the committee that counted the votes for the homecoming queen election. Each ballot consisted of one mark-sense card from which one nominee was selected. The cards were run through an IBM 519 to convert the pencil mark to one punched hole on the card. A special program was written, author unknown, to count the votes and determine the winner. The entire counting process started about 1800 hours and ran until about 2200 hours.

The first year I watched this process, one of our journalism students managed to get one of the San Francisco TV stations to run a live special about this unusual use of computers. So the main part of the computer room was filled with the TV crew and their equipment. Not wanting to be part of the show, I retreated to a separate room to the side of the computer that had window access to see the computer console. Near the end of the count, while the journalism student was describing the process live on TV, the computer "crashed". I was not able to determine why, but the program was used for other similar counting tasks without problems. However, not all was lost. The operator stated that he had just looked at the counts and knew what they were. He would restart the program, restore from memory the counts, and the counting could continue as if nothing had happened. A big deal was made about how a human had saved the day.

About that time I recognized the operator as a fellow band member. Sure enough, our candidate won with a resounding margin.

Global Positioning System - Position Errors

Stuart Bell <stu@national.mitre.org>
Tue, 1 Dec 92 08:22:15 EST

Several weeks ago, I completed a 2000+ mile offshore trip to relocate my home, a 36 foot Pearson sloop, the Shearwater, from Houston, Texas to Washington DC. Just prior to the trip, I purchased a Magellen Global Positioning System (GPS) receiver as an aid to navigation. The Shearwater is already equipped with a Micrologic Loran, so, in a sense the GPS was a backup - and the Loran was already a backup to Dead Reckoning - and a sextant.

Somewhere off Port Eads in the Gulf, the GPS began reporting high speeds (70+ knots) and a position far from my current location. I contacted the Coast Guard to request a GPS report - and they had no indication of errors. After some discussion to assure them that I was in no danger - and knew where I was, I logged the incident and was about to go back to sleep.
[others were on watch]

Five other boats contacted me to report that they, also, were seeing GPS position and velocity errors. I recontacted the Coast Guard to tell them it was probably not my receiver - although I neglected to ask the others if they were on different receivers. They were unable to accept a report and forward it to GPS control for conformation.

What is the risk? For a boat using GPS for navigation (that is long-range position confirmation), the risks are small, especially with sufficient backup devices). Since the outage only lasted about 3 hours and I only went about 18 miles during that time, the inconvenience was very minor. Suppose, however, I had been piloting - rather than navigating - that is entering a harbor or avoiding an obstruction with only a small margin of error. And suppose, also, I had only one means of navigation and had not maintained an accurate dead reconing plot - the normal case for most recreational sailors - and apparently major oil tankers. Well, this could have been a more serious incident.

Now, suppose I was an aircraft depending on GPS for navigation. Even if you don't use it as the sole means of navigation, GPS (or Loran) is so friendly, so precise, and correct so often that is very easy to fall into the trap of believing it when it is incorrect.

The risk, I believe, is twofold. First, the Coast Guard was not aware of the outage and once informed had no means of informing others or the GPS control station. Loran outage reports are accepted, coordinated, rebroadcast and followed up by the Coast Guard first getting the report.

Second, unlike Loran, my GPS (and the others operated by the folks I spoke with), reported correct operation, high accuracy, and acceptable performance - that is good geometric separation. Thus, if you were flying and were reported in a place different than you believed, you might believe the report - especially since it was, in one of the cases, close enough to be believable under flying speeds/conditions.

I see a problem in the making and don't know who to tell. /Stu Bell

Stuart Bell, MITRE Corporation, Z646, 7525 Coleshire Drive, McLean, VA 22102
stu@MITRE.ORG 1-703-883-1276 Fax: (703) 883-5519

Re: Laser Printer Sucks up Cat (RISKS-14.12)

Dan Sorenson <viking@iastate.edu>
Tue, 1 Dec 1992 04:41:02 GMT

... It does behoove us, from a safety standpoint, to correct what are known as "insidious hazards" around the home and office. Doug mentions the eject roller on his laser printer. My own suggestion is to take a plastic car windshield scraper that has the nylon bristles for removing snow, cut the handle with the bristles to length, and glue it to the top of the printer ejection area. The paper easily pushes under the bristles, but little to nothing penetrates them when trying to enter that area. I've done this on my Imagewriter II when I discovered a curious ferret had lost whiskers when inspecting the printing head as it whipped back and forth. Cost? $1.95 or so at Kwik Shop.

If you have long hair, such as I, a piece of nylon cut from some ladies hosiery and taped over the fan exhaust will do little to impede air flow and does work well to keep hair from being chewed up. If it is placed on the input side, it also makes a dandy dust filter. For those with metal desks or work benches, did you run a ground strap off the desk before playing with that flakey monitor? As my Occupational Safety instructor would pound into us, "It's the little things that'll get you!" Luckily, most of these are very inexpensive and quite simple to fix. In some companies, such fix suggestions are worth their weight in gold as they lower insurance premiums and prevent injury downtime.

To best see just how sly and innocuous these hazards can be, I suggest reading a book for new parents that goes into detail on how to child-proof the home. Many of these things apply to offices as well. Your friendly OSHA representative, next time he stops by, will also be happy to point out hazards that might not be covered under OSHA regs.

Dan Sorenson, DoD #1066 z1dan@exnet.iastate.edu viking@iastate.edu

Smokey is not always a bear

<ctsx!ctsx!alan@uunet.uu.net>
Tue, 1 Dec 92 10:10 PST

The November 30th issue of _AutoWeek_ details the risks of using radar to prevent bus accidents.

Greyhound has developed a system called VORAD to warn a bus driver if there is a car hidden off his right or if he's following too closely. The problem is the system sends a radar signal 10 times a second. An _AutoWeek_ reader and bus driver reports that more than once he's been passed by a car moving at speeds in excess of the speed limit and watched their radar detector light go off. Unfortunately the speeder usually pulls in front of the nearest large target (you can guess what) and *slams on the brakes* to fool the non-existent Smokey. And, of course, busses go a lot better than they stop...

I find it funny that a system designed to prevent accidents could potentially cause accidents by encouraging other drivers to make unsafe maneuvers.

Alan Dahl, Cellular Technical Services 2401 4th Ave., Suite 808, Seattle, WA 98121 PH: (206) 443-6400 alan@ctsx.celtech.com ouunet!ctsx!alan

A310 Aerobatics

Karl Swartz <kls@ohare.chicago.com>
Tue, 1 Dec 92 13:58:49 PST

[This is from the latest issue of Airliners (Winter 1992); I'm amazed I haven't seen anything about the incident elsewhere. I'm posting the article to sci.aeronautics.airliners as well and will pass along any RISKS-related discussion that comes up there. KS]

A310 Aerobatics

Following an autopilot-coupled go-around, the pilot attempted to counteract the autopilot's programmed pitch-up by pushing forward on the control column. (In most circumstances pushing on the control column disengages the autopilot but automatic disconnect is inhibited in go-around mode. The autopilot should be disconnected or a mode other than go-around should be engaged through the FCU - Flight Control Unit.)

As a result of the control inputs, the autopilot trimmed the stabilizer to -12 degrees (nose up) to maintain the go-around profile, but the elevator was deflected 14 degrees (nose down). After climbing about 600 feet (to around 2,100 feet) the autopilot captured its preselected missed approach altitude and disconnected as the go-around mode was no longer engaged. In the next 30 seconds, the grossly mistrimmed A310 pitched up to 88 degrees and airspeed dropped to less than 30 kt. (The stall warning activated then canceled itself as the airspeed fell below usable computed values and the autothrottle system dropped off.) At 4,300 feet, the A310 stalled, pitching down to -42 degrees while the pilot-applied control inputs showed full up elevator. Airspeed increased to 245 kt then the aircraft bottomed out at 1,500 feet, pulled +1.7 g, then climed rapidly.

The second pitch-up reached 70 degrees followed by a stall 50 seconds after the first. The nose dropped to -32 degrees and airspeed rose to 290 kt and the aircraft bottomed out at 1,800 feet. On the third pitch-up (to 74 degrees), the A310 climed to 7,000 ft then stalled again, about 60 seconds after the second stall. This time airspeed reached 300 kt in a -32 degree nose down attitude before the aircraft leveled off at 3,600 feet.

The fourth pitch-up reached 9,000 feet but this time the crew's use of thrust and elevator control (and very likely retrimming the stabilizer) prevented a stall and the A310 leveled off at 130 kt. Speed then increased accompanied by another milder pitch-up to 11,500 feet where control was eventually regained.

All aircraft systems operated in accordance with design specifications. The reaction of ATC (the incident happened at Moscow) or the passengers is not recorded.

Karl Swartz, 2144 Sand Hill Rd., Menlo Park CA 94025, USA 1-415/854-3409
kls@ditka.chicago.com   uunet!decwrl!ditka!kls
Send sci.aeronautics.airliners submissions to airliners@chicago.com

New Distributed Systems Engineering Journal

Morris Sloman <mss@doc.ic.ac.uk>
Wed, 2 Dec 92 16:32:38 GMT

DISTRIBUTED SYSTEMS ENGINEERING JOURNAL --- Call for papers

A new journal on all aspects of the architecture, realisation and management of distributed computing systems, for practising engineers and researchers in the field.

First issue July 1993

Co-published by The British Computer Society, The Institution of Electrical Engineers and Institute of Physics Publishing

Honorary Editors

Professor David Hutchison, Lancaster University, Department of Computing, Bailrigg, Lancaster LA1 4YR, UK. Tel: + 44 524 593798 Fax: + 44 524 381 707

Email:dh@comp.lancs.ac.uk

Dr. Rafael Alonso, Matsushita Information Technology Laboratory
182 Nassau Street, Princeton, New Jersey, 08544 USA
Phone: + 1 609 497 4600 Fax: + 1 609 497 4013 Email: alonso@mitl.com

Dr Morris Sloman, Imperial College of Science, Technology and Medicine,
Department of Computing, 180 Queen's Gate, London SW7 2BZ, UK. Tel:
+ 44 71 589 5111 ext 5040 Fax: + 44 71 581 8024 Email: mss@doc.ic.ac.uk

Editorial Board includes:

Dr Gordon Blair, Lancaster University, UK
Dr Brian Carpenter, CERN, Switzerland
Dr. Chris Cooper, Rutherford Appleton Laboratory, UK
Professor Flaviu Cristian, University of California at San Diego, USA
Mr Michel Gien, Chorus Systems, France
Professor Fred Halsall, University College Swansea, UK
Dr Peter Harrison, Imperial College, UK
Dr Ian Leslie, University of Cambridge, UK
Professor Peter Linington, University of Kent, UK
Professor Andrew Lister, University of Queensland, Australia
Professor Krithi Ramamritham, University of Massachusetts, USA
Professor Santosh Shrivastava, University of Newcastle, UK
Dr James Stamos, IBM Research Division, USA
Dr Ralf Steinmetz, IBM European Networking Centre, Germany
Dr Joseph Sventek, Hewlett-Packard Company, California, USA
Professor Mario Tokoro, Keio University/Sony CSL, Japan
Dr Ian Wilson, Olivetti Research Laboratory, UK

Scope

The area of interest of this journal centres on the integration of processing, storage and communication subsystems within a distributed or networked system. The emphasis will be on distributed rather than parallel processing and on practical engineering papers rather than theoretical approaches. We particularly welcome papers from industry and those which are based on implementation experience.

Distributed Processing

Distributed processing architecture
Distributed operating systems and environments
Standards and open distributed processing (ODP)
Configuration and management of distributed systems
Computer architecture support for distributed processing
Language support for distributed processing
Algorithms and protocols to support distributed processing

Computer Networks

Local, metropolitan and wide area networks
Network architectures and protocols
Network management

- Communications and network standards
- Open networking and open systems interconnection (OSI)
- Multiservice networks

Storage and Databases

- Data modelling
- Distributed data bases
- Distributed transaction processing
- Information retrieval and transformation
- Object stores
- Information and file servers
- Hypermedia systems

Information Systems & Applications

- Distributed multimedia systems
- Advanced home, business and industrial systems
- Computer support for cooperative work
- Distributed programming support environments
- User Interface design

These four main areas would be linked by consideration of system dependability, fault tolerance, security, performance engineering, timeliness or other architectural issues.

Submission Address

Submit five copies of papers for consideration to:

The Executive Editor, Distributed Systems Engineering Journal
The Institution of Electrical Engineers, Michael Faraday House
Six Hills Way, Stevenage, Herts. SG1 2AY UK
Phone: + 44 438 313311 Fax: + 44 438 742 840
Email: ieeproc@dm.rs.ch

If you need further details on the scope of the journal and other editorial matters, contact the Honorary Editors.

Brief guide for authors

Contributions will be considered for publication in Distributed Systems Engineering Journal if they have not been published previously and are not under consideration for publication elsewhere. They must be in English and should typically be 5000-6000 words in length.

The title page must include:
i) title of article,
ii) name(s) of author(s)
iii) address(es) of establishment(s) where work was carried out;
iv) short title of not more than 50 characters.
v) abstract of not more than 200 words.

Details of format for final submission will be provided for accepted papers. Authors who require more detail on presentation and style should consult the booklet Notes for Authors, obtainable free of charge from IOP Publishing at the address below or from the IEE.

Acceptance of papers for publication is subject to a peer review procedure and may be conditional on revisions being made in the light of comments from referees. However authors are solely responsible for the accuracy of statements in a paper.

There are no page charges, and 50 offprints of each article published will be supplied free of charge to the principal author.

Colour reproduction of illustrations is available but authors or their institutions are asked to pay the additional costs incurred over and above normal black on white reproduction. Authors requiring further advice are invited to contact: the Production Manager, IOP Publishing Ltd, at the address below.

Articles Submitted in Electronic Format

Articles can be submitted in Electronic format on IBM PC compatible or Macintosh Discs. The publishers can accept TEX source code. Authors who intend to submit final version in electronic format should still provide hard-copy versions for refereeing as normal.

For more details and specific guidelines on the preparation of articles in electronic format, please contact:

The Electronic Production Manager,
IOP Publishing Ltd, Techno House,
Redcliffe Way,   Bristol BS1 6NX, UK.
Tel 0272 297481; Fax: 0272 294218. Email: ioppl@gec-b.rl.ac.uk

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 14

Weds 2 December 1992

Contents

Akron BBS trial update!

David Lehrer <71756.2116@compuserve.com>
02 Dec 92 11:49:08 EST

Akron BBS trial update: Dangerous precedents in sysop prosecution

You may already know about the BBS 'sting' six months ago in Munroe Falls, OH for "disseminating matter harmful to juveniles." Those charges were dropped for lack of evidence. Now a trial date of 1/4/93 has been set after new felony charges were filed, although the pretrial hearing revealed no proof that *any* illegal content ever went out over the BBS, nor was *any* found on it.

For those unfamiliar with the case, here's a brief summary to date. In May 1992 someone told Munroe Falls police they *thought* minors could have been getting access to adult materials over the AKRON ANOMALY BBS. Police began a 2-month investigation. They found a small number of adult files in the non-adult area.

The sysop says he made a clerical error, causing those files to be overlooked. Normally adult files were moved to a limited-access area with proof of age required (i.e. photostat of a drivers license).

Police had no proof that any minor had actually accessed those files so police logged onto the BBS using a fictitious account, started a download, and borrowed a 15-year old boy just long enough to press the return key. The boy had no knowledge of what was going on.

Police then obtained a search warrant and seized Lehrer's BBS system. Eleven days later police arrested and charged sysop Mark Lehrer with "disseminating matter harmful to juveniles," a misdemeanor usually used on bookstore owners who sell the wrong book to a minor. However, since the case involved a computer, police added a *felony* charge of "possession of criminal tools" (i.e. "one computer system").

Note that "criminal tool" statutes were originally intended for specialized tools such as burglar's tools or hacking paraphernalia used by criminal 'specialists'. The word "tool" implies deliberate use to commit a crime, whereas the evidence shows (at most) an oversight. This raises the Constitutional issue of equal protection under the law (14th Amendment). Why should a computer hobbyist be charged with a felony when anyone else would be charged with a misdemeanor?

At the pretrial hearing, the judge warned the prosecutor that they'd need "a lot more evidence than this" to convict. However the judge allowed the case to be referred to a Summit County grand jury, though there was no proof the sysop had actually "disseminated", or even intended to disseminate any adult material "recklessly, with knowledge of its character or content", as the statute requires. Indeed, the sysop had a long history of *removing* such content from the non-adult area whenever he became aware of it. This came out at the hearing.

The prosecution then went on a fishing expedition. According to the Cleveland Plain Dealer (7/21/92)

"[Police chief] Stahl said computer experts with the Ohio Bureau of Criminal Identification and Investigation are reviewing the hundreds of computer files seized from Lehrer's home. Stahl said it's possible that some of the games and movies are being accessed in violation of copyright laws."

Obviously the police believe they have carte blanche to search unrelated personal files, simply by lumping all the floppies and files in with the computer as a "criminal tool." That raises Constitutional issues of whether the search and seizure was legal. That's a precedent which, if not challenged, has far-reaching implications for *every* computer owner.

Also, BBS access was *not* sold for money, as the Cleveland Plain Dealer reports. The BBS wasn't a business, but rather a free community service, running on Lehrer's own computer, although extra time on the system could be had for a donation to help offset some of the operating costs. 98% of data on the BBS consists of shareware programs, utilities, E-mail, etc.

The police chief also stated:

"I'm not saying it's obscene because I'm not getting into that battle, but it's certainly not appropriate for kids, especially without parental permission," Stahl said.

Note the police chief's admission that obscenity wasn't an issue at the time the warrant was issued.

Here the case *radically* changes direction. The charges above were dropped. However, while searching the 600 floppy disks seized along with the BBS, police found five picture files they think *could* be depictions of borderline underage women; although poor picture quality makes it difficult to tell.

The sysop had *removed* these unsolicited files from the BBS hard drive after a user uploaded them. However the sysop didn't think to destroy the floppy disk backup, which was tossed into a cardboard box with hundreds of others. This backup was made before he erased the files off the hard drive.

The prosecution, lacking any other charges that would stick, is using these several floppy disks to charge the sysop with two new second-degree felonies, "Pandering Obscenity Involving A Minor", and "Pandering Sexually Oriented Matter Involving A Minor" (i.e. kiddie porn, prison sentence of up to 25 years).

The prosecution produced no evidence the files were ever "pandered". There's no solid expert testimony that the pictures depict minors. All they've got is the opinion of a local pediatrician. All five pictures have such poor resolution that there's no way to tell for sure to what extent makeup or retouching was used. A digitized image doesn't have the fine shadings or dot density of a photograph, which means there's very little detail on which to base an expert opinion. The digitization process also modifies and distorts the image during compression.

The prosecutor has offered to plea-bargain these charges down to "possession" of child porn, a 4'th degree felony sex crime punishable by one year in prison. The sysop refuses to plead guilty to a sex crime. Mark Lehrer had discarded the images for which the City of Munroe Falls adamantly demands a felony conviction. This means the first "pandering" case involving a BBS is going to trial in *one* month, Jan 4th.

The child porn statutes named in the charges contain a special exemption for libraries, as does the original "dissemination to juveniles" statute (ORC # 2907.321 & 2). The exemption presumably includes public and privately owned libraries available to the public, and their disk collections. This protects library owners when an adult item is misplaced or lent to a minor. (i.e. 8 year olds can rent R-rated movies from a public library).

Yet although this sysop was running a file library larger than a small public library, he did not receive equal protection under the law, as guaranteed by the 14'th Amendment. Neither will any other BBS, if this becomes precedent. The 'library defense' was allowed for large systems in Cubby versus CompuServe, based on a previous obscenity case (Smith vs. California), in which the Supreme Court ruled it generally unconstitutional to hold bookstore owners liable for content, because that would place an undue burden on bookstores to review every book they carry, thereby 'chilling' the distribution of books and infringing the First Amendment.

If the sysop beats the bogus "pandering" charge, there's still "possession", even though he was *totally unaware* of what was on an old backup floppy, unsolicited in the first place, found unused in a cardboard box. "Possession" does not require knowledge that the person depicted is underage. The law presumes anyone in possession of such files must be a pedophile. The framers of the law never anticipated sysops,or that a sysop would routinely be receiving over 10,000 files from over 1,000 users.

The case could set a far ranging statewide and nationwide precedent whether or not the sysop is innocent or guilty, since he and his family might lack the funds to fight this--after battling to get this far.

These kinds of issues are normally resolved in the higher courts-- and *need* to be resolved, lest this becomes commonplace anytime the police or a prosecutor want to intimidate a BBS, snoop through users' electronic mail, or "just appropriate someone's computer for their own use."

You, the reader, probably know a sysop like Mark Lehrer. You and your family have probably enjoyed the benefits of BBS-ing. You may even have put one over on a busy sysop now and then.

In this case; the sysop is a sober and responsible college student, studying computer science and working to put himself through school. He kept his board a lot cleaner than could be reasonably expected, so much so that the prosecution can find very little to fault him for.

[The original message from David contained a plea for contributions for an independent legal defense fund, with any overflow to EFF. RISKS does not include such solicitations here, so I have excised those paragraphs. However, if you are interested in further info, you may of course contact David, or else Mark directly. See below. PGN]

Help get the word out. If you're not sure about all this, ask your local sysops what this precedent could mean, who the EFF is--and ask them to keep you informed of further developments in this case. Please copy this file and send it to whoever may be interested. This case *needs* to be watchdogged.

Please send any questions, ideas or comments directly to the sysop:

Mark Lehrer
CompuServe: 71756,2116   InterNet: 71756.2116@compuserve.com
Modem: (216) 688-6383   USPO: P.O. Box 275, Munroe Falls, OH 44262

holiday reading on Risks

Phil Agre <pagre@weber.ucsd.edu>
Mon, 30 Nov 92 21:36:53 -0800

Here are two books that subscribers to RISKS may consider reading over the holiday vacation. Neither one is directly concerned with computers, but both are deeply concerned with the social management of risk, technological and otherwise. I think it would be well worthwhile exploring their consequences for our emerging understanding of computer risks.

Brian Wynne, Risk Management and Hazardous Waste: Implementation and the Dialectics of Credibility, Berlin: Springer-Verlag, 1987. This book is the report of a project at the IIASA in Vienna on the politics of regulation of hazardous wastes. This is a fascinating enough topic on its own, but what's particularly relevant about this particular study is its attention to the administrative dimensions of regulation and risk. Wynne et al spell out in a sophisticated and sustained way an argument already made by Charles Perrow and others, that "risks" are located not exactly in technologies but in the institutions (and by extension the larger cultures and social arrangements) that contain them. This view has many consequences (at least, several more than I had thought about myself), which Wynne explains with some force.

Lorraine Daston, Classical Probability in the Enlightenment, Princeton: Princeton University Press, 1988. This is a detailed and scholarly history of early modern mathematical ideas of probability. Though not really a social history, it focuses on the developing practices of life insurance, lotteries, and gambling, tracing the shifting ideas about the morality and rationality of these things. It was not until the early 19th century, for example, that insurance ceased to be understood as a variety of gambling. And Daston explores at length various explanations for the great slowness with which insurance companies came to use probabilistic models rather than individual interviews and judgements.

Her central argument, though, concerns the rise of the idea of large-scale statistical regularities. She says: "Whereas De Moivre took the order revealed in stable statistical frequencies as incontrovertible evidence that an intelligent agent was at work in the world, Poisson argued that such order was only to be expected; we should suspect divine tinkering only when it was absent. For the mathematicians, the clock no longer implied a clockmaker. The ascent of statistical regularities ultimately marked the decline of the reasonable man, as probability theory shifted its sights from the psychology of the rational individual to the sociology of the irrational masses (page 187)." "Consequently, the targets of persuasion also differed: Quetelet wanted governments to change their ways on the basis of his figures, not individuals. But both sorts of probabilistic rationality presupposed the stable, orderly phenomena that made calculation possible, even if they singled out different *kinds* of phenomena as quantifiable. Classical probabilists believed that judicial decisions, but not traffic accidents, were regular; their successors believed just the reverse (page 385)."

Phil Agre, UCSD

Re: Books on Probability (Mellor, RISKS-14.08)

Pete Mellor <pm@cs.city.ac.uk>
Tue, 1 Dec 92 11:02:29 GMT

Phil Earnhardt has pointed out that the two books I recommended in RISKS DIGEST 14.08:

"How to take a chance" by Darrel Huff, and

"Making Decisions", D.V. Lindley, John Wiley & Sons, 2nd Ed., 1985

are not listed in _Books in Print_ in the US.

Thanks for the information, Phil. Both books are fairly old, so may well be out of print.

The ISBN of Lindley's book is: 0 471 90803 7, in case that helps you to find it. I bought it through our local university bookshop about 2 years ago, so I'm surprised that it's out of print, but it's possible.

I don't have a copy of Huff's book to hand, so I can't quote you the ISBN.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

FME'93 Call For Participation and Programme

Peter Gorm Larsen <pgl@imada.ou.dk>
Wed, 2 Dec 1992 14:53:53 GMT

The FME'93 Symposium
Industrial-Strength Formal Methods
Call for Participation and Programme
19 - 23 April 1993

Supported by the Commission
of the European Communities (CEC)
Organized by Formal Methods Europe

1. Symposium Programme

The first FME Symposium will be held at Odense Technical College in Denmark, during the week of 19. to 23. April, 1993. It is being organised by Formal Methods Europe, as the successor to the last four VDM symposia, to promote the interests of users, researchers and developers of precise mathematical methods in program development. This symposium will focus on The Application of Industrial-Strength Formal Methods.

The symposium is divided into two parts for which registration, symposium fees and proceedings are separate. The first two symposium days consists of two parallel tracks with tutorials on formal methods. The last three symposium days offer presentations of refereed papers, in parallel with presentations of project experience reports, short presentations of tools and presentations of European projects dealing with formal methods.

The FME'93 symposium programme features 8 half-day tutorials, 32 papers, 3 invited talks, 6 project reports, 20 tool presentations and exhibitions.

The papers to be presented cover a broad range of interests: among the formal methods represented are VDM, Z, LOTOS, RAISE, and B. They also come from different backgrounds, both industry and academia, and from 15 different countries.

FME'93 will be an intense and important event, and you are advised to submit your registration as soon as possible.

2. Symposium Sponsors

The symposium would not have been possible without the very kind support and financial assistance of the associations and corporations listed below:

Scandinavian Airlines System (SAS)
Odense Steel Shipyard Ltd.
Deutsche System Technik
Fyns Telefon
Praxis
Lloyd's Register
DDC International
Space Software Italia
Computer Resources International (CRI)
ICL Data A/S (SUN Division)

3. General Information

Odense:
Odense is Denmark's third largest city in the center of Denmark's second largest island, the Isle of Funen. Odense celebrated its 1000th anniversary in 1988, and Danmark's famous fairy-tale writer, Hans Christian Andersen was born in Odense.
The symposium will be held at Odense Technical College (Odense Teknikum) which is located 4 kilometers from the center of town.

Special Events:
Tuesday evening there will be a reception at the City Hall where the Mayor will give a short speech. Wednesday evening there will be a reception at IFAD. On Thursday evening the symposium banquet is to be held in the Knights' Hall of Nyborg Castle.

Fee:
We offer you three packages for this symposium:

Tutorial package: 2000 DKK (late registration 2500 DKK)
incl. tutorial material and reception at Odense City Hall.
Conference package: 2800 DKK (late registration 3300 DKK)
incl. conference proceedings, reception at Odense City Hall, reception at IFAD and the symposium banquet.
Symposium package: 4300 DKK (late registration 4800 DKK)
incl. both tutorial material and conference proceedings, reception at

Odense City Hall, reception at IFAD and the symposium banquet.

All packages in addition contain coffee and cookies at breaks and lunch at Odense Technical College, local transport to/from hotels and a free telephone card worth 50 DKK.

If it becomes necessary to cancel a reservation, this must be done in writing to KongresBureau Fyn before April 1th 1993 to obtain a refund (less 100 DKK). Cancellation after April 1st will incur a 500 DKK administration charge.

For further information please contact:

KongresBureau Fyn
Raadhuset
DK-5000 Odense C
Denmark
tel: +45 66 12 75 30, fax: +45 66 12 75 86

4. Tutorial Programme (April 19 and 20, 1993)

The two first days of the symposium are dedicated to 8 half-day tutorials on formal development. The programme is organised into two parallel tracks. The first track contains 2 tutorials about program development and 2 tutorials about proving such developments to be correct, and track 2 contains 4 tutorials about different ways to model parallelism.

Track 1	Functional Programming	- Phil Wadler
	Data Refinement	- Tim Clement
	Proof in Z with Tool Support	- Roger Jones
	Prototype Verification System	- John Rushby
Track 2	Coloured Petri Nets	- Kurt Jensen
	CCS with Tool Support	- Kim G. Larsen
	LOTOS with Tool Support	- Jeroen Schot
	Provably Correct Systems	- Anders P. Ravn

5. Tools Presentation (Wednesday, April 21, 1993)

During the symposium, exhibitions of tools for the support of formal methods will be organised. On April 21, in parallel with the conference, a short introduction to each of the following exhibited tools will be given. ICL Data are sponsoring the tools exhibition by providing most of the SUN hardware.

DST-fuzz	- DST
CADiZ	- York Software Engineering Ltd
ProofPower	- ICL
The Centaur-VDM environment	- CEDRIC-IIE
SpecBox	- Adelard
Mural	- Manchester University
The IFAD VDM-SL Toolbox	- IFAD

The IPTES Tool	- IFAD
LOTOS Tools	- ITA
Centaur	- INRIA
Pet Dingo	- NIST
ExSpect	- Eindhoven University
Design/CPN	- Elektronikcentralen
DisCo-tool	- Tampere University
The Boyer-Moore Theorem Prover	- CLI
B-Toolkit	- B-Technologies SALR
The RAISE Tools	- CRI
PVS	- SRI
TAV	- Aalborg University
FDR	- Formal Systems Ltd

6. Invited Speakers (April 21, 22 and 23, 1993)

Each morning during the conference an invited talk will be given by one of the 3 specially invited speakers. These are:

Cliff B. Jones, Manchester University (UK),
Reasoning about Interference in an Object-Based Design Method

Willem-Paul de Roever, Kiel University (D),
Correctness of a Fault Tolerant Algorithm: an application of
Starke's dense time temporal logic for refinement

Peter Lupton, IBM Hursley (UK),
The CICS Experience with Z: Successes and Problems

7. Project Reports (Thursday, April 22, 1993)

In parallel with the April 22 conference sessions, the following project reports will be presented. Project reports will focus on experiences and problems encountered in the use of formal methods in real projects.

Specification and Validation of a Security Policy Model (T. Boswell)
Role of VDM(++) in the Development of a Real-Time Tracking and Tracing System (E. Durr et.al.)
Experiences from Applications of RAISE (B. Dandanell et.al.)
The Integration of LOTOS with an Object-Oriented Development Method (M. Hedlund)
Towards an Implementation-Oriented Specification of TP Protocol in LOTOS (I. Widya et.al.)
LOTOS Introduction in a conventional Software Development Life Cycle: An Industrial Experience (G. Leon et.al.)

8. ESPRIT Project Presentation (Friday, April 23, 1993)

In parallel with the April 23 conference sessions, the following European projects on formal specification and design will be presented.

```
   SPEC and REACT
   DEMON and CALIBAN
   LOTOSPHERE
   PROOFS
   AFRODITE
   RAISE and LACOS
   IPTES


9.  Conference Programme (April 21, 22 and 23, 1993)

 * Wednesday, April 21: Cliff B. Jones (invited talk)

    Applications of Modal Logic for the Specification of Real-Time
      Systems (L. Chen et.al.)
    Generalizing Abadi & Lamport's Method to Solve a Problem posed
      by A. Pnueli (K. Engelhardt et.al.)
    Adding Specification Constructors to the Refinement Calculus (N. Ward)
    Real-Time Refinement (C. Fidge)
    A Concurrency Case Study using RAISE (C. George et.al.)
    A Metalanguage for the Formal Requirement Specification of Dynamic
      Systems (E. Astesiano et.al.)
    A VDM  study of Fault-Tolerant Stable storage towards a Computer
      Engineering Mathematics (A. Butterfield)
    Automating the Generation and Sequencing of Test Cases from
      Model-Based Specifications (J. Dick et.al.)
    Maintaining Consistency under Changes to Formal Specifications
      (K. Ross et.al.)
    The Parallel Abstract Machine: A Common Execution Model for
      FDTs (G. Doumenc et.al.)
    Putting Advanced Reachability Analysis Techniques Together:
      the `ARA' Tool (A. Valmari et.al.)
    Process Instances in LOTOS Simulation (S. Pickin et.al.)

 * Thursday, April 22: W-P. de Roever (invited talk)

    A Proof Environment for Concurrent Programs (N. Brown et.al.)
    Encoding W: A Logic for Z in 2OBJ (A. Martin)
    On the Derivation of Executable Database Programs from Formal
      Specifications (T. Gunther et.al.)
    Application of Composition Development Method for Definition of
      SYNTHESIS Information Resource Query Language
      Semantics (L. Kalinchenko et.al.)
    Different FDTs Confronted with Different ODP-viewpoints of
      the Trader (J. Fischer et.al.)
    Invariants, Frames and Postconditions: a Comparison of the VDM
      and B Notations (J. Bicarregui et.al.)
    Formal Verification for Fault-Tolerant Architectures: Some
      Lessons Learned (S. Owre et.al.)
    Verification Tools in the Development of Provably Correct
      Compilers (M. Krishna Rao et.al.)
    Formal Methods Reality Check: Industrial Usage (D. Craigen et.al.)
    The Industrial Take-up of Formal Methods in Safety-Critical
```

and Other Areas: A Perspective (J. Bowen et.al.)
Selling Formal Methods to Industry (D. Weber-Wulff)

* Friday, April 23: Peter Lupton (invited talk)

Integrating SA/RT with LOTOS (A. van der Vloedt et.al.)
The SAZ Project: Integrating SSADM and Z (F. Pollack et.al.)
Symbolic Model Checking for Distributed Real-Time Systems (F. Wang et.al.)
Model Checking in Practice: the T9000 Virtual Channel
  Processor (G. Barrett)
The Frame Problem in Object-Oriented Specifications: An Exhibition
  of Problems and Approaches (A. Borgida)
Algorithm Refinement with Read and Write Frames (J. Bicarregui)
Specifying a Safety-Critical Control System in Z (J. Jacky)
An Overview of the SPRINT Method (H. Jonkers)
Conformity Clause for VDM-SL (G. Parkin et.al.)

10. Registration form

Complete and send this registration form before March 1, 1993 to:

KongresBureau Fyn,
Raadhuset,
DK-5000 Odense C,
Denmark.

Registration

Prof [ ]   Dr [ ]   Mr [ ]   Mrs [ ]   Miss [ ]

Name: ____
First name: ____
Company: ____
Address: ____
____
Country: ____
Telephone: _____________________ Telefax: _______________________

Presenter of   regular
tool [ ]   paper [ ]   tutorial [ ]   ESPRIT [ ]   delegate [ ]

Registration Fee	Before March 1	After March 1
Tutorial package	DKK 2000	DKK 2500
Conference package	DKK 2800	DKK 3300
Symposium package	DKK 4300	DKK 4800
Chosen package	DKK	DKK

[ ] I enclose a banker's cheque in DKK, drawn on a Danish bank, made
payable to FME'93, KongresBureau Fyn.

[ ] Please charge my credit card:
    [ ] MasterCard [ ] Eurocard [ ] Visa [ ] JCB [ ] Access
    card no. ____
    exp. date ____

    card holders signature ____

Att. Registration only possible when accompanied by payment of fee.

Accommodation

I would like to reserve:

Cat.	single room	double room
A	[ ] DKK 720	[ ] DKK 890
B	[ ] DKK 590-645	[ ] DKK 705-795
C	[ ] DKK 300-395	[ ] DKK 430-525

I want to share a double room with: ___________________________________

Date of arrival: ___________________ Departure: _______________________

Att. Hotel bills are to be handled directly with the hotel. The prices
    include breakfast, taxes and service. Reservations will be made in
    the order received.

Date: ____________________ Signature: __________________________________

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 15

Monday 7 December 1992

Contents

Similar But Different User Interfaces and Traces of Memory

not Swift, not Suiss, Swiss!)
Thu, 3 Dec 92 16:37:13 -0500

I recently learned a hard lesson about the risks of superficially similar user interfaces. Most of the time I use GNU Emacs for editing, but my home PC is too low-powered top run the DOS version with acceptable alacrity, so I usually use Multi-Edit for files on my PC.

Now, when you exit GNU Emacs with C-x C-c, it prompts you to save the file you've been working on, like so:

```
    Save file /path/filename? (y or n)
```

And when you exit Multi-Edit with Alt-X, it prompts you to save the file you've been working on, something like:

```
    FILE NOT SAVED! Exit?
    Yes    No   Save file and exit
```

There's a superficial similarity in that both programs ask for confirmation before exiting with unsaved files, but the Emacs confirmation confirms saving, while the Multi-Edit confirmation confirms exiting. So to exit and save changes under Emacs, it's C-x C-c y; to exit and save changes under Multi-Edit, it's Alt-X s. It should come as no surprise that my fingers got ahead of my brain and I ended up exiting my Multi-Edit session with Alt-X y, and lost about an hour's worth of work.

Ah! But all was not lost. For I knew, that somewhere in my PC's RAM, large portions of my file might still be waiting. I immediately ran a small utility program called Corelook, and searched the memory for character strings that might be from my file. I wrote them down on a handy pad of paper, and between what I recovered from my PC's memory and what I dug out of my memory, I re-assembled the file.

But what if this hadn't been _my_ file to start with? Open PC labs are becoming more and more common on university campuses. Assume I was an unscrupulous computer science student. Pretend I saw a classmate working on a project in one of these open labs. When he was finished, I might just grab the PC he was using and search its RAM for anything that might be of interest. If the PC is running Windows, or any other program that uses virtual memory, looking at disk used for swap space could also prove very interesting.

Or, for those who are in the habit of leaving their PCs on at work 24 hours a day, after-hours snooping in your machine's RAM by a corporate spy disguised as a mild-mannered custodian could give your competition a few clues about what you're up to.

RISKS has seen some recent discussion of the use of supposedly deleted files on a disk; it's worth remembering that what's left in your RAM might be interesting to others as well.

- Tom Swiss / tms@cs.umd.edu

Name Confusion and Democratic Concept of Limited Government

Roy G. Saltman <SALTMAN@ECF.NCSL.NIST.GOV>
Fri, 4 Dec 1992 11:50:02 -0500 (EST)

Two correspondents, Don Norman and Jerry Leichter, have indicated their sympathy with the police in the situation of a Canadian citizen who was confused by the police with another person of the same name. Specifically, they indicated sympathy for the statement of the police representative who said the onus was upon the victim to change his name so as to avoid confusion.

While it would be prudent for the victim to modify his name for governmental as well as for commercial and other non-governmental purposes, he has done nothing wrong. In the U.S. specifically, and possibly in other democratic countries such as Canada, the individual is innocent until proven guilty, and government is the servant of the people, not the reverse. While there may be extenuating circumstances that could absolve the police, we have statutes providing compensation for false arrest and for violations of civil rights. Certainly, the two individuals with the same name lived at different locations, had different appearances, had different families and friends, engaged in different occupations or worked at different locations, and had different (Canadian equivalents of our) social security numbers. In this country, it is up to government agencies to get it right; it is not required of an innocent victim to do anything except obey current law.

An activity for which personal identification is essential is voter registration. If the bill on this subject passed by Congress in its previous session had become law (it was successfully vetoed by President Bush), the driver's license would have become the fundamental voter identification and registration document. Persons would have been required to register to vote when they obtained or renewed their driver's license unless they *declined in writing,* a fundamental shift in attitude about the concept of citizen participation in voting. As this bill is very likely to be introduced in the new Congress, I may revisit this subject in the near future.

[Don Norman will also. He has prepared a lengthy response to many of the contributions that have come in recently, but which have not appeared in RISKS. It will follow in a special double issue of RISKS. PGN]

Police and Database [name confusion with twist]

"Alan (A.G.) Carter" <agc@bnr.ca>
Thu, 3 Dec 1992 11:36:00 +0000

There was an interesting case in the UK in the mid-80s. The Data Protection Act (DPA) had recently come into force, providing persons whose details were stored in databases (known as Data Subjects) with certain rights.

A woman applied for a job with a local Council. She thought she was ideally suited and was surprised to be turned down. Her friend who already worked for the Council investigated for her and found that for the job concerned, the Council made a routine check with the Police National Computer (PNC). We don't want criminals in certain positions of trust. The PNC had claimed that she had been convicted for shoplifting.

The woman had no criminal record, so she sent her nominal fee to the PNC people and asked for her record. It was the record of another person with the same name, who had been convicted in the 1960s. As she had been denied employment on the basis of the false statement made about her, she decided to take the PNC people to court and obtain compensation, as allowed for in the DPA.

Then the Police lawyers came out with a wondrous bit of sophistry. Data Subjects are indeed entitled to compensation for losses caused by mis-representation of their records, but in this case, the woman was not a Data Subject. The other woman, with a criminal record, was a Data Subject, but our heroine had no criminal record. As she was not a Data Subject she could not have been mis-represented, and was entitled to no compensation.

The Police won the case.

Toronto Stock Exchange Virus Scare

Shyamal Jajodia <SHYAM@mitvmc.mit.edu>
Fri, 04 Dec 92 15:21:20 EST

The following report has been paraphrased from the EDPACS Newsletter for January 1993:

InformationWeek reported that someone described as a disgruntled former employee of the Toronto Stock Exchange telephoned a local TV station newsroom and claimed that he had placed a computer virus in the exchange computer system due to activate at 9-30 the following morning. An all night search of the system did not reveal any infection, and trading proceeded on the following trading day without interruption.

This risk is similar to the risk of bomb scares on flights. Seems that all systems vulnerable to threats that cannot be detected without considerable work are vulnerable to the risk of false alarms.
Shyamal Jajodia

Re: Akron BBS trial update!

Phil Karn <karn@qualcomm.com>
Thu, 3 Dec 92 01:29:24 -0800

I couldn't have invented a better reason to encrypt EVERYTHING on one's computer system than this. It's sad that it would ever be necessary, but until civilization matures a little more I don't see much of an alternative.

The law is at present an awfully unreliable safeguard of one's right to personal privacy. Even when one wins (is acquitted) one almost always loses - in lost time, personal anguish, diminished reputation and, of course, legal fees.

I agree with John Gilmore -- I have far more confidence in the ability of physics and mathematics to protect my privacy than in laws passed by a government that can violate or ignore them at will.

Phil

Risks of children using BBSes (Was: Re: Akron BBS trial update!)

Michael P. Deignan <kd1hz@anomaly.sbs.com>
Fri, 4 Dec 1992 21:09:40 -0500 (EST)

In a previous posting, we read how a BBS sysop was being "unjustly" accused of various crimes.

Just to balance things out, I would like to refer to the following articles:

This first article appeared in the Providence Journal Bulletin in April 1991. (Sorry, I don't have the exact date.)

"Computer Guru faces Sex Counts
Networks Abuzz Over Charges Against Bulletin Board Czar
By Christopher Rowland
Journal Bulletin Staff Reporter

Warwick - Michael P. Labbe reigned as a kind of supreme talk-show host for Rhode Island's home-computer buffs, allowing thousands of hobbyists to communicate electronically through an array of equipment in his basement.

But Labbe's network crashed last week, when police arrested him and an associate and charged them with sexually assaulting two teenage brothers whom he befriended using his computer.

The arrest has left the state's largest computer "bulletin board" in tatters, crippling a popular source for computer enthusiasts of technical information, business news, computer-game updates and gossip.

It also has stunned Labbe's subscribers, who have engaged in a steady electronic discussion of the allegations on various alternative bulletin boards.

Labbe, 25, and Jeffrey L. Whitman, 23, were released on bail after a bail hearing yesterday in Superior Court. They had been held at the Adult Correctional Institute since their April 15 arrest.

Labbe's system, established in 1984, was shut doen after his arrest. It was revived yesterday after his release, but without its crucial link to a national and international information network.

Labbe and Whitman are charged with first- and third-degree child molestation. Authorities allege that Labbe molested the youths during 1989, 1990, and 1991. Whitman is charged with molesting them in 1990.

Authorities said Labbe first contacted the two boys, ages 16 and 14, through his computer bulletin board, the "Eagle's Nest" - so dubbed because Labbe was active in Boy Scouts as a North Providence High School student and achieved the rank of Eagle Scout.

Warwick police said the victims were frequent visitors to Labbe's house, which visitors described as being an electronic showcase."

[...The article then goes on with testimonials about "what a good boy" he was and how "shocked" the interviewees are at the charges...]

Well, time passed. Until a few months ago, nobody knew what happened. That is, until this story was published:

"Warwick Man Sentenced On Felony Morals Charge
(no byline)

Warwick - A founding member of one of the state's largest computer bulletin board networks received a seven-year suspended sentence after pleading no-contest this week to a felony morals charge involving two teenagers whom he befriended using his computer.

Michael P. Labbe, 26, of Warwick was sentenced Thursday after reaching a plea agreement with the attorney general's office. The victims, who were 15 and 16 at the time of the offense, were present in the courtroom and had agreed with the sentence.

Labbe and Jeffrey L. Whitman of Cranston were each arraigned in District Court in April 1991 on charges of first-degree child molestation and third-degree sexual assault. First-degree child molestation, which carries up to life in prison, involves children 14 years or younger.

When the case was sent to the Superior Court, the attorney general's office amended the charges to a felony morals offense, which carries a maximum 10-year sentence. Whitman pleaded no-contest to the same charges last fall and also received a seven-year suspended sentence.

Labbe founded his computer bulletin board "Eagle's Nest" and contacted the victims through the network. The network, which Labbe operated with Whitman, was the oldest and largest bulletin board in Rhode Island and was geared to general hobbyists and teenagers.

As part of the plea agreement, both men were ordered to undergo counseling and to have to contact with either of the boys."

This case was depicted by many people on the local BBS scene as an attempt to "taint" Labbe's image, as part of an attempt by other BBS sysops who were "jealous" of him to 'take over BBSing in Rhode Island'. However, in the long run we see that in fact this wasn't the case, that Labbe did indeed engage in questionable activity with these underage boys, and eventually pleaded guilty to reduced charges to avoid a prison term.

The Risks in the case are numerous. First, as a parent, you should know what your children are doing, especially on computer bulletin board systems.

Second, Mike Labbe and the Eagle's Nest BBS is still a participating member of the RIME network. As Eagle's Nest BBS caters primarily to the under-age teen user, and the controlling members of the RIME network are aware that Labbe pleaded guilty to the charges, clearly they continue to support him and his 'actions'.

In a nutshell, it is important to read beyond the hype and disinformation which is presented by both sides of the issue and get down to the truth of the matter.

Michael P. Deignan   mpd@anomaly.sbs.com   ...!uunet!rayssd!anomaly!mpd
Telebit +1 401 455 0347

[Excuse me for noting it here, but mole-station is one of the classic mishy-phenations, along with works-tation and times-tamp, and reminds me to request that you all try to avoid sending me stuff with rampant autohy-phenations. It makes routine reformatting really ugly. PGN]

Lost Technology

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Fri, 4 Dec 92 11:30:39 -0500

Some time ago I was made aware of a company that was developing a software-based session encryption package that would allow remote dial-up users to authenticate both ends of the connection and prevent eavesdropping by a simple wiretap. At the time my opinion was that it was something that a great many companies and agencies needed.

With the current proliferation of "wireless LANs" the danger becomes even acute since a physical connection is unnecessary for capture of traffic.

One of the real advantages of the system was that it was purely software based making it much more portable and potentially far less expensive than hardware devices.

Recently, I found that the development of the product had ceased from a lack of funds. It seemed that the FBI wiretap proposals had given their sponsor cold feet.

It is particularly bothersome since the proliferation of error correcting modems has removed the only real barrier to full session encryption (line noise causing loss of synch).

With all of the RISKS of bringing to market a fully featured software product (actually developing the driver is not that difficult, it is the user interface, compatibility testing, and quality control that really adds up in time and effort), we must now add intimidation of the backers to the list.

Padgett

ps for anyone who might be interested, the company is CRYPTECH in Jamestown,
New York (716)484-0244. I have no other knowledge of the company besides
having seen the demo.

Re: Computer theft from GP's; encryption is not a cure-all

Julian Thomas <jt@giverny.aix.kingston.ibm.com>
Thu, 3 Dec 92 11:13:42 EST

I share your concern about the risk, but it is far too easy to get complacent about the protection afforded by encryption since the medical community isn't apt to be as sophisticated as members of the computing community when it comes to password security (selection of good passwords, not writing them down,...). The human element is normally the weak link in cases like these; it might be easier to subvert an office worker for a key than for a medical record itself.

To be effective, a records encryption scheme would need to be both powerful (ideally using different keys for different records), easy to use (so it doesn't make the job of the legitimate users significantly more difficult), and robust (resistant to subversion by either malice or ignorance). I have often used a diskette file (that can be separately physically secured) to load a password (or set of keys) into memory on system startup; other schemes will undoubtedly come to mind.

If the thefts are for the equipment, not the data, today, it may not be too long before the thieves find it profitable to pass the equipment on to the professional blackmailers rather than the usual fencers of hot equipment.

Snailmail: 83DA/988 IBM DSD Kingston Compuserve: 72355,20 MCIMAIL: 173-6393
<Alternative EMail address, jt@donald.aix.kingston.ibm.com may not work...>

Turn Signals

<sullivan@geom.umn.edu>
Thu, 3 Dec 92 22:17:06 CST

Seeing a couple of postings from Don Norman in a recent RISKS reminds me that I haven't seen mention of his book(s) here. I got a copy of "Turn Signals are the Facial Expressions of Automobiles", a collection of essays on the interaction of technology and society, a few months ago, and found it so engaging that I lost sleep reading it in one night. I haven't read his earlier book "The Design of Everyday Things".

Norman's essays touch on topics like misleading user interfaces (on things as simple as doors), the trend towards experiencing life through recordings, low-tech fixes for confusing airplane cockpits, the estimation of low-probability risks, and the ramifications of international computer networks. Of course, this is not an exhaustive list.

Addison Wesley: ISBN 0-201-58124-8 (I got my copy through Library of Science)

-John Sullivan, sullivan@geom.umn.edu

Estimating risks

Jerry Leichter <leichter@lrw.com>
Sat, 5 Dec 92 07:54:46 EDT

This Wednesday through Friday mornings (2-Dec through 4-Dec), NPR's Morning Edition ran an extended story on environmental problems and the present and future of the EPA and environmental laws. Unfortunately, I only caught the tail ends of two of the segments.

Of particular interest to this group - and I wish I'd heard the whole thing! - was Thursday's segment. At least the part I did hear discussed the problem of tradeoffs: With limited resources, how do we decide which risks are the ones most important to deal with? Much of the discussion centered on a question that has been recently discussed in RISKS: Is "the common man" competent to answer such questions in a rational way? The answer of the people they spoke to was basically, "yes". As has been discussed here, people do not look only at probabilities in deciding the importance of various risks; but they do follow an understandable, not at all arbitrary, procedure.

One interesting study they cited: If asked to rank the "danger of death" from a variety of causes, such as (say) smoking or driving, people come up with an ordering that does not match the probabilities of death from those causes. However, if the same people are asked to rank the "CHANCES of death", they produce the "correct" ranking. The "incorrect" ranking is not based on ignorance!

I seem to recall seeing messages from someone on NPR in RISKS. Anyone out there who could get a transcript of this segment for RISKS readers?

Jerry

Revenge via computer

Thomas Dzubin <tdzubin@cue.bc.ca>
Sun, 6 Dec 92 11:28:07 PST

San Francisco. A man sent his ex-wife (who had apparently asked him to retrieve some inaccessible files) a computer diskette that destroyed her entire hard disk, including software and manuscripts, and then displayed a vengeful limerick. James Welsh, a 32-year-old accountant has pleaded not guilty to three counts of "introducing a virus" into the computer. He could face three years in prison if convicted. Welsh's ex-wife, writer Kathleen Shelton, said she had a problem with a computer they formerly owned together. Welsh apparently sent her a computer disk with instructions for correcting the trouble. Police said, "She followed Welsh's instructions, which resulted in the destruction of approximately $8,000 worth of software and manuscripts, leaving only a limerick explaining Welsh's actions against her."

"A lying bitch named Kathleen,
Made in the courts quite a scene.
To have her ex, the hacker,
Enjoined not to smack her,
So I wiped her whole hard disk clean."

Detectives searched Welsh's home, seized $4,000 worth of computer hardware and allegedly found evidence of the "virus". Welsh's lawyer, Annette Lombardi, said: "There's not as much damage as charged. It's basically the cost of getting a guy to fix the computer and install new software." [Presumably a DIFFERENT GUY this time..., maybe someone who can write poetry that scans.] [Source _The Province_ Vancouver, B.C. Canada, plus the San Francisco Chronicle, 4 Dec 1992, edited by PGN]

Risk reduction: Human Factors (Moonen, RISKS-14.03)

<cnorloff@tecnet1.jcte.jcs.mil>
Mon, 7 Dec 92 11:27:41 EST

Ralph Moonen (rmoonen@ihlpl.att.com) writes in RISKS-14.03 that he's concerned about making concessions during design. He includes human factors as a concession, when it is, in fact, a prime design requirement in most systems. After all, humans operate most of the systems we design!

I'm a human factors engineer, and have seen incredibly bad designs built to meet schedule or performance requirements, with no regard to the human operators. People are part of the system, not merely users. And just because a designer can operate a system doesn't mean a typical user can operate a system. This has been proven time and time again. And the lesson has not been learned yet. Just reading through RISKS provides many examples of poor user design: bad interfaces, mental models foreign to current users, and systems not meeting users' needs.

Systems, including computer systems, must be designed with the human as the main enabling part of the system. The system should take advantage of humans strength and not overload human weaknesses.

Mr. Moonen's comment that they will see better products by following his points, but that he hasn't "touched the subject of user interaction" illustrates the problem: designers are designing for themselves rather than for the users.

Chris Norloff cnorloff@tecnet1.jcte.jcs.mil

Flood Stories

Lindsay F. Marshall <Lindsay.Marshall@newcastle.ac.uk>
Thu, 3 Dec 92 16:49:31 GMT

A while ago I asked for people's stories relating to computers and floods (not just of water - molten metal featured in one). Since then, I am sure new

readers have joined and new floods have happened, so if you haven't sent me
your flood story before can you please send it to me now.

Lindsay.Marshall@newcastle.ac.uk +44-91-222-8267 FAX +44-91-222-8572
Computing Laboratory, The University, Newcastle upon Tyne, UK NE1 7RU

Re: holiday reading on Risks (Agre, RISKS-14.14)

Gary McClelland <mcclella@yertle.Colorado.EDU>
Thu, 3 Dec 1992 08:50:58 -0700

>Lorraine Daston, Classical Probability in the Enlightenment, Princeton:
>Princeton University Press, 1988. This is a detailed and scholarly history
>of early modern mathematical ideas of probability.

I second the recommendation for reading Daston's histories. For those with limited time, I recommend as a shorter course this wchapter:

  Daston, L. J. The domestication of risk: Mathematical probability
  and insurance 1650-1830. In L. Kruger, L. J. Daston, & M.
  Heidelberger (Eds.), The probabilistic revolution: Volume 1.
  Ideas in history (pp. 237-260). Cambridge , MA: MIT Press, 1987.

It is interesting to look back and see the probabilists scratching their heads trying to understand the boneheadedness of both users and designers of insurance systems (e.g., the Bank of England almost went broke by selling lifetime annuities at a fixed price _not_ conditional on age). I think readers of RISKS often scratch their heads in the same way trying to understand the boneheadedness of both users and designers of computer systems. The good news is that the insurance companies finally got it right with respect to probability. The bad news is that it took a long time and required some fundamental shifts in thinking about probability and uncertainty. RISKS readers may therefore find some lessons in Daston's work on what must occur before designers and users of computing systems (ironically, of course, the insurance companies are now big users) more appropriately deal with the risks of computing. Alas, the Bank of England was near bankruptcy before they wised up so the message may not be comforting.

gary mcclelland, univ of colorado   mcclella@yertle.colorado.edu

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 16

Tuesday 8 December 1992

Contents

Name confusion and its implications.

Don Norman <norman@cogsci.ucsd.edu>
Tue, 8 Dec 1992 11:22:19 -0800

In RISKS-14.12 (30 November 1992), Jerry Leichter and I independently discussed the problems of name confusion -- where two different people might have identical names and (in at least one case) identical birthdates. Our contributions produced a large number of responses -- it took 76 single-spaced pages to print them all out! Peter Neumann, moderator of RISKS, asked me to provide a summary. This is it.

Before I review the individual comments, let me summarize my own views, which have become much enriched by this interaction. Because the topic is so complex, they can only be dealt with fairly by a rather lengthy, complex review. I apologize for the length of this contribution to RISKS, but not only would a shorter treatment be unfair, but this may be too short to do justice to all the issues.

First: an executive summary, in bullet format:

* No single, simple solution is possible. The issues are too complex. They

involve legal, moral, religious, and cultural factors that vary radically across the United States, North America, and the world. The choice of names creates intensely emotional responses: names define a person's self image and culture.

* Names serve two functions: 1. Cultural and self-image; 2: Societal identification. If we separate these functions, then the discussion is much simplified

* Societal identification leads to issues of privacy. Privacy issues are complex. Privacy is a culturally-based notion. What one person considers intensely private, another might consider public business. Some cultures simply cannot understand another's concern for privacy in some matters and lack of concern in others.

* Privacy also divides into several distinct areas: 1. Reliability and accuracy; 2. Misuse; 3. Privacy. Discussion of these issues is simplified if the different concerns are separated.

* Finally, once again, the issues are so complex that no single, simple solution is possible.

- -

This debate started with an analysis of the non-unique character of names and the statement that it didn't seem too onerous to require individuals to select unique names. Note that the suggestion still allowed people the same freedom in their choice of names as they now have, adding only the requirement that they be unique. I am now convinced that this belief is wrong -- names are critically important for a person or the family's self image and cultural values. It would indeed by onerous to establish artificial conventions -- now matter how well intentioned and gently enforced -- to name selection.

People's names derive from a wide variety of sources and serve a wide variety of purposes. Today, they are an essential component of self identity and self-image. It is dangerous to tamper with them. The real issue is that names serve so many functions that coupling the problem of unique identification with that of a person's name simply adds confusion. If we separate the self-image, self-identity function of the name from that of societal identification, then the problem simplifies. Let people be free to assign their children or themselves any reasonable name consistent with their culture, religion, and self values (and that are not deemed immoral or improper by society). It would not matter if there were multiple people with the same name. But then we must devise some other means of identification for society. Moreover, there is no need to have a single scheme: we might have different identifications for different purposes, thus helping thwart possible misuse. (Credit: The suggestion to separate the identification aspect of a name from its self-identity comes from several correspondents: the texts of their suggestions are appended to the latter part of this message.)

This now raises the question of how we can invent a unique identification scheme that addresses the problems of accuracy, misuses, and privacy. I also believe strongly that the identifier be a humane one -- easy to learn, easy to use. And it had better be one that is difficult to counterfeit. I suspect that this means that the identifier will have to have several versions: A simple one for non-critical usage (e.g., checking out library books or charging small amounts of money), but more complex and with more encryption and other personal identifiers when it comes to critical items. Here I can imagine the identification supplemented by various cryptographic schemes (the FBI and NSA permitting), including the use of random voice segments, or retinal/fingerprint/DNA scans -- the technical issues should be discussed elsewhere. Many would argue that databases for different functions be separated, not allowed to be interconnected (maybe with different, encrypted identification schemes so as to avoid possible misuses).

UNIVERSAL IDENTIFICATION

The discussion about names soon became a discussion about universal identification and the many issues associated with that. So now, a digression into those issues. Concern about access to personal records can be divided into at least three areas: accuracy, misuse, and privacy. These three different topics often get confused in discussion, but I think we will make more progress if we separate them:

ACCURACY OF RECORDS: If we rely on databases for credit ratings, police checks, medical records, and other aspects of modern life, then those records must be accurate. All too often they are erroneous, either by having incomplete, inaccurate, or fallacious information or by combining records of different individuals.

MISUSE: When people ask me what the problem is when others have access to personal files, I do not have a good answer. The problem, I think, is that in the United States, we do not practice what we preach. We claim that we have religious, political, sexual, and racial freedom, but we do not. If we really had that freedom, then maybe we wouldn't need so much privacy. If people wish to be adulterers, or gay, or communist, or purple-skinned, or to subscribe to (legal) pornographic magazines or films -- whatever --they should not be ashamed to let others know. But that is not our society, regardless of what the laws might state: Their lives would become intolerable if people knew (or thought they knew) that kind of information. Similarly, people shouldn't care if their employer knew their medical history. Unfortunately, they have to care, because they might get fired because their employer had erroneous beliefs about the implications of the history.

One common complaint is that it is possible to learn a lot about someone and then pretend to be them, gaining financial or other benefits (at their expense). But this is not a problem with open access to records. Rather the problem is that of insufficient verification of an individual's identity. To solve the identity problem we need other means -- a complex issue, but nonetheless, one that in principle can be separated from the general issue of privacy.

PRIVACY: Part of the privacy issue comes from the potential for misuse. But some of it is because some people wish to keep their activities known only to themselves or their close associates. Presumably this should be permitted within the bounds of public safety and public good and as long as their activities do not violate the laws of the country. The problem is that many will argue (correctly, in my opinion) that the definitions of "public safety" and "public good" are vague and question who has the right to make those decisions; others will question a person's rights when the laws of the country are thought to be immoral or improper. The reverse of privacy is secret collection of information -- when the person about whom the information is collected is not permitted access to the material, or in some cases, is even unaware of the fact that such a collection exists.

UNIQUE IDENTIFIERS

But even given all these concerns about privacy, geopolitical groups and countries will need unique identifiers for its citizens, if only for legitimate societal concerns -- e.g., licensing for some activities (for driving, flying, voting, being a medical doctor, ...), or keeping track of people (voting, social security benefits, income tax). The convenience of credit cards requires some unique identifiers. All this seems to require some sort of central clearing house to ensure uniqueness. However, unique identifiers have both virtues and difficulties, perhaps best summarized by Peter Neumann (not as RISKS moderator, but as contributor, in a private note):

> There is no easy answer. User Identification systems (UIDs) can disambiguate and could have staved off many of the ugly false arrest cases and other mistaken identities (e.g., see my CACM Inside Risks column of Jan 1992), if they were used properly. UIDs can also create many disasters, particularly when they are abused or not used properly."

One interesting fact I discovered was that the United States Social Security Number (SSN) is NOT a good choice of personal identifier for technical reasons. Forget all the civil libertarian concerns -- it is simply a crappy piece of technology, poorly implemented at that. Think about it: only nine digits to register 250 million people -- that's only a factor of four leeway, much of which is used up by non-used digits, etc. No check-digits, and such a dense packing of the encoding that any random guess or simple typing or memory error is apt to lead to someone else's account.

Chris Hibbert supplies an excellent discussion of social security numbers in his FAQ (Frequently Asked Questions). SSNs are intended to be unique but they goof now and then (it's happened in fewer than a hundred documented cases). When the Social Security Administration discovers this, they issue a new number to one of the people.

Reference: Hibbert, C. (Oct. 27, 1992). What to do when they ask for your Social Security Number. "Social Security Number FAQ (Frequently Asked Questions)." uunet news groups: alt.privacy, misc.legal, news.answers, alt.society.civil-liberty, comp.society.privacy. (hibbert@xanadu.com) (Copy provided me by Esther Lumsdon.)

- - - - - - - - - - - - - - - -

SUMMARY OF SUBMISSIONS

Note that I have not included all submissions, just the ones that made unique points. I have deleted considerable material from each response (else this document would run 70-90 pages), but aside from deletions, a spelling-check (I did correct spelling errors), and a few minor typographical edits, I have made no alterations. [PGN did a little cosmetic work as well, and caught a few more mispelings.]

Any line preceded by ">" comes from my original contribution to RISKS (except for the notorious Internet mail scheme that will precede the word "From" with ">" if it is the first word on a line -- another hack reminding us of our UNIX legacy.) All comments by me are preceded by the phrase:

COMMENT BY DN:
At times, it may be difficult to distinguish the boundaries of the contributions and my comments from the summaries. In an ideal world I would use indentation and different type fonts to make the distinction clear. But Internet is restricted to plain ASCII, so different fonts are out. And my mail system (Eudora), for all its virtues, is not WYSIWYG, so I can't use indentations -- not reliably anyway. (Sometimes I dream I am still using Emacs, but then I pinch myself and wake up.)

- - - - - - - - - - - - - - - -

NAMES AS SELF-IDENTITY

From: Will Taber <Will_Taber@dgc.com>

The most important function of any name is to identify us to ourselves. A person's name is a significant factor in how they come to see themselves. At some level, parents tend to pick names that reflect the person that they hope that their child will become. My wife and I had a hard enough time deciding on names that we liked. I am sorry, but any kind of global registry is just out of the question. Some things just are not worth changing for the convenience of database designers.

- - - - - - - - - - - - - - - - - - - -

From: "George Buckner" <GRB@NCCIBM1.BITNET>

Excuse me, but are we now proposing to have all names verified for uniqueness through a central database? What about the freedom of expression that would be restricted by such a scheme? I would insist that it is the arbitrary assumptions underlying the program logic (or lack thereof), not the persons name, which needs to be changed.

This is really another example of "risk of invalid assumptions". We see examples posted here all the time (i.e. programs which assume that no transaction will require more than N digits to accommodate). In this case an assumption was made that the full name, together with the birthdate and city of residence, would guarantee uniqueness.

... the problem is in assuming that you can guarantee uniqueness via a combination of name/birthdate/hair color/zodiac sign/whatever. It is these assumptions which impose arbitrary restrictions on data values. As Jerry Leichter pointed out, the safest way to handle this is to assign a unique number to each instance of an object in a file. This is nothing new

-businesses have been assigning unique customer ids/account numbers to people for years. Thus it doesn't matter how many John Q. Smiths, born on the same day, living in the same city, are contained in the database.

> Would a world-wide registry for names work?
Perhaps, but it is quite unnecessary, and quite undesirable:

"I'm sorry sir, but the computer has rejected the name you have chosen
for your child. It isn't unique."

> This is a serious request. how can we invent unique identifiers for people
> that
> 1. Make it easy to select a name
Select whatever name you choose. To hell with arbitrary
programming assumptions. Incorporate a separate field to hold
the unique ID.
> 2. Work for an entire country and potentially scale to the entire world
Moot question, if globally unique identifiers, SEPARATE FROM THE
NAME, are used. If it's unique globally then by definition it will
be unique within a country.
> 3. Do not violate civil liberties
This is a matter of coordinating policy with implementation.
Use of unique numbers (SSN) doesn't NECESSARILY infringe on civil
liberties, though it may make such violations easier. Likewise,
absence of these identifiers doesn't guarantee that our liberties
are safe.
> 4. Do not make it possible for others to misuse the system
This is related to point #3 above, and is thus another matter of
coordinating policy with implementation.

> In other words, how do we get the benefits and avoid the risks?
Yes, we always want to have it both ways, and to some degree, perhaps
we can. But remember that we are trying to accommodate two quite
divergent (if not mutually exclusive -at least on the surface)
imperatives.

And the price of liberty is STILL eternal vigilance.

- - - - - - - - - - - - - - - -

From: Eric Johnson <johnsone@camax.com>

* There are also cultural factors. In some communities (I think Australian Aborigines, but I may be mistaken), people take on different names in the course of their lifetimes. For example, if a close relative dies, the survivors may change their names. After a mourning period, the survivors may change their names again and may not go back to the original names.

* Icelanders still use the father's or mother's name as their last name, with the "daughter" ("dottir") or "son" (""sson") suffix. Thus, the last name changes for every generation (by sex). I think Russians may still have part of their names based on this. Also, Spanish names typically use the mother's and father's last name, I believe. These naming schemes may be tied into a person's cultural identify. In such a case, these people may not want to

change.

* Many immigrants to the USA had their names changed at the border by insensitive/confused immigration officials. Many people hold a strong cultural identity in their names. It seems that your proposal would hinder this.

* What about people who wish to name their children, especially sons, after their parents? (Just read 100 Years of Solitude to see a lot of common names :-) Some examples:
 William William Williams, Sr. (Bill Bill Bill :-)
 William William Williams, Jr.
 William William Williams III

* Marriage: This is still a touchy issue in the USA. Many people desire to change their last name when they marry (many also do not). In such cases, people won't care much about your national/international name registry. Even if the names were unique in the beginning, the changed name may not be. Do you think the religious right will go for this?

* Religion: Some people change their name when they a) convert religions or b) go through some religious experience. To use an example from a current movie, Malcolm Little changed his name to Malcolm X when he converted to Islam (or at least to the Nation of Islam's Islam). The "X" also had political significance (the theory--at least from X's autobiography--was that the TRUE last name was wiped out by whites in the past, so that the X acts as a placeholder until--presumably-- God will provide the real name. After Malcolm X went on the Hajj to Mecca, he changed his name again (to something like El-Hajj Malik Shabazz, his wife still calls herself Betty Shabazz). Many people also want to name their children after religious names (Rebecca, Matthew, Joseph, etc.). Eduard Shevardnadze recently was baptized in Georgia (the country, not the state). His new religious name is Georgi.

- - - - - - - - - - - - - - - -

From: Brian.Hawthorne@east.sun.com (Brian Holt Hawthorne - SunSelect Engineering - Norwood)
.....

An identifier should be static data, names are dynamic. Within a computer database, a personal name should be considered as stable as such things as weight, height, or hair color. Nobody would think of making these the primary identifiers of a person in anything other than short-term databases.

Just in mainstream U.S. culture, there are an unending number of events that may lead to a change in name: birth, Catholic confirmation, marriage, Amerindian rites of passage, divorce, adoption, etc. Taken in combination, it is nearly impossible to predict how many names an individual may have, and what these names may mean to them and to their peers.

It is not up to me as an individual to ensure that my name is convenient to somebody's database, even, or perhaps especially, if that database is maintained by the police. If they have a need to enter me in their data, it is their responsibility that that entry be distinguishable from others. All of the other data you suggested (birth date, birth place, etc.) are much better identifiers than my personal name, as it is unlikely that I will be able to change my birth date once it has occurred!

In order to provide any serious answers to Don's serious request for a way to invent unique identifiers for people, we need to decide what these identifiers are going to be used for.

For casual conversation, there is no problem, we already know how to do this. "John Smith. No, not that one, John Smith from Poughkeepsie. With the blue eyes."

In written form, we have also solved the problem.
"Don Norman from the Cognitive Science Department of the University of California, San Diego at La Jolla."

This leaves open the need for identifiers in databases (whether computerized or not). The requirements of these identifiers differ for different databases. Do they need to be unique for all individuals in the world? In that case, the identifier probably needs some location information. Do they need to be inherently bound to an individual? In that case, there probably needs to be some birth, fingerprint or other static information in the identifier itself.

None of these requirements imply that personal names would make a good identifier for such purposes.
....

P.S. Along the lines of databases asserting control over personal information, if you were receiving this message directly, instead of in a digest, you would see that my email address had been changed from rowan@sea.east.sun.com to brian.hawthorne@East.Sun.COM and that my name had been changed from Rowan Hawthorne to Brian Hawthorne. This is because the corporate machine (at least the human parts) fails to understand that some of us have an additional name, known as a "nickname". My friends call me Rowan, people on the net call me rowan, but since the IRS considers me to be Brian the company follows suit. I suppose I could change my name legally to Rowan, but I enjoy having the two different names for different purposes. Forcing me to either abandon my nickname, or adopt it in all situations seems a bit draconian.

- - - - - - - - - - - - - - - -

From: "Russell Aminzade: Trinity College of VT" <AMINZADE@UVMVAX.BITNET>
....
I would NEVER grant any authority the right to select a name for me, but I'm quite comfortable having my ADDRESS assigned by someone.
...
Norman states that "Names.. are a technological invention to make it easy to identify people uniquely." Jerry Leichter suggests something similar: "Any society has to have a way to identify individuals. At onetime, when the scale of society was small, a single name, plus perhaps a city of origin, or a parent's name, or a job name, was enough identification..." But names do much, much more. Names define who we are emotionally, socially and spiritually. I know a family that named their daughters Hope Faith, and Charity. My family

named the three boys Robert, Ronald, and Russell for quirkish reasons. And what about names like "He Who Conquers" or "Dances With Wolves." Something more than a unique identifier here.

Addresses, however, fit the description that Norman and Leichter use. They are bureaucratic, assigned by others. We can accept an address that has something like 05667 or @UCSD.EDU. I'm quite comfortable with AMINZADE@UVMVAX.UVM.EDU, but I doubt my parents would have been willing to give me that name. Makes it lots easier to develop a unique identifier.

A personal "address" begins to make sense when telephone, mail, and other information services are smart enough to route our communications to the person rather than to the device. We're at the threshold of being able to do this now, so perhaps now is the time to talk about personal addresses.

(Also see the comment by Roy G. Saltman in RISKS-14.15)

- - - - - - - - - - - - - - - -

COMMENT BY DN: I start with a question:

From: Bob_Frankston@frankston.com
....
In countries that do allow the use of national identifiers in databases, are they universally used to avoid name confusions?

COMMENT BY DN: I forwarded the question to Chris Hibbert. He responded:

From: hibbert@xanadu.com (Chris Hibbert)

This is a very broad question, but there's a little bit that's worth saying. Countries that have good universal unique identifiers fall into two camps, mostly free, and mostly not. In the ones that are mostly free, (Canada, e.g.) the SIN is used in government databases, but cross-matching isn't routinely allowed, and private companies don't seem to use the same number as the government. (I don't actually have solid references to back this up, but I've read the annual reports of the Canadian Privacy Commissioner, and am extrapolating from the kind of complaints they do and don't get compared to the US.)

In more intrusive societies, the same identifiers are used throughout the government, and the government pushes for the efficiency that results from consolidated databases, so data matching isn't even a concern. The government of Thailand (I think) has a single database which all the government departments share access to. This makes it possible for someone in one department to make a decision based on your interactions with another department. (This generalization is based on even less information.)

Anyway, my bottom line is that I believe there's a lot of benefit in not using the same identifier in our dealings with different parties. That's behind a lot of my attention to SSNs. They wouldn't be a problem if they were only used by the IRS or the SSA, but the fact that my employer can find out about my medical history, or (in some states) someone who sees my driver's license can find out my credit rating or pretend to be me and ruin it is a real weakness of this system.

- - - - - - - - - - - - - - - -

From: xanadu!hibbert@uunet.UU.NET (Chris Hibbert)
...
Jerry Leichter lays the problem at the feet of the individuals being identified.

> If [Steven Reid] stands by his insistence that "Steven Reid, born on xx/yy/zzzz" is all the identifying information he will give, he cannot expect to be distinguished from the other Mr. Reid who just as adamantly insists on his right to identify himself in the same way.

In my experience, (e.g., the case of Terry Dean Rogan) people in this situation are eager to be distinguished, and go to enormous trouble to convince the authorities to support them in this. The problem becomes intractable when the authorities involved insist that they have to treat the identifier stored by their computers as if they provide secure unique identification. If the computer systems were made more flexible they could store more information and allow people to work around the problems when they arise. In other situations, the relevant authorities ignore the extra distinguishing info that is there. Robert Ellis Smith's compendium of Privacy War Stories lists numerous cases where the authorities arrested someone with a name similar to one on a warrant, even though the physical descriptions were very different. (As much as a foot in height, 100 pounds in weight, differing hair color, etc.) What's a person to do if using any variant of your own name is close enough to match against someone the police are looking for?

The Montreal police also need to realize that in a metropolitan area like that, they have to be aware that names aren't close to unique. I don't know if they have a large Korean or other Asian community there, but common names there are much more common than in groups descended from western european societies. And in these cases, physical descriptions aren't going to help much. (I didn't say "they all look alike", I said our western system of classifying people doesn't distinguish orientals at all. Hair color, eye color, height don't vary in the way we're used to, and most caucasian police are much worse at guessing ages of orientals who turn gray, go bald, and wrinkle in different ways than whites.

[THIS SPECIAL DOUBLE ISSUE IS CONTINUED IN RISKS-14.17.]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 17

Tuesday 8 December 1992

Contents

THIS SPECIAL DOUBLE ISSUE IS CONTINUED FROM RISKS-14.16

From: amos@cs.huji.ac.il (amos shapir)

Having lived most of my life in a country that uses the national id system, I find it quite useful. I also find it hard to understand what harm there is in such a system, let alone that it constitutes an "obvious" risk to human rights. ....

>In other words, how to we get the benefits and avoid the risks?

We can't. Since the development of technology will sooner or later make such a system inevitable, we'd better be prepared to take both benefits and risks.

- - - - - - - - - - - - - - - -

From: J. Brad Hicks <mc/G=Brad/S=Hicks/OU=0205925@mhs.attmail.com>

My life has been complicated horribly by name confusion, so I've put a lot of thought into this. There are two theses I would like to put forward:

1) If you manage to make name, or name plus any other attributes, a unique key, then you will acquire all of the problems that go with a national identity number.

2) There is nothing that can be done to names, as socially used, that will make them adequate unique keys.

UNIQUE NAME = NATIONAL IDENTITY "NUMBER"? Let's suppose that you have an application for which you wish to track people by their National Identity Numbers, whether for good or ill. Being a sensible programmer, and knowing that NIN formats could change, you make it a nice long alphanumeric field. Then let us suppose that name alone, or name plus date of birth plus number, or name plus some combination of attributes, turns out to be sufficient to accurately identify anybody. What's to stop you from putting that string into the key field? In that case "JAMES BRADLEY HICKS 07/11/1960 1" =becomes= my National Identity Number. If it is unique, it can be used for database lookups, just as efficiently as a number.

NAME CAN'T BE PART OF A UNIQUE KEY? Let's take the hypothetical case of Jonathan Quincy Customer, of 1234 Main Street, Springfield, NI 66666. Even if there are no other Jonathan Quincy Customers anywhere else in the "target area" (city, country, world, whatever), you're going to run into problems looking him up by name. (1) What if he signs it John? or Johnny? (2) What if the clerk misspells it "Jonathan"? or "Jon"? (3) What if it's actually "Johnnathon" or some other non-standard spelling? Then you'll never untangle it, since the clerks everywhere "know" how to spell it and will screw it up all the time.

(Maybe you think that you can solve this problem with training. When US cities began converting from candlelight to gas lamps, people frequently BLEW UP THEIR HOUSES at night, killing everybody inside, because deep down in their reflexes they "knew" that you turn off a wall light by blowing it out. With their LIVES on the line, it took many of them YEARS to be trained not to do this. If your system requires people to unlearn things, even as minor as spellings of names, your system will not work in the real world.)

(4) What if he routinely goes by his middle name?

The credit bureaus, I'm told by a friend who used to program for one, "solve" problems 1-4 by using as their primary key last name + first initial of first name + first letter of street name + "city", i.e., standard metropolitan area. (I live in Maryland Heights, a suburb of St. Louis. For such purposes, they would use "Saint Louis" not "Maryland Heights", presumably by lookup on ZIP code.) (5) What happens to his records if/when he moves? Or the city renames the street?

Then of course, as with the X.400 spec, really ugly things happen when you try to parse the name string into separate fields, such as "last name" in the example above. Which one is the "last name" or "surname"? If he is of Latin American origin, it could be =either= Quincy =or= Customer. In China, the patronymic would be "Jonathan", and "Quincy Customer" the given name. (In the X.400 spec, if the name is "Jonathan Quincy Customer" and Quincy is the surname, how should the rest be recorded in the given name field? "Jonathan Customer"? Won't half the systems in the world reconstruct that as "Jonathan Customer Quincy"? Is this why there's a separate initials field?) (6) So knowing all of this, what would the clerk type in to the "last name" field?

(What =do= non-Europeans who run into this idiocy say when they're asked for their "first name, middle initial, last name"?)

Even assuming you parse it right, (7) what about Jonathan's cousin Jane who lives across the street? OK, some of them untangle this by using house numbers as well. (8) Somebody had better warn him not to name his first child "Jane" or "Janet" or "James" or "Johann", or he'll get what happened to me. As soon as Johann grows up enough to apply for a credit card, while living at the same address, the two files will be cross-linked inextricably.

My name is James Bradley Hicks. My father is James Bedford Hicks. Observe, the name is an adequate identifier in these cases, but no, I am NOT "James B. Hicks, Jr." But almost all of the computers out there use first name, middle initial, last name for an identifier, and as I've said, the credit bureaus don't even use that much. For us, it's no problem: he's Jim (or to some people who've known him since The War, "Bud") and I'm Brad. But when he and I were both working for IBEW Local 1, both of our work hours got credited to his pension account; they turned out to be flatly incapable of untangling this other than by "renaming" me as Brad J. Hicks.

Then, the other day (thanks to a tip in RISKS) I requested my TRW report. ONE HUNDRED PERCENT of my report is in error. You see, item 1 was just a query, and item 2 was an "address and SSN correction", because they saw on some report that I had as a previous address "1371 Broadlawns" in St. Louis (I grew up there), and they were still getting credit reports from "1371 Broadlawns" ... my father, of course. They even "corrected" my social security number ... to his. From then on, there were no separate files for us; if I had any credit activity, their search didn't find it, and all of his showed up when they searched for mine.

I'll work with them to correct this, but there is no way under the current system to stop it from happening again, so for the rest of our lives, our credit records are going to be screwed up.

Speculation:

Whatever the problems are of having a "national identity number", we've got them already. When the cop pulls you over, he can and usually does ask for your driver's license, which almost certainly has enough information on it to find you in any database that he cares about. You show that same id, with name and address, to anybody who you want to cash a check. You even have to show it on some cash transactions, like gun purchases or renting a hotel room. Banning the use of National Identification Numbers (to the pitiful extent that this was even done) did not solve the problem.

Since not having an NIN didn't solve the problem, having an NIN won't make things any worse, and they =will= make one thing better: if there are ambiguities or things that are easy to mis-key on your existing identity card, right now you can get confused with a deadbeat or a fleeing felon, with ugly results. With an NIN with adequate check digits, it seems to me that you would acquire no problems that we don't have now and eliminate the problem of false identification.

J. Brad Hicks
Internet: mc/gn=Brad/sn=Hicks@mhs
attmail.com
X.400: c=US admd=ATTMail prmd=MasterCard sn=Hicks gn=Brad

Yes, I work for a credit card company, but (a) I'm not speaking for them, I'm only speaking my own personal opinion, and (b) as far as I can tell, my opinions on this are not influenced by my work. (And no, I can't do anything about your credit card balance. Not only is the joke unfunny, we don't even =know= your credit card number OR balance; that's the issuing bank's responsibility.)

- - - - - - - - - - - - - - - -

COMMENT BY DN: I have been deleting signatures in order to save space, but this particular signature actually is relevant: it points out one of the fears of universal access to databases. (And the fact that the e-mail address requires explanation is another sign of the difficulty of getting unique -- and understandable -- addresses.)

- - - - - - - - - - - - - - - -

From: tarl@coyoacan.sw.stratus.com (Tarl Neustaedter)

As you can tell from my email address, I am not one of those people whose name gets easily confused with someone else's. But having a unique name is not the same as having a standardized unique identifier that everything uses. The former is a comfort and a privilege, the latter is a frightening idea.

With computerized databases today, merging databases is trivial as long as you can make the associations between entries. A standardized identifier which is validated at time of data entry (e.g., SSN), will permit this association. A unique name, when the name isn't guaranteed to be unique, or guaranteed to be correctly spelled, does not permit such an association. And thus the barriers to a centralized database of everything are still high.

With my name, I get to observe the process first hand with junk mail. I give to various political causes and some charities, most of which have variously misspelled my name. When I receive new junk mail, I will frequently receive three or four identical pieces of mail addressed to slightly different people. The new purveyor of junk mail has purchased several databases, and done an imperfect merge - the possibilities of instead generating databases describing the individuals are fairly clear.

O.K.. - Mr. 57Zy65zz; it says here that you have given money to both
the NRA and HCI, you are currently taking prozac, you checked into a
drug rehab unit last year, and I just stopped you for crossing a solid
yellow line. Clearly, you are so screwed up as to be a danger to
yourself and others - I'll have to take you in.

Fantasy? Sure. But we have shown ourselves, as a society, to be unable to limit use of data for the purpose that it was collected. So we shouldn't be asking how to generate unique standard identifiers for individuals, but instead should be asking how to prevent bureaucracies from doing so.

- - - - - - - - - - - - - - - -

WHY USE OF SOCIAL SECURITY NUMBERS IS A PROBLEM

COMMENT BY DN:: The following is an excerpt from Chris Hilbert's "Frequently Asked Questions about Social Security Numbers."

Date: 24 Nov 1992 06:00:37 GMT
From: hibbert@xanadu.com (Chris Hibbert)
Subject: Social Security Number FAQ

What to do when they ask for your Social Security Number

by Chris Hibbert

Computer Professionals
for Social Responsibility
....
Why use of Social Security Numbers is a problem

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't at all secure; if someone makes up a nine-digit number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number: to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants, e.g.), or to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally giving a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers.

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whichever record it shows up on. When it happens accidentally, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

The market for stolen numbers increased in 1986, with the passage of the Immigration reform law. While making up a number is usually good enough to fool the public library, employers submit the number to the IRS, which cross checks with its own and SSA's records. Because of the checks, illegal workers need to know what name goes with the number so they won't be caught as quickly.

- - - - - - - - - - - - - - - -

DN COMMENT: The following contribution was in answer to a series of question I posed to Chris as I put together this summary.

From: hibbert@xanadu.com (Chris Hibbert)

One of the few points in your article that I disagreed with was the idea that we might solve a lot of problems by requiring people to use unique names. There are many problems that we might use unique universal IDs to solve, but there are also a lot of problems we'd create or exacerbate with such a system. One of the protections of our privacy currently is that not every database uses the same universal IDs, and so it's often a fair bit of trouble for someone who knows you in one context to find other information about you.

...

When people ask me about designing databases and want to know what to use for a universal ID, my usual answer is to suggest that they think real hard about how secure the system has to be, and what the penalties are for not realizing that someone already has an account. I don't have a good answer for making sure that you always match returning customers with their accounts, but assigning account numbers and requiring them to remember them works pretty well.

- - - - - - - - - - - - - - - -

MAKING ENTRIES IN DATABASES UNIQUE

COMMENT BY DN: Many people suggested that life would be solved if only we ensured that whenever a new name was entered into a database, it would be entered uniquely, so as not to combine records of different people. In my opinion, these proposals are technically reasonable and fundamentally flawed. They are flawed because they assume one or more of the following:

1. the person entering the data knows if this is a new entry or not.

This can't possibly be true when the database might have hundreds of millions of names (the world population is measured in the billions), when there are thousands of people entering the information, and when the person about whom the information is being entered either does not know, does not care, or deliberately does not wish to cooperate.

Every large database of names I know of suffers from problems of: the same person multiply entered (Donald A Norman is not the same as Donald Norman who is not the same as D.A. Norman. To say nothing of mistyping: D. Narman), and, simultaneously, the same records confusing two different people (the d. norman who wrote paper 1 is not really the same as the d. norman who wrote paper 2). (See the discussion of the U.S. Social Security database.)

I see no simple solution to this problem, despite the clever solutions proposed by respondents, of which I will here reprint a few:
END COMMENT BY DN:

- - - - - - - - - - - - - - - -

From: Will_Taber@dgc.mceo.dg.com

The initial problem is that the police database was designed with the assumption that name/DOB would be unique. A much simpler solution would seem to be to provide an occurrence number in the database. Each time a STEVEN REID or a JOHN A SMITH or a REGIS Q MISSLETHWAITE is entered into the database the occurrence number for that name is incremented and stored in the record for that individual. The database now has a unique ID for each individual and when there is confusion, information other than name (DOB, Address, Phone Number, what ever is available and relevant) can be used to determine which person is the one in question.

- - - - - - - - - - - - - - - -

From: shapiro@mica.Colorado.EDU (Andrew Shapiro)

In order for the police to identify someone they would type that persons name. If more than one person share that name then the computer would ask for some other identification, like DOB. If a single individual still cannot be identified the computer would guide the officer by asking for more information.

This system allows people to chose and use any name they would like while at the same time allows computer operators to identify individuals without confusion. I do not believe that people should be forced to conform to the inflexible programs software engineers write.

- - - - - - - - - - - - - - - -

From: s_titz@ira.uka.de (Olaf Titz)

There already is a system where all people have names chosen by themselves. It's IRC (Internet Relay Chat), where every person is known by a name ('nickname' is the term actually used; the real names of the people are known too) that he can choose himself freely, provided it does not exceed 9 characters and is globally unique. The latter is currently becoming a problem as the user base of IRC grows to several thousand people. Of course everyone wants a nick that has a meaning and fits the person, so the choice becomes increasingly difficult for new users. Some people have proposed to deal with the problem in an in this context already well-known way: adding information of locale. But many don't like that idea.

(More information on IRC can be found in a paper by Elizabeth Reid (emr@munagin.ee.mu.oz.au) titled 'Electropolis', which is carried by many anonymous FTP servers, including ftp.uni.kl.de.)

- - - - - - - - - - - - - - - -

COMMENT BY DN: The schemes above rely too much on the good faith of the person about whom the information is being entered. It is apt to lead to less commingling of records at the price of multiple records for the same person. I don't think the problem is in retrieval: the problem is in data entry. See some of the horror stories above.

Many people commented on the fact that there already exist registries for ensuring unique identification:

- - - - - - - - - - - - - - - -

From: faustus@ygdrasil.CS.Berkeley.EDU (Wayne A. Christopher)

A friend of mine in Sweden got a letter one day from the government, telling her that her name was too common, and would she mind changing her last name to her mother's maiden name? This may seem excessively paternalistic to many people in the US, but I guess it does make some sense.

- - - - - - - - - - - - - - -

From: craig@mnemosyne.MicroUnity.com (One of the people named Craig Hansen)

I believe the Screen Actors Guild has such a registry; many people have found their given name already taken and have been forced to take a "Stage Name." Ultimately, though, identifiers such as SSN are already unique, and these unique identifiers are at the root of the privacy concerns, because they are globally unique identifiers for information. The SSN makes it easy to join together pieces of the information from different databases, which permits the assembling of a dangerously complete dossier from a series of apparently benign releases of information.

COMMENT BY DN: See the discussion of SSN.

- - - - - - - - - - - - - - - -

From: Jim Morris <jhm+@andrew.cmu.edu>

How about a completely non-coercive service in which people (or their parents) could register their names and a few lines about themselves, subject to good taste, privacy, and other concerns. Then prospective parents could scan it and make their own judgments about what they are getting their kids into. I would imagine that the spread of names would increase.

- - - - - - - - - - - - - - -

From: Simon Marshall <S.Marshall@sequent.cc.hull.ac.uk>

I'd like to suggest the application of computer password techniques. We all know that the best password is computer generated gibberish, right? Even if we stick to lower case letters, two 5-letter identifiers, such as ``yloof lirpa'', would give something like 141 thousand billion different permutations, enough for a long time to come.

Though this technique is not often used for passwords, since they are difficult to remember, writing down your name in case you forget it would not render it useless. Indeed, just imagine the commercial possibilities, selling names that actually make sense to those with more money than sense. How much money do you think you could get if the computer came up with ``jdanq uayle'' for your name? Maybe not much, but you'd want to sell it anyway.

- - - - - - - - - - - - - - -

From: mcclella@yertle.Colorado.EDU (Gary McClelland)
>In other words, how to we get the benefits and avoid the risks?

I'll give it a try using Don's model of the California license plate system and the name database of the American Kennel Club as models to be modified for this larger purpose:

1. "Used" names only are recorded in the database.

2. Database is encrypted to prevent casual reading (although the experts at, say, NSA might still be able to read it).

3. From terminals lots of places, parents, new immigrants, people wanting to change their names, etc. could try out potential names. The test name is encrypted and checked for a match in the database. System replies only "OK" or "used."

4. Finding an unused name could be a pain. Here is where the AKC strategy applies. They encourage outlandish and multiple names to avoid duplicates (this can even be fun!). Just as one does not use the official AKC name for the dog very often (not on the dog tag, not when you want the dog to fetch your slippers, and not even with the vet, just for official registration forms at dog shows), one would use one's official name only on official documents (that is another problem of deciding just what documents require one's full name but that is not a new problem) and it could be used whenever it was necessary to avoid name collisions such as the Ottawa example that started this thread.

5. Some folks don't like long, complicated names for either themselves or their dogs. The AKC deals with this by simply adding a short number to the end of names that are duplicates. In this case, if the system indicated a desired name was a duplicate, one could be given the option of adding a short number (a true PIN!) or arbitrary character string to make the name unique. One would use this short extra part of one's name only for official purposes.

Obvious risks:
a. all those existing programs and official written forms that haven't left enough room for the long names

b. one could purposely try to select a confusing name by trying test names until finding a duplicate and then adding a short PIN such as "1"

I'm sure there are other obvious risks but they aren't "obvious" to me right now. Have at it!

BTW, once the system is set up I want to request
Gary Hubbard Willie McCovey McClelland

- - - - - - - - - - - - - - - -

NAMES; JR. AND SR. DO NOT MEAN RELATIONS

COMMENT BY DN: One interesting fact about names emerged:

From: Craig Partridge <craig@aland.bbn.com>

In your posting to RISKS, you left out one other trend. The advent of Jr. and Sr. (or Older and Younger) or other distinguishing features to label people. If a town had two John Smiths, quite often one would be John Smith Jr., the other John Smith Sr., even if they were not related. Furthermore, someone who was the John Smith Jr. in early life could become the John Smith Sr. in later life. Sufficiently confusing that the practice was largely dropped and we only use Jr. and Sr. for son and father these days.

COMMENT BY DN: I asked Craig: Did they ever use "the taller" or "the fatter" (fat John Smith)? He replied:

Not that I've heard of, once last names came into effect. (Before then it was quite common of course). What I've seen is using town names to distinguish (John Smith of Wayland) and Jr. and Sr. if that wasn't enough. My uninformed guess is that town name plus Jr. and Sr. worked pretty well in most cases.

But the Jr. and Sr. to mean younger and older stayed common practice until quite recently. Certainly through the 18th century in the US. (A common warning in genealogy books is to be aware of this practice and not assume Sr. is father of Jr.).

- - - - - - - - - - - - - - - -

COMMENT BY DN: My thanks to the many people who responded, some of whom were most helpful with multiple messages, clarifying, finding references, etc.

Don Norman (of Apple). Also Donald A. Norman (of the University of California, San Diego).

Donald A. Norman
Until December 31, 1992 Starting January 1, 1993
Cognitive Science Apple Computer, Inc

University of California, San Diego   1 Infinite Loop, MS 301-3G
La Jolla, CA 92093   Cupertino, CA 95014
E-mail (permanently valid): dnorman@ucsd.edu or AppleLink: dnorman

[And super thanks to Don for pulling this material
together. I think this was a very valuable effort. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 18

Thursday 10 December 1992

Contents

Miscarriages -- chip workers in the U.S., VDT users in Finland

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 10 Dec 92 9:55:54 PST

The four-year study by the University of California at Davis reports that women making computer chips have a 40% higher incidence of miscarriages than other workers in the same factories. It covered 15,000 workers at 14 factories in seven states. A previous study by the University of Massachusetts reported a 70% increased risk among women in a particular factory of Digital Equipment Corp. [Source: San Francisco Chronicle, 4 December 1992, p.1.]

Researchers in Finland have identified a statistically significant incidence of miscarriages among women using computer video display terminals that emit electromagnetic radiation of type ELF -- triple the expected normal. A report is being published in the American Journal of Epidemiology. [Source: San Francisco Chronicle, 10 December 1992, p.A7]

Incidentally, Paul Brodeur has another article on electromagnetic radiation effects in the New Yorker dated 7 December 1992. [RISKS readers will recall the previous series of three articles being discussed here, e.g., RISKS-9.06 and .07.]

> [Forewarned is not necessarily forearmed, even if you have four arms. But this problem really demands greater attention, even if there are some who say these studies are not definitive.]

Programming errors affect state lottery

Mark Seecof <marks@capnet.latimes.com>
Tue, 8 Dec 92 13:11:49 -0800

[unquoted paraphrasing and bracketed comments mine --Mark S.]

A story by Virginia Ellis in the Los Angeles Times (page A3, Tues 3 Dec 92) reports that programming errors associated with adding a new "keno" game to the Calif. state lottery "apparently caused some wagers made early Nov. 17 not to be logged into the main database. As a result terminals at retail outlets were unable to identify those tickets as winners. A separate programming oversight caused a similar problem in northern Calif. on Nov. 23, when for part of the day no tickets for any games could be cashed and validated, officials said."

The state controller's office is said to be asking whether pre-deployment testing of the new software was adequate. "Lottery Director Sharon Sharp acknowledged that the lottery pressed GTECH, the Rhode Island company that operates and maintains its computers, to get the games on-line by mid-Nov. but she insisted there was still time for keno to be adequately tested. ``We felt 110% comfortable,'' she said. ``In fact, we could have tested it for three more months and this still could have happened.''"

The lottery director downplayed the trouble, calling programming problems par for the course. Players affected by the troubles took a different view. At least one "replay" winner who couldn't get his free ticket from the computer was told by the lottery to use a complex by-mail procedure to collect his winnings. He decided that his time plus 29 cents postage was too much for a $1 return. The lottery director said that the system has an "elaborate backup system" which "ensures that no winner will be lost. She [Sharp] said she has since appointed an internal task force of computer technicians and auditors to investigate the problems and determining if damages should be assessed against GTECH." Another lottery official suggested that "operator error" may've been involved.

[And now the most interesting part...]

"The problems come just three months after the Calif. Lottery Commission approved a change in the GTECH contract that decreases by hundreds of thousands of dollars per day the maximum damages that can be assessed against the company for errors that affect computer performance. The change was approved without public discussion. Sharp said she proposed the change because the company was being asked to get the keno game ready on a short deadline. ``What was important was to be able to get the... cooperation of our supplier. The cooperation meant much more that whatever financial windfall you would or you wouldn't receive from... damages,'' she said. Since its introduction Nov. 16, Sharp said keno has added about $7 million a week to lottery revenues."

[I think that GTECH must have known that the lottery's proposed keno deployment schedule was too ambitious. Otherwise, why condition cooperation on the damage waiver? This story documents that the Lottery Commission traded off the risk of poor performance against the benefit of early deployment. The question is, did its assessment of this tradeoff calculate the costs (in time, irritation, and lost winnings due to unreasonable transaction costs to recover after computer failure) to players of failure, or only the costs to the lottery of delayed deployment? Should costs to players of failure be considered by the lottery? Or should it look only to its own balance sheet?]

Mark Seecof <marks@latimes.com>
Publishing Systems Department, Los Angeles Times

Systems causing unintended changes in behaviour

Doug Moore <doug.moore@canrem.com>
Wed, 9 Dec 1992 19:00:00 -0500

A couple of items in RISKS touched upon computer systems and technology affecting people's behaviour and causing changes in our society. There is a risk that some changes may be undesirable and unintended.

Sometimes the change comes about because the system lacks sufficient information and or isn't smart enough to handle it. When working at Bell Canada back in the '70s, I saw an example of that. A system was supposed to compare numbers of long distance operators working with the number required to handle the load of calls. Over the long term it was hoped the information would help in predicting staffing requirements based on various factors. However, it was also used to evaluate managers on their current success or lack of success in matching the number working with the number needed. One serious flaw was that the program assumed the actual number of operators working could be changed every half hour. This assumption was at odds with the union contract that put minimums on the number of hours in a shift and limits on scheduling of shifts. The result was that at the end of each day managers would spent an hour or more doing nothing but telling operators to unplug or plug into the system in an attempt to fool it. The managers' and operators behaviour was changed in a direction the company didn't intend.

On other occasions a change can come about simply because it is in some ways easier for a system to deal with data where quantities or levels are significant, compared to other data, and managers may place too much emphasis on that data.

The Metro Toronto Police may have changed their system now, but at one time, their system reported each week statistics on the activities of each police officer - just in order to ensure sound management of staff resources of course. Such things like numbers of parking tickets issued were easy to input and report. A wide variety of other activities, such as taking a lost child home, or spending some time checking into a broken window at a business, could not be as easily input or reported in meaningful ways, yet the value of those other activities may be far more. Supervisory officers would, of course, recognize the value of such activities in principle, but the common reaction to the weekly report was to notice such things as few parking tickets being issued, to require explanations when that happened, and to tell the officers to spend more time on issuing parking tickets so that next week's report wouldn't "look so bad". The net result of such a system to change the police officers' behaviour. While they would be unlikely to ignore other matters that came up, the officers would none the less concentrate on the activities that easily produced large numbers on the reports - such as issuing parking tickets.

In both of these examples changes happened that were not intended by anyone. How to predict and avoid or manage such changes may not be simple when a system is being designed or managed, but an effort is needed.

Doug Moore   Canada Remote Systems - Toronto, Ontario
                 World's Largest PCBOARD System - 416-629-7000/629-7044

ACM Code of Ethics and Professional Conduct; Ethics Starter Kit

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 9 Dec 92 10:56:39 PST

Adopted by the ACM Council on 16 Oct 1992, and certainly of interest to the entire RISKS community, not just to ACM members and Boy Scout programmer merit-badge seekers:

1. GENERAL MORAL IMPERATIVES.   As an ACM member I will
   1.1 Contribute to society and human well-being
   1.2 Avoid harm to others
   1.3 Be honest and trustworthy
   1.4 Be fair and take action not to discriminate
   1.5 Honor property rights including copyrights and patents
   1.6 Give proper credit for intellectual property
   1.7 Respect the privacy of others
   1.8 Honor confidentiality

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.
   As an ACM computing professional, I will
   2.1 Strive to achieve the highest quality, effectiveness, and dignity
     in both the process and products of professional work.
   2.2 Acquire and maintain professional competence.
   2.3 Know and respect existing laws pertaining to professional work.
   2.4 Accept and provide appropriate professional review

2.5 Give comprehensive and thorough evaluations of computer systems
and their impacts, including analysis of possible risks
2.6 Honor contracts, agreements, and assigned responsibilities
2.7 Improve public understanding of computing and its consequences
2.8 Access computing and communication resources only when
authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.
As an ACM member and an an organizational leader, I will
3.1 Articulate social responsibilities of members of an organizational
unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information
systems that enhance the quality of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's
computing and communication resources.
3.4 Ensure that users and those who will be affected by a system have
their needs clearly articulated during the assessment and design
of requirements; later, the system must be validated to meet [its]
requirements.
3.5 Articulate and support policies that protect the dignity of users
and others affected by a computing system.
3.6 Create opportunities for members of the organization to learn the
principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE. As an ACM member, I will
4.1 Uphold and promote the principles of this code.
4.2 Treat violations of this code as inconsistent with membership
in the ACM.

- -

Incidentally, a computer ethics "Starter Kit" intended for computer science/ engineering teachers, libraries, and media resource centers is available from the Research Center on Computing and Society, Southern Connecticut State University, 501 Crescent St., New Haven CT 06515 (rccs@scsu.ctstateu.edu, fax 1-203-397-4681). Ask for the RCCS Publications Catalog, which includes (among many other things) three videos, (1) Computer Ethics in the Computer Science Curriculum, (2) What is Computer Ethics?, and (3) Teaching Computer Ethics: Strategies and Cases, a monograph (Teaching Computer Ethics, proceedings of the teaching track from the National Conference on Computing and Values), and the CPSR collection of course syllabi by Batya Friedman and Terry Winograd. Prof. Terrell Ward Bynum is the Director of the RCCS.

PGN

Computers do it better

Don Norman <norman@cogsci.ucsd.edu>
Wed, 9 Dec 1992 10:09:55 -0800

The following just appeared on AppleLink, Apple's semi-public bulletin board and e-mail system. I have censored out identities. We all knew that the common, every-day errors many of us have with e-mail can lead to potential disasters affecting a huge number of people when world-wide WANs/LANs exist. Here is an example, this one evidently triggered by the blind carbon copy mechanism, which may reside invisibly on a message. Invisible information is never a good idea because it can lead to very visible results.

[Bad object-oriented software engineering, despite
parameterized information hiding (including X,
below) and inheritance of ancestors! ENCAPSULATION
is the key to GOOD information hiding. PGN]

In the Internet mail system, a blind cc is visible to the sender (as a line labelled bcc: list-of-names) but is not only invisible to the receivers, it ISN'T THERE, so that any reply by any of the receivers cannot go to the bcc list. That seems like the better way to do things. (Although a bcc list with 2,800 recipients is pretty amazing.)

Item [nnnnnnn] 8-Dec-92 14:48PST
From: [A]
To: Mailing List
Sub: BRAZIL LAN/MAIL ERROR

Please get this information to your workgroup immediately.

An unknown error or bug has caused an estimated 2800 people to be blind carbon copied on a message sent by [W] called BRAZIL ACCESSORY KITS. The area of the LAN affected has not totally been identified, so I am sending this memo to all Technical Coordinators.

It is important that you and your users DO NOT RESPOND to this memo, as each response is sent to another 2800 mailboxes.

Additionally, your users should delete any message called BRAZIL ACCESSORY KITS, or re:BRAZIL ACCESSORY KITS or fw:BRAZIL ACCESSORY KITS.

Various telecom and LAN managers are working with [W] and [X] to identify the problem. [Y] (phone number) is available if you need additional information.

[Rampent mispelings corekted bye PGN.]

Traces of Memory and the Orange Book

<kmeyer@aero.org>
Tue, 08 Dec 92 15:57:12 PST

Hardly an issue of RISKS goes by without a story of someone obtaining residual data--data that the original owner thought was gone. It's usually from a disk (issues of medical records, bbs files, and Prodigy come to mind), although most recently (RISKS 14.15) Tom Swiss points out that utilities exist to scour RAM for bits.

There's a common moral to all these stories that I feel a need to interject here: We'd all be better off (at least from a privacy perspective) if the

products we used minimally had security features equivalent to the C2 criteria
of the Orange Book ("U.S. Department of Defense Trusted Computer Security
Evaluation Criteria").

Specifically relating to residual data, it states: "No information, including
encrypted representations of information, produced by a prior subject's
actions is to be available to any subject that obtains access to an object
that has been released back to the system."

Of course, Tom wouldn't have been able to recover his own lost file, but one
might argue that a decent user interface would have prevented that in the
first place...

Kraig R. Meyer kmeyer@aero.org

[I might add that it is not just the reuse of the object that is risky, but the residues left over from incomplete deletion, irrespective of whether there is ever any reuse of the object. If an object is deallocated, its memory contents (primary, secondary, tertiary, backup, whatever) may still remain and be accessible to penetrators, system administrators, etc., EVEN IF THE ORIGINAL OBJECT IS NEVER REUSED. PGN]

Library sans card catalog

Patrick White <patbob@sequent.com>
Tue, 8 Dec 92 13:39:54 -0800

Here's a computer related risk I didn't expect to run into at my local public
library...

Over the last few years, the public library system has been converting the
card catalog and checkout system over to a (remote) centralized computer that
provides all sorts of nifty features like dial in access, ability to check if
a book is checked out, requesting books from other libraries and much more.
Well, in the last year or so, they found that the paper card catalog was not
being kept up to date, so, since they had the computer, they got rid of it.

Last week, a transformer blew and the computer went down (since it had no UPS,
it went down hard and recovery included fixing hardware as well as restoring
data).

While the computer was down, it was still possible to check out books
(apparently they had some sort of backup procedure in place for that), but
there was no card catalog -- one had to ask at the reference desk to get a
list of places to go look around in the stacks for books on their topic.

I talked with one of their computer services people and was told that they
plan to put in a UPS for next time so the machine can be taken down safely and
the data preserved, but there are no plans for anything beyond that (in
particular, no decentralization was planned). Obviously, another blown
transformer or some down power/phone lines (we are expecting an unusually
nasty winter thus year) could take out the card catalog again.

This certainly isn't a life-threatening sort of risk, but does illustrate one
risk of computerizing an index at a site distant from the records.

Pat White (patbob@sequent.com, work: (503) 578-3463)

Defence against hackers may be illegal; login banners grow

John Lloyd <JAL@VS32.dnet>
Mon, 7 Dec 92 17:41:57 PST

The following excerpt from CERT Advisory CA-92:19 suggests that it
may be a federal crime in the U.S. for computer system administrators
to take certain actions to defend their systems against a hacker.

The risk described here is not entirely about computing: it is mostly
a legal risk created, I think, by legislators and administrators that
are insufficiently aware of computing technologies and practises. A cynic
might suggest other reasons for these kinds of legal opinions.

Lines marked with > are direct quotes; see two other comments by me later.

John A Lloyd (enough to distinguish me from others, I hope!)
Supervisor, Technical Support
MacDonald, Dettwiler and Associates Ltd
Richmond BC Canada
jal@mda.ca

```
>
>CA-92:19                    CERT Advisory
>                         December 7, 1992
>                     Keystroke Logging Banner
>
>The CERT Coordination Center has received information from the United States
>Department of Justice, General Litigation and Legal Advice Section, Criminal
>Division, regarding keystroke monitoring by computer systems administrators,
>as a method of protecting computer systems from unauthorized access.
>
>The information that follows is based on the Justice Department's advice
>to all federal agencies.  CERT strongly suggests adding a notice banner
>such as the one included below to all systems.  Sites not covered by U.S.
>law should consult their legal counsel.
>
>   The legality of such monitoring is governed by 18 U.S.C. section 2510
>   et seq.  That statute was last amended in 1986, years before the words
>   "virus" and "worm" became part of our everyday vocabulary.  Therefore,
>   not surprisingly, the statute does not directly address the propriety
>   of keystroke monitoring by system administrators.
>
>   Attorneys for the Department have engaged in a review of the statute
>   and its legislative history.  We believe that such keystroke monitoring
>   of intruders may be defensible under the statute.  However, the statute
>   does not expressly authorize such monitoring.  Moreover, no court has
```

> yet had an opportunity to rule on this issue. If the courts were to
> decide that such monitoring is improper, it would potentially give rise
> to both criminal and civil liability for system administrators.
> Therefore, absent clear guidance from the courts, we believe it is
> advisable for system administrators who will be engaged in such
> monitoring to give notice to those who would be subject to monitoring
> that, by using the system, they are expressly consenting to such
> monitoring. Since it is important that unauthorized intruders be given
> notice, some form of banner notice at the time of signing on to the
> system is required. Simply providing written notice in advance to only
> authorized users will not be sufficient to place outside hackers on
> notice.

In other words, you must "give notice" lest you be convicted of snooping (and, of course being a victim of unauthorized monitoring your attacker will go free.) How do you ensure that snoops, crackers and disgruntled employees are guaranteed to view a message when you can't guarantee they are prevented from logging in in the first place? Catch-22, eh?

> An agency's banner should give clear and unequivocal notice to
> intruders that by signing onto the system they are expressly consenting
> to such monitoring. The banner should also indicate to authorized
> users that they may be monitored during the effort to monitor the
> intruder (e.g., if a hacker is downloading a user's file, keystroke
> monitoring will intercept both the hacker's download command and the
> authorized user's file). We also understand that system administrators
> may in some cases monitor authorized users in the course of routine
> system maintenance. If this is the case, the banner should indicate
> this fact. An example of an appropriate banner might be as follows:
>
> This system is for the use of authorized users only.
> Individuals using this computer system without authority, or in
> excess of their authority, are subject to having all of their
> activities on this system monitored and recorded by system
> personnel.
>
> In the course of monitoring individuals improperly using this
> system, or in the course of system maintenance, the activities
> of authorized users may also be monitored.
>
> Anyone using this system expressly consents to such monitoring
> and is advised that if such monitoring reveals possible
> evidence of criminal activity, system personnel may provide the
> evidence of such monitoring to law enforcement officials.
>
>Each site using this suggested banner should tailor it to their precise
>needs. Any questions should be directed to your organization's legal
>counsel.

Given that notices that appear on the outside of shrink-wrap software boxes have been held not to constitute a contract; nor that system demands for "passwords" and "identification" are considered insufficient evidence that authorized secure access is intended, I find it unlikely that any mere textual bulletin supplied AFTER logging in would be considered sufficient notice to

unauthorized users. Most systems let you interrupt such displays anyway. And
are you sure that your cracker can read at 9600 baud?

>The CERT Coordination Center wishes to thank Robert S. Mueller, III,
>Scott Charney and Marty Stansell-Gamm from the United States Department
>of Justice for their help in preparing this Advisory.
>
>If you believe that your system has been compromised, contact the CERT
>Coordination Center or your representative in FIRST (Forum of Incident
>Response and Security Teams).
>
>Internet E-mail: cert@cert.org
>Telephone: 412-268-7090 (24-hour hotline)
>   CERT personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
>   on call for emergencies during other hours.
>
>CERT Coordination Center
>Software Engineering Institute
>Carnegie Mellon University
>Pittsburgh, PA 15213-3890
>
>Past advisories, information about FIRST representatives, and other
>information related to computer security are available for anonymous FTP
>from cert.org (192.88.209.5).

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 19

Tuesday 22 December 1992

Contents

Computer error leaves Bundestag speechless

Debora Weber-Wulff <weberwu@inf.fu-berlin.de>
Fri, 11 Dec 1992 09:02:51 GMT

The German Bundestag, which had just moved into its brand-new, expensive quarters in Bonn (they'll be moving to Berlin someday, but this building was started when the Wall was still up), has been forced to move back into its old plenary building because of computer errors.

The new building was installed with a special sound control system that was specifically designed to eliminate all the problems with feedback, screeching, volume adjustments and such that had plagued the old system. During the big budget debate (where the cost overruns in the new building were to be discussed as well :-) the sound system turned itself down to a whisper - no one could follow the speeches. After a 5 hour pause while technicians searched for the cause, the Bundestag moved back into the old building to resume the debates.

The cause: The architects had worked out an extremely symbolic form and used symbolic materials to create the building. The plenary chamber is round and completely enclosed in (bullet-proof) glass, to underline the transparancy of the parliamentary process. This glass, however, does not absorb the sound, but rather it bounces it back. The computers, detecting feedback, turn down the volume to avoid this problem. A steady state is only achieved when the microphones are turned off. It will take until March to either replace the computerized system or put carpeting over the glass walls.

```
Debora Weber-Wulff                 dww@inf.fu-berlin.de
Institut fuer Informatik           +49 30 89691 124
Nestorstr. 8-9                     (INCLUDE "standard.disclaimer")
D-W-1000 Berlin 31                 (PRINTN (WITTY-MESSAGE TODAY))
```

Doctor service phone logs skewed

<steen@kiwi.swhs.ohio-state.edu>
Fri, 11 Dec 92 13:13:26 EST

A new central system is being tested in Denmark for people to call a doctor service at off hours, and possibly get a housecall (this is for non-emergency cases, i.e., not the equivalent of 911). The patients in the Danish city of Odense complained loudly that the waiting for a phone call to be answered was too long, while the provider said their computerized logs showed no caller had to wait more than 10 minutes. After many complaints they tested the equipment, which showed it was not able to register waits longer than 10 minutes! Steen Hansen

If you are interested in further details, please e-mail lea@dde.dk (Leif Erik Andersen), who quotes the danish radio news on Dec 9, 1992.

> Den nye laegevagt paa Fyn har maattet erkende, at systemet ikke var saa velfungerende som laegerne haevdede. Paa trods af gentagne klager fra patienter over lange ventetider paa telefonen, haevdede laegevagtens ansatte at ingen havde ventet i mere en ti minutter. I gaar kom det saa frem, at edb-registreringen ikke kunne registrere ventetider laenger end de ti minutter! Laegerne stolede blindt paa udstyr, som slet ikke var beregnet til at registrere ventetid, ifoelge Fyns Telefon. Laegevagtens leder, Per Holm Pedersen, har givet fynboerne en 'uforbeholden undskyldning'. [DR, onsdag]

Statistical biasing (Re: Moore, RISKS 14.18)

Clay Jackson <uswnvg!cjackso@uunet.UU.NET>
Fri, 11 Dec 92 17:39:28 GMT

|A couple of items in RISKS touched upon computer systems and technology
|affecting people's behaviour and causing changes in our society. There is
|a risk that some changes may be undesirable and unintended.

When I was a supervisor in a large phone-in technical support operation (a few years back now), we introduced a metrics program that recorded a number of statistics about the calls the techicians were processing. Two of those statistics were "Available Time" (time spent being available to take calls, even if there were no calls coming to your phone) and time per call. One of the other managers decided to set minimum standards for all of the metrics. So, an enterprising tech wrote a program on a PC to dial home (where no one was there to answer the phone), wait some random time and then hang up and dial again. Until we caught on, that person's statistics were the best in the group; and the others in the group (who knew what was going on) were grumbling. Fortunately, we caught it before permanent damage (i.e., a changed performance rating or some sort of salary adjustment) was done.

Clay Jackson - N7QNM, US WEST NewVector Group Inc, Bellevue, WA

Solution found to risks of computers in elections!

<wolit@mhuxd.att.com>
Fri, 18 Dec 92 16:43 EST

According to the Associated Press today, officials in South Korea decided to use the abacus to tabulate 24 million votes in Friday's presidential elections. The abacus was used to avoid a recurrence of charges in the 1987 presidential race that the computer count was electronically manipulated. The Central Election Management Committee employed about 300 abacus experts to oversee the counting.

It's curious that these people find manual manipuation -- an unnecessary backformation, since manipulation MEANS movement by hand -- of an election to be preferable to electronic manipulation.

wolit@mhuxd.att.com
Jan I. Wolitzky, AT&T Bell Laboratories, 600 Mountain Avenue, Room 3D-590,
Murray Hill, NJ 07974-2070 1-908-582-2998 Fax: 1-908-582-5417

[A Deutsche Press-Agentur news item quoted a Committee official who said, "We are sorry we can't use the fast and economical way of tallying with computers but we like to be fair and accurate above all." PGN]

Overheard by Don Knuth on recent trip

Les Earnest <les@sail.stanford.edu>
Tue, 15 Dec 92 14:48:18 -0800

From: Phyllis Winkler <winkler@cs.stanford.edu>
Subject: Overheard by Don Knuth on recent trip

Q. What kind of computer music will President Clinton play on his saxophone?

A. Al Gore rhythms.

--- Cornell U Linguistics Department

Flying Books Threaten Computer Inventory

Bill McGeehan <IRMTAQA2@SIVM.SI.EDU>
Mon, 14 Dec 92 10:51:19 EST

A story in the Washington Post on 7 Dec 92 entitled "Va. Book Vendor Rescued from a Storied Ending" ended with lessons in both safety in the library and computer security. The following is a summary of that article:

Mike Keck was nearly buried alive in his Alexandria Virginia bookstore, From Out of the Past. Mike was working in the "aviation" section when a metal shelf attached to a wall came "flying" loose, tipped over and started a domino effect that quickly toppled almost one million magazines. "As I fell, I twisted to protect myself; the twisting broke the socket of my hip." His wife, Barbara said, "Once it started, there was no stopping it. All the racks gave way". The rescue squad had to use a torch to cut away the twisted metal that was trapping Mike.

Barbara also said "I videotaped it ... for insurance purposes. Right now the computer doesn't look like it was damaged. ALL MY INVENTORY IS IN IT, AND I HOPE IT WILL BE OK."

I was struck by this thought: would that be a MILLION records? Wouldn't some offsite backup be appropriate?

Bill McGeehan, Smithsonian Institution, OIRM Computer Security Manager
IRMTAQA2@SIVM.SI.EDU IRMTAQA2@SIVM.BITNET Voice: (202) 633-9035

Navy Cancels Jammer System

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 19 Dec 92 14:52:17 PST

WASHINGTON (AP, 15 Dec 92)
The Navy on Tuesday canceled $835 million worth of contracts for an electronic radar-jamming system criticized for years inside the Pentagon and on Capitol Hill. The Airborne Self-Protection Jammer was being developed by the Navy for a variety of carrier-based warplanes, such as the F-14, F/A-18 and the E/A-6. The Pentagon had spent more than 15 years and $1.5 billion to develop the system. It had ordered 136 of the devices, which were supposed to confuse enemy surface-to-air missile radars. But the system, which was being developed by a number of firms, never passed its flight tests. At one point, the Navy acknowledged that testing standards on the system had been relaxed, but the system was unable to meet even the lowered standards. Over the years, the jammer became a symbol of weapons kept in development before the bugs were

ironed out.
In its statement, the Navy said, "The decision to terminate ... was made because it was determined in operational testing that the system was not operationally effective and not operationally suitable." The Navy said it was canceling nine production contracts with: Consolidated Electronic Countermeasures, which is composed of I.T.T. of Nutley N.J., and Westinghouse of Baltimore., Md.; I.T.T. and Westinghouse, operating separately; Westinghouse Electronic Systems Co., (Welsco) of Baltimore, Md., and Smith Industries of Florham Park, N.J. ...
Earlier this year, Sens. David Pryor, D.-Ark., and William V. Roth Jr., R-Del., charged that the Pentagon had manipulated its testing data to minimize the system's problems, but the Navy promised it would apply toughened standards.

public information

Phil Agre <pagre@weber.ucsd.edu>
Thu, 17 Dec 92 17:17:47 -0800

A number of advocacy groups have recently been involved in efforts to make public information, for example from the Congress, available electronically. One of the reasons frequently cited for such efforts is the desire for open government. This notion of open government is normally opposed to a set of images of behind-closed-doors government in which politicians cut deals with cigar-smoking lobbyists. Although open government is a good thing in the abstract, I wonder if many of the motivations for it are misplaced, leading to false solutions to deeper problems. As evidence for this possibility, I would cite the following article:

Robert L. Heath, Working through trade associations and public information organizations, in Robert L. Heath, ed, Strategic Issues Management: How Organizations Influence and Respond to Public Interests and Policies, San Francisco: Jossey-Bass, 1988.

This is a brief description of NAMNET, a computer network that has been operated by the National Association of Manufacturers since 1987. NAM, of course, has long been famous for its aggressive and well-funded lobbying on issues such as labor organizing and workplace health and safety regulations. (It opposes these things.) Among the many features of NAMNET is software support for what has become known in business as "grassroots lobbying", in which a special interest with substantial infrastructure (whether in-house or contracted from commercial firms) mobilizes its allies in a highly selective and focused way on very short notice to influence the proceedings of, for example, a legislature.

Now, some people argue that electronic open government will level the playing field by giving The People access to the same information as special interests. But maybe it doesn't work that way. Techniques like NAM's (and others, such as direct mail techniques based on the application of massive computing power to databases of personal information) have brought a quiet revolution to the day-to-day conduct of politics. Far from being run behind closed doors, information technology now allows politics to be conducted through the rapid, top-down, real-time mobilization of massive "constituencies". And these methods quickly come down to money: it is now entirely feasible to purchase a precise, measurable amount of pressure on any given issue on any Senator of your choice. The more money you have, the more pressure you can buy. (For more of this, see Wm. Greider's book "Who Will Tell the People?")

So how about it? If we wish to strengthen democracy, should we welcome electronic "open government" or oppose it? What alternative models of information technology's relationship to government would be less amenable to high-powered manipulation and more amenable to the electronic cultures within which we might reinvent democracy?

Phil Agre, UCSD

Call for Comments on Computing and the Clinton Administration

Gary Chapman <chapman@silver.lcs.mit.edu>
Wed, 16 Dec 92 12:43:20 -0500

PLEASE CIRCULATE THIS WHEREVER YOU FEEL IT IS APPROPRIATE
BUT ONLY WHERE YOU FEEL IT IS APPROPRIATE

AN OPPORTUNITY TO HAVE YOUR SAY ABOUT COMPUTING IN THE FUTURE

This is Gary Chapman, director of the Cambridge, Massachusetts, office of Computer Professionals for Social Responsibility. I edit The CPSR Newsletter, a quarterly publication that goes to all CPSR members and about 400 other people, including a lot of policymakers, members of Congress, administration officials, etc.

We're going to try something unusual for the next CPSR Newsletter, and I'm putting out a call for help. We're going to publish a special issue on "What the Clinton Administration Can Do For The Computing Profession and the Public." I'm sending out this message to ask people to send me SHORT contributions to this issue, just brief comments about what the new administration can do to help support computing in the United States, or perhaps the world.

Here are a few basic guidelines for these submissions:

1. SHORT MEANS SHORT -- In order to publish as many of these as we can, we need to keep each contribution to about 100-150 words, max, one or two paragraphs. In fact, anything longer will probably be eliminated out of fairness to others.

2. YOU MUST IDENTIFY YOURSELF -- Again, briefly, with just your name and one line that says something about you, such as Joe Blow or Sally Smith, Programmer, BillyBob Corporation, or Centerville, Ohio, or something like that, whatever you prefer.

3. ADDRESS ISSUES OF PUBLIC POLICY -- In order to make these

contributions relevant to the Clinton administration, they should concern issues about which government can or should do something, or stop doing, whatever. These include major issues such as privacy, access to information, computer networks like the Internet or NREN, R&D priorities, equitable access to computers, intellectual property, defense policy, risks to the public, etc. We're not really interested in contributions that are self-serving, parochial, excessively arcane or trivial, belligerently and unconstructively critical, and so on. We will favor messages that discuss the intersection of computing and major issues of concern to the public at large.

4. PLEASE INCLUDE A WORKABLE E-MAIL ADDRESS -- In case I have to get back to you about the text. We won't publish e-mail addresses, I promise.

5. GET ALL CONTRIBUTIONS TO ME BY JANUARY 15, 1993. My e-mail address is chapman@silver.lcs.mit.edu.

This is not limited to people in the United States, although overseas contributors will have to make a case for what the Clinton administration should do to help international computing -- the focus will be on U.S. government policy.

We're going to try and get this issue into the hands of the key players on computing and high tech policy in the new administration. For the most part we already know who those people are, and we're talking to them about the issues that CPSR is working on. This newsletter will give them a good impression, we hope, of the concerns of the computing profession and people who use computer networks. Consider this an opportunity for a kind of "hard copy" town hall.

Thanks for your help! Get those messages coming!

Gary Chapman, Coordinator The 21st Century Project
Computer Professionals for Social Responsibility
Cambridge, MA chapman@silver.lcs.mit.edu

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 20

Thurs 31 December 1992

Contents

Another Jail Computer Glitch

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 30 Dec 92 11:16:35 PST

Around 7pm on 27 December 1992, the new San Joaquin (California) County Jail computer system automagically unlocked all of the cell doors in a high-risk area, with a highly audible series of loud clicks, releasing about 120 potentially dangerous inmates who were being held in an "administrative segregation pod." Fortunately, the pod was itself isolated by other doors that remained locked. The glitch was attributed to a spurious signal from the "incoder card" whose responsibilities include opening those doors in emergencies. [Source: San Francisco Chronicle, 30 Dec 1992, p.A14, article by Peter Fimrite]

Fimrite's article also noted other California cell-door problems. Less than a year after the supposedly escape-proof Pelican Bay State Prison near Crescent City CA opened, inmates learned how to pop open the pneumatic cell doors at will. A similar system in the Santa Rita Jail in Alameda County was also found to be pickable. [If it had required breaking DES, that situation might have been DES-pickable!]

For those of you new to RISKS (or in case Fimrite or his Chron colleages see this in RISKS), our archives include the following computer-related cases. (Rather than grep-ing through the back issues, I give references to back issues of the ACM SIGSOFT Software Engineering Notes, containing material derived from the earlier issues of RISKS. S 10 1 is dated Jan 84, S 12 4 is Oct 87, S 13 4 is Oct 88, S 17 1 is Jan 92.)

..... Earlier prison problems
Santa Clara prison data system (inmate altered release date) (S 10 1)
Drug kingpin escapes LA County prison via bogus release message (S 12 4)
Convicted forger released from Tucson jail via bogus fax (S 17 1)
Seven Santa Fe inmates escaped; prison control computer blamed (S 12 4)
Oregon prisoner escaped; frequent-false-alarm alarm ignored (S 12 4)
New Dutch computer system frees criminals, arrests innocent; old system
  eliminated, and no backup possible! (S 12 4)
New El Dorado jail cell doors won't lock -- computer controlled (S 13 4)

Antiviral technology target of legal action

Peter G. Neumann <neumann@csl.sri.com>
Thu, 31 Dec 92 11:31:38 PST

The Washington Post has an article by John Burgess (at least some of which appears in today's San Francisco Chronicle) discussing a federal judge's order to McAfee Associates of Santa Clara CA, to stop distributing their Pro-Scan Version 2.31 and ViruCide Version 2.33 and derivative products. Imageline Inc. of Richmond VA (maker of PicturePak and ValuePak) has sued McAfee Associates for libel, fraud, and other misdeeds, because those antiviral products mistakenly identify Imageline products as containing viruses. Stay tuned for further details.

Dutch chemical plant explodes due to typing error

<rmoonen@ihlpl.att.com>
Wed, 23 Dec 92 09:26 GMT

In the first half of this year the chemical factory Cindu exploded causing several deaths and a chaos. It was confirmed yesterday that a simple typing error led to this tragic accident. Apparently the computerised chemical processing installation was fed with data in which a comma was placed at a wrong digit, causing the wrong amount of chemicals to be mixed in the installation. This led to an enormous explosion and the closure of the factory.

The Dutch news said that the responsible person has been found and he will be charged with negligible conduct causing death.

BTW: This year has been disaster-year for the Netherlands. We have had 2 serious plane crashes: the well-known El al 747 that crashed into two apartment buildings, the DC10 with 300 Dutchmen aboard that crashed in Faro this week. We had the Cindu explosion, an earthquake (yes, in Holland) 2 major train-accidents, and quite a few lesser accidents. I hope the next year will have some mercy on us :-)

--Ralph Moonen

911 in Massachussetts

Barry Shein <bzs@world.std.com>
Wed, 30 Dec 1992 01:24:42 -0500

I assume you have already been inundated with the issue of the woman who was murdered by (her ex-husband I believe) here in Boston. It seems she dialed 911 when she heard him at the door but unfortunately her exchange was a Brookline exchange (a neighboring township a few blocks away, not politically part of Boston), so the 911 call went to the Brookline Police. On hearing her address the Brookline police informed her she needed to call the Boston Police.

I am not certain of the exact details of what ensued (I'm not sure anyone outside of the Police departments is certain yet), the Brookline police claim the delay would not have made any difference in the outcome (her murder), but of course that's a fairly convenient position for them to take.

This has been a front-page story in the Boston Globe these last few days. Makes one want to pick up their phone and dial 911 and see exactly who you get and ask whether they would actually come should you need them.

-Barry Shein

Software Tool & Die   bzs@world.std.com uunet!world!bzs 617-739-0202

What about "little brother?"

Brian Seborg <seborg@first.org>
Wed, 23 Dec 92 12:28:17 EST

In the past we have tried to control information collected by "Big Brother" or the Federal Government. I believe that this has for the most part been accomplished. What has not been done, and what seriously needs to be addressed is the collection and dissemination of information by numerous "Little Brothers." Specifically, additional guidance is needed to protect information maintained by credit reporting agencies, State Government agencies, retail stores, and other entities which routinely collect information that can be linked to an individual by name or other unique identifier.

Since I teach a computer security class at a local college, the issue of privacy seems even more important once you know how many ways the information can be compromised. After a lecture on privacy one of my students mentioned that he worked with some private investigators, and he mentioned that they routinely had access to all kinds of information on people, and that agencies such as the state department of motor vehicles routinely sold access to their records to just about anyone.

To illustrate the problem I asked the student to initiate an inquiry and to see what he could find out with only my name as information. The next class he brought me the results of his spending about 30 minutes at a computer terminal. Here is a partial list of what he provided me in printed form: my current address, the addresses of all my previous residences, a list of all of the automobiles I have ever owned, my social security number, my drivers license number, a list of all of the credit cards I have ever owned including cancelled cards, their credit limits, the credit card numbers, and the current balance, the name and address of my employer, my father and brother's name and address, the name of my wife, the name address and phone numbers of all of my neighbors, their date of residence, and the type of home they had, my criminal record (blank) along with any pending cases, my traffic record (not blank unfortunately! :-)), my race, my income, the amount of my mortgage, my credit rating, etc. I imagine that most people have no idea that such information about them is so easily accessible. Imagine the potential for coming up with a detailed profile of a person once you begin associating individuals to the groceries they buy if the current trend of using check cashing cards or bank-cards to pay for groceries really catches on! For example, could you imagine who might want to have access to lists of customers which bought specific products? Giant supermarkets (a large chain in our area) already has the computer printing out coupons based on the purchases you have made, what would they do with this information if they could associate you with the groceries you bought? One could imagine the following phone call after purchasing a bladder control product: "Yes, Mr. Seborg, this is the office of Dr. Nosey, Urologist, we are offering five dollars off your initial consultation, when can we schedule you for your first appointment?" Or worse, you could have someone inferring some personal profile based on your patterns of consumption. Far fetched, maybe, but I bet you may think before you use that bank card, or check cashing card next time at the grocery store, eh?

Brian Seborg, VDS Advanced Research Group seborg@csrc.ncsl.nist.gov

Re: Electronic democracy (Agre, RISKS-14.19)

Barbara Simons <simons@almaden.ibm.com>

Wed, 23 Dec 92 12:36:33 PST

>Now, some people argue that electronic open government will level the
>playing field by giving The People access to the same information as special
>interests. But maybe it doesn't work that way. ....

Agre then goes on to ask if we should welcome or oppose electronic "open government" if our primary interest is in strengthening democracy.

I agree that there are many pitfalls related to the question of electronic democracy as it is usually described. The one that I find most disturbing is the question of access. Users of the net tend to be white males from a certain age group and socio-economic class. There are very few representatives of the impoverished underclass on the net, and women are very much underrepresented. Also underrepresented are old people and very young people. If we were to increase access to government for users of the net, we would be increasing access for a relatively prosperous, well educated, and successful group, at the expense of much of the rest of the country. This is not a healthy situation for a democracy.

There is a serious risk of disenfranchisement contained within the standard description of electronic democracy. While this may not be the sort of risk usually discussed in this forum, it is nonetheless significant, and it is possible only because of computers.

Barbara Simons

Re: Programming errors affect state lottery (Seecof, RISKS-14.18)

Charles D. Ellis <cde@aplexus.jhuapl.edu>
Fri, 18 Dec 1992 19:19:28 GMT

GTECH, the company which got the mysteriously beneficial contract change indemnifying them from operational goofs is in the news big time here in Maryland.

It seems that allofasudden/outoftheblue they were awarded a contract for Keno which was a total surprise to all, including the state legislature. The no-bid award was justified due to a "fiscal emergency".

They must have one hell of a contracts department!

Charlie Ellis cde@aplexus.jhuapl.edu

Re: Bundestag speechless (Weber-Wulff, RISKS-14.19)

Boris Hemkemeier <boris@math30.mathematik.uni-bielefeld.de>
Sun, 27 Dec 1992 20:01:46 +0100

The earlier report is only the half story. The president of the German Bundestag has a new priority button that switches off all microphones except his own. After resuming the debates in the new building, Johnny Klein put a heavy book on the button and didn't notice the effect. Security personal prevented technicians from entering the Bundestag. Then the parliament decided to move back to his old building, which incidentally is controlled by the same (working!) computer. (See the German newspaper, Die Zeit, "Johnny griff daneben", for details.)

Boris Hemkemeier
boris@mathematik.uni-bielefeld.de.

[Eine KLEINe NICHTmusik! PGN]

Re: ... Bundestag speechless (Weber-Wulff, RISKS-14.19)

"Markus U. Mock" <mock@ira.uka.de>
Wed, 23 Dec 92 15:39:43 MET

[...] If this event shows the risks of complex technical systems, the light was actually cast on the un-informed 'user' community and the lack of information transfer to those who will use the systems. [...]

Markus U. Mock, University of Karlsruhe, Dept. of Computer Science
mock@ira.uka.de ukj6@dkauni2.bitnet

Bundestag sound problems (RISKS 14.19)

Daniel Burstein <0001964967@mcimail.com>
Wed, 23 Dec 92 04:15 GMT

Hmm, seems I recall seeing this problem demonstrated at length in the mid 1960's. Didn't Don Adams and Barbara Feldon (and Edward Platt) repeatedly run into problems of this sort when using the "Cone of Silence" over at "Control"?

Since the show was a continuing news documentary describing actions of spy agencies, one would have thought that if anyone had studied it intensly, it would have been the (then) East and West Germans...

Danny <dburstein@mcimail.com> <----direct e-mail address

(A quick note to our younger crowd: The television show in question was "Get Smart," which was kind of a spoof on the entire spy genre. It is currently in syndication throughout the United States, and quite a few other countries as well).

Latest (?) credit card scams

Jerry Leichter <leichter@lrw.com>
Tue, 29 Dec 92 16:56:45 EDT

As I was paying for some magazines at a local bookstore today, I happened to notice two interesting bulletins to store owners - passed on to the people minding the cash registers - about the latest in credit card fraud. There are two closely related frauds involved:

1. Credit cards with their magnetic stripes re-recorded with a different, but valid, account number. Since these days pretty much the entire system runs on what is read off the magnetic stripe, with a complete receipt printed for you without a need to emboss anything from the original card, this is a great way to charge things to someone else.

   Their recommendation: Cross-check the information embossed on the card with the information printed on the receipt. There's a reward offered to anyone who finds a "magnetically forged" card this way. In practice, don't bet the ranch. It's hard enough to find anyone who bothers to check the signature any more; how many people will bother to check long strings of digits? It's worth keeping in mind that unless the card IS checked, there is no good way to prove, or even reliably detect, the fraud later: The only information in the system is what came off the magnetic stripe. (Well, you do have the signature - but do stores even bother to keep all those signed, printed receipts? Finding any particular one would be a horrible job.)

2. Someone has apparently gone into business creating fake credit cards with valid (stolen) credit card numbers on them. They are currently easily detectable because they all bear the name of some particular non-existent bank. If the creator had thought about this a bit, he would have created fake Citibank or AT&T cards - even if it were hard to get them to look *exactly* like the real ones, they'd still be much, much harder to detect than cards "issued" by a specific "First Federal of Oshkosh", which since it doesn't exists has issued NO real cards. (I hope I haven't given anyone a new idea.)

The potential losses here are staggering. I don't know who ends up stuck with the immediate bill for these losses - certainly not the owner of the valid, stolen credit card (though proving that a fraud has taken place could be time consuming and painful), most likely not the retailer (after all, he DID get a "valid card/good transaction" response from whatever agency he checks with). There should be some interesting finger-pointing between the issuing banks and the transaction approving agencies.

In the end, of course, we all end up paying. Check your monthly bills carefully!

-- Jerry

Risks of satellite-controlled anti-theft devices

Jim "The Big Dweeb" Griffith <griffith@xcf.Berkeley.EDU>
Tue, 29 Dec 92 23:49:54 -0800

Here in the Bay Area, there has been a rash of carjacking crimes. In San Francisco alone, there have been around 60 carjackings in the past six months or so. Several people have been injured when resisting a carjacker - the latest being a young man who was shot in the head on Christmas Eve when he wouldn't give up his car. The police recommend that drivers should give up their cars to would-be car-jackers, since a life is more valuable than a car.

Naturally, Silicon Valley has been working on the problem, the first solution being a remote-controlled ignition kill switch, operated from a fob such as those used with active car alarms. One of our local stations had a blurb about the latest innovation, which uses pager technology to allow a car owner to dial a 1-800 number, triggering a pager-like satellite signal which causes a particular car to kill its ignition. This way, car owners can calmly let a carjacker escape with the vehicle, then walk to the nearest telephone and stop the car in its tracks.

I thought this was a rather clever use of technology, so I gleefully told one of my house-mates about it. His reaction was "gee Jim, now I can hassle you without ever leaving the house". This kind of stopped me in my tracks, and after having thought about it a bit, a number of risks seem evident. Basically, any kind of "wrong number" risk can potentially create a serious traffic hazard, as well as resulting in personal annoyance (depending on the mechanism used to re-allow ignition - especially when the user doesn't have a car-phone). You've then got yet another number that you must guard as closely as an ATM code, but which contains significantly more digits to remember (the 1-800 number plus a password-like code), and keeping track of that while keeping it away from others is hard. Plus, a single fault at a pager company can cause large-scale regional traffic disruptions (if the device becomes popular, which it probably will).

Jim

OECD Security Guidelines

Marc Rotenberg <Marc_Rotenberg@washofc.cpsr.org>
Wed, 30 Dec 1992 17:51:47 EST

The Organization for Economic Cooperation and Development (OECD) has adopted international Guidelines for the Security of Information Systems. The Guidelines are intended to raise awareness of the risks in the use of information systems and to establish a policy framework to address public concerns.

The OECD Security Guidelines should be of special interest to RISKS readers. They are similar in form to the 1980 OECD Privacy Guidelines and will probably have a substantial impact on security policy.

Of course, there are lots of issues left open by the Guidelines, including the relationship between privacy and security. But the principles offer a good starting point for public discussion on security and risks-related issues.

A copy of the press release and an excerpt from the Guidelines

follows. For additional information or for a copy of the Guidelines, contact
Ms. Deborah Hurley, OECD, 2, rue Andre-Pascal, 75775 Paris Cedex 16, France
33-1-45-24-93-71 (tel) 33-1-45-24-93-32 (fax).

Marc Rotenberg, Director, CPSR Washington office and Member, OECD Expert
Group on Information System Security rotenberg@washoc.cpsr.org

===

OECD ADOPTS GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

The 24 OECD Member countries on 26th November 1992 adopted Guidelines for the Security of Information Systems, culminating almost two years' work by an OECD expert group composed of governmental delegates, scholars in the fields of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users.

The term information systems includes computers, communication facilities, computer and communication networks and the information that they process. These systems play an increasingly significant and pervasive role in a multitude of activities, including national economies, international trade, government and business operation, health care, energy, transport, communications and education.

Security of information systems means the protection of the availability, integrity, and confidentiality of information systems. It is an international issue because information systems frequently cross national boundaries.

While growing use of information systems has generated many benefits, it has also shown up a widening gap between the need to protect systems and the degree of protection currently in place. Society has become very dependent on technologies that are not yet sufficiently dependable. All individuals and organizations have a need for proper information system operations (e.g. in hospitals, air traffic control and nuclear power plants).

Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be used to their full potential and further growth and innovation may be prohibited.

The Guidelines for the Security of Information Systems will provide the required foundation on which to construct a framework for security of information systems. They are addressed to the public and private sectors and apply to all information systems. The framework will include policies, laws, codes of conduct, technical measures, management and user practices, ad public education and awareness activities at both national and international levels.

Several OECD Member countries have been forerunners in the field of security of information systems. Certain laws and organizational and technical rules are already in place. Most other countries are much farther behind in their efforts. The Guidelines will play a normative role and assist governments and the private sector in meeting the challenges of these worldwide systems. The Guidelines bring guidance and a real value-added to work in this area, from a national and international perspective.

PRINCIPLES

1. Accountability Principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures practices and procedures for the security of information systems should take into account of and address all relevant consideration and viewpoints, including technical, administrative, organizational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organization so as to create a coherent system of security.

7. Timeliness Principle

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of information systems.

8. Reassessment Principle

The security information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data ad information in a democratic society.

[Source: OECD Guidelines for the Security of Information Systems (1992)]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 21

Thurs 31 December 1992

Contents

Third Conference on Computers, Freedom and Privacy -- CFP'93

Bruce R Koball <bkoball@well.sf.ca.us>
Thu, 31 Dec 1992 00:21:00 -0800

The Third Conference on Computers, Freedom and Privacy -- CFP'93
9-12 March 1993, San Francisco Airport Marriott Hotel, Burlingame, CA

Sponsored by:
Association for Computing Machinery,
Special Interest Groups on:
Communications (SIGCOMM)
Computers and Society (SIGCAS)
Security, Audit and Control (SIGSAC)

Co-Sponsors and Cooperating Organizations:

American Civil Liberties Union
American Library Association
Asociacion de Technicos de Informatica
Commission for Liberties and Informatics
Computer Professionals for Social Responsibility
Electronic Frontier Foundation
Freedom to Read Foundation
IEEE Computer Society
IEEE-USA Committee on Communications and Information Policy
Internet Society
Library and Information Technology Association
Privacy International
USD Center for Public Interest Law

U.S. Privacy Council
The WELL (Whole Earth 'Lectronic Link)

Patrons and Supporters (as of 24 December 1992):

American Express Corp.
Apple Computer, Inc.
Dun & Bradstreet Corp.
Equifax, Inc.
Information Resource Service Company
Mead Data Central, Inc.
National Science Foundation (pending)
RSA Data Security, Inc.

CFP'93 Electronic Brochure 1.1

SCOPE:

The advance of computer and telecommunications technologies holds great promise for individuals and society. From convenience for consumers and efficiency in commerce to improved public health and safety and increased participation in democratic institutions, these technologies can fundamentally transform our lives.

At the same time these technologies pose threats to the ideals of a free and open society. Personal privacy is increasingly at risk from invasion by high-tech surveillance and eavesdropping. The myriad databases containing personal information maintained in the public and private sectors expose private life to constant scrutiny.

Technological advances also enable new forms of illegal activity, posing new problems for legal and law enforcement officials and challenging the very definitions of crime and civil liberties. But technologies used to combat these crimes can pose new threats to freedom and privacy.

Even such fundamental notions as speech, assembly and property are being transformed by these technologies, throwing into question the basic Constitutional protections that have guarded them. Similarly, information knows no borders; as the scope of economies becomes global and as networked communities transcend international boundaries, ways must be found to reconcile competing political, social and economic interests in the digital domain.

The Third Conference on Computers, Freedom and Privacy will assemble experts, advocates and interested people from a broad spectrum of disciplines and backgrounds in a balanced public forum to address the impact of computer and telecommunications technologies on freedom and privacy in society. Participants will include people from the fields of computer science, law, business, research, information, library science, health, public policy, government, law enforcement, public advocacy and many others.

General Chair

Bruce R. Koball, CFP'93, 2210 Sixth Street, Berkeley, CA 94710
510-845-1350 (voice) 510-845-3946 (fax) bkoball@well.sf.ca.us

Steering Committee

Mary J. Culnan   Peter G. Neumann
Georgetown University   SRI International

Dorothy Denning   David D. Redell
Georgetown University   DEC Systems Research Center

Les Earnest   Marc Rotenberg
GeoGroup, Inc.   Computer Professionals
                                  for Social Responsibility
Mike Godwin
Electronic Frontier Foundation   C. James Schmidt
                                  San Jose State University
Janlori Goldman
American Civil Liberties Union   Barbara Simons
                                  IBM
Mark Graham
Pandora Systems   Lee Tien
                                  Attorney
Lance J. Hoffman
George Washington University   George Trubow
                                  John Marshall Law School
Donald G. Ingraham
Office of the District Attorney   Willis Ware
Alameda County, CA   Rand Corp.

John McMullen   Jim Warren
NewsBytes   MicroTimes & Autodesk, Inc.

Simona Nass
Student - Cardozo Law School

Affiliations are listed for identification only.

Pre-Conference Tutorials:
On Tuesday 9 March, the day before the formal conference begins, CFP'93
is offering a number of in-depth tutorials on a wide variety of subjects
on four parallel tracks. These presentations will range from interesting
and informative to thought-provoking and controversial. The tutorials
are available at a nominal additional registration cost.

Conference Reception:
Following the Tutorials on Tuesday evening, you are invited to meet new
and old friends and colleagues at an opening reception.

Single Track Main Program:
The technological revolution that is driving change in our society has
many facets and we are often unaware of the way they all fit together,
especially the parts that lie outside of our own expertise and interest.

The primary goal of CFP'93 is to bring together individuals from disparate disciplines and backgrounds, and engage them in a balanced discussion of all CFP issues. To this end our main program, starting on Wednesday 10 March, is on a single track enabling our attendees to take part in all sessions.

Registration is Limited:
CFP'93 registration will be limited to 550 attendees, so we advise you to register as early as possible and take advantage of the early registration discounts.

Luncheons and Banquets:
A key component of the CFP conferences has been the interaction between the diverse communities that constitute our attendees. To promote this interaction CFP'93 is providing three luncheons and evening two banquets with the cost of conference registration.

EFF Pioneer Awards
All conference attendees are invited to the Awards Reception sponsored by the Electronic Frontier Foundation (EFF) on Wednesday evening, 10 March. These, the second annual EFF Pioneer Awards, will be given to individuals and organizations that have made distinguished contributions to the human and technological realms touched by computer-based communications.

Birds of a Feather Sessions:
CFP'93 will provide a limited number of meeting rooms to interested individuals for special Birds of a Feather sessions after the formal program each evening. These sessions will provide an opportunity for special interest discussions that were not included in the formal program and will be listed in the conference materials. For further information contact CFP'93 BoF Chair:

C. James Schmidt, University Librarian
San Jose State University, One Washington Square
San Jose, CA 95192-0028   schmidtc@sjsuvm1.sjsu.edu
voice 408-924-2700   voice mail 408-924-2966

====

CFP'93 Featured Speakers:

Nicholas Johnson

Nicholas Johnson was appointed head of the Federal Communications Commission by President Johnson in 1966, serving a seven year term. In his role as commissioner, he quickly became an outspoken consumer advocate, attacking network abuses and insisting that those who use the frequencies under the FCC license are the public's trustees. He has been a visiting professor of law at the College of Law at the University of Iowa since 1981 and is currently co-director of the Institute for Health, Behavior and Environmental Policy at the University of Ohio.

Willis H. Ware

Willis H. Ware has devoted his career to all aspects of computer science--hardware, software, architectures, software development, public policy and legislation. He chaired the "HEW committee" whose report was the foundation for the Federal Privacy Act of 1974. President Ford appointed him to the Privacy Protection Study Commission whose report remains the most extensive examination of private sector record-keeping practices. Dr. Ware is a member of the National Academy of Engineering, a Fellow of the Institute of Electronic and Electrical Engineers, and a Fellow of the American Association for Advancement of Science.

John Perry Barlow

John Perry Barlow is a retired Wyoming cattle rancher, a lyricist for the Grateful Dead, and a co-founder of the Electronic Frontier Foundation. He graduated from Wesleyan University with an honors degree in comparative religion. He writes and lectures on subjects relating to digital technology and society, and is a contributing editor of numerous publications, including Communications of the ACM, NeXTworld, MicroTimes, and Mondo 2000.

Cliff Stoll

Cliff Stoll is best known for tracking a computer intruder across the international networks in 1987; he told this story in his book, "The Cuckoo's Egg" and on a Nova television production. He is less known for having a PhD in planetary science, piecing quilts, making plum jam, and squeezing lumps of bituminous coal into diamonds.

====

CFP'93 Tutorials:

Tuesday 9 March - Morning Tutorials

Information Use in the Private Sector
Jack Reed, Information Resource Service Company
Diane Terry, TransUnion Corp.   Dan Jones, D.Y. Jones & Assoc.

This tutorial will deal with the use of personal information from the point of view of some private sector information vendors and users. It will include a discussion of the Fair Credit Reporting Act and the "Permissible Purposes" for obtaining a consumer credit report. Information used for purposes outside the FCRA will be discussed in relationship to privacy and societal needs for businesses and individuals.

Access to Government Information:
James Love, Director, Taxpayer Assets Project

The tutorial will examine a wide range of problems concerning citizen access to government information, including how to ask for and receive information under the federal Freedom of Information Act, what types of information government agencies store on computers, what the barriers are to citizen access to these information resources, and how citizens can change government information policy to expand access to taxpayer-funded information resources.

Exploring the Internet -- a guided journey
Mark Graham, Pandora Systems   Tim Pozar, Late Night Software

This tutorial will give participants a practical introduction to the most popular and powerful applications available via the world's largest computer network, the Internet. There will be hands-on demonstrations of communications tools such as e-mail, conferencing, Internet Relay Chat, and resource discovery and navigation aids such as Gopher, WAIS, Archie and World Wide Web. Extensive documentation will be provided.

Constitutional Law for Non-lawyers (1/2 session):
Mike Godwin, Staff Counsel, Electronic Frontier Foundation

This tutorial is designed to inform non-lawyers about the Constitutional issues that underlie computer-crime and computer civil-liberties cases. The tutorial focuses on the First and Fourth Amendments, but includes a discussion of the Fifth Amendment and its possible connection to the compelled disclosure of cryptographic keys. It also includes a discussion of the appropriateness of "original intent" as a method for applying the Constitution in the modern era.

Civil Liberties Implications of Computer Searches & Seizures (1/2 ses.):
Mike Godwin, Staff Counsel, Electronic Frontier Foundation

This tutorial assumes only a very basic knowledge of Constitutional law (the prior tutorial provides an adequate background), and outlines how searches and seizures of computers may raise issues of First and Fourth Amendment rights, as well as of federal statutory protections. It includes a discussion of what proper search-and-seizure techniques in such cases may be.

Tuesday 9 March - Afternoon Tutorials

Practical Data Inferencing: What we THINK we know about you.
Russell L. Brand, Senior Computer Scientist, Reasoning Systems

What do your transaction trails reveal about you? Are you a good risk to insure? Are you worth kidnapping, auditing or suing? Which products should I target at you? Are you a member of one of those groups that I would want to harass or discriminate against? This tutorial will be a hands-on approach to digging for data and to piecing it back together. Time will be divided between malicious personal invasions and sweeping searches that seek only profit, followed by a brief discussion about improper inferences and their practical impact on innocent files and lives. Legal and moral issues will not be addressed.

Telecommunications Fraud
Donald P. Delaney, Senior Investigator, New York State Police

Illegal call sell operations in New York City are estimated to be a billion dollar industry. This tutorial will provide an overview of the problem, from finger hacking to pay phone enterprises, and will include an up-to-date assessment of the computer cracker/hacker/phone phreak impact on telephone company customer losses. Also discussed will be unlawful access of telephone company switches; unlawful wiretapping and monitoring; cards, codes and 950 numbers; New York State law and police enforcement; methods of investigation and case studies.

Private Sector Marketplace and Workplace Privacy
Ernest A. Kallman, Bentley College, H. Jeff Smith, Georgetown University

This tutorial will give participants a general overview of privacy issues affecting uses of personal information (e.g., medical information, financial information, purchase histories) in the marketplace as well as privacy concerns in the workplace (e.g., privacy of electronic and voice mail, work monitoring). The tutorial will also set the boundaries for privacy arguments in the middle and latter 1990s.

SysLaw
Lance Rose, Attorney and Author "SysLaw"

The SysLaw tutorial session will explore in depth the freedom and privacy issues encountered by computer bulletin boards (BBS), their system operators and their users. BBSs are estimated to number over 45,000 today (not counting corporate systems), and range from small, spare-time hobby systems to systems with thousands of users, grossing millions of dollars. BBSs are a grassroots movement with an entry cost of $1,000 or less, and the primary vehicles for new forms of electronic communities and services. Subjects covered will include: First Amendment protection for the BBS as publisher/distributor; data freedom and property rights on the BBS; how far can sysops control BBS user activities?; and user privacy on BBSs today.

Note: Tutorial presenters will offer expert opinions and information. Some may advocate particular viewpoints and thus may put their own "spin" on the issues. Caveat Listener.

====

CFP'93 Main Program Sessions:

Wednesday 10 March

Electronic Democracy
Chair - Jim Warren, MicroTimes and Autodesk, Inc.

The effects of computer and telecommunications technologies on democratic processes and institutions are increasing dramatically. This session will explore their impacts on political organizing, campaigning, access to representatives and agencies, and access to government information that is essential for a free press and an informed electorate.

Electronic Voting -- Threats to Democracy
Chair - Rebecca Mercuri, University of Pennsylvania

This panel session will invite representatives covering a broad spectrum of involvement with the controversial subject of electronic vote tallying to address such issues as: Is a secure and reliable electronic voting system feasible? What threats to these systems are identifiable? Should electronic voting systems be open for thorough examination? Can auditability be assured in an anonymous ballot setting? Can voting by phone be practical and confidential? Did Congress exempt voting machines from the Computer Security Act?

Censorship and Free Speech on the Networks
Chair - Barbara Simons, IBM

As online forums become increasingly pervasive, the notion of "community standards" becomes harder to pin down. Networks and BBSs will link--or create--diverse, non-geographic communities with differing standards, laws, customs and mores. What may be frank discussion in one forum may be obscenity or defamation or sexual harassment in another. This session will explore the questions of what kinds of freedom-of-speech problems face us on the Net and what kinds of legal and social solutions we need.

Portrait of the Artist on the Net
Chair - Anna Couey, Arts Wire

Computer forums and networks make possible both new artforms and new ways of remote collaboration and exhibition. The growth of the Net creates opportunities for the blossoming of dynamic and interactive artforms and of artistic cultures -- provided that networks become widely accessible and remain open to artistic expression without political interference. This session will examine the potentials and the problems of art and artists on the Net.

Thursday 11 March

Digital Telephony and Crypto Policy
Chair - John Podesta, Podesta and Associates

The increasingly digital nature of telecommunications potentially threatens the ability of law enforcement agencies to intercept them when legally authorized to do so. In addition, the potential widespread use of cryptography may render the ability to intercept a communication moot. This session will examine these issues and the proposals that have been put before Congress by law enforcement agencies to address these perceived problems.

Health Records and Confidentiality
Chair - Janlori Goldman, American Civil Liberties Union

As the new Administration and Congress consider proposals to reform the United States health care system, it is imperative that confidentiality and security safeguards be put in place to protect personal information.

Currently, no comprehensive legislation exists on the confidentiality of health information. This session will explore the current and potential uses of health care information, and proposals to safeguard the information.

The Many Faces of Privacy
Chair - Willis Ware, Rand Corp.

Privacy at any cost is foolish, unwise and an untenable position, and privacy at zero cost is a myth. This two-part session will explore the balancing act between the two extremes and the costs and benefits that accrue. The first part will present several examples of systems and applications in the public and private sectors that stake out a position in this continuum. The second part will be a panel discussion exploring the issues raised by the examples previously presented.

The Digital Individual
Chair - Max Nelson-Kilger, San Jose State University

We are all represented by personal records in countless databases. As these records are accumulated, disseminated and coalesced, each of us is shadowed by an ever larger and more detailed data alter-ego, which increasingly stands in for us in many situations without our permission or even awareness. How does this happen? How does it affect us? How will it develop in the future? What can we do? This session will investigate these questions.

Friday 12 March

Gender Issues in Computing and Telecommunications
Chair - Judi Clark, Bay Area Women in Telecommunications

Online environments are largely determined by the viewpoints of their users and programmers, still predominantly white men. This panel will discuss issues of freedom and privacy that tend to affect women -- such as access, identity, harassment, pornography and online behavior -- and provide recommendations for gender equity policies to bulletin board operators and system administrators.

The Hand That Wields the Gavel
Chair - Don Ingraham, Asst. District Attorney, Alameda County, CA

An inevitable result of the settlement of Cyberspace is the adaptation of the law to its particular effects. In this session a panel of criminal lawyers addresses the fallout from a hypothetical computer virus on the legal responsibilities of system managers and operators. The format will be a simulated court hearing. Attendees will act as advisory jurors in questioning and in rendering a verdict.

The Power, Politics, and Promise of Internetworking
Chair- Jerry Berman, Electronic Frontier Foundation

This session will explore the development of internetworking infrastructures, domestically and worldwide. How will this infrastructure and its applications be used by the general public? What will the global network look like to the average user from Kansas to Kiev? How will politics, technology and legislation influence the access to, and cost of, the Net? How can the potential of this powerful medium be fully realized?

International Data Flow
Chair - George Trubow, John Marshall Law School

The trans-border flow of information on international computer networks has been a concern for governments and the private sector. In addition to concerns for privacy and data security, the economic and national security implications of this free flow of information among scientists, engineers and researchers around the world are also cause for concern. This session will assemble a number of speakers to compare the various perspectives on the problem.

====

Some of the Speakers in the CFP'93 Main Program:

Phillip E. Agre, Department of Communication, University of California, San Diego
Jonathan P. Allen, Department of Information and Computer Science, University of California, Irvine
Sheri Alpert, Policy Analyst, author: "Medical Records, Privacy, and Health Care Reform"
William A. Bayse, Assistant Director, Federal Bureau of Investigation
William Behnk, Coordinator, Legislative Information System, State of California
Jerry Berman, Acting Executive Director, Electronic Frontier Foundation
Paul Bernstein, Attorney
Kate Bloch, Hastings College of the Law
Richard Civille, Computer Professionals for Social Responsibility
Roger Clarke, Reader in Information Systems, Department of Commerce, Australian National University
Dorothy Denning, Chair, Computer Science Department, Georgetown University
Robert Edgar, Simon and Schuster Technology Group
Kathleen Frawley, American Health Information Management Association
Emmanuel Gardner, District Manager, Government Affairs, AT&T
Mike Godwin, Staff Counsel, Electronic Frontier Foundation
Joe Green, University of Minnesota
Sarah Grey, computer department, We The People, Brown presidential campaign organization (invited)
Will Hill, Bellcore
Carl Kadie, co-editor, Computers and Academic Freedom News newsletter
Mitch Kapor, Chairman, Electronic Frontier Foundation
David Lewis, Deputy Registrar, Department of Motor Vehicles, Commonwealth of Massachusetts
James Love, Director, Taxpayers Assets Project
Judy Malloy, Associate Editor, Leonardo Electronic News
Irwin Mann, Mathematician, New York University
David McCown, Attorney

Rob Mechaley, Vice President, Technology Development, McCaw Cellular
Communications, Inc.
Robert Naegele, Granite Creek Technology Inc., Voting Machine Examiner,
consultant to NY State
Barbara Peterson, Staff Attorney, Joint Committee on Information
Technology Resources, Florida Legislature
Jack Reed, Chairman, Information Resource Service Company
Virginia E. Rezmierski, Assistant for Policy Studies to the Vice
Provost for Information Technology, University of Michigan
Jack Rickard, Editor, Boardwatch Magazine
Randy Ross, American Indian Telecommunications
Roy Saltman, National Institute of Standards and Technology
Barbara Simons, IBM
Robert Ellis Smith, Publisher, Privacy Journal
David Sobel, Computer Professionals for Social Responsibility
Ross Stapleton, Research Analyst, Central Intelligence Agency
Jacob Sullum, Associate Editor, Reason Magazine
Mark Trayle, composer
Greg Tucker, Coordinator, David Syme Faculty of Business,
Monash University, Australia
Joan Turek-Brezina, Chair, Health and Human Services Task Force on
Privacy of Private-Sector Health Records

====

Registration:
Register for the conference by returning the Conference Registration Form along with the appropriate payment. The registration fee includes conference materials, three luncheons (Wednesday, Thursday and Friday), two banquet dinners (Wednesday and Thursday) and evening receptions (Tuesday, Wednesday and Thursday). Payment must accompany registration.

Registration Fees are:

If mailed by:	7 February	8 March	on site
Conference Fees:	$300	$355	$405
Tutorial Fees:	$135	$165	$195
Conference & Tutorial	$435	$520	$600

Registration is limited to 550 participants, so register early and save!

By Mail:	By Fax:
(with Check or Credit Card)	(with Credit Card only)
CFP'93 Registration	Send Registration Form
2210 Sixth Street	(510) 845-3946
Berkeley, CA 94710	Available 24 hours

By Phone:	By E-Mail:
(with Credit Card only)	(with Credit Card only)
(510) 845-1350	cfp93@well.sf.a.us
10 am to 5 pm Pacific Time	

CFP'93 Scholarships:
The Third Conference on Computers, Freedom and Privacy (CFP'93) will

provide a limited number of full registration scholarships for students and other interested individuals. These scholarships will cover the full costs of registration, including three luncheons, two banquets, and all conference materials. Scholarship recipients will be responsible for their own lodging and travel expenses. Persons wishing to apply for one of these fully-paid registrations should contact CFP'93 Scholarship Chair, John McMullen at: mcmullen@mindvox.phantom.com

Hotel Accommodations:
The Third Conference on Computers, Freedom and Privacy will be held at the San Francisco Airport Marriott Hotel in Burlingame, CA. This facility is spacious and comfortable, and is easily accessible from the airport and surrounding cities. Because of the intensive nature of the conference, we encourage our attendees to secure their lodging at the conference facility. Special conference rates of $99/night, single or multiple occupancy, are available. Our room block is limited and these conference rates are guaranteed only until 9 February 1993, so we urge you to make your reservations as early as possible. When calling for reservations, please be sure to identify the conference to obtain the conference rate. Hotel Reservations: (415) 692-9100 or (800) 228-9290.

Refund Policy:
Refund requests received in writing by February 19, 1993 will be honored. A $50 cancellation fee will be applied. No refunds will be made after this date; however, you may send a substitute in your place.

====

Registration Form

Name (Please print):____

Title:____

Affiliation:____

Mailing Address:____

City, State, Zip:____

Country:____

Telephone:__________________________Fax:________________________

E-mail:____

Privacy Locks:
We will not sell, rent, loan, exchange or use this information for any purpose other than official Computers, Freedom and Privacy Conference activities. A printed roster will be distributed to attendees. Please indicate the information you wish to be excluded from the roster:

__Print only name, affiliation and phone number
__Print name only
__Omit all information about me in the roster

Registration Fees (please indicate your selections):

If mailed by:	7 February	8 March	on site
Conference Fees:	$300__	$355__	$405__
Tutorial Fees	$135__	$165__	$195__
Conference & Tutorial	$435__	$520__	$600__

If you have registered for the Tutorials, select one from each group:
9:00 AM - 12:00 Noon
__Information Use in Private Sector
__Constitutional Law for Non-lawyers & Civil-liberties
Implications of Computer Searches and Seizures
__Access to Government Information
__Exploring the Internet

1:30 PM - 4:30 PM
__Practical Data Inferencing: What we THINK we know about you.
__Telecommunications Fraud
__Private Sector Marketplace and Workplace Privacy
__SysLaw

Payments: Total Amount____________

Please indicate method of payment: __Check (payable to CPF'93)
(payment must accompany registration) __VISA
__MasterCard

Credit card #______________________________Expiration date____________

Name on card____

Signature____

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 22

Monday 4 January 1993

Contents

Things that cannot possibly go wrong

Pete Mellor <pm@cs.city.ac.uk>
Mon, 4 Jan 93 13:50:17 GMT

The following extract from Douglas Adams' latest book* contain a lesson for designers of complex systems, particularly computerised ones (e.g., fly-by-wire):

> ... all mechanical or electrical or quantum-mechanical or hydraulic or even wind, steam or piston-driven devices, are now required to have a certain legend emblazoned on them somewhere. It doesn't matter how small the object is, the designers of the object have got to find a way of squeezing the legend in somewhere, because it is their attention which is being drawn to it rather than necessarily that of the user's.
>
> The legend is this:
>
> `The major difference between a thing that might go wrong and a thing

> that cannot possibly go wrong is that when a thing that cannot possibly
> go wrong goes wrong it usually turns out to be impossible to get at or
> repair.'

* "Mostly Harmless" (The fifth book in the increasingly inaccurately named "Hitch Hiker's Guide to the Galaxy" trilogy) by Douglas Adams, Heinemann, London, 1992, ISBN 0434 00926 1

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

[TDR] DISA yaks to FCC on PCS

"Paul Robinson, Contractor" <FZC@CU.NIH.GOV>
Mon, 04 Jan 1993 18:41:26 EST

"DISA yaks to FCC on PCS"

Article Summary
Government Computer News, January 4, 1993, Page 38

This is a summary of an article about a technology you've probably never seen, complained about by an agency you've probably never heard of.

In an article titled "Defense agency wants PCS voice services in public domain", author S. A. Marud tells how the Defense Information Systems Agency (DISA) has jumped into the Federal Communications Commission (FCC) inquiry into the standards to be set on the operation of the startup Personal Communications Services (PCS) industry.

PCS is a wireless digital technology which operates at 2 gigahertz. Cellular is analog. Also, one advantage of the service is that a number can be assigned to a person, not to a telephone.

Two groups in DISA, the Federal Wireless Services User Forum (FWSUF) and the Interagency Cellular Radio Working Group (ICRWG) were the impetus for filing comments. They want to be certain that PCS supports at least Group 3 / Group 4 Fax, paging, images, and voice and data encrypted with an STU-III device. i.e. that a group 3 fax modem should work the same whether it's plugged into a wall jack or a PCS phone. PCS should also support dialing "0" for Operator and 911 for Emergency. ICRWG wants there to be two nationwide carriers for PCS, or in the alternative, at least one frequency block reserved nationally to one carrier and the rest awarded to local carriers.

DISA's concerns on National Security and Emergency Preparedness makes it want certain basic services (Such as area code 710?) to be part of the new system, and that at least voice services to be available through the public switched (read local telco, AT&T, FTS-2000, MCI etc.) network. The systems should be made to be interoperable (meaning the phone you use in Dallas should also work in Kansas City, Chicago, New York and Los Angeles), either from the start or soon after some industry standards can be developed. DISA would also prefer that PCS licenses be issued for large areas if no nationwide carrier(s) are authorized.

DISA is worried that PCS may be declared to be "private carriers" which means that the government cannot mandate that they be part of the Telecommunications Priority System (TSP) which allows the government to seize telephone lines. TSP was invoked by the federal government for more than 4000 circuits and services during Hurricane Andrew.

Certain industry groups are watching the rulemaking process on PCS, including the Wireless Information Network Forum (which represents computer and communications companies including Apple, AT&T & IBM), Cellular Telecommunications Industry Association (CTIA) (guess who they represent). CTIA is worried that the FCC might decide that PCS license won't be issued to a cellular operator in the same area.

A decision on how the PCS industry is to be structured is expected from the FCC sometime in Fall 1993.

Paul Robinson -- TDARCOS@MCIMAIL.COM These opinions are mine alone.

Re: Dutch chemical plant explodes (RISKS-14.20)

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Thu, 31 Dec 92 13:28:39 -0800

It is this type of oversimplified explanation that encourages misunderstandings about accidents and how to prevent them and maybe leads to more and unnecessary accidents in the future.

> The Dutch news said that the responsible person has been found and he will be charged with negligible conduct causing death.

I certainly hope it is not the poor schnook that was typing and made a perfectly predictable and inevitable error. We should not be blaming accidents on people who do human things and make errors that are inevitable. Who are they going to put in jail? The programmer who wrote code that allowed such a predictable input error to cause a dangerous output? The person who wrote the requirements and neglected this? The chemical engineers who built a plant that could blow up with one error like that? The managers who allowed all this to happen? What about the regulatory authorities who gave a license for such a dangerous design?

Actually, everything I've said above could be COMPLETELY WRONG! Without a complete investigation, nobody should be talking about the "cause" of an accident. Were there interlocks? If so, why didn't they work? If not, why weren't there any? etc. etc. There are hundreds of factors that we know nothing about that could have been the real causes of the accident.

The Bhopal explosion was blamed by Union Carbide as a maintenance error. But a complete investigation turned up hundreds of factors that were involved, most of which go back to poor management. The maintenance error was probably the least important (if it actually ever happened, nobody knows, it's just the explanation that Union Carbide management put forth). An accident was inevitable at Bhopal because of all the other factors. Something else just would have been the proximate cause, and it sounds like an accident was inevitable in this case too. The chemical industry can ignore all the lessons from Bhopal because it was a "maintenance error." We are probably going to hear for years now about the chemical plant that blew up because of a typing error or computer error (when it may not have had anything very significant to do with the accident).

The law likes to simplify causes down to one simple event. But we, as scientists and engineers, should require more than this.

Nancy

> [Similar messages were received from many others, including PINE_RIDGE@ORVB.SAIC.COM (Brad Dolan) and horning@src.dec.com (Jim Horning), both of whom gagged on NEGLIGIBLE/NEGLIGENT, ergo@netcom.com (Isaac Rabinovitch), who wondered why the designer was not held responsible, desj@ccr-p.ida.org (David desJardins), who distinguished blame and fault and discussed the range of implications... The following message gives some details. PGN]

---

large accident at CINDU plant in The Netherlands (additional info)

<MEULEN@tno.nl>
Mon, 4 Jan 93 16:21 MET

In RISKS-14.20 a contribution on the accident at the chemical factory Cindu appeared. The information provided was sparse and slightly erroneous. As we were involved in the accident examination we have more detailed information which I give here:

FACTS, Database for Industrial Safety Acc.#: 11057 Extended abstract
Country: NL   Date : 1992 0708

At a chemical factory a heavy explosion occurred which caused the death of 3 firemen of the works fire brigade and injured 11 workers included 4 firemen of the works fire brigade. The damage was estimated at several 10th of millions NL guilders. There was a severely material damage. The fragments where found at a distance of 1 km.

The accident started with a typing error in a prescription by a laboratory worker. Instead of tank 632 he typed tank 634. In tank 632 there was stored resin feed classic (UN-1268) and normally used in the batch process. In tank 634 DCDP (dicyclopentadiene) was stored. The operator, who had to check if the tank contents was equal with the prescription, filled the reactor with the wrong chemicals. The batch process started with steam heating via the coil in the reactor. After temperature was rising, first the operator tried to cool the reactor with more water of the water mains and later on the works fire brigade was alarmed to cool the reactor.

An administrator, who checked the prescription every morning, found the error and tried to contact the operator, but it was too late. Because the works fire brigade expected that the contents of the reactor would released via the safety valve and the bursting disc, they were connecting deluge guns to prevent spreading of the expected fire. The firemen did not wear the prescribed personal safety articles, such as hand gloves and breathing apparatus, because they expected to do a relative, easy job.

After releasing chemicals via the safety valve and the bursting disc, several seconds later the reactor ruptured, the contents of the reactor released and an explosion followed.

The local fire brigade was alarmed and together with the works firebrigade, they tried to prevent the fire to spread to the other installations, such as cylinders filled with boron trifluoride. To prevent enormous damage to the environment due to polluted fire fighting water, it was decided to let the fire burn out by itself.

[This information is compiled by TNO with greatest care from qualified source documents. TNO cannot accept responsibility for any inaccuracy. Meine van der Meulen (meulen@tno.nl), The Netherlands Organization for Applied Scientific Research TNO, Department of Industrial Safety, Apeldoorn, The Netherlands Phone: +31 55 493493]

Re: Antiviral company target of legal action

McAfee Associates <mcafee@netcom.com>
Sun, 3 Jan 93 23:45:49 -0800

RISKS Vol. 14, Issue 20 paraphrased a Washington Post article that appeared in the San Francisco Chronicle about the temporary restraining order Imageline, Inc. of Richmond, VA has been granted against McAfee Associates.

McAfee Associates believes the suit to be without merit and will vigorously defend ourselves against it. Allow me to share some pertinent facts with you:

1. The temporary restraining order [TRO] applies to our retail product, PRO-SCAN, and then only to a particular version of it. This particular version has not been shipped since October 1991, and has less than 100 registered users.

2. PRO-SCAN accounts for approximately 6% of our sales and less than 2% of our licensing activity. It is essentially provided as a convenience for people who do not wish to use a modem to download our shareware products.

3. The particular version of PRO-SCAN employs different technology then our shareware VIRUSCAN series, e.g., they are separate programs. The TRO in no way effects the main product line, which is distributed electronically.

In summary, while we intend to vigorously defend ourselves, this litigation is unlikely to have any impact on our overall business.

Aryeh Goretsky, Manager, Technical Support Department, McAfee Associates, Inc.
3350 Scott Blvd, Bldg 14, Santa Clara, CA 95054-3107 1-408-988-3832
FAX 1-408-970-9727 mcafee@netcom.COM CompuServe ID: 76702,1714

Microprocessor design faults

Brian A Wichmann <baw@seg.npl.co.uk>
Wed, 16 Dec 92 17:07:59 GMT

Microprocessor design faults
B A Wichmann
National Physical Laboratory, Teddington, Middlesex, TW11 0LW, UK

Introduction

Modern microprocessors are very reliable. Generally, we take this for granted and we are therefore not concerned about the possibility of a chip having a design fault. However, in some applications, and error could have serious consequences, so that all reasonable precautions must be taken against such potential errors.

This note makes some proposals which would allow users of critical applications to protect themselves against such problems in a reasonable manner.

The problem

Modern microprocessor chips are getting very complex indeed. The current gate count can exceed 2.5 million. One must therefore expect that new versions of such chips will contain logical bugs. A common form of bug is in the microcode, but since the distinction between a microcode fault and another form of design bug is difficult to define, the distinction is not made here. We are *not* concerned with fabrication faults.

The price/performance improvements have also been dramatic, which has been encouraged in a highly competitive market. Of the three attributes, performance, price and reliability, the issue of reliability comes third for most users. Hence the commercial market is not in the business of producing chips without design faults.

Several research projects have been undertaken or proposed to produce a design which can be formally verified mathematically \cite{viper,veri-micro}. Unfortunately, it is very difficult for industry to use chips other than those to commercial designs, due to the investment in compilers and other tools. Hence it is much more advantageous to provide commercially designed chips with as high a reliability as is feasible.

Chip suppliers are naturally concerned about the use of their products in applications which are critical for fear that any error could result in claims for damages. Also, open reporting of bugs is not welcome, since it could be potentially damaging to their market share unless it was required of all suppliers. In consequence, suppliers do not feely provide information on bugs, or even allow the user to decode the external marking on the chip to discover the mask version used. Attempts to report bugs openly have not been successful \cite{micro-rpt}.

A consequence of the above is that it is very difficult of users undertaking a critical application to protect themselves against a potential design bug. One approach that has been tried with one project is to use identical chips from the same mask so that rig and development testing will extrapolate to the final system. In some cases, the suppliers have provided information under a non-disclosure agreement, be this seems to be restricted to major projects.

In contrast, quite a few software vendors have an open bug reporting scheme --- and almost all provide a version number to the user. Hence it appears in this area, software is in `advance' of hardware.

Some information

Over a period of three years, I have collected examples of design errors in chips from several different sources. In August 1992, I posted a message on Comp.risks (a bulletin board moderated by Peter Neumann), requesting other examples. Unfortunately, there are problems publishing this information in its entirety as follows:

 * Some of the information comes from sources which have probably signed non-disclosure agreements and hence they have asked for the information not to be published;

 * It would be difficult (and expensive) for me to trace all my sources to ask permission to publish;

 * Much of the information does not contain some details which could result in it being misleading --- perhaps the bug only applies to very early releases of a chip;

 * It is clear that the information I have is not comprehensive.

Hence I have decided to extract from this information some useful points rather than attempt to publish it as fully as possible.

The key issues extracted are as follows:

 * Early chips are unreliable:

There have been some dramatic errors in very early releases of chips.

 * Rarely used instructions are unreliable:

One report sent to me reported that some instructions not generated by the `C' compiler were completely wrong. Another report noted that special instructions for 64-bit integers did not work, and when this was reported, the supplier merely removed them from the documentation!

 * Undocumented instructions are unreliable:

Obviously, such instructions must be regarded with suspicion.

 * Exceptional case handling is unreliable:

A classic instance of this problem is an error which has been reported to me several times of the jump instructions on the 6502. When such an instruction straddled a page boundary, it did not work correctly. This issue potentially gives the user most cause for concern, since it may be very difficult to avoid the issue. For instance, with machine generated code form a compiler, the above problem with the 6502 would be impossible to avoid.

Hence is would appear that the reliability growth models which have been applied to large software systems apply equally to complex chips. This appears to imply that the chips on the market represent to best that the supplier thinks that the market requires, rather than one which has either every known bug removed or one which has been shown correct by formal or informal reasoning.

Conservative system design should therefore use `well-established' chips, avoid rarely used or undocumented instructions. Much of this is conventional wisdom.

The key issue is the extent to which chips which pass the above criteria could be expected to be fault-free (in operation). Just one example reported to me shows that we cannot expect too much. A compiler vendor had a bug reported which the supplier of the software had some difficulty in tracing. Eventually, it was found that the chip in question microcoded the integer divide instruction by making it interruptible. Unfortunately, the status of the registers was not preserved correctly after the interrupt. Clearly, a bug of that type could go undetected for years and yet cause the system to fail tomorrow.

The above has clear implications for those producing systems requiring very high reliability. Even formal proof that the machine-code implements the mathematical specification of the system is insufficient. Unfortunately, no figure can be provided as an upper limit on the reliability of a single processor system (without design diversity).

A proposal

It is currently very difficult for a designer of a high reliability system to minimise the risks from design faults in chips for the reasons given above. Of course, the risks are {\em small}, but for very critical systems, all reasonable steps must be taken to reduce the risk to ALARP (As Low As Reasonably Practical).

Further improvements would be possible if there was greater visibility of the design process for the chips by the supplier to the users developing critical systems. My proposal for this is as follows:

 1. The actual version of the device is determinable from the external marking;

2. The supplier is registered to ISO 9000;

3. The supplier's quality assurance procedures requires that all user reported bugs are recorded, and that the list for any specific version of the device is available to any user who might reasonably require it. (Obviously, suppliers should be able to charge for this, perhaps also in the chip costs as well, and perhaps it might only be applied to the `older' chips);

4. Government procurement should request conformance to this scheme. (Government and its agencies are responsible for many of the most critical systems, and such a requirement would ensure the availability of chips following this proposal.)

References

\bibitem{micro-rpt}
Microprocessor Report. MicroDesign Resources Inc. ISSN 0899-9341.

\bibitem{veri-micro}
W A Hunt. FM8502: A verified microprocessor. Institute for Computer Science,
University of Texas, Technical Report 47. 1986.

\bibitem{viper}
J Kershaw. Safety Control Systems and the VIPER Microprocessor.
RSRE Memorandum No 3805. Malvern. Worcs. 1985.

Appendix

Document Details

* Status: This is a working document.

* Project: None.

* File: Stored on the Sun in file baw/misc/chip2.tex.

* History: First written, 16th December 1992.

* Actions: BAW to copy to DTI (SQU and IMT2) and also the BCS Task Force
  and Specialist Group Committee.

Call for Papers - 1993 National Computer Security Conference

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>
Fri, 1 Jan 93 20:37 EST

CALL FOR PAPERS
16th NATIONAL COMPUTER SECURITY CONFERENCE
Sponsored by the National Computer Security Center and

the National Institute of Standards and Technology

SEPTEMBER 20-23, 1993
BALTIMORE, MD

The National Computer Security Conference audience represents a broad range of interests drawn from government, industry, and academic communities. Their interests include technical research topics, security applications, and management issues. Papers may be addressed toward the entry level or skilled practitioner. Special emphasis will be placed on papers addressing the special needs of users and creating better security for user information technology resources.

We are pleased to invite academic Professors to recommend Student papers in the application of Computer Security methodology. Three student submissions will be selected by the Technical Committee for publication in the Conference Proceedings. To be considered, the submission must be authored by an individual student with the assistance of their academic Professor and be recommended by their academic Professor. Only one copy for student submission is required.

BY FEBRUARY 8, 1993: Send eight copies of your draft paper* or panel suggestions to the following address. See author instructions for your submission format.

* Government employees or those under Government sponsorship must so identify their papers.

Mailing Information
National Computer Security Conference
ATTN: NCS Conference Secretary, AS 11
National Computer Security Center
Fort George G. Meade, MD 20755-6000

BY MAY 15, 1993: Speakers selected to participate in the conference will be notified when their camera-ready paper is due to the Conference Committee. All referee comments will be forwarded to the primary author at this time.

For additional information on submissions, please call (410) 850-0272.

Preparation Instructions for the Authors
To assist the Technical Review Committee, the following is required for all submissions:

Page 1: Type of submission (paper, panel, tutorial)
Title of submission
Keywords
Abstract (not to exceed 250 words)
Author(s)
Organization(s)
Phone number(s)
Net address(es), if available

Point of Contact

Submissions having U.S. Government sponsorship must also provide the following information:

U.S. Government Program Sponsor or Procuring Element
Contract number (if applicable)
U.S. Government Publication Release Authority
Note: Responsibility for U.S. Government pre-publication review lies with the author(s).

The submission (pages 2-9, these are the 8 pages of your submission):

Title of submission - do not include author(s), address(es) or organization(s)
Abstract (with keywords)
The paper
(Suggested Length: 8 pages, including figures and diagrams; pitch: no smaller than 8 point; 1 inch margins on top, bottom and sides.)

A Technical Review Committee, composed of Government and Industry Computer Security experts, will referee submissions only for technical merit for publication and presentation at the National Computer Security (NCS) Conference. No classified submissions will be accepted for review.

The Conference Committee provides for a double "blind" refereeing. Please place your names and organizations ONLY on page 1 of your submission, as defined above. Failure to COMPLY with the above instructions may result in non-selection BEFORE the referee process. Papers in excess of 8 pages may also result in non-selection BEFORE the referee process.

Papers drafted as part of the author's official U.S. Government duties may not be subject to copyright. Papers submitted that are subject to copyright must be accompanied by a written assignment to the NCS Conference Committee or written authorization to publish and release the paper at the Committee's discretion. Papers selected for presentation at the NCS Conference requiring U.S. Government pre-publication review must include, with the submission of the final paper to the committee, a written release from the U.S. Government Department or Agency responsible for pre-publication review. The release is required no later than July 1, 1992. Failure to comply may result in rescinding selection for publication and for presentation at the 16th NCS Conference.

Technical questions can be addressed to the NCS Conference Committee by mail (see Mailing Information) or by phone, (410) 850-0CSC [0272]. For other information about the conference, please call (301) 975-2775.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 23

Thursday 7 January 1993

Contents

Leap Year Causes Problems for ATM Machines

Conrad Bullock <Conrad.Bullock@actrix.gen.nz>
Thu, 7 Jan 93 17:20:30 NZT

Extracts from two newspaper articles on an ATM glitch which corrupted thousands of customer cards on Dec 31st in New Zealand.
These articles are both from general circulation newspapers. The second gives a little more information.

"Year too long for money machines", By Roger Fea, New Zealand Herald, Jan 2, 1993.

The passing leap year caught several thousand ASB Bank customers short on Thursday - when the bank's money machines refused to process their transactions.

The ASB's managing director, Mr Ralph Norris, said that a "faulty date checking routine" had corrupted the magnetic strip on the customers' money machine cards.

The fault had to do with the fact that 1992 was a leap year and that Thursday was the 366th and last day of the year.

The money machines were programmed to acknowledge the extra day but instead of the year 1992 being encoded, the figure 02 was used.

The problem became apparent about 10 am on Thursday and covered a period from midnight to noon that day, when it was fixed.

Only those customers who made two separate transactions during the period were initially affected. The first transaction went through but the problem occurred when their cards were inserted a second time.

Mr Norris said all customers who used their cards during the 12 hours - possibly about 10,000 - were now carrying corrupted cards.

If they used them subsequently up until Monday or Tuesday their transactions would be similarly rejected. By that time a new programme would be in place which would bypass the problem.

[Information about cards still working with other bank's machines and EFT-POS, as well as various apologies and contact information.]

"Leap year spikes cashcards", NZPA, Waikato Times, Jan 2, 1993.

About 1500 TSB Bank customers in Taranaki had their Cashflow cards "corrupted" yesterday by a computer software fault that could ripple around the world with disastrous consequences.

TSB customers, who used their cards between midnight Wednesday and about 12:30pm Thursday to make withdrawals, found they could not use the cards again and needed replacement cards.

"It's quite a serious problem we are talking about ... which has the potential to ripple around the world," TSB information services manager John Hollins said.

The 18 TSB automated teller machines (ATMs) throughout the region operated on a version of an NCR-based machine code which made no allowance for leap years. So after a first withdrawal on Thursday the machines no longer recognised the cards and came up with an "unable to process" message, Mr Hollins said.

[Information about the ASB being affected, but not the Trust Banks, which the ASB and TSB were once part of.]

Bank customers overseas who used ATMs which operated on the same NCR code could also expect problems after their first withdrawals on the last day of 1992, which had been a leap year, Mr Hollins said.

However, customers who used Cashflow machines for other transactions - such as account balance queries, transfers of money, or deposits - were not affected.

[EFT-POS still worked OK, various apologies].

Background from Conrad:

Both ASB and TSB are regional banks (although the ASB are starting to move into other regions). The nationwide trading banks (which also use NCR ATMs, amongst others) do not seem to have been similarly affected.

This is another instance where New Zealand, as the first country in the world to see the new day, also gets to experience date-related bugs first - such as the recent 3pm Nov 1 1992 bug which broke many banking systems running on Tandem CLX hardware - as the bug hit NZ (then Australia, then Japan.....) a workaround was developed, and problems were averted in Europe and the US.....

Ross Perot Campaign Steals Credit Data?

<KitchenRN@ssd0.laafb.af.mil>
Tue, 05 Jan 93 13:11:00

News reports indicated that the Ross Perot campaign is being investigated by the FBI, Secret Service, and Federal Trade Commission for allegedly using stolen computer codes to obtain credit reports on some campaign workers. Investigators refused to discuss the case, but former Perot campaign employees, Equifax (the credit reporting company) and Orix Consumer Leasing of Secaucus, NJ admitted having spoken to investigators.

Equifax said at least seventeen credit files of former Perot campaign workers may have been accessed illegally. Some Equifax reports were obtained using the security code of Orix, which claims to never have requested the credit reports on Perot volunteers. Officials at Orix and Equifax have said they believe Orix's security codes were stolen. [Source: LA Times 2 or 3 Jan 93]

Richard N Kitchen kitchenrn@ssd0.laafb.af.mil

Computer failures in B767

Wm Randolph Franklin <wrf@ecse.rpi.edu>
Tue, 5 Jan 1993 18:05:37 GMT

The B767 aircraft suffers repeated failures of the computer that controls the individual passenger lights, sound, etc. Unlike earlier aircraft, all the switches on the armrests, including the individual light switches, sound channel and volume, and attendant call button, are controlled by a computer. On a recent flight that I was on, from Milan to Washington, the computer wedged shortly into the flight. Although one attendant figured that the situation would have to wait until the plane landed, another managed to reset the computer. According to the attendants, these computer problems happen all the time.

Now of course this is not a life-critical system, but it is certainly ominous that such a simple task cannot be implemented correctly. I'm also curious about replacing 300 local light switches by a centralized computer with 300 inputs and 300 outputs. Ditto for the channel controls.

Wm. Randolph Franklin, wrf@ecse.rpi.edu, (518) 276-6077; Fax: -6261
ECSE Dept., 6026 JEC, Rensselaer Polytechnic Inst, Troy NY, 12180 USA

Laserprinter Forgery

Matt Healy <matt@wardsgi.med.yale.edu>
Tue, 5 Jan 1993 22:40:24 GMT

Years ago (pre-wordprocessing) I used an IBM Selectric typewriter with a correction key. For a lousy typist like me, this was *wonderful*. However, the manual warned against using a correctable (carbon film) ribbon for typing legal documents because undetectable alterations would be too easy.

Well, recently on a Delta flight from Hartford to Atlanta one of the options on the inflight sound system was an interview with Frank Abagnale, a reformed forger who now advises companies on fraud prevention.

Abagnale said that output from most laserprinters and photocopiers can be removed in a similar manner with correction tape because the toner powder, like carbon film ribbon, only sits on the surface of the paper but does not impregnate the fibers. I tried it and he's right.

He said some of his clients have had checks altered in this manner. He suggested two solutions:

1: use an impact printer with inked fabric ribbons

2: there is a fixative, similar to the stuff artists
use to protect charcoal drawings, that can be sprayed
over the printout, making removal of toner more difficult.

Matt Healy matt@wardsgi.med.yale.edu

PS: In the Selectric, IBM had the best keyboard I have ever used. Why didn't they use it for the PC? Closest approximation I have used recently is an old Leading Edge Model D.

> [If you wish to answer Matt's question, send mail to HIM, not to RISKS. By the way, the Selectric touch was fine, but the ball kept getting out of alignment. I have some wonderful concrete (abstract) poetry generated in 1969 using just such a ball. I had a real ball! PGN]

Large Foreign Exchange Rates

faculty R. Y. Kain <kain@ee.umn.edu>
Wed, 6 Jan 93 11:02:32 -0600

During the fall I recall that there was a RISKS contribution in which the writer speculated about the number of digit positions required to specify a real currency exchange rate, concluding that something like four or five digits would surely be adequate. This is incorrect - my daughter was previously in Zaire in the Peace Corps and is now in Congo in the Peace Corps. They (she and her husband had to leave Zaire when the Peace Corps cancelled the program in the country due to unrest which was partly due to the economy, which is in a shambles. When they went in the Peace Corps (Thanksgiving 1990 for Zaire), the exchange rate was something like 400 Zaires per dollar (officially) and about 800 Zaires per dollar in the real market. When they left the country the rate was about 80,000 Zaires per dollar (Sept. 1991), and the official rate had been dropped for some time. This weekend the rate is about 2,500,000 Zaires per dollar!! (And the largest piece of money is a [recently printed] note for 5,000,000 Zaires, but the government has said that in order to control things they were going to remove that one from circulation!)

So in the face of unreasonable people (dictators, etc.), perhaps we need to use a floating point representation for the exchange rates - but I do think that one decimal digit for the exponent should be adequate. (And no one should need seven digit accuracy in the mantissa.)

Richard Y. Kain, EE Department, University of Minnesota kain@ee.umn.edu

---

Stolen to order systems

Lord Wodehouse <w0400@ggr.co.uk>
06 Jan 93 13:22:00 GMT

A letter in the UK magazine DEC User Jan 1993 page 6 shows a new danger"

> I think all readers should consider the implications of what happened to our company on 26th September 1992.
>
> At about 7:00am, our alarm was triggered, police and managers alerted, but by 7:07am we were already too late. In a precise but crude act, a single window was shattered by two lumps of concrete and our main PDP 11/84 processor was detached from all peripherals and lifted through the broken window.
>
> Naturally, we have restoration media of the recovery list, programmes and latest data. We were back in operation on Wednesday night thanks to our maintenance contract, software support and up-to-date back-up media.
>
> We are still reviewing potential motives and ramifications, but there have been other thefts in the area and complete systems are apparently reaching the former Eastern Bloc. In the meantime, if anyone offers you a cheap PDP, please let me know.
>
> A McManus
> Financial controller, Ritrama (UK)

[BTW, I guess the letter shows 1) a criminal problem, and 2) why you make backups.)

Lord John - The Programming Peer w0400@ggr.co.uk
tlx - 8951942 GLXPRI G fax - +44 81 423 4070

Prosecution in the Cindu case

<MEULEN@tno.nl>
Wed, 6 Jan 93 09:41 MET

The statement

> The dutch news said that the responsible person has been found and he will be charged with neglig[ent] conduct causing death.

in RISKS-14.20 on the Cindu accident aroused some excitement. In my first contribution in RISKS-14.21 I forgot to add details.

Although there were some rumours that employees of Cindu would be prosecuted, the public prosecutor decided not do so. He thinks the employees were punished enough already by what had happened and that the case is too complex to be able to focus responsibility for the accident to one person. The rumours focused on the man who forgot to check the recipe before executing it. He was an apprentice operator, 3 months in service, and was alone when the accident happened.

Dutch government charges the Cindu company as a whole for breaking several environmental, health, safety, and economical laws. The public prosecutor demands a fine of one million guilders (approx. US$600,000) and a suspended sentence (trial period of two years) to close the plant if another accident happens again. The latter is quite new in the Netherlands.

The judge pronounced judgement on 5 January: a fine of 200,000 guilders (approx. US$100,000) mainly for breaking health and safety laws. (Of course Cindu is liable for damage etc., but this is civil law).

Meine van der Meulen, meulen@tno.nl, The Netherlands Organization for
Applied Scientific Research TNO, Department of Industrial Safety,
Apeldoorn, The Netherlands, Phone: +31-55-493493.

[Also noted by Anton van Reeken, A.vanReeken@be.rulimburg.nl.]

Re: Microprocessor Design Faults (Wichmann, RISKS-14.22)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Tue, 5 Jan 93 11:22:00 -0500

Mr. Wichmann makes the point that while often market pressures result in manufacturers concealing bugs in chips he states that:

> "In contrast, quite a few software vendors have an open bug reporting scheme --- and almost all provide a version number to the user."

Unfortunately recent events have indicated that Microsoft does not always adhere to this maxim, choosing instead to "slipstream" certain corrections.

Further from reports I have received, Microsoft employees have been distributing misinformation on incidents.

The situation is as follows: when MS-DOS 5.00 was released, the CHKDSK program apparently contained a flaw that causes corruption of disks containing over approximately 65,280 clusters if the /F switch is used. Depending on cluster size, this indicates that disks or partitions containing approximately 128MB, 256MB, 512MB, 1024MB, or 2048MB are at risk.

The problem had been corrected in a version of MS-DOS 5.00 dated 11-91 however other than the date, the only way to check is with a byte-for-byte check since both versions are exactly the same length (16,200 bytes). For reference, the earlier version contains the string 8B 4F 0F 8B F9 at offset DS:263E while the "fixed" one contains 8B 7F 0F 32 ED at the same offset.

The sad part is that people have reported MicroSoft personnel as first recommending the undocumented VER /R switch and using only "Revision A". Unfortunately *every* version of MS-DOS 5.00 reports "Revision A". Just today I received a note from someone who contacted Microsoft and was told to "execute COMMAND.COM and check the version number" again both the old (04-91) and the new (11-91) versions report exactly the same thing.

Further, this mirrors the response received when I called to report that certain corrupt values in the partition table could cause a floppy boot to hang ("You must have a bad floppy...").

To make matters worse, Microsoft appears unwilling to post an approved "patch" to the problem preferring to handle it on an individual basis (sounds kind of like WordPerfect here - call with a problem and they send you a set of "magic" disks).

Thus it would seem that Mr. Wichmann has been spared contact with Microsoft in his assessment. I only wish it was true...

Padgett <padgett@tccslr.dnet.mmc.com>

ps. Apparently the 11-91 version of MS-DOS 5.00 Revision A
    contains a number of changes to other programs however
    IO.SYS, MSDOS.SYS, and COMMAND.COM appear to be the same.

pps. IBM PC-DOS 5.00 is said to return something meaningful to
    VER/R - the version dated 2-92 apparently has the CHKDSK
    "fix".

Release of Maps to NGOs?

Daniel J Yurman <djy@inel.gov>
Mon, 4 Jan 93 16:37:10 MST

PROCEDURES FOR RELEASE OF GIS DATA TO THE PUBLIC

There are many instances where non-governmental organizations request data and maps, e.g. coverages, from geographic information systems (GIS) owned by Federal and State agencies, but operated for these agencies by contractors. Release of data from these systems usually requires the contractor to submit the requested data / maps to the agency which in turn releases its to the requesting organization. GIS pose a special case because map coverages often involve multiple layers of data from third parties and have widely varying levels of quality.

This posting presents a hypothetical case regarding release of GIS data, poses some questions, offers a straw man, and requests feedback. The contractor and the agency face substantial risks if the data are misused, misinterpreted, or the results of these actions create problems for the users.

REQUESTS AND LIABILITY

Examples of non-governmental entities include other contractors doing work for the same or other State agencies, businesses which want to use the data for their own purposes, and "good government" groups and other interest groups, who have reason to believe the data / maps will add value to their work.

The issue is raised about the use of released data for purposes for which they are not intended and the ability of the original contractor and the agency to protect themselves against problems with the quality of the released data. For instance, should the original contractor prepare a "caveat emptor" statement.

Further, the original GIS contractor gets much of its data from its primary customer, the Agency, and from other State agencies. The contractor does not "own" the data, does not own the hardware and software of the GIS -- it was paid for with tax dollars -- and, yet may be held liable by its customer for inappropriate release or failure to properly qualify the release of these same data.

CASE EXAMPLE

Let's take a hypothetical State Alcoholic Beverage Control Agency (ABC) which has collected information on package sales by retail outlet, by product, and other useful marketing information. The State Agency sells all alcoholic beverages in the State except beer and wine, which are sold in grocery stores. It also regulates the sale of alcoholic beverages in restaurants and bars.

The State has built a GIS to make maps of sales data to support "targeting" of different products by demographics, but also to help keep tabs on public consumption habits in order to monitor "demand" for package sales v. restaurant sales. The ABC Agency argues it must have this data in map form so that it does not overstock stores near high volume bars and in resort areas. This has raised privacy issues and the legislature is asking whether the Agency has gone overboard in meeting its regulatory mandates.

WHY THE DATA ARE REQUESTED

Some of the questions coming from the legislature are motivated by lobbying pressures from the liquor industry. The industry has a generally adversarial relationship with the ABC Agency. It will likely use the GIS data to make a case in the current legislative session for changing the extent of the ABC Agency's powers. On the other side, a civil rights organization has requested the GIS maps in order to show there are a disproportionate number of liquor licenses in minority neighborhoods, and to show that the ABC Agency discriminates against minority applicants for these licenses.

Numerous requests have been received by the Agency for copies of its maps. Suppose you are the contractor who runs the GIS for the ABC Agency. What would you do in terms of qualifying the release of the GIS data, electronic files, and hardcopy maps? What kind of release procedures would you want to use to cover your operation?

STRAW MAN

I'll start by offering a "straw man" caveat emptor statement.

> The primary objective of this data is to support specific legislative, regulatory, and administrative objectives of the ABC Agency and decision making which affects its operations. This agency takes no responsibility for interpretation or use of this data for purposes other than for which it was originally intended. ABC Agency databases and GIS coverages include many types of information with varying degrees of quality and reliability depending on the original sources.
>
> Further, it is the policy of the ABC Agency to accept and use the best data possible and to provide its users with information on the quality of that data. ABC data are subject to periodic updates, and it is the responsibility of external users to obtain these updates.

Whether the data is ready for release or not the ABC Agency may be forced by Freedom of Information Act requirements in the hypothetical state to release the data and gis coverages. The absence of a legislative mandate to make the data public in other instances may not be a sufficient reason to withhold it.

This case revolves around marketing and regulatory data for alcoholic beverages, but a parallel case could be developed for releasing GIS data on hazardous waste sites which impinges on public safety, privacy, and real estate values.

SUMMARY

The original question is -- what should the contractor and the government agency do when faced with multiple requests for GIS data by non-governmental entities? What kind of "release policy and procedures" should be developed, and does anyone have any examples?

Dan Yurman, Idaho National Engineering Laboratory, PO Box 1625,
Idaho Falls, ID 83415 djy@inel.gov 1-208-526-8591 Fax: 1-208-526-6902

AFCEA ACCE Conference Announcement

John Wack <wack@ariel.ncsl.nist.gov>
Thu, 7 Jan 93 11:00:51 EST

Announcing the 4th AFCEA Computing Conference & Exposition Conference,
Sponsored by the Armed Forces Communications and Electronics
Association (AFCEA) in cooperation with the Association for
Federal Information Resources Management (AFFIRM).

Objective:
A forum for military, civil government and industry computer hardware, software and systems professionals and users to exchange information and strengthen professional knowledge regarding capabilities, technology and application of information systems.

Focus:
This is not a DoD-only conference. The scope and focus of the conferences has continued to broaden to include presentations and demonstrations directed towards civil government and industry. Individuals from government, industry, and academia are invited to attend and will find the conference interesting and pertinent.

Dates:
Conference - February 2-4, 1993
Exposition - February 3-4, 1993

Location:
Hyatt Regency Crystal City
2799 Jefferson Davis Highway
Arlington, Virginia

Hotel Reservations:
AFCEA has blocked rooms at the Hyatt Regency Crystal City at special conference rates of $126.00/Single and $140.00/Double. Call (703) 418-1234 or (800) 233-1234 and be sure to mention that you are an ACCE '93 attendee to receive the discount rates.

Security Tracks:

Panel: Critical Programs Lead the Way

Recent policy and mission assignments in DoD strongly support the goal to achieve adequate levels of security at an affordable price. To meet this goal, security requirements must be addressed early, from the top down, and throughout a systems life cycle to be effective. The panel will cover a cross section of activities representing the latest DoD approach to systems security. Presentations will address the vital role of security architecture, discuss current programs for meeting critical multilevel security requirements, and describe a specific security product being developed for the Navyis COPERNICUS program.

Moderator: Mr. Robert Ayers, Program Manager, Defense Information
Systems Security Program, Defense Information Systems Agency (DISA)

Panelists:

Mr. James S. Demerest, III Chief, DISSP Architecture Division National
Security Agency (NSA), The Road to the DoD Goal Security Architecture

lit. Col. John Sheldon, Program Manager Multi-level Security Technology
Insertion Program Defense Information Systems Agency (DISA), The Multilevel
Security Technology Insertion Program

Mr. Michael S. Harrison, SPAWAR INFOSEC Support Office, Embeddable INFOSEC
Product

Panel: Standards - the Key to Interoperability

To achieve security in an open systems environment requires the development of comprehensive standards touching nearly every dimension of information technology. While progress is being made in selected areas, the broadly based security standards structure needed to support the performance and user demands of emerging networks is yet to be developed. The immensity of the task requires Government and industry to work closely together on a national and international basis. The National Institute of Standards and Technology (NIST) plays a fundamental role in this effort. NIST, DoD, and industry presenters on the panel will discuss status, issues, and the direction for a number of important security standards activities.

Moderator: Dr. Stuart Katzke, Chief, Computer Security Division
National Institute of Standards and Technology (NIST)

Panelists:

Major Truce George, PhD., USAF, Sr. Techical Assistant Strategic Network
Division National Security Agency (NSA),
Status of Computer to Computer Security Protocols

Prof. Thomas C. Bartee, Institute for Defense Analysis (IDA),
Converging Labeling Standards

Mr. Paul T. Cummings Sr. Software Engineering Manager, Manager ULTRIX MLS+
Digital Equipment- Corporation,
Initiatives of the Trusted Systems Interoperability Group

Mr. F. Lynn McNulty, Associate Director for Computer Security National
Institute of Standards and Technology- (NIST),
Infrastructure for the Digital Signature Standard

Panel: Near-Term Implementations

Current demands for network security cannot wait for mid- or long-term solutions. The need is now! This panel will address actions to provide solutions to real time network security demands. Panel members will present accomplishments and near-term plans in analyzing systems, Beta Testing, and ongoing systems security applications. The discussions will describe a System Security Profile, an ongoing Beta Test of the Preliminary Message Security

Protocol, products applications at the Air Mobility Command on the Global
Defense Support System (GDSS), and the plans for the Reserve Component
Automation System (RCAS), the first Army system with MLS.

Moderator: Mr. Charlie C. Baggett, Jr., Chief, Information Systems
Security Programs Group National Security Agency (NSA)

Panelists:

Mr. Robert Wandell, Work Center Chief for System Security Profiles
National Security Agency (NSA), System Security Profiles

lit. Col. Philip Toler, USAF DMS Implementation Team Defense
Information Systems Agency (DISA),
Pre-Message Security Protocol (PMSP) E-Mail Beta Test

Major Paul Law, USAF Implementation Team Air Mobility Command,
Global Decision Support System Applications

Ms. Victoria Thompson, Reserve Component Automation System (RCAS) PMO
Air Mobility Command, RCAS Information Systems Security

Panel: Evaluation, Certification and Accreditation

The explosive growth of information technology is outstripping our capacity to perform the security evaluations needed at the product level. Similarly, there are insufficient resources to perform the certification and accreditation processes required at the system level. The panel will discuss plans and programs to enhance evaluation, certification, and accreditation capability.

Moderator: Mr. Daniel J. Ryan, Director Information Systems Security
Office of the Deputy Assistant Secretary of Defense (CI&SCM)

Panelists:

Commander Debbie Campbell, USN Standards, Criteria and Guidelines Division
National Security Agency (NSA), Converging Certification and Accreditation
Approaches in the Federal Government

Mr. Stanley J. Chincheck, Head of Communication Security Section Naval
Research Laboratory, Project Outreach - First Results

Mr. Larry D. Merritt, Director for Securities Air Force Cryptologic
Support Center, The Air Force INFOSEC Certification Program

Tutorial: Understanding System Security Solutions

The Information Systems Security field is complex and filled with jargon. This three-hour session is directed at providing a clear, plain English understanding of the fundamentals of information protection and the solutions now available. In addition, there will be a special presentation on how to conduct INFOSEC business in the DoD.

Presenters:

Mr. James P. Litchko, Director of Business Development Trusted
Information Systems, Security Tool Kit `93

Mr. Joel E. Sachs, Vice President of Business Development Arca Systems, Inc.,
Multilevel Security - What It Is and What It Can Do

Mr. Daniel J. Ryan, Director, Information Systems Security Office of the
Deputy Assistant Secretary. of Defense (CI&SCI), How to Conduct INFOSEC
Business in the DoD

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 24

Monday 11 January 1993

Contents

Organizational Analysis in Computer Science

Rob Kling
Department of Information & Computer Science
University of California at Irvine,
Irvine, CA 92717, USA
kling@ics.uci.edu (714-856-5955)

January 10, 1993 [Working Draft 11b]

Note: To appear: The Information Society, 9(2) (Mar-Jun, 1993). A much shorter version of this paper will appear as "Computing for Our Future in a Social World" in Communications of the ACM, February 1993, in a Forum that discusses Computing the Future: A Broader Agenda for Computer Science and Engineering. Hartmanis, Juris and Herbert Lin (Eds). Washington, DC: National Academy Press, 1992.

ABSTRACT

Computer Science is hard pressed in the US to show broad utility to help justify billion dollar research programs and the value of educating well over 40,000 Bachelor of Science and Master of Science specialists annually in the U.S. The Computer Science and Telecommunications Board of the U.S. National Research Council has recently issued a report, "Computing the Future (Hartmanis and Lin, 1992)" which sets a new agenda for Computer Science. The report recommends that Computer Scientists broaden their conceptions of the

discipline to include computing applications and domains to help understand them. This short paper argues that many Computer Science graduates need some skills in analyzing human organizations to help develop appropriate systems requirements since they are trying to develop high performance computing applications that effectively support higher performance human organizations. It is time for academic Computer Science to embrace organizational analysis (the field of Organizational Informatics) as a key area of research and instruction.

INTRODUCTION

Computer Science is being pressed on two sides to show broad utility for substantial research and educational support. For example, the High Performance Computing Act will provide almost two billion dollars for research and advanced development. Its advocates justified it with arguments that specific technologies, such as parallel computing and wideband nets, are necessary for social and economic development. In the US, Computer Science academic programs award well over 30,000 Bachelor of Science (BS) and almost 10,000 Master of Science (MS) degrees annually. Some of these students enter PhD programs and many work on projects which emphasize mathematical Computer Science. But many of these graduates also take computing jobs for which they are inadequately educated, such as helping to develop high performance computing applications to improve the performance of human organizations.

These dual pressures challenge leading Computer Scientists to broaden their conceptions of the discipline to include an understanding of key application domains, including computational science and commercial information systems. An important report that develops this line of analysis, "Computing the Future" (CTF) (Hartmanis and Lin, 1992), was recently issued by the National Computing and Telecommunications Board of the U.S. National Research Council.

CTF is a welcome report that argues that academic Computer Scientists must acknowledge the driving forces behind the substantial Federal research support for the discipline. The explosive growth of computing and demand for CS in the last decade has been driven by a diverse array of applications and new modes of computing in diverse social settings. CTF takes a strong and useful position in encouraging all Computer Scientists to broaden our conceptions of the discipline and to examine computing in the context of interesting applications.

CTF's authors encourage Computer Scientists to envision new technologies in the social contexts in which they will be used. They identify numerous examples of computer applications in earth science, computational biology, medical care, electronic libraries and commercial computing that can provide significant value to people and their organizations. These assessments rest on concise and tacit analyses of the likely design, implementation within organizations, and uses of these technologies. For example, CTF's stories of improved computational support for modelling are based on rational models of organizational behavior. They assume that professionals, scientists, and policy-makers use models to help improve their decisions. But what if organizations behave differently when they use models? For example suppose policy makers use models to help rationalize and legitimize decisions which are made without actual reference to the models?

One cannot discriminate between these divergent roles of modelling in human organizations based upon the intentions of researchers and system designers. The report tacitly requires that the CS community develop reliable knowledge, based on systematic research, to support effective analysis of the likely designs and uses of computerized systems. CTF tacitly requires an ability to teach such skills to CS practitioners and students. Without a disciplined skill in analyzing human organizations, Computer Scientists' claims about the usability and social value of specific technologies is mere opinion, and bears a significant risk of being misleading. Further, Computer Scientists who do not have refined social analytical skills sometimes conceive and promote technologies that are far less useful or more costly than they claim. Effective CS practitioners who "compute for the future" in organizations need some refined skills in organizational analysis to understand appropriate systems requirements and the conditions that transform high performance computing into high performance human organizations. Since CTF does not spell out these tacit implications, I'd like to explain them here.

BROADENING COMPUTER SCIENCE:
FROM COMPUTABILITY TO USABILITY

The usability of systems and software is a key theme in the history of CS. We must develop theoretical foundations for the discipline that give the deepest insights in to what makes systems usable for various people, groups and organizations. Traditional computer scientists commonly refer to mathematics as the theoretical foundations of CS. However, mathematical formulations give us limited insights into understanding why and when some computer systems are more usable than others.

Certain applications, such as supercomputing and computational science are evolutionary extensions of traditional scientific computation, despite their new direction with rich graphical front ends for visualizing enormous mounds of data. But other, newer modes of computing, such as networking and microcomputing, change the distribution of applications. While they support traditional numerical computation, albeit in newer formats such as spreadsheets, they have also expanded the diversity of non-numerical computations. They make digitally represented text and graphics accessible to tens of millions of people.

These technological advances are not inconsistent with mathematical foundations in CS, such as Turing machine formulations. But the value of these formats for computation is not well conceptualized by the foundational mathematical models of computation. For example, text editing could be conceptualized as a mathematical function that transforms an initial text and a vector of incremental alterations into a revised text. Text formatting can be conceptualized as a complex function mapping text strings into spatial arrays. These kinds of formulations don't help us grasp why many people find "what you see is what you get" editors as much more intuitively appealing than a system that links line editors, command-driven formatting languages, and text compilers in series.

Nor do our foundational mathematical models provide useful ways of conceptualizing some key advances in even more traditional elements of computer systems such as operating systems and database systems. For example, certain mathematical models underlie the major families of database systems. But one can't rely on mathematics alone to assess how well networks, relations, or object-entities serve as representations for the data stored in an airline reservation system. While mathematical analysis can help optimize the efficiency of disk space in storing the data, they can't do much to help airlines understand the kinds of services that will make such systems most useful for reservationists, travel agents and even individual travellers. An airline reservation system in use is not simply a closed technical system. It is an open socio-technical system (Hewitt, 1986; Kling, 1992). Mathematical analysis can play a central role in some areas of CS, and an important role in many areas. But we cannot understand important aspects of usability if we limit ourselves to mathematical theories.

The growing emphasis of usability is one of the most dominant of the diverse trends in computing. The usability tradition has deep roots in CS, and has influenced the design of programming languages and operating systems for over 25 years. Specific topics in each of these areas also rest on mathematical analysis which Computer Scientists could point to as "the foundations" of the respective subdisciplines. But Computer Scientists envision many key advances as design conceptions rather than as mathematical theories. For example, integrated programming environments ease software development. But their conception and popularity is not been based on deeper formal foundations for programming languages. However, the growth of non-numerical applications for diverse professionals, including text processing, electronic mail, graphics, and multimedia should place a premium on making computer systems relatively simple to use. Human Computer Interaction (HCI) is now considered a core subdiscipline of CS.

The integration of HCI into the core of CS requires us to expand our conception of the theoretical foundations of the discipline. While every computational interface is reducible to a Turing computation, the foundational mathematical models of CS do not (and could not) provide a sound theoretical basis for understanding why some interfaces are more effective for some groups of people than others. The theoretical foundations of effective computer interfaces must rest on sound theories of human behavior and their empirical manifestations (cf. Ehn, 1991, Grudin, 1989).

Interfaces also involve capabilities beyond the primary information processing features of a technology. They entail ways in which people learn about systems and ways to manage the diverse data sets that routinely arise in using many computerized systems (Kling, 1992). Understanding the diversity and character of these interfaces, that are required to make many systems usable, rests in an understanding the way that people and groups organize their work and expertise with computing. Appropriate theories of the diverse interfaces that render many computer systems truly useful must rest, in part, on theories of work and organization. There is a growing realization, as networks tie users together at a rapidly rising rate, that usability cannot generally be determined without our considering how computer systems are shaped by and also alter interdependencies in groups and organizations. The newly-formed subdiscipline of Computer Supported Cooperative Work and newly-coined term "groupware" are responses to this realization (Greif, 1988; Galegher, Kraut and Egido, 1990).

BROADENING COMPUTER SCIENCE:

FROM HIGH PERFORMANCE COMPUTING TO HIGH PERFORMANCE ORGANIZATIONS

The arguments of CTF go beyond a focus on usable interface designs to claims that computerized systems will improve the performance of organizations. The report argues that the US should invest close to a billion dollars a year in CS research because of the resulting economic and social gains. These are important claims, to which critics can seek systematic evidence. For example, one can investigate the claim that 20 years of major computing R&D and corporate investment in the US has helped provide proportionate economic and social value.

CTF is filled with numerous examples where computer-based systems provided value to people and organizations. The tough question is whether the overall productive value of these investments is worth the overall acquisition and operation costs. While it is conventional wisdom that computerization must improve productivity, a few researchers began to see systemic possibilities of counter-productive computerization in the early 1980s (King and Kraemer, 1981). In the last few years economists have found it hard to give unambiguously affirmative answers to this question. The issue has been termed "The Productivity Paradox," based on a comment attributed to Nobel laureate Robert Solow who remarked that "computers are showing up everywhere except in the [productivity] statistics (Dunlop and Kling, 1991a)."

Economists are still studying the conditions under which computerization contributes to organizational productivity, and how to measure iteasy. But there is no automatic link between computerization and improved productivity. While many computer systems have been usable and useful, productivity gains require that their value exceed all of their costs.

There are numerous potential slips in translating high performance computing into cost-effective improvements in organizational performance. Some technologies are superb for well-trained experts, but are difficult for less experienced people or "casual users." Many technologies, such as networks and mail systems, often require extensive technical support, thus adding hidden costs (Kling, 1992).

Further, a significant body of empirical research shows that the social processes by which computer systems are introduced and organized makes a substantial difference in their value to people, groups and organizations (Lucas, 1981; Kraemer, et. al. 1985; Orlikowski, 1992). Most seriously, not all presumably appropriate computer applications fit a person or group's work practices. While they may make sense in a simplified world, they can actually complicate or misdirect real work.

Group calendars are but one example of systems that can sound useful, but are often useless because they impose burdensome record keeping demands (Grudin, 1989). In contrast, electronic mail is one of the most popular applications in office support systems, even when other capabilities, like group calendars, are ignored (Bullen and Bennett, 1991). However, senders are most likely to share information with others when the system helps provide social feedback about the value of their efforts or they have special incentives (Sproull and Kiesler, 1991; Orlikowski, 1992). Careful attention to the social arrangements or work can help Computer Scientists improve some systems designs, or also appreciate which applications may not be effective unless work arrangements are changed when the system is introduced.

The uses and social value of most computerized systems can not be effectively ascertained from precise statements of their basic design principles and social purposes. They must be analyzed within the social contexts in which they will be used. Effective social analyses go beyond accounting for formal tasks and purposes to include informal social behavior, available resources, and the interdependencies between key groups (Cotterman and Senn, 1992).

Many of the BS and MS graduates of CS departments find employment on projects where improved computing should enhance the performance of specific organizations or industries. Unfortunately, few of these CS graduates have developed an adequate conceptual basis for understanding when information systems will actually improve organizational performance. Consequently, many of them are prone to recommend systems-based solutions whose structure or implementation within organizations would be problematic.

ORGANIZATIONAL INFORMATICS

Organizational Informatics denotes a field which studies the development and use of computerized information systems and communication systems in organizations. It includes studies of their conception, design, effective implementation within organizations, maintenance, use, organizational value, conditions that foster risks of failures, and their effects for people and an organization's clients. It is an intellectually rich and practical research area.

Organizational Informatics is a relatively new label. In Europe, the term Informatics is the name of many academic departments which combine both CS and Information Systems. In North America, Business Schools are the primary institutional home of Information Systems research and teaching. But this location is a mixed blessing. It brings IS research closer to organizational studies. But the institutional imperatives of business schools lead IS researchers to emphasize the development and use of systems in a narrow range of organizations -- businesses generally, and often service industry firms. It excludes information systems in important social sectors such as health care, military operations, air-traffic control, libraries, home uses, and so on. And Information Systems research tries to avoid messy issues which many practicing Computer Scientists encounter: developing requirements for effective systems and mitigating the major risks to people and organizations who depend upon them.

The emerging field of Organizational Informatics builds upon research conducted under rubrics like Information Systems and Information Engineering. But it is more wide ranging than either of these fields are in practice.

Organizational Informatics Research

In the last 20 years a loosely organized community of some dozens of researchers have produced a notable body of systematic scientific research in Organizational Informatics. These studies examine a variety of topics, including:

- how system designers translate people's preferences into requirements;
- the functioning of software development teams in practice;
- the conditions that foster and impede the implementation of computerized systems within organizations;
- how people and organizations use systems in practice;
- the roles of computerized systems in altering work, group communication, power relationships, and organizational practices.

Researchers have extensively studied some of these topics, such as computerization and changing work, appear in synoptic review articles (Kling and Dunlop, in press). In contrast, researchers have recently begun to examine other topics, such software design (Winograd and Flores, 1986; Kyng and Greenbaum, 1991), and have recently begun to use careful empirical methods (e.g. Suchman, 1983; Bentley, et. al, 1992; Fish, et. al., 1993). I cannot summarize the key theories and rich findings of these diverse topics in a few paragraphs. But I would like to comment upon a few key aspects of this body of research.

Computer Systems Use in Social Worlds

Many studies contrast actual patterns of systems design, implementation, use or impacts with predictions made by Computer Scientists and professional commentators. A remarkable fraction of these accounts are infused with a hyper-rational and under-socialized view of people, computer systems, organizations and social life in general. Computer Scientists found that rule driven conceptions to be powerful ways to abstract domains like compilers. But many Computer Scientists extend them to be a tacit organizing frame for understanding whole computer systems, their developers, their users and others who live and work with them. Organizations are portrayed as generally cooperative systems with relatively simple and clear goals. Computer systems are portrayed as generally coherent and adequate for the tasks for which people use them. People are portrayed as generally obedient and cooperative participants in a highly structured system with numerous tacit rules to be obeyed, such as doing their jobs as they are formally described. Using data that is contained in computer systems, and treating it as information or knowledge, is a key element of these accounts. Further, computer systems are portrayed as powerful, and often central, agents of organizational change.

This Systems Rationalist perspective infuses many accounts of computer systems design, development, and use in diverse application domains, including CASE tools, instructional computing, models in support of public policy assessments, expert systems, groupware, supercomputing, and network communications (Kling, 1980; Kling, Scherson and Allen, 1992).

All conceptual perspectives are limited and distort "reality." When Organizational Informatics researchers systematically examine the design practices in particular organizations, how specific groups develop computer systems, or how various people and groups use computerized systems, they find an enormous range of fascinating and important human behavior which lies outside the predictive frame of Systems Rationalism. Sometimes these behaviors are relatively minor in overall importance. But in many cases they are so significant as to lead Organizational Informatics researchers to radically reconceptualize the processes which shape and are shaped by computerization.

There are several alternative frames for reconceptualizing computerization as alternatives to Systems Rationalism. The alternatives reflect, in part, the paradigmatic diversity of the social sciences. But all of these reconceptions situate computer systems and organizations in richer social contexts and with more complex and multivalent social relations than does systems rationalism. Two different kinds of observations help anchor these abstractions.

Those who wish to understand the dynamics of model usage in public agencies must appreciate the institutional relationships which influence the organization's behavior. For example, to understand economic forecasting by the US Congress and the Executive branch's Office of Management and Budget, one must appreciate the institutional relations between Congress and the Executive branch. They are not well described by Systems Rationalist conceptions because they were designed to continually differ with each other in their perspectives and preferred policies. That is one meaning of "checks and balances" in the fundamental design of the US Federal Government. My colleagues, Ken Kraemer and John King, titled their book about Federal economic modelling, DataWars (Kraemer, et. al., 1985). Even this title doesn't make much sense within a Systems Rationalist framework.

Modelling can be a form of intellectual exploration. It can also be a medium of communication, negotiation, and persuasion. The social relationships between modelers, people who use them and diverse actors in Federal policymaking made these socially mediated roles of models sometimes most important. In these situations, an alternative view of organizations as coalitions of interest groups was a more appropriate conceptualization. And within this coalitional view of organizations, a conception of econometric models as persuasion support systems rather than as decision support systems sometimes is most appropriate. Organizational Informatics researchers found that political views of organizations and systems developments within them apply to many private organizations as well as to explicitly political public agencies.

Another major idea to emerge from the broad body of Organizational Informatics research is that the social patterns which characterize the design, development, uses and consequences of computerized systems are dependent on the particular ecology of social relationships between participants. This idea may be summarized by saying that the processes and consequences of computerization are "context dependent." In practice, this means that the analyst must be careful in generalizing from one organizational setting to another. While data wars might characterize econometric modelling on Capitol Hill, we do not conclude that all computer modelling should be interpreted as persuasion support systems. In some settings, models are used to explore the effects of policy alternatives without immediate regard for their support as media for communication, negotiation or persuasion. At other times, the same model might be used (or abused with cooked data) as a medium of persuasion. The brief accounts of models for global warming in CTF fit a Systems Rationalist account. Their uses might appear much less "scientific" if they were studied within the actual policy processes within which they are typically used.

Repercussions for Systems Design

Even when computerized systems are used as media of intellectual exploration, Organizational Informatics researchers find that social relationships influence the ways that people use computerized systems. Christine Bullen and John Bennett (1991) studied 25 organizations that used groupware with diverse modules such as databases, group calendars, text annotating facilities and electronic mail. They found that the electronic mail modules were almost universally valued, while other system facilities were often unused.

In a recent study, Sharyn Ladner and Hope Tillman examined the use of the Internet by university and corporate librarians. While many of them found data access through databases and file transfer to be important services, they also reported that electronic mail was perhaps the most critical Internet feature for them.

> The participants in our study tell us something that we may have forgotten in our infatuation with the new forms of information made available through the Internet. And that is their need for community. To be sure, our respondents use the Internet to obtain information not available in any other format, to access databases ... that provide new efficiencies in their work, new ways of working. But their primary use is for communication. Special librarians tend to be isolated in the workplace -- the only one in their subject specialty (in the case of academe), or the only librarian in their organization (in the case of a corporate library). Time and time again our respondents expressed this need to talk to someone -- to learn what is going on in their profession, to bounce ideas off others, to obtain information from people, not machines.
>
> There are tremendous implications from the Internet technology in community formation -- the Internet may indeed provide a way to increase community among scholars, including librarians. The danger we face at this juncture in time, as we attach library resources to the Internet, is to focus all of our energies on the machine-based resources at the expense of our human-based resources, i.e., ourselves (Ladner and Tillman, 1992).

In these studies, Organizational Informatics researchers have developed a socially rich view of work with and around computing, of computing within a social world.

These studies have strong repercussions for the design of software. A good designer cannot assume that the majority of effort should go into the "computational centerpiece" of a system, while devoting minor efforts to supporting communication facilities. One of my colleagues designed a modelling system for managers in a major telephone company, after completing an extensive requirements analysis. However, as an afterthought, he added a simple mail system in a few days work. He was surprised to find that the people who used these systems regularly used his crude electronic mail system, while they often ignored interesting modelling capabilities. Such balances of attention also have significant repercussions. Many people need good mail systems, not just crude ones: systems which include facile editors, ease in exporting and importing files, and effective mail management (Kling and Covi, 1993).

Assessing people's preferences for systems' designs is an exercise in social inquiry. While rapid prototyping may help improve designs for some systems, it is less readily applicable to systems which are used by diverse groups at numerous locations. Computer scientists are beginning to develop more reliable methods of social inquiry to better understand which systems designs will be most useful (Bentley, et. al. 1992; Kyng and Greenbaum, 1991). Root and his colleagues (1993) recently reported the way that the explicit use of social theory helped them design more effective group meeting systems. Unfortunately, these newer methods are rarely taught to CS students. When computer specialists build an imbalanced system, it should not be a surprise when the resulting organizational value of their efforts is very suboptimal.

[CONTINUED in RISKS-14.25.]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 25

Monday 11 January 1993

Contents

[CONTINUED FROM RISKS-14.24]

System Security and Reliability

In a simplified engineering model of computing, the reliability of products is assured through extensive testing in a development lab. The social world of technology use is not perceived as shaping the reliability of systems, except through irascible human factors, such as "operator errors." An interesting and tragic illustration of the limitations of this view can be found in some recent studies of the causes of death and maiming by an electron accelerator which was designed to help cure cancer, the Therac-25 (Jacky, 1991, Leveson and Turner, 1992).

The Therac-25 was designed and marketed in the mid 1980s by a Canadian firm AECL as an advanced medical technology. It featured complete software control over all major functions (supported by a DEC PDP-11), among other innovations. Previous machines included electro-mechanical interlocks to raise and lower radiation shields. Several thousand people were effectively treated with the Therac-25 each year. However, between 1985 and 1987 there were six known accidents in which several people died in the US. Other were seriously maimed or injured.

Both studies concur that there were subtle but important flaws in the design of the Therac-25's software and hardware. AECL's engineers tried to patch the existing hardware and (finally) software when they learned of some of the mishaps. But they treated each fix as the final repair.

Both studies show how the continuing series of mishaps was exacerbated by diverse organizational arrangements. Jacky claims that pressures for speedy work by low-skilled machine operators coupled with an interface design that did not enhance important error messages was one of many causes of the accidents. Leveson and Turner differ in downplaying the working conditions of the Therac-25's operators and emphasize the flawed social system for communicating the seriousness of problems to Federal regulators and other hospitals. Both studies observe that it is unlikely for the best of companies to develop perfect error-free systems without high quality feedback from users. Their recommendations differ: Jacky emphasizes the licensing of system developers to improve minimal standards of competence. Leveson and Turner propose extensive education and training of software engineers and more effective communication between manufacturers and their customers.

However, both studies indicate that an understanding of the safety of computer systems must go beyond the laboratory and extend into the organizational settings where it is used. In the case of the Therac-25, it required understanding a complex web of interorganizational relationships, as well as the technical design and operation of the equipment. The need for this kind of organizational understanding is unfortunately slighted in the CS academic world today. CTF discusses only those aspects of computer system reliability which are amenable to understanding through laboratory-like studies (Hartmanis and Lin, 1992:110-111). But cases of safety critical systems, like the Therac-25, indicate why some Computer Scientists must be willing to undertake (and teach) organizational analysis.

[From the title of the above section, I presume Rob had not yet gotten around to commenting on system security in complementary context to the discussion on human safety. But it seems that similar conclusions can be drawn. Apologies for the interjection. PGN]

Worldviews and Surprises about Computerization

These few paragraphs barely sketch the highlights of a fertile and significant body of research about computer systems in use. Perhaps the most important simplification for traditional computer scientists is to appreciate how people and their organizations are situated in a social world and consequently compute within a social world. People act in relationship to others in various ways and concerns of belonging, status, resources, and power are often central. The web of people's relationships extend beyond various formally defined group and organizational boundaries (Kling and Scacchi, 1982; Kling, 1992). People construct their worlds, including the meanings and uses of information technologies, through their social interactions.

This view is, of course, not new to social scientists. On the other hand, there is no specific body of social theory which can easily be specialized for "the case of computing," and swiftly produce good theories for Organizational Informatics as trivial deductions. The best research in Organizational Informatics draws upon diverse theoretical and methodological approaches within the social sciences with a strong effort to select those which best explain diverse aspects of computerization.

ORGANIZATIONAL INFORMATICS WITHIN COMPUTER SCIENCE

CTF places dual responsibilities on Computer Scientists. One responsibility is to produce a significant body of applicable research. The other responsibility is to educate a significant fraction of CS students to be more effective in conceiving and implementing systems that will enhance organizational performance. It may be possible to organize research and instruction so as to decouple these responsibilities. For example, molecular biologists play only a small role in training doctors. However, CS departments act like an integrated Medical school and Biology department. They are the primary academic locations for training degreed computing specialists, and they conduct a diverse array of less applicable and more applicable research. In practice, the research interests of CS faculty shape the range of topics taught in CS departments, especially the 150 PhD granting departments. CS curricula mirror major areas of CS research and the topics which CS faculty understand through their own educations and subsequent research. As a consequence, CS courses are likely to avoid important CS topics which appear a bit foreign to the instructor.

An interesting example of this coupling can be illustrated by CTF, in a brief description of public-key encryption systems and digital signatures (Hartmanis and Lin, 1992:27). In the simple example, Bob and Alice can send messages reliably if each maintains a secret key. Nothing is said about the social complications of actually keeping keys secret. The practical problems are similar to those of managing passwords. In real organizations, people lose or forget their passwords. Also, some passwords can be shared by a group of with shifting membership, and the "secret key" can readily become semi-public. In practice, the management of keys is a critical element of system security. But Computer Scientists are prone to teach courses on cryptography as exercises in applied mathematics, such as number theory and Galois theory, and to skirt the vexing practical problems of making encryption a practical organizational activity.

Today, most of the 40,000 people who obtain BS and MS degrees in CS each year in the U.S. have no opportunities for systematic exposure to reliable knowledge about the best design strategies, common uses, effective implementation, and assessments of value of computing in a social world (Lewis, 1989). Yet a substantial fraction of these students go on to work for organizations attempting to produce or maintain systems that improve organizational performance without a good conceptual basis for their work. Consequently, many of them develop systems that underperform in organizational terms even when they are technically refined. They also recommend ineffective implementation procedures and are sometimes even counterproductive.

One defensible alternative to my position is that CS departments should not take on any form of organizational analysis. They should aggressively take a role akin to Biology departments rather than taking on any instructional or research roles like Medical schools. To be sincere, this position requires a high level of restraint by academic Computer Scientists. First and foremost, they should cease from talking about the uses, value or even problems of computerized systems that would be used in any organizational setting. Research proposals would be mute about any conceivable application of research results. Further, they should make effective efforts to insure that anyone who employs their graduates should be aware that they may have no special skills in understanding organizational computing. It would take an aggressive "truth in advertising" campaign to help make it clear that Computer Scientists have no effective methods for understanding computerization in the social world.

Further, Computer Scientists would forsake their commitments to subfields like software engineering which tacitly deals with ways to support teams of systems developers to work effectively (Curtis, et. al. 1988). Computer Scientists, in this view, would remove themselves from addressing organizational and human behavior, in the same way that molecular biologists are removed from professionally commenting on the practices of cardiologists and obstetricians. CTF argues that this view would be self-defeating. But it would be internally consistent and have a distinctive integrity.

In contrast, CS faculty are often reluctant to wholly embrace Organizational Informatics. But some CS subfields, such as software engineering, depend upon organizational analysis (Curtis, et. al., 1988). Further, CS faculty do little to advertise the distinctive limitations in the analytical skills of our programs' graduates. Part of the dilemma develops because many CS faculty are ambivalent about systematic studies of human behavior. Applied mathematics and other modes of inquiry which seem to yield concise, crisp and concrete results are often the most cherished. As a consequence, those who conduct behaviorally oriented research in CS departments are often inappropriately marginalized. Their students and the discipline suffers as a result.

Between 1986 and 1989, the total number of BS and MS CS degrees awarded annually in the US declined from about 50,000 to approximately 40,000. The number of students majoring in CS rapidly declined at a time when computerization was becoming widespread in many fields. A significant fraction of the decline can be attributed to many students finding CS programs insular and indifferent to many exciting forms of computerization. The decline of military R&D in the U.S. can amplify these trends or stimulate a more cosmopolitan view in CS departments. The decline in military R&D is shifting the job market for new CS graduates towards a markedly more civilian orientation. This shift, along with the trend towards computing distributed into diverse work groups, is leading to more job opportunities for people with CS education who know Organizational Informatics.

The situation of CS departments has some parallels with Statistics departments. Statistics are widely used and taught in many academic disciplines. But Statistics departments have often maintained a monkish isolation from "applications." Consequently, the application of statistics thrives while Statistics departments have few students and modest resources. Might the status of Statistics indicate a future possibility for an insular approach to CS?

The best Organizational Informatics research in North America is conducted by faculty in the Information Systems departments in business schools and by scattered social scientists (cf. Boland and Hirschheim, 1987; Galegher, Kraut and Egido, 1990; Cotterman and Senn, 1992; Sproull and Kiesler, 1991). But Computer Scientists cannot effectively delegate the research and teaching of Organizational Informatics to business Schools or social science departments.

Like Computer Scientists, faculty in these other disciplines prefer to focus on their own self-defined issues. Computer Scientists are much more likely to ask questions with attention to fine grained technological nuances that influence designs. For example, the professional discussions of computer risks have been best developed through activities sponsored by the ACM's Special Interest Group on Software (SIGSOFT). They are outside the purview of business school faculty and, at best, only a few social scientists are interested in them. Generally, technology plays a minor role in social science theorizing. And when social scientists study technologies, they see a world of possibilities: energy technologies, transportation technologies, communication technologies (including television), medicinal drugs and devices, and so on. They see little reason to give computer-related information technologies a privileged role within this cornucopia. As a consequence, the few social scientists who take a keen interest in studying computerization are unfortunately placed in marginal positions within their own disciplines. Often they must link their studies to mainstream concerns as defined by the tastemakers of their own fields, and the resulting publications appear irrelevant to Computer Scientists.

Further, faculty in these other disciplines are not organized to effectively teach tens of thousands of CS students, students who are steeped in technology and usually very naive about organizations, about systems development and use in organizations. In North America there is no well developed institutional arrangement for educating students who can effectively take leadership roles in conceptualizing and developing complex organizational computing projects (Lewis, 1989).

CTF is permeated with interesting claims about the social value of recent and emerging computer-based technologies. While many of these observations should rest on an empirically grounded scientific footing, Computer Scientists have deprived themselves of access to such research. For example, the discussion of systems risks in the ACM rests on a large and varied collection of examples and anecdotes. But there is no significant research program to help better understand the conditions under which organizations are more likely to develop systems using the best risk-reducing practices. There is an interesting body of professional lore, but little scholarship to ground it (See Appendix).

Computer Scientists have virtually no scholarship to utilize in understanding when high performance networks, like the National Research and Education Network, will catalyze social value proportional to their costs. Consequently, many of the "obvious" claims about the value of various computing technologies that we Computer Scientists make are more akin to the lore of home remedies for curing illness. Some are valid, others are unfounded speculation. More seriously, the theoretical bases for recommending home medical remedies and new computer technologies can not advance without having sound research programs.

WHAT IS NEEDED

CTF sets the stage for developing Organizational Informatics as a strong subfield within Computer Science. CTF bases the expansion of the discipline on a rich array of applications in which many of the effective technologies must be conceived in relationship to plausible uses in order provide attractive social value for multi-billion dollar public investments.

The CS community needs an institutionalized research capability to produce a reliable body of knowledge about the usability and value of computerized systems and the conditions under which computer systems improve organizational performance. In Western Europe there are research projects about Organizational Informatics in a few Computer Science departments and research funding through the EEC's Espirit program (Bubenko, 1992; Iivari, 1991; Kyng and Greenbaum, 1991). These new research and instructional programs in Western Europe give Organizational Informatics a significantly more effective place in CS education and research than it now has in North America.

The CS community in the U.S. has 30 years of experience in institutionalizing research programs, especially through the Defense Advanced Research Projects Agency and the National Science Foundation (NSF). There are many approaches, including national centers and individual investigator research grants. All such programs aim to develop and sustain research fields with a combination of direct research funds, the education of future researchers, and the development of research infrastructure. They are all multimillion dollar efforts. Today, NSF devotes about $125K annually to Organizational Informatics as part of the Information Technology in Organizations program. This start is far short of the level of funding required to develop this field within CS.

The North American CS curricula must also include opportunities for students to learn the most reliable knowledge about the social dimensions of systems development and use (Denning, 1992). These opportunities, formed as courses, can provide varied levels of sophistication. The most elementary courses introduce students to some of the key topics in Organizational Informatics and the limitations of Systems Rationalism as an organizing frame (for example, Dunlop and Kling, 1991a). More advanced courses focus on specific topics, such as those I have listed above. They teach about substantive problems and theoretical approaches for analyzing them. While many of these approaches are anchored in the sociological theory of organizations, CS students usually won't grasp the importance of the theories without numerous computing examples to work with. They also have trouble grasping the character of computing in organizations without guided opportunities for observing and analyzing computerization in practice. Consequently, some courses should offer opportunities for studying issues of computerization in actual organizations.

Fortunately, a few CS departments offer some courses in Organizational Informatics. In addition, some CS faculty who research and teach about human behavior in areas like Human-Computer Interaction and Software Engineering can help expand the range of research an instruction. Unfortunately, only a fraction of the CS departments in the US. have faculty who study and teach about computing and human behavior.

While the study of Organizational Informatics builds upon both the traditional technological foundations of CS and the social sciences, the social sciences at most universities will not develop it as an effective foundational topic for CS. On specific campuses, CS faculty may be able to develop good instructional programs along with colleagues in social sciences or Schools of Management.

But delegating this inquiry to some other discipline does not provide a national scale solution for CS. Other disciplines will not do our important work for us. Mathematics departments may be willing to teach graph theory for CS students, but the analysis of algorithms would be a much weaker field if it could only be carried out within Mathematics Departments. For similar reasons, it is time for academic Computer Science to embrace Organizational Informatics as a key area of research and instruction.

REFERENCES

Bentley, Richard, Tom Rodden, Peter Sawyer, Ian Sommerville, John Hughes, David Randall and Dan Shapiro. 1992. "Ethnographically Informed Systems Design for Air Traffic Control." Proc. Conference on Computer-Supported Cooperative Work, Jon Turner and Robert Kraut (ed.) New York, ACM Press.

Boland, Richard and Rudy Hirschhiem (Ed). 1987. Critical Issues in Information Systems, New York: John-Wiley.

Bullen, Christine and John Bennett. 1991. Groupware in Practice: An Interpretation of Work Experience" in Dunlop and Kling 1991b.

Bubenko, Janis. 1992. "On the Evolution of Information Systems Modeling: A Scandinavian Perspective." in Lyytinen and Puuronen, 1992.

Cotterman, William and James Senn (Eds). 1992. Challenges and Strategies for Research in Systems Development. New York: John Wiley.

Curtis, Bill, Herb Krasner and Niel Iscoe. 1988. "A Field Study of the Software Design Process for Large Systems," Communications. of the ACM. 31(11):1268-1287.

Denning, Peter. 1991. "Computing, Applications, and Computational Science." Communications of the ACM. (October) 34(10):129-131.

Denning, Peter. 1992. "Educating a New Engineer" Communications of the ACM. (December) 35(12):83-97

Dunlop, Charles and Rob Kling, 1991a. "Introduction to the Economic and Organizational Dimensions of Computerization." in Dunlop and Kling, 1991b.

Dunlop, Charles and Rob Kling (Ed). 1991b. Computerization and Controversy: Value Conflicts and Social Choices. Boston: Academic Press.

Ehn, Pelle. 1991. "The Art and Science of Designing Computer Artifacts." in Dunlop and Kling, 1991.

Fish, Robert S., Robert E. Kraut, Robert W. Root, and Ronald E. Rice. "Video as a Technology for Informed Communication." Communications of the ACM,36(1)(January 1993):48-61.

Galegher, Jolene, Robert Kraut, and Carmen Egido (Ed.) 1990. Intellectual Teamwork: Social and Intellectual Foundations of Cooperative Work. Hillsdale, NJ: Lawrence Erlbaum.

Greif, Irene. ed. 1988. Computer Supported Cooperative Work: A Book of Readings. San Mateo, Ca: Morgan Kaufman.

Grudin, Jonathan. 1989. "Why Groupware Applications Fail: Problems in Design and Evaluation." Office: Technology and People. 4(3):245-264.

Hartmanis, Juris and Herbert Lin (Eds). 1992. Computing the Future: A Broader Agenda for Computer Science and Engineering. Washington, DC. National Academy Press. [Briefly summarized in Communications of the ACM,35(11) November 1992]
[[TO BE DISCUSSED AT ACM CSC in Indianapolis, 16-18 Feb 1992... PGN]]

Hewitt, Carl. 1986. "Offices are Open Systems" ACM Transactions on Office Information Systems. 4(3)(July):271-287.

Iivari, J. 1991."A Paradigmatic Analysis of Contemporary Schools of IS Development." European J. Information Systems 1(4)(Dec): 249-272.

Jacky, Jonathan. 1991. "Safety-Critical Computing: Hazards, Practices, Standards, and Regulation" in Dunlop and Kling 1991b.

Jarvinen, Pertti. 1992. "On Research into the Individual and Computing Systems," in Lyytinen and Puuronen, 1992.

King, John L. and Kenneth L. Kraemer. 1981. "Cost as a Social Impact of Telecommunications and Other Information Technologies." In Mitchell Moss (Ed.) Telecommunications and Productivity, New York: Addison-Wesley.

Kling, Rob. 1992. "Behind the Terminal: The Critical Role of Computing Infrastructure In Effective Information Systems' Development and Use." Chapter 10 in Challenges and Strategies for Research in Systems Development. edited by William Cotterman and James Senn. Pp. 153-201. New York: John Wiley.

Kling, Rob and Charles Dunlop. 1993. "Controversies About Computerization and the Character of White Collar Worklife." The Information Society. 9(1) (Jan-Feb)

Kling, Rob and Lisa Covi. 1993. Review of Connections by Lee Sproull and Sara Kiesler. The Information Society, 9(1) (Jan-Feb, 1993).

Kling, Rob, Isaac Scherson, and Jonathan Allen. 1992. "Massively Parallel Computing and Information Capitalism" in A New Era of Computing. W. Daniel Hillis and James Bailey (Ed.) Cambridge, Ma: The MIT Press.

Kling, Rob and Walt Scacchi. 1982. "The Web of Computing: Computing Technology as Social Organization", Advances in Computers. Vol. 21, Academic Press: New York.

Kraemer, Kenneth .L., Dickhoven, Siegfried, Fallows-Tierney, Susan, and King, John L. 1985. Datawars: The Politics of Modeling in Federal Policymaking. New York: Columbia University Press.

Kyng, Morton and Joan Greenbaum. 1991. Design at Work: Cooperative Work of Computer Systems. Hillsdale, NJ.: Lawrence Erlbaum.

Ladner, Sharyn and Hope Tillman. 1992. "How Special Librarians Really Use the Internet: Summary of Findings and Implications for the Library of the Future" Canadian Library Journal, 49(3), 211-216.

Leveson, Nancy G. and Clark S. Turner. 1992. "An Investigation of the Therac-25 Accidents". Technical Report #92-108. Department of Information and Computer Science, University of California, Irvine.

Lewis, Philip M. 1989. "Information Systems as an Engineering Discipline." Communications of the ACM 32(9)(Sept):1045-1047.

Lucas, Henry C. 1981. Implementation : the Key to Successful Information Systems. New York: Columbia University Press.

Lyytinen, Kalle and Seppo Puuronen (Ed.) 1992. Computing in the Past, Present and Future: Issues and approaches in honor of the 25th anniversary of the Department of Computer Science and Information Systems. Jyvaskyla Finland, Dept. of CS and IS, University of Jyvaskyla.

Orlikowski, Wanda. 1992. "Learning from Notes: Organizational Issues in Groupware Implementation." Proc. Conference on Computer-Supported Cooperative Work, Jon Turner and Robert Kraut (Ed.) New York, ACM Press.

Sarmanto, Auvo. 1992. "Can Research and Education in the Field of Information Sciences Foresee the Future of Development?" in Lyytinen and Puuronen, 1992.

Sproull, Lee and Sara Kiesler. 1991. Connections: New Ways of Working in the Networked Organization. Cambridge, Mass.: MIT Press.

Suchman, Lucy. 1983. "Office Procedures as Practical Action: Models of Work and System Design." ACM Transactions on Office Information Systems. 1(4)(October):320-328.

Winograd, Terry and Fernando Flores. 1986. Understanding Computers and Cognition. Norwood, NJ: Ablex Publishing.

ACKNOWLEDGEMENTS

This paper builds on ideas which I've developed over the last decade. But they have been deepened by some recent events, such as the CTF report. They were also sharpened through a lecture and followon discussion with colleagues at the University of Toronto, including Ron Baeker, Andy Clement, Kelley Gottlieb, and Marilyn Mantei. Rick Weingarten suggested that I write a brief position paper reflecting those ideas. At key points, Peter Denning and Peter Neumann provided helpful encouragement and sage advice. I also appreciate the efforts of numerous other friends and colleagues to help strengthen this paper through their comments and critical assistance. The paper is immeasurably stronger because of the prompt questions and suggestions that I received in response to an evolving manuscript from the following people: Mark Ackerman, Jonathan P. Allen, Bob Anderson, Lisa Covi, Brad Cox, Gordon Davis, Phillip Fites, Simson Garfinkel, Les Gasser, Sy Goodman, Beki Grinter, Jonathan Grudin, Pertti Jarvinen, John King, Heinz Klein, Trond Knudsen, Kenneth Kraemer, Sharyn Ladner, Nancy Leveson, Lars Matthiesen, Colin Potts, Paul Resnick, Larry Rosenberg, Tim Standish, John Tillquist, Carson Woo and Bill Wulf.

APPENDIX

Published Materials about Computer Risks

Unfortunately, there is no single good book or comprehensive review article about the diverse risks of computerized systems to people and organizations, and ways to mitigate them. The Internet board, comp.risks, is the richest archive of diverse episodes and diverse discussions of their causes and cures. While its moderator, Peter Neumann does a superb job of organizing discussions of specific topics each year and also creates periodic indices, there is no simple way to sift through the megabytes of accumulated comp.risks files.

Computerization and Controversy edited by Charles Dunlop and Rob Kling (1991) includes two major sections on "security and reliability" and "privacy and social control" which identify many key debates and reprint some key articles and book excerpts which reflect different positions. Another major source is a series of articles, "Inside Risks, which Peter Neumann edits for Communications of the ACM.

This is a list of this series of articles, to date:
(All articles are by Peter Neumann unless otherwise indicated.)

Jul 90. 1. Some Reflections on a Telephone Switching Problem
Aug 90. 2. Insecurity About Security?
Sep 90. 3. A Few Old Coincidences
Oct 90. 4. Ghosts, Mysteries, and Risks of Uncertainty
Nov 90. 5. Risks in computerized elections
Dec 90. 6. Computerized medical devices, Jon Jacky
Jan 91. 7. The Clock Grows at Midnight
Feb 91. 8. Certifying Programmers and Programs
Mar 91. 9. Putting on Your Best Interface
Apr 91. 10. Interpreting (Mis)information
May 91. 11. Expecting the Unexpected Mayday!
Jun 91. 12. The Risks With Risk Analysis, Robert N. Charette
Jul 91. 13. Computers, Ethics, and Values
Aug 91. 14. Mixed Signals About Social Responsibility, Ronni Rosenberg
Sep 91. 15. The Not-So-Accidental Holist
Oct 91. 16. A National Debate on Encryption Exportability, Clark Weissman
Nov 91. 17. The Human Element
Dec 91. 18. Collaborative Efforts
Jan 92. 19. What's in a Name?
Feb 92. 20. Political Activity and International Computer Networks, Sy Goodman
Mar 92. 21. Inside ``Risks of `Risks' ''
Apr 92. 22. Privacy Protection, Marc Rotenberg
May 92. 23. System Survivability
Jun 92. 24. Leaps and Bounds (Leap-year and distributed system problems)
Jul 92. 25. Aggravation by Computer: Life, Death, and Taxes,
Aug 92. 26. Fraud by Computer
Sep 92. 27. Accidental Financial Losses
Oct 92. 28. Where to Place Trust
Nov 92. 29. Voting-Machine Risks, Rebecca Mercuri
Dec 92. 30. Avoiding Weak Links
Jan 93. 31. Risks Considered Global(ly)
Feb 93. 32. Is Dependability Attainable?
Mar 93. 33. Risks of Technology

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 26

Tuesday 12 January 1993

Contents

Florida Rental Car Scam

Dewey Coffman <dewey@sooner.ctci.com>
Sun, 10 Jan 93 18:16:35 CST

Ex-Car Rental Owners Indicted, FORT LAUDERDALE, Fla. (AP)
Value Rent-A-Car Inc. rigged its COMPUTER system to set up a scam overcharging customers who returned their cars with less than a full tank, a federal indictment says. The indictment returned Friday says Steven M. Cohen, one of three former owners charged, fixed Value's computer system in 1988 to add five gallons to the fuel tank capacity of every vehicle in Value's fleet.
This allowed the company to overcharge customers who turned in the car with less than a full tank.
Federal prosecutor Lothar Genge said that through 1991, about 47,000 customers were slapped with the phony charge, which ranged from a couple of dollars to $10 or $15. Mitsubishi Motor Sales bought the company in 1990 and is looking for ways to pay back the overcharges, Genge said.

Computer games may endanger your health

Olivier MJ Crepin-Leblond <o.crepin-leblond@ic.ac.uk>
Thu, 7 Jan 1993 22:47:24 +0000

Nintendo Inquiry Launched

The Government is probing claims of health hazards to children playing computer games like Nintendo. The informal inquiry follows reports that two boys in Cardiff had been struck down with epileptic fits.

Baroness Denton, junior Consumer Affairs Minister, has called for an urgent report: `It is important to know if there are any health risks.
[From Teletext service on Carlton TV & Channel 4 (UK), Thursday 7th Jan 93]

Olivier M.J. Crepin-Leblond, Digital Comms. Section, Elec. Eng. Department
Imperial College of Science, Technology and Medicine, London SW7 2BT, UK

Ford's honesty saves county $2 million

"I. LOVTUSKI" <CIGAS@RCKHRST1.BITNET>
07 Jan 1993 16:59:41 -0500 (CDT)

Here is an excerpt from an article in the Kansas City Star, January 7, 1993:

Ford's honesty saves county $2 million, by Anne Lamoy

An alert bookkeeper at the Ford Claycomo assembly plant saved Clay County from cheating itself out of $2 million. When paying the county's business personal property taxes recently, Ford's bookkeeper realized that the plant's two tax bills were much smaller than in previous years. Much, much

smaller. "When the original bills were printed, they left off a digit,"
Clay County Assessor Shirley Quick said Wednesday. "And that digit meant $1
million." In fact, both tax bills were exactly $1 million short, thanks to
a computerized data entry error.

The article goes on to state that Ford is the only company that owes more than 1 million in business personal property taxes in the county. It doesn't say whether this is the first time their bill contained 7 digits.

John Cigas, Rockhurst College cigas@rckhrst1.bitnet

Name+birthdate=no drivers license

Bruce Hayden <bhayden@csn.org>
Fri, 8 Jan 1993 05:33:14 GMT

Today on a trouble shooting talk show in Denver, a caller called in to complain that his license had been revoked, and he had to leave his car since he couldn't drive.

Apparently, he had renewed his drivers license recently (required every three years in Colorado). At that time, a database check was made of the other 49 states. There was a match, based on birthdate and name. The other person with the same name and birthdate, had a suspended Penn. drivers license, based on a drunk driving conviction.

Based on that match, his license was summarily revoked, and notice was mailed to him to that effect. (Which he apparently had not yet received). The license showed revoked at a routine traffic stop some time later. It is not clear how automatic the revocation process is. In any case, no hearing is offered before the revocation.

The driver was especially upset because:
1) he had had a Colorado drivers license for 25 years.
2) he had never been to Pennsylvania, and
3) he didn't drink.

The burden is apparently upon him to prove the the Colorado DMV that they had the wrong man. At present he is still fighting the organization trying to get his license reinstated.

Bruce E. Hayden (303) 758-8400 bhayden@csn.org

Student Load Errors Blamed on Computer

Steve Peterson <peterson@fs.fs.com>
Tue, 12 Jan 93 10:57:50 CST

The following appeared in the Minneapolis Star Tribune, 1/12/92:

STUDENT LOAD ERRORS BLAMED ON COMPUTER (AP)

Because of a computer problem, thousands of college students have been sent notices ordering them to begin repaying loans that aren't due, a loan-processing company in St. Paul [Minnesota] says.

Shirley Chase, an attorney for EduServ Technologies, formerly known as Hemar Corp., said problems with a new computer system caused a backlog in processing student requests to defer payments. She said the company hopes to clear up the backlog by the end of February. More than 10,000 deferment forms are backlogged, she said.

Because of the backlog, some students who are entitled to postpone their loan payments have gotten notices urging them to pay and some have been contacted by a collection agency. Chase said EduServ has "bent over backward" to make sure no adverse credit reports are filed with credit bureaus because of the delay. EduServ processes loans issued by banks and other lenders and make sure payments are current.

Comment: Given that they probably had a choice of whether to send dunning notices to everyone or temporarily stop sending them, it shouldn't be surprising which choice they made.

Steve Peterson, FOURTH SHIFT Corporation, 7900 International Drive,
Bloomington, MN 55425 USA peterson@fs.com

[My daughter reported in from Massachusetts that she had seen a message displayed in front of JD Auto Sales off Rte 128 in Swampscott MA, with something like the following message:

TO ERR IS HUMAN.
TO BLAME IT ON A
COMPUTER IS EVEN MORESO.

An old RISKS theme, worthy of reminder. PGN]

"Softkiller" as Arts?

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Mon, 11 Jan 1993 13:41:30 +0100

FLATZ, leading performance artist from Munich (Bavaria) recently advertised "SOFTKILLER - the first buyable computer art virus". For MS-DOS systems, you may buy a diskette (in limited version: 20 diskettes each 1,800 DM equiv. about 1,100$; or unlimited version: 500 diskettes each 300 DM equiv. 185$) which after start will display some FLATZ head on the screen while formatting the disk. Advertised shortly before xmas as "the ultimate donation for PC owners", FLATZ explicitly warns that SOFTKILLER overwrites disks on data and will overwrite itself after execution.

After publication of this advertisement, Bavarian Criminal Agency became involved to analyse whether this might imply a crime of "computer sabotage" (German Penal Code, section 303b) according to which the destruction of programs and data which are essential for some person or institution will be prosecuted. In the analysis, FLATZ admitted that his software was not self-reproducing and therefore no virus. Moreover, his "attack on the computerworld" is mentioned in capital letters on the envelope. On the other side, distribution via BBS (though not foreseen by him) this warning is lost.

At this time, no test or reverse engineering of SOFTKILLER has been done. Probably, it is technically not worth the effort. But with some probability, other artists may come up with similar "ideas". Happy,Healthy and Riskless 1993

Klaus Brunnstein (University of Hamburg, North Germany, January 10, 1993)

Computer Theft of Criminal Records

Gary McClelland <mcclella@yertle.Colorado.EDU>
Fri, 8 Jan 1993 11:22:59 -0700

An AP story in the Boulder Daily Camera (1/8/93) reports a familiar story with a few new variations.

A private investigator and two police employees have been indicted by a Denver grand jury for improperly obtaining the criminal histories of 8,559 individuals. The Private Eye paid $3 to $5 per search and as much as $1,300 per week (he kept great records!). The scheme unraveled when a co-worker of the police employee who was doing the snooping became angry that her colleague was spending so much time looking up names that she was falling behind in her regular work. So after seeing a "criminal history format" on her screen that she was not supposed to be using, the co-worker turned her in. A computer log revealed that on the day she was caught, she had run checks on 95 people! It turns out that a transaction recording system allowed investigators to reconstruct all 8559 criminal history searches. With such a great logging system it seems strange that no one noticed 8559 extra searches; if the co-worker hadn't got the extra work dumped on her, these folks would still be stealing criminal records.

gary mcclelland, univ of colorado, mcclella@yertle.colorado.edu

Computer hacking of flight details "was illegal"

<Jonathan.Bowen@prg.ox.ac.uk>
Tue, 12 Jan 93 15:04:24 GMT

Today's UK newspapers are full of the story on the British Airways (BA) "dirty tricks" campaign against Virgin and their successful suing by Richard Branson. Of particular relevance to "risks" is the following extract from the Independent newspaper (p6, 12 January 1993):

... The [BA] team were told that in future, their key task would be
to access highly confidential information from their rival's
[Virgin's] computer system.
  "We were shown how to get the information by tapping into our computer

terminals in the Helpline office. We tapped in with our regular BA code
and called up the Virgin flight numbers".
  In common with many other airlines, Virgin rents out a segment of a
vast computer known as Babs - British Airways Booking System. Mr Khalifa
and his colleagues simply tapped into it. "We could see on the Babs
computer system when flight is open [sic], when it closed, if it was
delayed and how many passengers were due to board".
  For the next nine months the Helpline hackers provided BA with critical
information on Virgin's flights.

Jonathan Bowen, Oxford University

[A much longer version of this article was reported by Bob Dowling <rjd4@cus.cam.ac.uk>. PGN]

Upcoming Telephone Number problems

rob horn <horn%temerity@leia.polaroid.com>
Fri, 8 Jan 93 11:48:27 EST

I don't recall mention on Risks of the impending problems with modem networks. The North American telephone numbering plan is being changed. This is going to gradually lead to problems for all the people with long distance numbers that are pre-stored in documents, files, programs, and modems.

The change (as I understand it) is that the leading 1 digit should be used ONLY when dialing outside the area code, rather than the current system that imposes the need when dialing outside the local calling area. Then the area code restriction to the form x0x or x1x will be removed. I expect the change to be done carefully by the telco's so that mistakes will cause failure to connect rather than incorrect connection.

Just to make things interesting, this change is being staged area code by area code. So for people who plan to fix their internal stored numbers you need to know when your area is being changed.

Rob Horn   hornr@mr.polaroid.com

FAA prohibits pilot knowing GPS altitude in IFR flight

Jim Easton <jim@mpl.UCSD.EDU>
Fri, 8 Jan 93 12:34:43 PST

I was recently informed that the KLN-90 GPS(Global Positioning System) navigation unit used in airplanes was designed so that the pilot cannot display the altitude the unit calculates from satellite data. It does display the barometric altitude and will issue a warning if the barometric altitude differs significantly from the GPS altitude.

On asking Bendix/King why they would deny a pilot information already computed in the unit, the spokesperson explained that the calculated GPS altitude is often several hundred feet different from the "officially correct" barometric altitude, and that pilots might be so stupid as to try to fly by the GPS altitude - thus putting themselves at risk of a collision. Accordingly, the TSO(Technical Standards Order) by which the FAA defines approval of GPS navigation systems for IFR(Instrument Flight Rules) prohibited them from making GPS altitude information available to the pilot.

Last month I was flying in the clouds in mountains and experienced a failure of the primary pressure altimeter in the aircraft. Cross checking a second pressure altimeter with the GPS altitude on a non-TSO GPS navigator verified that it was the primary altimeter that was wrong. Not having this information could easily have resulted in my death. I would much prefer to educate pilots about GPS altitude errors than to deny them the possibility of having what could be lifesaving information.

Jim Easton, Box 889, Bonita, CA 91908 (619)548-0138

Risks of networks

Jerry Leichter <leichter@lrw.com>
Sat, 9 Jan 93 08:03:32 EDT

[I pulled the following from a recent TELECOM Digest, and it may very well have appeared elsewhere previously. But if ever there was an indication that the Internet is not the safe playground we like to think it is, it's this.
Not only do we have to face new risks; we have to face new forms of old ones.
-- Jerry]

Date: Thu, 7 Jan 1993 03:34:36 -0500
From: Monty Solomon <monty@proponent.com>
Subject: Sci.electronics Phone Fraud!

[Moderator's Note: Monty also passed this along for us today. PAT]

From: larryc@shell.portal.com (Larry WB Ching)
Newsgroups: sci.electronics
Subject: SCI.ELECTRONICS Phone fraud !!!
Summary: A recent attempt to rip-off sci.electronics correspondents.
Keywords: fraud, con artists, phone numbers
Message-ID: <C077BC.GBn@unix.portal.com>
Date: 1 Jan 93 23:16:23 GMT
Sender: news@unix.portal.com
Organization: Portal Communications -- 408/973-9111 (voice) 408/973-8091

At about 6PM Thursday evening, I got a phone call. The operator said that he had a collect call to me from Charles Pooley in New York. The name was familiar, but I didn't remember exactly why. I said I would accept the call, but then the "operator" said the call couldn't get through because I had the call collect option blocked. He then said he could pass the call through if I gave him my calling card number. I said that I'd rather call Mr. Pooley myself, and could the "operator" give me Mr. Pooley's number. There was a pause, then a phone number

with a San Jose area code! It didn't occur to me until later that , if
the call was from New York, why was the call-from number (408) !??!

I remembered that Charles and I had been corresponding on a topic from sci.electronics. I was lucky enough to have an old message from him lying around, and emailed him a message about my mysterious phone call.

Charles Pooley replyed to me today -- turns out the guy tried the same scam on him too! But this time, the bogus operator said the collect call was from me to Charles! Charles was also wary, and didn't give the crook his calling card number.

So - WATCH OUT! How this con artist chose my name and Charles' to try is beyond me. As far as public postings in sci.electronics, I don't think Charles and I had exchanged more than four public postings. Most of our correspondence has been via "private" email.

This has definitely raised my paranoia level. If, out of the millions of public postings during 1992, someone should choose two correspondents who have exchange only a slight amount of messages .... I mean, why us? Or, is there a "boilerroom" operation going on, with a bunch of phony operators, armed with USENET listings -- calling people with this con?

OH! - I may have put my phone number in one of my public sci.electronics postings - that's probably how the scamsters make their selection. Makes sense ...

CHILDREN BEWARE!!!

larryc@shell.portal.com

[Moderator's Note: I note the public access site you use for Usenet (Portal Com) is located in area 408 (San Jose, CA). PAT]

[Also sent to RISKS by Mike LeVine,
levine%fidler.decnet@chinalake.navy.mil]

version numbers

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>
7 Jan 93 14:35:00 EST

Alas, Microsoft isn't the only software company sliding corrections in without notice -- there are (at least) two versions of Digital Research's (really wonderful) DR-DOS 6.0 floating around out there as well. In this case, the problem isn't quite so critical: the early version will not run Windows 3.1, apparently because of some hooks Microsoft inserted (rampant speculation). Windows 3.0 will run, however. The new version, which has been fairly freely distributed, but which has the SAME version number, corrects the Windows incompatibility (which some might call an advantage). DR-DOS users should check to make sure that their COMMAND.COM is dated 4-07-92 (or later?).

For me, this has created no serious problems, but I can forsee
situations in which failure to adhere to a reasonable numbering system
could lead to all kinds of headaches -- "What version of our software
are you using?" "Version 6.37a." "Yes, but WHICH version 6.37a...?"

Andrew Marchant-Shapiro   Depts of Sociology and Political Science
USmail: Union College, Schenectady NY 12308   AT&T: (518) 370-6225
INTERNET: marchana@gar.union.edu   BITNET: marchana@union.bitnet

---

About Computer Expense...

"Paul Robinson, Contractor" <FZC@CU.NIH.GOV>
Mon, 11 Jan 1993 17:19:55 EST

The following item appeared on the Operations List on Bitnet, and I thought
I'd pass it on because it is unfortunately very true.

Date: Sun Jan 10, 1993 1:09 am EST
From: Mainframe Operations Discussion List
          EMS: INTERNET / MCI ID: 376-5414
          MBX: OPERS-L@vm1.cc.uakron.edu

TO: Multiple recipients of list OPERS-L
          EMS: INTERNET / MCI ID: 376-5414
          MBX: OPERS-L@akronvm.bitnet
Subject: Re: Some Good Old Standbys

> I came across these in a Usenet post and found them quite relevant

And one I saw in a humor column recently:

  If the automobile industry were like the computer industry
  over the past 30 years, a Rolls-Royce would now cost $5.00,
  would get 300 miles to the gallon, and once a year would
  explode killing all passengers inside!
                    - tom

  mvac23!thomas@udel.edu lapp@cdhub1.dnet.dupont.com (work)
  {ucbvax,mcvax,uunet}!udel!mvac23!thomas

Re: Large Foreign Exchange Rates (Kain, Risks-14.23)

Mark Brader <msb@sq.com>
Fri, 8 Jan 1993 01:28:00 -0500

> So in the face of unreasonable people (dictators, etc.), perhaps we
> need to use a floating point representation for the exchange rates
> - but I do think that one decimal digit for the exponent should be
> adequate.

He walks right into it!

According to the Guinness Book of World Records, in June 1946 the
Hungarian pengo [two acute accents on the o] reached a valuation of
1 / 1.3e20 of the gold pengo of 1931. Now I don't know what *that*
value was, but I think we can assume that the exchange rates with
at least some other currencies must have exceeded 1e19.

The German inflation of 1923 also went well past the 1e10 mark --
no pun intended -- if I recall correctly.

Mark Brader, Toronto utzoo!sq!msb, msb@sq.com

Re: Large Foreign Exchange Rates (R. Y. Kain, RISKS-14.23)

Peter Trei <ptrei@bistromath.mitre.org>
Thu, 7 Jan 93 15:08:41 EST

>So in the face of unreasonable people (dictators, etc.), perhaps we need to
>use a floating point representation for the exchange rates - but I do think
>that one decimal digit for the exponent should be adequate.
     ^^^
    I wouldn't be too certain. I don't have it hand, but I recall an
occasion when a South American currency (Paraguay?) depreciated to
billions (43 billion?) to one versus it's gold equivalent (it's in the
Guinness book of records).

It is easy to underestimate the size of data a program may be asked to deal with, especially several years down the line. (See the Bank of New York problems, recorded here several years ago, when a program suddenly had more than 2^16 transactions/day). The cautious programmer will be generous to a fault. The best case I've seen was in a banking program where dollar amounts were stored as 96 bit integer quantities of pennies - this rolls over at nearly $8E26, or about 792 trillion trillion dollars.

Peter Trei

Re: Large Foreign Exchange Rates (Kain, RISKS-14.23)

<Dik.Winter@cwi.nl>
Fri, 8 Jan 1993 01:04:30 GMT

The lack of need for seven digit accuracy is correct, the single digit exponent is not. I have a German banknote of 1,000,000,000 Mark, barely enough to buy a bread by one month after issue. I have also seen German stamps of 1,000,000,000,000,000,000 Mark (Eine Trillionen Mark, German trillions of course). That was in the early twenties of course. And I add that at that time Germany was a democratic country, no unreasonable people were involved.

dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland
home: bovenover 215, 1025 jn amsterdam, nederland; e-mail: dik@cwi.nl

Correction on Computers, Freedom and Privacy 1993 (RISKS-14.21)

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 7 Jan 93 14:34:46 PST

Bruce Koball reports that the net address for cfp93 information and registration reported in RISKS-14.21 should have been cfp92@well.sf.ca.us. However, Bruce's address was correct, so this should not have caused anyone too much trouble.

CSESAW93 call for papers

Catherine A. Meadows <meadows@itd.nrl.navy.mil>
Fri, 8 Jan 93 10:49:36 EST

CALL FOR PAPERS

1993 Complex Systems Engineering Synthesis and Assessment
Technology Workshop (CSESAW '93)

July 20-22, 1993
Washington, DC

This is a call for papers to be presented at the 1993 Complex Systems Engineering Synthesis and Assessment Technology Workshop (CSESAW '93) which will be held July 20-22, 1993. The theme of this year's workshop is integration. This workshop will explore issues related to the design synthesis and assessment of complex, computer-based, mission-critical systems. Many DoD related systems tend to be large, complex, fault tolerant, distributed, real-time, time-critical systems.
Of interest is the development and enhancement of the system level ability to specify, capture, synthesize, analyze, model, prototype, test and implement such systems. The emphasis is on developing forward engineering capabilities; however, reverse engineering capabilities will also be addressed.

TOPICS OF INTEREST

INTEGRATION OF CAPTURE, OPTIMIZATION, AND ASSESSMENT TECHNOLOGIES
INTEGRATION OF DEPENDABLE SYSTEM DESIGN INTO SYSTEM ENGINEERING
INTEGRATION OF SECURE SYSTEMS DESIGN INTO SYSTEM ENGINEERING
APPLICATION OF SIMULATION, MODELING, MEASUREMENT, METRICS,
AND PROTOTYPING WITHIN SYSTEM ENGINEERING
REQUIREMENTS ELICITATION, SPECIFICATION AND TRACEABILITY

Authors are requested to submit (5) copies of the paper of no more than 7,000 words (5 pages or less). Include a cover letter listing the author(s), paper title, area of interest, and the name, address, FAX, telephone number, and e-mail address (if available) of the author who is responsible for all correspondence and preparation for the workshop by 15 April 1993. The accepted papers will be published as a Proceedings, which will be distributed within the Government and also made available to the general public.

Submission Deadline:	15 April 1993
Acceptance Notification:	15 May 1993
Final Paper Submission:	1 June 1993

Submission Address:

Steve Howell
Naval Surface Warfare Center
Code B40
10901 New Hampshire Avenue
Silver Spring, MD 20903-5000

e-mail inquiries: showell@nswc-wo.navy.mil
phone inquiries: 301-394-3987
fax inquiries: 301-394-1175

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 27

Weds 13 January 1993

Contents

Under 50 miles hurts with Hertz [Hertz hat kein Herz?]

"Bruce Baker" <bruce_baker@qm.sri.com>
3 Nov 1992 10:48:24 -0800

Hertz Rent-A-Car has recently implemented an advanced fuel purchase option. The option permits drivers to pay for gas at the average self service price in the area of the car rental. The option only benefits those drivers who use more than a full tank of gas. Otherwise, you must show your gas receipts upon returning the car, if you claim that you are returning the car with a full tank.

An interesting quirk of this system is the programming of the portable check-in palm-top computers used by the attendants who wander along the lanes where you return your car. If you have driven less than 50 miles, the system is programmed to automatically charge you $5.00 for gas, even if you have a receipt showing that you have filled it up. Hmmm... let's see... if the average distance driven by those who have driven less than 50 miles is about 35 miles, that equates to about one gallon of gas for the $5.00 charge (vs. about $1.15 at the tank). Are Ross Perot's gas prices already here? To override the check-out slips provided by the attendants from their palm-tops, you have to take your receipt into the main check-in area. If you're in a hurry, chances are you won't. Then Hertz has the full tank of gas *and* your $5.00. Luckily, my attendant informed me of this quirk. Chalk up another one for American ingenuity!

Bruce N. Baker, SRI International

[My apologies to Bruce. He sent me this long ago and it slipped through the crack. It should have preceded the first item in RISKS-14.26. PGN]

Re: Computer games may endanger your health (RISKS-14.26)

Rick Russell <wrr3118@tamsun.tamu.edu>
Tue, 12 Jan 93 20:02:02 CST

When I read this passage, I knew I'd heard a story somewhere like this before. It turns out the story is in the Nintendo Entertainment System manual!

The Super Nintendo Entertainment System "Consumer Information and Precautions Booklet", which comes with SNES and NES systems sold in the US (and the UK, to the best of my knowledge), issues the following warning:

> EPILEPSY WARNING: READ BEFORE USING YOUR NES OR SUPER NES
>
> A very small portion of the population may experience epileptic seizures when viewing certain kinds of flashing lights or patterns that are commonly present in outr daily environment. These persons may experience seizures while watching some kinds of television pictures or playing certain video games. Players who have not had any previous seizures may nonetheless have an undetected epileptic condition. Consult your physician before playing video games if you have an epileptic condition. Consult your physician if you experience any of the following symptoms while playing video games: altered vision, muscle twitching, other involuntary movements, loss of awareness of your surroundings, mental confusion, and/or convulsions.

Looks like this British case is another classic version of RTFM!

Rick Russell | TAMU Meteorology | wrr3118@tamsun.tamu.edu

Re: Computer games may endanger your health (OMJ C-L, RISKS-14.26)

J. Eric Townsend <jet@nas.nasa.gov>
12 Jan 93 14:07:54

Owners of Commodore 64's might remember a program in the C64 Programming manual (I think) which changed the color palette for the text, screen and border as fast as the 64 was capable. There was a warning message to the effect of "don't run this if you or someone in your family has a history of epileptic problems".

J. Eric Townsend -- jet@nas.nasa.gov -- 415.604.4311 (DoD# 0378)

Medical Records on smart cards

John Gray <phyjwdg@vaxb.hw.ac.uk>
Mon, 11 Jan 93 14:09 BST

Over the holidays, in the "Aberdeen Press and Journal" and its evening equivalent, the "Evening Express", was a description of a trial scheme for holding patients medical records on cards:

> ... The 750,000 pound patient data-card system is one of the first of its type in Europe, according to one of its pioneering developers, Dr James Beattie. Around 8000 hi-tech cards, the size of a credit card, will be distributed to patients registered with the Inverurie Health Centre. NHS Chief Executive in Scotland, Don Cruickshank, said if it proves successful, the system could become the basis for an all-Scotland one. He said: 'This project has the potential to greatly improve the communication of individual medical histories and to which the individual patients will themselves have access'. Special machines which can read the coded cards will be installed at various points in the North-east.

[The article then states that the machines will be installed in the health centre, another doctor's surgery, three outpatients clinics in Aberdeen (for diabetes, asthma and hypertension) and "chemists shops in Inverurie and Kintore"]

> ... When a patient has treatment from a clinic, their card will note what has happened and course of action taken which will be available to their own doctor much more quickly than at present ", he [Dr Beattie] said. Dr Beattie hopes cards will be distributed in about a years time. The pilot project will run until 1996, when it will be evaluated by health chiefs.

[What intrigued me first was the level of security: the Evening Express of the same day was more explicit on some technical details:]

> Plastic cards which can hold more than 1,000 pages of information on NHS patients... To maintain confidentiality, the cards can be read only by

special machines. A portable version will be used by GPs on home visits. Mr Cruickshank said patients will also have access to their own medical records, using number similar to those used for bank cash cards.

[It also mentions that half the population will remain as a control group for the study.]

Brief note for those not in the UK: The NHS (National Health Service) is an arm of the government which is responsible for the vast majority of medical services in the UK. Thus, perhaps 90+% of the population would be involved if the scheme were implemented nationwide. I'm not going to dwell on why I think this is of interest to Risks, but I'll mention two points:

1) If an entire medical record is stored on card, it will contain a great deal of very confidential information (about as much so as it gets) and a lot of very important information: how secure is a chemist's shop for such a system? Also, such a system on its own would be very vulnerable to card failure.

2) Because the cards are read electronically, there is a risk/benefit in terms of doing computerised card searches remotely (although the article doesn't say the machines will be networked, I can imagine that happening eventually.

> [I didn't know there were any 750,000 pound patients!
> Wow. That is really heavy. Somewhat like the
> seven foot patrolmen I read about last week. PGN]

DoJ Has NOT "Authorized" Keystroke Monitoring

Dennis D. Steinauer <dds@csmes.ncsl.nist.gov>
Mon, 14 Dec 92 17:08:12 EST

Date: Fri, 11 Dec 92 16:14:11 EST
>From: dds (Dennis D. Steinauer)
To: privacy@cv.vortex.com
Subject: DoJ Has NOT "Authorized" Keystroke Monitoring

The Subject line on the recent [PRIVACY] reposting by David Banisar of the 7 Dec 92 advisory from CERT/CC is highly misleading and inappropriate. As with some newspapers, it is important that people read more than just the headlines.

The Department of Justice hasn't "authorized" anything. Rather, they are advising system administrators that certain activities, namely the monitoring or recording of user-to-computer session transmissions (hence "keystroke monitoring") MAY be found illegal in certain circumstances and that notice should be given to users.

The CERT advisory was extracted from a letter to the National Institute of Standards and Technology (NIST) from DoJ. Justice asked NIST in its role of providing computer security guidance to Government to circulate the letter and provide appropriate guidance. We have made the letter available, without comment, through several government and other channels (including CERT, I4, etc.).

The letter is intended to advise system administrators of an ambiguity in U.S. law that makes it unclear whether session monitoring, often conducted by system administrators who suspect unauthorized activity, is basically the same as an unauthorized telephone wiretap. I repeat, the law is *unclear* -- and the fact that one can argue either way on the issue does not clarify the law as currently written. DoJ advises, therefore, that if system administrators are conducting session monitoring or anticipate the need for such monitoring, they should ensure that all system users be notified that such monitoring may be undertaken.

The DoJ advice, therefore, is not "authorizing" anything -- even implicitly. They have simply observed the types of activities that diligent system managers often undertake (a la Cliff Stoll in "The Cuckoo's Egg") in an attempt to protect their systems from unauthorized users, and they have rendered some prudent legal advice.

Clearly, there are lots of issues here -- technical and otherwise -- that will need to be discussed and sorted out. Indeed, changes in agency/organizational policies and even the law are probably needed. However, none of this changes the fact that system administrators need now to be aware of the potential impact of their activities, and the DoJ advice attempts to do this.

We (NIST) are developing additional guidance for system administrators to assist them in implementing the DoJ recommendations. I expect that others will be doing likewise. We also hope to encourage discussion of the related technical and other issues. In the meantime, system administrators are well advised to read the basic DoJ advice and examine their systems and agency policies to determine if, where, and how notices should be provided to users.

We welcome comments and suggestions, particularly regarding approaches that various organizations take in dealing with this issue.

Dennis D. Steinauer, National Institute of Standards and Technology
A-216 Technology, Gaithersburg, MD 20899 USA 1-301-975-3359 FAX 1-301-948-0279
DSteinauer@nist.gov (e-mail) NIST Security BBS: 301-948-5717 (cs-bbs.nist.gov)

More on the Orange Book

<kmeyer@aero.org>
Mon, 14 Dec 92 09:38:46 PST

In response to an article I wrote, W. Murray (WHMurray@DOCKMASTER.NCSC.MIL) cautions against applying the orange book in situations for which it was never intended. While the orange book is not an appropriate criteria for many environments, it is currently the ONLY criteria regularly used in the United States to assess the security features of operating systems--and as such, there is a lot that can be learned from it, even in non-military environments.

It is an unfortunate fact that many vendors of commercial operating systems either do not know or do not care about security--the result being that most of us do not have much in the way of security in the computer systems we use every day. If we insist on keeping the bugs of DOS and UNIX for backward compatibility into eternity, we will never have secure systems.

Kraig R. Meyer, Trusted Computer Systems Dept,
The Aerospace Corp, El Segundo, CA kmeyer@aero.org

Slipstreamed Software Changes, the Titanic, and my Pontiacs

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Wed, 13 Jan 93 09:24:59 -0500

Re: Version numbers (Marchant-Shapiro, RISKS-14.26)

> ... "Version 6.37a." "Yes, but WHICH version 6.37a...?"

Actually this is nothing new. My other hobby is automobiles and we regularly get into arguments as to whether certain options were available, both sides citing references as "proof".

A recent case concerned the Pontiac GTO "Judge" in 1970 - for years there had been a rumour of a 455 option that year but all available sales literature showed only a 400 engine. Recently a brochure turned up dated November that looked exactly (same cover artwork and everything as the September issue which is very common). but which did mention a 455 engine option. Turns out that 17 cars were built.

Shortly after the Titanic incident, the White Star Line refitted the Olympic with an extensive increase in the double hull coverage also fitted to the third ship in the series (the ill-fated Britannic which incidentally sunk much faster than its sibling), along with a number of other "safety" features.

The ones I liked the best were the giant cranes used with rotary lifeboat launchers. Originally billed as being able to launch all boats from either side of the ship, there was one minor difficulty - some of the smokestacks would have had to be jettisoned first. Minor problem.

This was also apparently "slipstreamed", at least I never saw a mention of "Triple Screw Steamship Revision A" - but then what can you expect from a company that would add a fourth stack for pure sales appeal (well maybe the cigars in the lounge did need that much ventilation...).

The fact is that manufacturers have been quietly fixing products at least since the introduction of mass production and it is always a stressful time for the engineers when the easy changes of development are replaced by the rigorous requirements of configuration control. Sometimes even management is not told about such "fixes", occasionally with disastrous results (it is very easy to remove the motor mounts in one of my cars so that the engine can be raised allowing the spark plugs to be changed. Seems that the power steering was in the way of an air conditioner duct so it was moved just a wee bit 8*).

Public Service for Cornell Hackers

<dclawson@clipr.colorado.edu>
Wed, 13 Jan 93 09:56:50 -0700

"Public Service for Hackers"   by John Marcham
_Cornell_Alumni_News_ magazine

Two former [Cornell] students will develop a computer program to make it easier for a quadriplegic man in Tennessee to use a computer he owns, as part of their punishment for launching a computer virus that damaged programs and caused hard drive crashes last February.

David Blumenthal '96 and Mark A. Pilgrim '94 were sentenced by a Tompkins County Court judge to pay restitution to users whose computers were jammed by the men's virus, at and near Stanford University and in Japan, and to perform ten hours of community service per week for a year.

A computer buff who knew the quadriplegic and heard of the Cornell virus case wrote the judge in Ithaca, and asked if the students' public service could be worked off developing a less expensive and cumbersome program for the disabled man, who uses a mouthstick and outdated software to operate his McIntosh computer.

The judge and the former students agreed to the proposal: the students start work in November. A third former student, found guilty of a lesser infraction, was asked by not required to do public service, and declined.

Killing me with kindness -- have a (M)Herz?

Bear Giles <bear@eagle.fsl.noaa.gov>
Wed, 13 Jan 93 21:13:49 GMT

After nearly two _months_ at the integrator to repair a bad motherboard, I finally got my computer back last night (tip 'o the hat to UPS for leaving it outside of my apartment in near-zero (Fahrenheit) weather)... and it still has frequent parity errors. In fact, the problem is worse now than two months ago!

A curious fact has come up: I ordered a 20 MHz system, and have an invoice stating they shipped a 20 MHz system, but apparently they actually shipped 25 MHz systems. The manager I talked to claimed he was doing me a "favor" by shipping a better system -- and doesn't seem to understand my statement that I would have refused a 25 MHz system out of concern for unreliability.

(When I purchased my system a year ago 16 MHz 386-SXs were standard and 20 MHz systems were just starting to get carried. A 25 MHz would have been first-generation and hence rather unreliable, as my extensive down-time demonstrates).

Bear Giles bear@fsl.noaa.gov

revoke license where i.birthdate=dwi.birthdate and name like "%...%"

Jim Roberts <roberts@stsci.edu>
Wed, 13 Jan 93 09:51:50 EST

The RISK of having your licence revoked is greater than merely that of having the same name and birthdate as another person, as discussed in RISKS 14.26 by Bruce Hayden - you need only a *similar* name and birthdate in common.

Yesterday I received in the mail from the state of Maryland, in which I live, a notice that my driver's licence is revoked based on a DWI arrest by a person with a similar name in 1985. On all official documents, including driver's licenses, I use my full name William James Roberts. The miscreant with the same birthdate and named James Roberts resided in Florida, a state I have never visited, and was arrested in Tennessee. To have my license reinstated, I must *prove* to the hearing *board* that I am not the DWI James Roberts, something I suspect it will not be easy to do.

If one has a real DWI he gets a day in *court*, but if one has merely a computer generated DWI he has no such right.

The notice indicated that James Roberts had no sex (sigh), weighed 0 pounds, was 0 ft 0 in in height, and had blank eyes. So the folks who programmed the database join use the fact that the information you are required to have on your driver's license is not useful when they want to roll up the numbers on license revocations. I suspect that if I were Barbara James Roberts (sex:F), I would have gotten the same notice. In that case it might be easier to fight. But what if I were a woman with an ambiguous middle name, say Barbara Kelly Roberts and the revokee were just Kelly Roberts, really a male but to Maryland an M or F? Then I would again be in difficulties.

The next step in the widening scope of the database joins may be just to use your birthdate and the Soundex code of your last name. That should considerably improve the numbers achieved by the "responsible" bureaucrats in their hunt for more revocations.

Jim Roberts roberts@stsci.edu 6559::roberts

name+birthdate=no driver's license

Andrew Koenig <ark@europa.att.com>
Wed, 13 Jan 93 10:45:55 EST

A common mistake (and sometimes, I suspect, a deliberate decision) in system design is to assume that things that are purportedly the same in theory are actually the same in practice. Thus, for example, politicians who want to prohibit people from using illegal drugs think it is equivalent to punish people who fail drug tests, forgetting that there are sometimes false positives, fraudulently altered results, and so on.

So it is with the driving story. Someone else turns up who appears enough like you, at least superficially, and suddenly it's up to you to prove innocence.

Here's another example. This was told to me second hand, so I won't swear it's true, but it's plausible enough and the lesson is there anyway.

New Jersey, like many (all?) other states, has a mechanism for revoking driver's licenses for various reasons. Moreover, they have laws mandating stiff penalties for people caught driving with a revoked license. But how does one tell if a license has been revoked? New Jersey's answer is to have a list of revoked licenses; their law specifically prohibits driving while one's name is on the revoked list.

I know a guy who says his name was placed on the revoked list due to a clerical error. He had not done anything wrong, and had never been informed that his name was on the list. He found out about it when he was stopped for speeding; of course he was immediately charged with driving while on the revoked list.

At the hearing, the state readily admitted that his name had been placed there in error. However, they argued that that was irrelevant: the law prohibits driving while one's name is on the list and that's just what he had done. The judge had no option but to find him guilty.

Re: Upcoming Telephone Number problems (Rob Horn, RISKS-14.26)

Andrew Klossner <andrew@frip.wv.tek.com>
Tue, 12 Jan 93 14:45:31 PST

> "The change (as I understand it) is that the leading 1 digit
> should be used ONLY when dialing outside the area code, ...

No, the change is that a leading 1 will always be followed by an area code. The old practice of dialing 1-nnn-nnnn to make a long distance call within one's area code is being abolished. This will separate the area code and exchange number spaces, which at present are distinguished by the second digit (0 or 1 for area code, other for exchange). This is vital because North America has run out of area codes.

In Oregon, we will convert to this scheme in July, and we will still use a leading 1 when making toll calls within the area code, but we will have to punch the area code as well. This preserves the characteristic that "a leading 1 means you're paying money," considered desirable.

Andrew Klossner andrew@frip.wv.tek.com uunet!tektronix!frip.WV.TEK!andrew

Upcoming Telephone Number problems

<kmeyer@aero.org>
Wed, 13 Jan 93 14:21:05 PST

You will probably both get dozens of messages about this...anyway:

In Risks 14.26, Rob Horn stated that the North American dialing scheme is changing; but in fact, it started changing (at least) 5 or 6 years ago and the dialing scheme is no longer consistent around the country.

In the old days, area codes were 3 digits of the pattern x0x or x1x; prefixes (the first 3 digits of a "local" number) could not be either of these patterns. Toll calls within your area code were dialed as 1 + number; toll calls outside of your area code were dialed as 1 + area code + number.

When area codes started running out of prefixes, the dialing instructions started changing. I know of three different dialing schemes currently being used in the U.S.:

(1) The original scheme, described in the paragraph above,
(2) The scheme used in Southern California, in which you do not dial
   "1" to call a number in your area code (even if it is a toll call)
(3) The scheme used in the Detroit area, in which you dial 1 + 313
   to place a toll call within your area code.

When they start using area codes that don't conform to the x0x or x1x format, any regions still using dialing scheme (1) will have to switch to either scheme (2) or scheme (3).

Kraig R. Meyer

Re: Upcoming Telephone Number problems (Horn, RISKS-14.26)

Randal L. Schwartz <merlyn@reed.edu>
Wed, 13 Jan 93 14:31 PST

What's worse is that some areas (like California) have chosen to go strictly with "+1 means area code", while other areas (such as Oregon and Washington) have retained the "+1 means long distance" meaning as well. This gets confusing for computer autodialers, as well as humans.

This means that in-area-code-but-long-distance numbers are dialed differently in the two plans:

Local, in-area-code: both=xxx-xxxx
Local, out-area-code: Oregon=n/a, California=1 yyy xxx-xxxx
Long distance, in-area-code: Oregon=1 yyy xxx-xxxx, California: xxx-xxxx
Long distance, out-area-code: both=1 yyy xxx-xxxx

(Oregon doesn't have any local calls that are in a differing area code.)

Blech. Your PUC at work. :-)

[Further comments from D King, king@ukulele.reasoning.com.]

Upcoming Telephone Number problems

"Spencer W. Thomas" <Spencer.W.Thomas@med.umich.edu>
Wed, 13 Jan 93 09:49:35 EST

What's happened in 313 is exactly the opposite -- we now have to dial 1-313-xxx-yyyy for calls WITHIN the area code, instead of just dialing 1-xxx-yyyy. This allows them to use the x[01]x prefixes as new exchanges (postpones the need to split the area code by a few years). I hadn't thought of it before, but of course, when this is done everywhere, then it will be possible to use (almost) any 3 digit area code, too.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 28

Tuesday 19 January 1993

Contents

Racetrack goes to the dogs as computer fails (from Mark Colan)

John Markoff, NY Times, San Fran 1-415 362 3912 <markoff@nyt.com>
Thu, 14 Jan 1993 10:32:04 -0800

> Date: Thu, 14 Jan 93 10:21:45 EST
> From: Mark_Colan.LOTUS@CRD.lotus.com
> Subject: heard on BBC this morning

> At the tail end of the sports news at the end of NewsHour, the morning BBC
> show heard on WBUR, was the mention of an error in a betting computer at a
> greyhound race track. The computer continued to accept bets well after the
> conclusion of the race. Needless to say, many gleeful track-betters bought

> tickets for the dog that had already won, and claimed their winnings.
>
> The article also mentioned that some people are just born losers.
> After the race had finished, 139 people bet on dogs that had *lost*!
>
> The government management reported that they intended to reclaim all of the
> unfairly-won monies. However, they stated that they intend to *keep* the
> money from the losers.

[Slight edit by PGN.]

Earthwinds balloon crash

<sullivan@geom.umn.edu>
Tue, 19 Jan 93 12:26:02 CST

There is a long article in the NYTimes Science section on Jan 19, 1993, about the crash last week of the Earthwinds balloon just after it took off to try to fly around the world. The three men of the crew have been trading accusations since the crash, and many people blame the problems on the lack of "adequate engineering and planning, particularly in the integration of its labyrinthine electronic and plumbing systems".

-John Sullivan@geom.umn.edu

More on the Air-Inter politics

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
19 Jan 93 13:38:39 GMT (Tue)

>From the International Herald Tribune, 19 Jan 1993

Paris Charges Ex-Official in Air Crash

COLMAR, France (AP) - A former official of the French domestic airline Air-Inter was charged Monday with negligent homicide in the crash of a passenger jet a year ago that killed 87 people. Jacques Rantet, Air-Inter's former director of flight security, was charged ... with negligence leading to death and injury in the crash of the Airbus A320. Nine people survived after the airliner crashed into a mountainside as it approached Strasbourg airport on Jan. 20, 1992.

Attempted Mindvox Break-in

John F. McMullen <mcmullen@mindvox.phantom.com>
Mon, 18 Jan 93 13:55:17 EST

The following appeared on Newbytes, a copyrighted commercial service, on January 18, 1993. It is republished here with the express consent of the authors:

Phantom Access Foils Cracking Attempt 01/18/93 NEW YORK, NEW YORK, U.S.A.,1993 JAN 18 (NB) -- An attempt to illegally break into, or "crack" the "Mindvox" conferencing stem contained in Phantom Access, a flat-rate New York-based online service recently featured in various news publications, was detected and rebuffed.

Bruce Fancher, co-owner of Phantom Access, told Newsbytes, "There was no real damage and we have notified all of our users about the attempt in the hope that they will be even more conscious of security. The nature of this attempt points out one of the things that users of any on-line system must be aware of in order to protect her/his privacy."

The attempt came to the attention of the owners of the system, Fancher and Patrick Kroupa, when subscribers reported receiving the following message:

> It has been brought to my attention that your account has been 'hacked' by an outside source. The charges added were quite significant which is how the error was caught. Please temporarily change your password to 'DPH7' so that we can judge the severity of the intrusion. I will notify you when the problems has been taken care of. Thank you for your help in this matter. -System Administrator"

The system owners immediately sent a message to all subscribers declaring the message to be fraudulent. In addition to pointing out the textual errors in the message -- for example, Mindvox is a "flat rate" system and charges are not accumulated -- the owners admonished users to both safeguard their passwords and insure that they are not easy to decipher.

Fancher told Newsbytes that the review of Mindvox in a recent issue of Mondo 2000, its mention in an issue of Forbes, and his speaking engagements on behalf of the system have led to more rapid growth than had been anticipated. He said, "We are moving to larger space on February 1st and will be upgrading our equipment from a single Next system to multiple Suns. We will also increase the number of dial-in ports and greatly increase the speed of our Internet connection. We are very grateful for the user response to date."

(Barbara E. McMullen & John F. McMullen/Press Contact: Bruce Fancher, Phantom Access, dead@phantom.com (e-mail), 212-254-3226 70210.172@compuserve.com mcmullen@mindvox.phantom.com knxd@maristb.bitnet mcmullen@well.sf.ca.us [...]

New E-journal on computer security

<jbcondat@attmail.com>
31 Dec 69 23:59:59 GMT

A new computer security e-journal is being published in France.
It's the first in my country:

* weekly;
* name: _Chaos Digest_;

 * latest issue available: #1.03 (18 Jan 1993);
 * for a subscription send an e-message to: jbcondat@attmail.com

Thanks, and hope to hear from you soon!
                                         Fax: +33 1 47877070
Jean-Bernard Condat, Chaos Computer Club France [CCCF], B.P. 8005,
69351 Lyon Cedex 08, France jbcondat@attmail.com   +33 1 40101775

Lautro assessment of computer reliability

Pete Mellor <pm@cs.city.ac.uk>
Mon, 18 Jan 93 17:55:52 GMT

A student on a short course on software reliability that I gave late last year informed me that Lautro, the UK insurance companies' watch-dog organisation, has recently been putting the wind up a lot of companies by doing spot checks on computer systems.

Lautro has real "teeth", and can stop a company from trading if they are not satisfied with the service it provides to the public. Nowadays, this includes deficiencies in service due to computer cock-ups.

Apparently, a number of insurance companies are beginning to take software reliability rather seriously all of a sudden!

Unfortunately, we only had time for a short conversation, and I do not have any further information. I would be extremely interested to know, for example, what Lautro measure when they perform their audit.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Released GSA Docs Slam FBI Wiretap Proposal

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 15 Jan 1993 23:22:47 -0500

"GSA Memos Reveal that FBI Wiretap Plan was
Opposed by Government's Top Telecomm Purchaser"

The New York Times reported today on a document obtained by CPSR through the Freedom of Information Act. ("FBI's Proposal on Wiretaps Draws Criticism from G.S.A.," New York Times, January 15, 1993, p. A12)

The document, an internal memo prepared by the General Services Administration, describes many problems with the FBI's wiretap plan and also shows that the GSA strongly opposed the sweeping proposal. The GSA is the largest purchaser of telecommunications equipment in the federal government.

The FBI wiretap proposal, first announced in March of 1992, would have required telephone manufacturers to design all communications equipment to facilitate wire surveillance. The proposal was defeated last year. The FBI has said that it plans to reintroduce a similar proposal this year.

The documents were released to Computer Professionals for Social Responsibility, a public interest organization, after CPSR submitted Freedom of Information Act requests about the FBI's wiretap plan to several federal agencies last year.

The documents obtained by CPSR reveal that the GSA, which is responsible for equipment procurement for the Federal government, strongly opposed two different versions of the wiretap plan developed by the FBI. According to the GSA, the FBI proposal would complicate interoperability, increase cost, and diminish privacy and network security. The GSA also stated that the proposal could "adversely _affect national security._"

In the second memo, the GSA concluded that it would be a mistake to give the Attorney General sole authority to waive provisions of the bill.

The GSA's objections to the proposal were overruled by the Office of Management and Budget, a branch of the White House which oversees administrative agencies for the President. However, none of GSA's objections were disclosed to the public or made available to policy makers in Washington.

Secrecy surrounds this proposal. Critical sections of a report on the FBI wiretap plan prepared by the General Accounting Office were earlier withhold after the FBI designated these sections "National Security Information." These sections included analysis by GAO on alternatives to the FBI's wiretap plan. CPSR is also pursuing a FOIA lawsuit to obtain the FBI's internal documents concerning the wiretap proposal.

The GSA memos, the GAO report and others that CPSR is now seeking indicate that there are many important documents within the government which have still not been disclosed to the public.

Marc Rotenberg, CPSR Washington office   rotenberg@washofc.cpsr.org

Note: Underscores indicate underlining in the original text.
Dashes that go across pages indicate page breaks.

[Computer Professionals for Social Responsibility is a nonprofit, public interest membership organization. For membership information about CPSR, contact cpsr@csli.stanford.edu or call 415/322-3778. For information on CPSR's FOIA work, contact David Sobel at 202/544-9240 (sobel@washofc.cpsr.org).]

- -

(#4A)

Control No. X92050405
Due Date: 5/5/92

Brenda Robinson (S)

After KMR consultations, we still _"cannot support"_ Draft Bill. No. 118 as substantially revised by Justice after its purported full consideration of other agencies' "substantive concerns."

Aside from the third paragraph of our 3/13/92 attachment response for the original draft bill, which was adopted as GSA's position (copy attached), Justice has failed to fully address other major GSA concerns (i.e., technological changes and associated costs).

Further, by merely eliminating the FCC and any discussion of cost issues in the revision, we can not agree as contended by Justice that it now " ... takes care of kinds of problems raised by FCC and others ...."

Finally, the revision gives Justice sole unilateral exclusive authority to enforce and except or waive the provisions of any resultant law in Federal District Courts. Our other concerns are also shown in the current attachment for the revised draft bill.

Once again OMB has not allowed sufficient time for a more through review, a comprehensive internal staffing, or a formal response.

/Signature/

Wm. R. Loy KMR 5/5/92

Info: K(Peay),KD,KA,KB,KE,KG,KV,KM,KMP,KMR,R/F,LP-Rm.4002

(O/F) - 9C1h (2) (a) - File (#4A)

- -

ATTACHMENT
REVISED JUSTICE DRAFT BILL
DIGITAL TELEPHONY

The proposed legislation could have a widespread impact on the government's ability to acquire _new_ telecommunications equipment and provide electronic communications services.

Existing Federal government telecommunications resources will be affected by the proposed new technology techniques and equipment. An incompatibility and interoperability of existing Federal government telecommunications system, and resources would result due to the new technological changes proposed.

The Federal Communications Commission (FCC) has been removed from the legislation, but the Justice implementation may require modifications to the "Communications Act of 1934," and other FCC policies and regulations to remove inconsistencies. This could also cause an unknown effect on the wire and electronic communications systems operations, services, equipment, and regulations within the Federal government. Further, to change a major portion of the United States telecommunications infrastructure (the public switched network within eighteen months and others within three years) seems very optimistic, no matter how trivial or minimal the proposed modifications are to implement.

In the proposed legislation the Attorney General has sole _unilateral exclusive_ authority to enforce, grant exceptions or waive the provisions of any resultant law and enforce it in Federal District Courts. The Attorney General would, as appropriate, only "consult" with the FCC, Department of Commerce, or Small Business Administration. The Attorney General has exclusive authority in Section 2 of the legislation; it appears the Attorney General has taken over several FCC functions and placed the FCC in a mere consulting capacity.

The proposed legislation would apply to all forms of wire and electronic communications to include computer data bases, facsimile, imagery etc., as well as voice transmissions.

The proposed legislation would assist eavesdropping by law enforcement, but it would also apply to users who acquire the technology capability and make it easier for criminals, terrorists, foreign intelligence (spies) and computer hackers to electronically penetrate the public network and pry into areas previously not open to snooping. This situation of easier access due to new technology changes could therefore affect _national security_.

(1)

- -

The proposed legislation does not address standards and specifications for telecommunications equipment nor security considerations. These issues must be addressed as they effect both the government and private industry. There are also civil liberty implications and the public's constitutional rights to privacy which are not mentioned.

It must be noted that equipment already exists that can be used to wiretap the digital communications lines and support court-authorized wiretaps, criminal investigations and probes of voice communications. The total number of interception applications authorized within the United States (Federal and State) has been averaging under nine hundred per year. There is concern that the proposed changes are not cost effective and worth the effort to revamp all the existing and new telecommunications systems.

The proposed bill would have to have the FCC or another agency approve or reject new telephone equipment mainly on the basis of whether the FBI has the capability to wiretap it. The federal-approval process is normally lengthy and the United States may not be able to keep pace with foreign industries to develop new technology and install secure communications. As a matter of interest, the proposed restrictive new technology could impede the United States' ability to compete in digital telephony and participate in the international trade arena.

Finally, there will be unknown associated costs to implement the proposed new technological procedures and equipment. These costs would be borne by the Federal government, consumers, and all other communications ratepayers to finance the effort. Both the Federal government and private industry communications regular phone service, data transmissions, satellite and microwave transmissions, and encrypted communications could be effected at increased costs.

(2)

[Documents disclosed to Computer Professionals for Social Responsibility (CPSR), under the Freedom of Information Act December 1992.]

Four charged with theft of registration microfilms in Sapporo Japan

<hank@westford.ccur.com>
Mon, 18 Jan 93 01:39:10 EST

>From The Japan Times Wednesday January 13,1993

SAPPORO (Kyodo)

Four men went on trial here Tuesday for allegedly taking out residency register microfilm from a Sapporo ward office, then selling duplicates of it that they had made. The defendants are accused [of] duplicating all of the Sapporo citizens' residency registrations, using the microfilm and selling it to direct marketing companies.

Katsumi Shibuki, 32, an office worker of Chuo Ward Sapporo, Jun Hongo, 24, a company executive of the same ward, and two others were charged with theft.

During their first trial hearing at the Sapporo District Court, all four admitted taking microfilm that is kept at the ward office for resident perusal. However, an attorney for Hongo entered a plea of innocent of behalf of his client, contending that the defendants took out the microfilm only for temporary use and therefore the act does not constitute theft.

The three other defendants refused to enter a plea Tuesday as their attorneys argued that legal problems are involved in charging their clients with theft for their act. In their opening statement, prosecutors said the four made several preliminary inspections of the ward office where the microfilm was kept and then purchased a microfilm duplicator, thus premeditating the crime. They noted that Shibuki borrowed the microfilm on the pretext of reading it, but his accomplices took it out and duplicated it in their Sapporo office.

The prosecutors charged that the defendants collaborated and each assumed a different role. According to the indictments, the four were accused of taking out 482 residency register microfilm entries kept at all of Sapporo's eight ward offices between April and May 1992.

A few comments. Japan has a universal citizen registration law that requires all residents to report their place of residence to their local government. This is in addition to a family registration system that tracks all births deaths, marriages and divorces. That data may be similarly ill secured however it is of less interest to direct marketeers than the residence data which is kept up to date within about 15 days. Although this system is very ancient the law regarding data security has obviously not caught up with the technology. As more and more local governments are keeping this data on personal computers all of the attendant risks to privacy will appear. Obviously what is needed is a law that relates specifically to the data and not to the media. It is clear from the article that the prosecutors believe that the accused did something illegal but they don't seem to have a statute appropriate for the circumstances. A final observation is that while the case for theft seems very weak to someone familiar with American or English law things in Japan are not so obvious. People have been convicted in Japan for intent to commit a felony when no felony was actually committed. The courts may also take a similarly broad interpretation of theft even though the physical objects taken were promptly returned.

Nintendo and Epileptic attacks

Marvin Moskowitz <marvinm@catman.tti.com>
Fri, 15 Jan 93 07:52:56 PST

In article <CMM.0.90.1.726985062.risks@chiron.csl.sri.com> Rick Russell writes:
> The Super Nintendo Entertainment System "Consumer Information and Precautions
> Booklet", which comes with SNES and NES systems sold in the US (and the UK,
> to the best of my knowledge), issues the following warning:
>
>   EPILEPSY WARNING: READ BEFORE USING YOUR NES OR SUPER NES

Well, I guess all this should be no surprise to anyone who has read Crichton's "Andromeda Strain." The flashing lights causing a seizure was a major device he used. His background as a physician lent some credibility to the novel.

Marvin S. Moskowitz, Transaction Tech, Inc., 3100 Ocean Park Blvd.,
Santa Monica, CA 90405 1-310-450-9111 x3197 marvinm@soldev.tti.com

Re: Computer games may endanger your health (Russell, RISKS-14.27)

Robert A. Morris <ram@cs.umb.edu>
Sun, 17 Jan 1993 18:07:40 -0500

> EPILEPSY WARNING: READ BEFORE USING YOUR NES OR SUPER NES
> Consult your physician if you experience any of the following symptoms while
> playing video games: altered vision, muscle twitching, other involuntary
> movements, loss of awareness of your surroundings, mental confusion, and/or
> convulsions.

Of course, the search for most of these conditions are among the _goals_ of video game players....

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 29

Weds 27 January 1993

Contents

Synthesis report on DoD software problems

James H. Paul <PAUL@NOVA.HOUSE.GOV>
Mon, 25 Jan 1993 10:50:35 -0500 (EST)

The General Accounting Office (GAO) has issued a report summarizing the findings from its recent studies of software problems in major weapons. The report is entitled "MISSION CRITICAL SYSTEMS: Defense Attempting to Address Major Software Challenges." Copies may be obtained by calling GAO's distribution center at 301-275-6241 and requesting IMTEC-93-13, dated December 24, 1992 (a nice Christmas present for Congressman Dellums, who is now ascending to chair the Committee on Armed Services of the House of

Representatives.)

Some may be interested to know that GAO has virtually decided to abolish its Information Management and Technology Division. Future investigations of information system failures will be carried out by the program divisions. I've indicated to our congressional affairs representative at GAO that I don't think much of this, particularly with the Government's well-known difficulties in designing, procuring, managing and maintaining large-scale systems. Sorry to say my views didn't appear to derail the express train.

EM Radiation - is smoking safer?

Paul Big-Ears Menon <pnm@goanna.cs.rmit.oz.au>
Thu, 21 Jan 1993 14:23:49 +1000

A snippet in today's Melbourne daily - "The Age" (21 Jan '93):

"Television sets were once accused of killing flies and video games are still suspected of prompting epileptic fits. But blowing up a petrol station? That, it seems, is the province of the mobile phone.

As a warning Shell has issued in the UK makes clear, mobile phones can do more than propel private conversations on to front pages [sorry Chuck]. According to British Shell, service station customers who use mobile phones while filling their cars could ignite petrol vapo[u]r through sparks emitted by the phones' electromagnetic radiation.

And that is not all. A man in Florida is suing a mobile phone maker claiming the antenna on one of its phones caused excessive exposure to the microwave radiation it emits. This, he claims, contributed to a brain cancer that killed his wife. ..."

Is it safer to smoke at a petrol station?

We've had walkie talkies (ok - two way radios) for years with no perceivable or admitted risk to the health of users. I presume mobile phones have less power output than their predecessors, as area transponders/repeaters/xceivers are likely to be more sensitive than 2-ways, and are located to obviate high output end-user devices.

Nevertheless, I was reminded of EMR's existence just recently. I've purchased a Heart Rate Monitor (HRM) to monitor the quality & consistency of my runs. It's a two piece type: one is a band around the chest, which transmits to a digital receiver on the wrist. Now, apart from my curiosity about how this works (ie, what is transmitted & how) not getting me anywhere (this is a consumer device), I was intrigued with its performance in the field.

My running route takes me under some high tension lines. Guess what? The HRM goes bonkers! At first I thought it was just the transmitter not fitted properly, but I eliminated this as the result here is totally different. It took a few more runs under these lines to recognise the cause. I don't think I could survive a heart rate of 228-230 beats/minute! On checking the manual, it warns of strange behaviour (the device, not the user) under HT lines.

With the plethora of EMR everywhere, I wonder if strange behaviour in _humans_ is the only outlook for the future...

Paul Menon, Computer Science, Royal Melbourne Institute of Technology, 124
La Trobe Street, Melbourne, Victoria 3001, Australia +61 3 660 - 3209/2348

Brazilian Banking Reserve Data Disappear: The Post-Hacker Era

Sanford Sherizen <0003965782@mcimail.com>
Thu, 21 Jan 93 19:56 GMT

A Reuters report found in the NY Times (21 Jan 1993) states that computer disks holding secret information on Brazil's banking reserves have disappeared from the central bank. The federal police are investigating the loss. According to the report, President Itamar Franco "took the unusual step" of releasing information on the reserves to offset any damage or financial speculation from loss of the disks. The disks held information on day-to-day reserve operations and details like where the reserves are invested, what they consisted of and how the reserves were generated.

COMMENTS: This disappearance may be related to ex-President Collar's involvement in the looting of Brazil. At a minimum, the data disappearance seems to be another indication of the Post-Hacker Era, where governments and companies have learned that computers can be used as an essential aspect of crime and/or to cover up a crime. The lines between "hacker" activities and "legitimate" activities may become increasingly less clear. In order to commit a white collar or economic crime, individuals or organizations will almost have to use computer techniques. While there continues to be an (often unconscious) image that many have that computer crime is "bad individuals" against "good" organizations, the Organization as Computer Criminal is rapidly becoming a serious problem. One but certainly not the only instance of this is the recent British Airways's penetration of Virgin Air's reservations system.

Clinton Transition Team E-Mail

David Daniels <0004381897@mcimail.com>
Wed, 20 Jan 93 05:32 GMT

It is only fitting that this happened on the eve of tomorrow's presidential inauguration: I sent a message today to the Clinton Transition Team and got the following response. Does this mean that they are not keeping up with their e-mail? So much for electronic democracy!!! :-}

TO: * David Daniels / MCI ID: 438-1897
Subject: Non-delivery notification

Message [...] sent Tue, Jan 19, 1993 07:16 PM EST, could not be delivered to:

To: Clinton Transition Team
     EMS: CompuServe
     MBX: [75300,3115]

for the following reasons:

   Mail Delivery Failure. No room in mailbox.

----- Returned message -----

        [Too many people looking for jobs? PGN]

Computer promises nothing

Conrad Bullock <Conrad.Bullock@actrix.gen.nz>
Wed, 27 Jan 93 21:58:56 NZT

The Evening Post, Wellington, New Zealand, 27th January, 1993 (Excerpted)

ACC Promises Nothing

A computer glitch two weeks ago means some accident compensation clients have been sent multiple identical letters promising them cheques for $0.00. Teacher Angela Watt received three envelopes yesterday from the Accident Rehabilitation and Compensation Insurance Corporation relating to her son Andrew, who sprained his ankle while picking apricots. The first letter gave Andrew's medical fee number and requested that he keep it in a safe place. The second did the same thing but added mysteriously that "although you have claimed $0.00, legislative regulations provide maximum limits of payment of $0.00. Payment of this amount will be forwarded." Confused and craving enlightenment, Mrs Watt opened the third letter. She found a cheque for $29 - a refund for Andrew's doctor's fee.

Palmerston North branch manager Jo Burney said the corporation reprogrammed its Wellington computer on January 12 to stop it sending out individual letters for every part of a client's claim. "Under the old system, you would get separate letters and cheques for each part of a claim - the doctor's fee, the prescription charge and the physiotherapy," she said.

The new computer programme was supposed to save all the claims, add them up and send out one letter and one cheque. "Something happened ... there was one letter all right but it was sent out three times in some cases."

The FBI and Lotus cc:Mail

<joltes@husc.harvard.edu>
Wed, 20 Jan 93 17:58:49 EST

An interesting tidbit came to light while I was attending a demonstration of Lotus' cc:Mail and Notes products at the Boston NetWorld this month. During the Notes portion of the presentation someone asked how secure the information in the various databases was, and how the encryption was done.

The presenter said that the data was considered very secure, so much so that the FBI had approached Lotus to ask that a "back door" be left in the software in order to give the Bureau a method for infiltrating suspects' filesystems. She said they were specifically targeting "drug dealers and other bad people."

Given this backdoor, what was to stop the Bureau from inspecting confidential materials on any system? The risks seem obvious. Additionally, it makes one wonder how many other vendors of supposedly "secure" software have been similarly approached by various Federal organizations, and how many have agreed to create the back doors as requested.

Happily, the presenter said that Lotus refused to honor the FBI's request. Bravo!

Dick Joltes, Manager, Networks and Hardware, Harvard University Science Center
joltes@husc.harvard.edu

A stopped clock never foils?

Paul Eggert <eggert@twinsun.com>
Wed, 20 Jan 93 21:31:33 PST

One way to discourage intruders from using covert channels to foil security is to turn off the system clock, or at least to hide it from users. But this breaks a lot of software, so it's too drastic for all but the most security-conscious sites. So I was surprised to see J.-B. Condat's letter in RISKS 14.28, which began:

```
Date: 31 Dec 69 23:59:59 GMT
From: jbcondat@attmail.com
Subject: New E-journal on computer security
...
```

Unix cognoscenti will recognize that date: it corresponds to the internal Unix time value of -1, which is returned by system functions when the clock is not available. I guess Condat and the Chaos Computer Club France must really be practicing what they preach!

Racetrack goes to the dogs as computer fails (RISKS-14.28)

Conrad Bullock <Conrad.Bullock@actrix.gen.nz>
Sat, 23 Jan 1993 23:59:12 +1200

> > At the tail end of the sports news at the end of NewsHour, the morning BBC
> > show heard on WBUR, was the mention of an error in a betting computer at a
> > greyhound race track. The computer continued to accept bets well after the
> > conclusion of the race. Needless to say, many gleeful track-betters bought
> > tickets for the dog that had already won, and claimed their winnings.

This happened in New Zealand, with the computer system run by the NZ TAB (Totalisator Agency Board), on the 7th of January, at the Waikato aGreyhound

Club meeting.

The problem started when the track to computer site communication links proved unreliable - basically a noisy data line, with lots of dropouts. Switching to a backup dialup line did not help. When they switched to a backup modem, it blew a fuse. They then tried to switch to a cellular modem backup, they failed to establish a connection (I am unsure on the engineering details here). (Apparently all these backup services had worked OK on the previous day). The upshot was that operation continued on the noisy line, with reduced throughput.

Because of these communication difficulties, after consultation with the Auckland computer site, the track tote manager decided to delay all races by 30 minutes. Unfortunately, the human-human communications link failed here, as both the track operators, and the Auckland site operators delayed the races by the required 30 minutes, thus resulting in the computer believing races had been delayed by 60 minutes.

When the race was started, the track operators performed a standard `Race close' function, to shut off betting. (NZ TAB operates `betting to the jump'). However, because in the computers' eyes, the race was being closed 30 minutes early, the control function being used asked for the `Override for Early close' field to be set to `Y'.

The operator, apparently used to closing races at approximately the right time, or after the scheduled time, had never seen this diagnostic before, and/or had `sent' the control function, and walked away before seeing the diagnostic.

This problem was not noticed/solved for about 3 minutes, and since a greyhound race is over in about 20 seconds, this allowed time for a number of bets to be placed after the result was known. The bets were placed all around the country - not just at the track.

[Exactly what happened in this 3 minute period has not been sorted out - there was a flurry of human-human communication between the track, the Auckland computer site, and the master computer site, once it was realised that betting was still being taken. Procedures were not correctly followed. Part of the problem is that this has never happened before in the 12 years of operation this system has had. Too reliable?]

Once the `double deferment' problem was noticed, the track tried to move the race start times forward by half an hour. However, the software would not allow them to move subsequent race start times to a time which was prior to the scheduled start time of a race which has already been run. This was not a major problem, since the early race close could be used OK. [Perhaps a case of error-checking being a little too stringent?]

I would hesitate to blame the problems on `computer failure'. Perhaps `communications failure' - between the computer and the operators (For having a slightly different interaction in this instance), and human-human (the double deferment, and the site/track communications when the problem was noticed). The only hardware failure was a dodgy comms link. Software failure? Not really. Computer system failure? I guess so, you've got to count the operations side of things.

> > The article also mentioned that some people are just born losers.
> > After the race had finished, 139 people bet on dogs that had *lost*!

This is explained by the popularity of a product called `Easybet'. This is a bet in which the computer selects three runners for a race (runners are selected randomly, weighted by favouritism), and the ticket wins if the three selected runners come in 1st, 2nd and 3rd (a boxed trifecta). The default race for an `Easybet' is the next race to close. Since the race hadn't been `closed', many `Easybets' were sold on the race which had already been run. Many of the losing tickets sold after the race had been run were actually `Easybets' which didn't win.

> > The government management reported that they intended to reclaim all of the
> > unfairly-won monies. However, they stated that they intend to *keep* the
> > money from the losers.

The `loss' was approximately NZ$7000, mostly from trifecta bets (selecting 1st, 2nd and 3rd in the right order), with a payout of over $200 per $1 invested. NZ$5000 of this was placed at a single agency. The agent has been arrested and charged, after allegedly encouraging customers to bet after the result was known, and allegedly placing bets him/herself (illegal).

Since the TAB in New Zealand operates on a pari-mutuel system, where the prize pool is a percentage of the money placed on a particular bet type for that race, the late bets increased the number of winning units, thus `diluting' the dividend paid on winning bets. The TAB is making up the dividend to the correct amount, for bets placed before the race was run.

[Also commented upon by Martin D. Hunt <martinh@gaya.gp.co.nz>.]

Request to Post Office on Selling of Personal Information

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 22 Jan 1993 14:47:48 EST

In May 1992, the US Postal Service testified before the US House of Representatives' Government Operations Subcommittee that National Change of Address (NCOA) information filled out by each postal patron who moves and files that move with the Post Office to have their mail forwarded is sold to direct marketing firms without the person's consent and without informing them of the disclosure. These records are then used to target people who have recently moved and by private detective agencies to trace people, among other uses. There is no way, except by not filling out the NCOA form, to prevent this disclosure.

This letter is to request information on why your personal information was disclosed and what uses are being made of it. Patrons who send in this letter are encouraged to also forward it and any replies to their Congressional Representative and Senators.

Eligible requestors: Anyone who has filed a change of address notice with the Postal Service within the last five years.

Records Officer
US Postal Service
Washington, DC 20260   PRIVACY ACT REQUEST

Dear Sir/Madam:

This is a request under the Privacy Act of 1974 (5 USC 552a). The Act requires the Postal Service, as a government agency, to maintain an accounting of the date, nature, and purpose of each disclosure of information about individuals. I request a copy of the accounting of all disclosures made of address change and mail forwarding information that I provided to the Postal Service. This information is maintained in USPS System of Records 010.010.

On or about (date), I filed a change of address notice requesting that my mail be forwarded from (old address) to (new address). The name that I used on the change of address form was (name).

This request includes the accounting of all disclosures made by the Postal Service, its contractors, and its licensees.

I am making this request because I object to the Postal Service's policy of disclosing this information without giving individuals an option to prevent release of this information. I want to learn how my information has been disclosed and what uses have been made of it. Please let the Postmaster General know that postal patrons want to have a choice in how change of address information is used.

If there is a fee in excess of $5 for this information, please notify me in advance. Thank you for consideration of this request.

Sincerely,

CC: Your Congressional Representative
US House of Representatives
Washington, DC 20510

Your Senators
US Senate
Washington, DC 20515

TAPSOFT '93, APRIL 13-16, 1993, ORSAY, FRANCE

Cliff B Jones <cliff@computer-science.manchester.ac.uk>
Tue, 19 Jan 93 12:24:12 GMT

PROGRAM [and REGISTRATION FORM info]

[NO REGISTRATIONS BY EMAIL. REGISTRATION FORM FROM CLIFF OR FTP
FROM RISKS CRVAX.SRI.COM archive directory (CD RISKS:) as "TAPSOFT.93".]

TAPSOFT'93 is the fourth International Joint Conference on the Theory and Practice of Software Development. Its predecessors where held in Berlin, Pisa, Barcelona and Brighton. This year TAPSOFT will take place at Orsay, the beautiful campus of the University "Paris-Sud".

Continuing with the tradition of high scientific quality of these meetings, TAPSOFT'93 will consist of three parts:

I. The COLLOQUIUM ON TREES IN ALGEBRAS AND PROGRAMMING (CAAP)
Program Committee: A. Arnold, N. Dershowitz, H. Ganzinger, J. Goguen, J.-P. Jouannaud (Chair), J.-W. Klop, D. Kozen, U. Montanari, M. Nivat, L. Pacholski, B. Rovan, W. Thomas

II. The COLLOQUIUM ON FORMAL APPROACHES OF SOFTWARE ENGINEERING (FASE)
Program Committee: E. Astesiano, M. Dincbas, H. Erhig, M.-C. Gaudel (General Chair), S. Gerhart, D. Jacobs, C. Jones, T. Maibaum, F. Orejas, J. Sifakis, A. Tarlecki

III. The ADVANCED SEMINAR with
INVITED SURVEYS by H.-D. Ehrich, J. Guttag, C. Jones, B. Mahr, W. Thomas
INVITED CONFERENCES by A. Arnold, P-P. Degano, N. Dershowitz, G. Longo

CONFERENCE LOCATION: Building 338 (Batiment des Colloques), Faculte des Sciences, Universite de Paris-Sud, Orsay, France
ACCESS: from Paris, 40 min. by RER line B, Orsay-ville station

PROGRAMME OF THE CONFERENCE
Tuesday 13

9:00 Registration and Coffee
*9:45 Opening session
*10:00 Invited Survey : "Are Formal Methods Useful "J. V. Guttag, MIT (USA), chaired by M.-C. Gaudel

*12:00 Invited Conference: "On the Expressive Power of Models of Concurrency", P.-P. Degano, Univ. di Pisa (I) chaired by A. Arnold

***14:30 CAAP Session 1 : Specifications and Proofs, chair : J. Goguen
- 14:30 Compositionality Results for Different Types of Parameterization and Parameter Passing in Specification Languages, H. Ehrig, T. U. Berlin (D), R. M. Jimenez & F. Orejas, Univ. Pol. de Catalunya (S)
- 15:00 Proving Ground Confluence and Inductive Validity in Constructor Based Equational Specifications, K. Becker, Univ. Kaiserlautern (D)
- 15:30 Associative-Commutative Discrimination Nets, L. Bachmair, T. Chen, I.V. Ramakrishnan, SUNY, Stony Brook (USA)

***14:30 FASE Session 1 : Case Studies in Formal Design and Development, chair : J. V. Guttag
- 14:30 Algebraic Specification and Development in Geometric Modeling, Y. Bertrand, J.-F. Dufourd, J. Francon, P. Lienhart, Univ. Louis Pasteur & CNRS, Strasbourg (F)
- 15:00 A Case Study in Transformational Design of Concurrent Systems, E. R. Olderog & S. Rssig, Univ. Oldenburg (D)

- 15:30 Yeast : a Case Study for a Practical Use of Formal Methods, P.
  Inverardi, IEI-CNR Pisa (I), B. Krishnamurthy, AT&T Bell Lab, Murray
  Hill (USA), D. Yankelevich, Univ. Pisa (I)

16:00 Coffee Break

*16:30 Invited Conference: "Vertical Verification of Concurrent Systems",
A. Arnold, Labri-CNRS, Univ. Bordeaux (F) chaired by C. B. Jones

17:45 University Reception

Wednesday 14

*9:30 Invited Survey: "Using Object-based Concepts to Control Concurrency",
C. B. Jones, Univ. of Manchester (UK) chaired by H.-D. Ehrich

11:00 Coffee Break

***11:30 CAAP, Session 2: Concurrency, chair : U. Montanari

- 11:30 From pi-calculus to higher-order pi-calculus - and back, D. Sangiorgi,
  Univ. Edinburgh (UK)
- 12:00 Hyperedge Replacement with Rendez-vous, G. David, F. Drewes & H.-J.
  Kreowski, Univ. Bremen (D)
- 12:30 True Concurrency Semantics for a Linear Logic Programming Language
  with Broadcast Communication, J.-M. Andreoli, L. Leth, R. Pareschi &
  B. Thomsen, ECRC, Munich (D)

***11:30 FASE, Session 2: Compositionality, Modules and Development, chair :
A. Tarlecki,

- 11:30 A General Framework for Modular Implementations of Modular System
  Specifications, M. Bidoit, LIENS-CNRS (F), R. Hennicker,
  Ludwig-Maximilians Univ., Mnchen (D)
- 12:00 Reducing the Runtime Costs for Modularity, M.T. Vandevoorde, MIT (USA)
- 12:30 Application of the Composition Principle to UNITY-like Specifications,
  P. Collette, Univ. Catholique de Louvain (B)

13:15 Lunch

*14:30 Invited Conference: ""Trees, Ordinals and Termination", N. Dershowitz,
Hebrew Univ., Jerusalem (IL), chaired by F. Orejas

15:30 Coffee Break

***16:00 CAAP Session 3: Automata and Counting, chair : B. Rovan

- 16:00 When is a Functional Tree Transduction Deterministic, H. Seidl, Univ.
  des Saarlandes (D)
- 16:30 Automata on Infinite Trees with Counting Constraints, D. Beauquier,
  LITP, Paris (F), D. Niwinski, Univ. Warsaw (POL)
- 17:00 Directed Column-Convex Polyominoes by Recurrence Relations, E.
  Barcucci, R. Pinzani & R. Sprugnoli, Univ. di Firenze (I)

***16:00 FASE Session 3: Formal Development, chair : B. Krieg-Bruckner

- 16:00 Object Organisation in Software Environments for Formal Methods, J.
  Han, Univ. of Queensland (AUS)
- 16:30 Monads, Indexes and Transformations, F. Bellegarde, Western Washington
  Univ. (USA), and J. Hook, Oregon Graduate Institute, Beaverton (USA)
- 17:00 A Technique for Specifying and Refining TCSP processes by using Guards
  and Liveness Conditions, R. Pea, Univ. Computense de Madrid (S), L.
  M. Alonso, Univ. del Pais Vasco (S)

Thursday 15

*9:30 Invited Survey: "Applications of Type Theory", B. Mahr, T. U. Berlin (D)
chaired by G. Longo
11:00 Coffee Break
***11:30 CAAP Session 4: Constraints Solving and Enumerations,
chair : L. Pacholski
-11:30 Feature Automata and Recognizable Sets of Feature Trees, J. Niehren,
DFKI, Saarbrcken (D), A. Podelski, DEC-PRL, Rueil-Malmaison (F)
-12:00 About the Theory of Tree Embedding, A. Boudet & H. Comon, LRI-CNRS,
Univ. Paris-Sud (F)
-12:30 Linear Unification of Higher-Order Patterns, Z. Qian, Univ. Bremen (D)

***11:30 FASE Session 4 : Foundations and Analysis of Formal Specifications,
chair : E. Astesiano
-11:30 Theory Revision for Requirements Capture, W. Li, Beijing Univ. (China)
-12:00 Exception Handling and Tern Labelling, G. Bernot, LIVE Evry (F), P.
Le Gall, LRI-CNRS Orsay (F)
- 12:30 Gate Splitting in LOTOS Specifications using Abstract Interpretation,
F. Giannotti & D. Latella, CNR, Pisa (I)
13:15 Lunch
*14:30 Invited Survey: "Constructing Systems as Objects Communities", H.-D.
Ehrich, T.U. Braunschweig (D), chaired by H. Ganzinger
16:00 Coffee Break
***16:30 CAAP Session 5: Rewriting, chair : J.-W. Klop
-16:30 Term Rewriting in CT 7, A. Corradini, Univ. di Pisa (I)
-17:00 Optimal Reductions in Interaction Systems, A. Asperti & C. Laneve,
INRIA-Rocquencourt (F)
-17:30 Optimal Solutions to Pattern Matching Problems, L. Puel, LRI-CNRS,
Univ. Paris-Sud (F), A. Suarez, LIENS-CNRS (F)

***16:30 FASE Session 5 : Verification of Concurrent Systems, ch. T. Maibaum
-16:30 Testing for a Conformance Relation based on Acceptance, M.Y. Yao,
G.V. Bochmann, Univ. of Montreal (CDN)
-17:00 Testability of a system though an Environment, K. Drira & P. Azema,
LAAS-CNRS, Toulouse (F), B. Soulas & A.-M. Chemali, EDF-DER, Moret sur
Loing (F)
-17:30 Automating (Specification = Implementation) using Equational Reasoning
and LOTOS, C. Kirkwood, Univ. of Glasgow (UK)
20:00 Banquet

Friday 16

*9:30 Invited Survey: "The Erhenfeucht Fraisse Game in Theoretical Computer
Science", W. Thomas, Univ. Kiel (D), chaired by M. Nivat
11:00 Coffee Break
***11:30 CAAP Session 6: Logic and Trees, chair : W. Thomas
-11:30 On Asymptotic Probabilities in Logics that captures DSPACE(log n) in
Presence of Ordering, J. Tyszkiewicz, Univ. Warsaw (POL)
-12:00 A Propositional Dense Time Logic based on nested sequences, M. Ahmed &
G. Venkatesh, Indian Inst. of Tech., Bombay (IND)
- 12:30 La vraie Forme d'un Arbre, J. Betrema & A. Zvonkin, Labri-CNRS, Univ.
Bordeaux (F)

***11:30 FASE, Session 6 : Model Checking, chair : J. Sifakis
-11:30 Model Checking using Net Unfolding, J. Esparza, Univ. Hildesheim (D)

-12:00 Reachability Analysis on Distributed Executions, C.Diehl, C. Jard &
       J.-X. Rampon, IRISA (F)
-12:30 Program Verification and Abstraction, S. Graf & C. Loiseaux, IMAG (F)
                 13:15 Lunch
*14:30 Invited Conference: "The Meaning of "parametricity" in Polymorphic
       Functional Languages", G. Longo, chaired by J.-P. Jouannaud
***15:30 CAAP-FASE Common Session: Type Inference, chair : J.-P. Jouannaud
-15:30 Polymorphic Type Inference with Overloading and Subtyping, G.S. Smith,
       Cornell Univ. (USA)
- 16:00 Type Reconstruction with Recursive Types and Atomic Subtyping, J.
       Tiuryn & M. Wand, Northeastern Univ., Boston (USA)

***17:00 CAAP Session 7: Analysis of Algorithms, chair : M. Soria
-17:00 (Un)expected Path Lengths of Asymmetric Binary Search Trees, U.
       Trier, Goethe Univ., Frankfurt (D)
-17:30 Tree Size in a Dynamic List Structure, G. Louchard, Univ. Libre
       Bruxelles (B)

***17:00 FASE Session 7: Parallel Calculus, chair : H. Erhig
-17:00 A Fully Parallel Calculus of Synchronizing Processes, D. Latella &
      P. Quaglia, CNR, Pisa (I)
-17:30 Generic Systolic Arrays : A methodology for Systolic Design, E.P.
      Gribomont, Univ. de Liege (B), V. Van Dongen, CRI, Montreal (CDN)

[And if you attend, please be sure to ask what this has to do with
preventing RISKS. Of course, IT SHOULD HAVE GREAT RELEVANCE. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 30

Tuesday 2 February 1993

Contents

Clever Tactics Against Piracy

Jay Rolls <jrolls@frg.bbn.com>
Fri, 29 Jan 93 14:16:11 +0100

I thought the info-mac readers would find this article interesting.....
Jay Rolls, Stuttgart, Germany <jrolls@bbn.com>

[sent to RISKS by gio@DARPA.MIL (Gio Wiederhold) via many others]

COMPUTER CHEATS TAKE CADSOFT'S BAIT

Employees of IBM, Philips, the German federal interior ministry and the federal office for the protection of the constitution are among those who unwittingly 'turned themselves in' when a German computer software company resorted to an undercover strategy to find out who was using illegal copies of one of its programs.

Hundreds of customers accepted Cadsoft's offer of a free demonstration program that, unknown to them, searched their computer hard disks for illegal copies. Where the search was successful, a message appeared on the monitor screen inviting the customer to print out and return a voucher for a free handbook of the latest version of the program. However, instead of a handbook the users received a letter from the Bavarian-based software company's lawyers.

Since the demonstration program was distributed last June about 400 people have returned the voucher, which contained coded information about the type of computer and the version of the illegally copied Cadsoft program being used. Cadsoft is now seeking damages of at least DM6,000 (ECU3,06E2) each from the illegal users.

Cadsoft's tactics are justified by manager Rudolf Hofer as a necessary defence against pirate copying. The company had experienced a 30% drop since 1991 in sales of its successful Eagle design program, which retails at DM2,998. In contrast, demand for a DM25 demo version, which Cadsoft offered with the handbook of the full version, had jumped, indicating that people were acquiring the program from other sources.

Although Cadsoft devised its plan with the help of lawyers, doubts have been raised about the legal acceptability of this type of computer detective work. In the case of government offices there is concern about data protection and official secrets. The search program may also have had side-effects that caused other files to be damaged or lost. Cadsoft is therefore preparing itself for what could be a long legal battle with some customers. So far it has reached out-of-court agreement with only about a quarter of those who incriminated themselves.

Educational computer game banned in Milpitas CA

Chocolate Flavored Clorox <shaun@octel.com>
Thu, 21 Jan 93 10:59:25 PST

RISK in paragraph three.

The following appeared in the _Milpitas Post_ Vol. 37 No. 2, January 13, 1993, of Milpitas, CA on page 1.

Superior Court ruling upholds `Wizards' ban, by Christina Kirby

A SUPERIOR court judge has upheld the Milpitas Unified School District's 2-year-old ban on the Wizards spelling game. The ruling was handed down last Friday.

The computer game was banned in 1990 by the school board following complaints from parents that it promoted satanic worship.

Teachers, seeking to reverse the ban, argued that it infringed on their rights to choose teaching materials, and broke laws prohibiting state agencies, such as school districts, from supporting any religion.

The court ruled that the school district had acted within its authority and had not violated the California constitution by banning the game.

"With all due respect, we don't agree with the court's decision," said Catherine Porter, an attorney representing the teachers. "Based on the California constitution, we do believe that we provided significant evidence to show that the purpose and effect of the ban was religious and not secular."

Pleased by the ruling, Milpitas Superintendent Jack Mackay said, "We always thought the board was acting within its authority to maintain a secular environment."

Porter said Monday that the teachers would be discussing whether or not to appeal the decision.

shaun@octel.com

"Two charged with computer fraud in credit scam"

Norm deCarteret 813-878-3994 (TL 438) <normdec@vnet.ibm.com>
Sat, 30 Jan 93 11:20:36 EST

Source: St Pete Times, 1/26/93, pg 3B, Tim Roche

A personnel supervisor "who knew the ins and outs of a computer system that managed charger accounts for thousands of jewelry store customers along the Eastern Seaboard" and a former co-worker worked a scam using the supervisors ability to alter the computers database, illustrating the risks of:

- inadequate controls within the computer system
- retail store policy shortcomings
- the procedure by which they let users who have had their card stolen continue to charge purchases
- flaws in the system accountability

"Using computer passwords of other employees, detectives said, Benjamin Francois was able to alter customer records and list a credit card as lost or stolen. Then his friend, John Wise, would appear at a jewelry store and claim to be the customer whose credit card was missing. By store policy, Wise only was required to give sales clerks a name, Social Security number and a secret code that would allow customers whose cards were lost or stolen to continue charging merchandise. "If the clerk asked to see some identification, Wise would explain ... he had no photo to prove he was the customer, but he would give the clerk the secret code Francois had obtained from the computer."

Affected between June 2nd and last September were:

- jewelry stores in Tampa, Orlando, Palm Beach and Altamonte Springs FL

- Jewelers Financial Services, which ran accounts for:
  . Zales Jewelers, Bailey Banks & Biddle Jewelers, Gordons Jewelers

Francois was able to delete the references to stolen or lost cards on the charge accounts after the purchases were made. The two men were arrested after a tip in November led police investigators to "verify the mainframe database" records.

Of particular interest: system controls allow Francois to manipulate the database, then hide the activity so that, apparently, the real customers were not billed. If the report is correct, it was the November tip and not any system controls that revealed the thefts. Apparently the charges were allowed to fall into some sort of accounting black hole.

Norm deCarteret   Advantis - Tampa FL

Bible belt broadcast bungle

Peter J. Scott <pjs@euclid.Jpl.Nasa.Gov>
Thu, 28 Jan 93 08:31:21 -0800

Heard this on the radio this morning: a major Christian radio network is alerting its member stations to check their latest shipments of religious compact discs before airing them. It seems that some other CDs were mislabelled at the factory and shipped along with the religious ones. Unfortunately the itinerant CDs were by the Dead Kennedys. A spokesman for the radio network said, "This is what happens whenever people get around machines." The CBS newsreader, with masterful understatement, said, "The Dead Kennedys CDs included songs such as, `I Kill Children,' which some Christian listeners may not find inspirational."

Peter J. Scott, Member of Technical Staff | pjs@euclid.jpl.nasa.gov
Jet Propulsion Laboratory, NASA/Caltech | SPAN: GROUCH::PJS

Phone Fraud numbers

John Mello <jmello@igc.apc.org>
Tue, 2 Feb 93 14:31:12 PST

The major telecomm carriers are reporting that 1992 was a bad year for the phone baddies intent on ripping off phone service from corporations. Sprint reported fraud claims by its business customers dived 96 percent, to $670,000, or $1,350 per incident compared to an average loss of $35,000 in 1991. AT&T says fraud claims made to it dropped about 88 percent and MCI says it has also seen a drop in claims. In other words, 1992 losses were a far cry from the $1 billion to $3 billion a year claimed as losses in past years. The major reason for the drop: customer awareness

Re: Clinton Transition Team E-Mail

James Barrett <barrett@forge.gatech.edu>
Thu, 28 Jan 1993 18:12:46 GMT

> Mail Delivery Failure. No room in mailbox.

This is because Jock Gill who handles Email for Clinton was at the inauguration and not near his computer for a week. The link is back up and generating *lots* of mail (press releases) from Clinton.

Re: EM Radiation (and cell phones) (Menon, RISKS-14.29)

Lauren Weinstein <lauren@cv.vortex.com>
Wed, 27 Jan 93 16:55 PST

The issues surrounding the topic of possible negative health effects from cellular phone use are going to be among the hottest (no pun intended) in coming years.

There are no definitive studies that fully address the complexities of the situation, especially in view of increasing circumstantial evidence that non-ionizing radiation may have more biological effects than previously thought.

It's true that walkie-talkies, ham radios, etc. have been around for many years--but there are some potentially significant differences with cellular phones:

1) Most walkie-talkie, police radios, ham radios, etc. are operated in a push-to-talk mode. You're only transmitting when you're actually talking. Cell phones transmit continuously, so exposure is continuous during calls.

2) Cell phones operate at higher frequencies than most common service or ham radios (common hand-held ham radios, for example, usually go no higher than the 440 Mhz band. Cell phones operate in the 800-900 Mhz region, which puts them just about in the microwave range.

Recently there have been a number of concerns raised about microwave exposure to the operators of police radar units. We're talking longer exposure and higher frequencies in the radar case--but nobody knows where the "thresholds" might be for exposure to possibly show effects in some persons. The bottom line is that the higher the frequency, the more "energetic" the effects.

In at least a couple of the cases of persons accusing cell phones of causing tumors, part of their evidence is the shape and direction of tumor growth--they apparently are aligned with the antenna and growing inward from the outside. Of course, this says nothing about cause and effect--but it has to at least be considered.

It's true that cell phones use quite low power. But a little power packs a bigger "punch" at these frequencies, and with the antenna right next to the

head the *field strength* (which matters more than the absolute power) can be
quite high (inverse square law applies).

Concerns about health effects from hand-held radios have been around for a long time. But with the millions of people using continuously transmitting, ultra high frequency units who never did before, some new dimensions are added to the picture--and they are definitely worthy of serious consideration.

By the way, not all cellular systems are created equal when it comes to radiation exposure. The new CDMA digital system, for example, throttles back the power from the portable unit depending on how close you are to the cell site--the site transmitter sends a signal back to the handheld controlling the power level. The main reason for doing this is to drastically increase battery life, but it has the additional benefit of reducing overall exposure as well.

--Lauren--

Re: EM Radiation - is smoking safer? (Menon, RISKS-14.29)

Andrew Klossner <andrew@frip.wv.tek.com>
Wed, 27 Jan 93 17:03:44 PST

"We've had walkie talkies (ok - two way radios) for years with
no perceivable or admitted risk to the health of users."

Not so. Long term (over 20 years) use of two-way radios by police officers has been linked to higher incidences of glaucoma. This is one reason why the transmitter unit is now worn on the belt, with the microphone pinned to the lapel.

(This means that the transmitter irradiates the gonads instead of the eyeballs ... a possible new risk?)

-=- Andrew Klossner (andrew@frip.wv.tek.com)
(uunet!tektronix!frip.WV.TEK!andrew)

CERTIFICATION-PROPOSED US LEGISLATION

AProf Alan Underwood <alanu@fitmail.fit.qut.edu.au>
Mon, 1 Feb 93 10:07:02 EST

>From Alan Underwood, School of Information Systems, Queensland University of Technology. e-mail alanu@snow.fit.qut.edu.au

I am seeking assistance in obtaining copies of any current US/European legislation (proposed or enacted) for the certification of computing professionals. Also, I have seen some reference to 6(?) US States considering such legislation. I would like to know which States so that I can visit them on an upcoming sabbatical.

Any assistance would be appreciated.

Erratum: GAO ordering number

James H. Paul <PAUL@NOVA.HOUSE.GOV>
Thu, 28 Jan 1993 10:51:23 -0500 (EST)

Sorry, folks -- human error strikes again. GAO's distribution center is at (202) 275-6241. The warehouse is in Maryland, but they don't take the orders there. Mea culpa, mea culp, mea maxima culpa.

[stu@national.mitre.org (Stuart Bell) notes FAX (301) 258-4066, no charge for single copies -- just provide all info.]

[and later from James Paul:]

Well, it's worse than I thought. GAO has been migrating to the new Government telephone system and apparently this has caught up with their ordering operation. When you dial (202) 275-6241, you are now directed to call (202) 512-6000. At the same time the message says you will automatically be switched over to the new number. I really apologize for all the confusion. Me, I just get 'em directly.

The Federal Criteria for Information Technology Security review

nicki lynch <lynch@csmes.ncsl.nist.gov>
Fri, 29 Jan 93 16:08:16 EST

The **PRELIMINARY DRAFT** of the U.S. Federal Criteria for Information Technology Security (FC) (which will eventually replace the "Orange Book") is available on-line. The files are located on both the NIST Computer Security Bulletin Board and on the NCSC's DOCKMASTER computer system. DOCKMASTER has the FC available in UNIX compressed postscript format, while the NIST BBS has the FC available in PKZIP postscript format. When printed out, both volumes of the document total approximately 280 pages double-sided. By the first week of February, the FC (without the figures) should be available in ASCII format at both sites. The figures will also be available individually in postscript form.

What follows are instructions on how to download the files from both sites, how to register your name for announcements, and how to send in comments.

- -

TO DOWNLOAD THE FILES FROM DOCKMASTER:

The files can be found on DOCKMASTER in the directory:

```
>site>pubs>criteria>FC
```

- -

TO DOWNLOAD THE FILES FROM NIST'S BBS:

Volumes 1 and 2 of the FC can be accessed through the Internet via anonymous ftp. To download, ftp to csrc.nist.gov or to 129.6.54.11.

Log in as "anonymous" and use your Internet address as the password. The FC postscript files are in directory /bbs/nistpubs. The files are fcvol1.ps.Z and fcvol2.ps.Z, for volumes one and two respectively. Both of these volumes have been ZIPped using PKZIP. The PKZIP program is available in /bbs/software should you need to download it.

REGISTERING YOUR NAME:

When you receive an electronic copy of the draft FC, please send us you name, mailing address, telephone, and e-mail address to the e-mail address listed below and state that you have an electronic copy of the FC. If you distribute the document to additional people in your organization, please send us the same information on those people as well. We will put the names into our database for any further announcements, meeting notices, draft announcements, etc., related to the effort. NIST will be sending out a LIMITED NUMBER of hard copies, but due to the substantial expense of sending out such a large document - even at book rate, we would prefer people to receive the document via electronic means. Therefore, by sending us your name and the names of those in your organization who have the downloaded copies of the document, it saves us from having to send additional hard copies.

COMMENTS:

We are soliciting TECHNICAL, SUBSTANTIVE comments on the document. The deadline for comments is March 31, 1993. All those who contribute substantive comments will be invited to a two-day workshop at the end of April 1993 to resolve the comments. The workshop will be held in the Washington-Baltimore area in a to-be- announced location.

Please send your comments to:

lynch@csmes.ncsl.nist.gov

or, if you prefer, you can send us a 3.5" or 5.25" diskette in MSDOS or UNIX format (please indicate which) to:

Federal Criteria Comments
ATTN: Nickilyn Lynch
NIST/CSL, Bldg 224/RM A241
Gaithersburg, MD 20899

We would prefer to receive electronic copies of comments and/or name registrations, but we will also receive hardcopy comments/name registrations at this same address. You can also contact us via the following fax:

FAX: (301) 926-2733

Thank you in advance for your interest in this effort.

Federal Criteria Group, National Institute of Standards and Technology

Preliminary Program for 1993 Security & Privacy

Dick Kemmerer <kemm%cs@hub.ucsb.edu>
Tue, 02 Feb 93 18:02:25 PST

```
   1993 IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY

May 24-26, 1993, Claremont Resort, Oakland, California

Sponsored by the IEEE Technical Committee on Security and Privacy
In cooperation with the International Association of Cryptologic Research

Symposium Committee
  Teresa Lunt, General Chair
  Cristi Garvey, Vice Chair
  Richard A. Kemmerer, Program Co-Chair
  John Rushby, Program Co-Chair

            PRELIMINARY PROGRAM

MONDAY
9:00--9:30: Welcoming Remarks: Teresa Lunt and Dick Kemmerer
9:30--10:30:   VIRUSES AND INTRUSION DETECTION   Doug McIlroy, Session Chair
  9:30--10:00:  Measuring and Modeling Computer Virus Prevalence
            Jeffrey Kephart and Steve White
 10:00--10:30:  USTAT: A Real-Time Intrusion Detection System for UNIX
            Koral Ilgun

11:00--12:00:   CAUSALITY AND INTEGRITY:  George Dinolt, Session Chair
  11:00--11:30: Preventing Denial and Forgery of Causal Relationships
        in Distributed Systems
            Michael Reiter and Li Gong
  11:30--12:00: Message Integrity Design
                        Stuart Stubblebine and Virgil Gligor

2:00--3:30:     PANEL: Privacy Enhanced Mail
                        Panelists: TO BE ANNOUNCED

4:00--5:00: AUTHENTICATION PROTOCOLS:  Teresa Lunt, Session Chair
  4:00--4:30    Authentication Method with Impersonal Token Cards
            Refik Molva and Gene Tsudik
  4:30--5:00:   Interconnecting Domains with Heterogeneous Key
        Distribution and Authentication Protocols
            Frank Piessens, Bart DeDecker and Phil Janson

6:00:   POSTER SESSIONS
```

```
TUESDAY
9:00--10:30:    TIMING CHANNELS: John Rushby, Session Chair
   9:00-- 9:30: Modelling a Fuzzy Time System
          Jonathan Trostle
   9:30--10:00: On Introducing Noise into the Bus-Contention Channel
          James Gray
  10:00--10:15: Discussant:  TO BE ANNOUNCED
  10:15--10:30: Open Discussion

11:00--12:00:   INFORMATION FLOW: John McLean, Session Chair
  11:00--11:30  A Logical Analysis of Authorized and Prohibited
        Information Flows
          Frederic Cuppens
  11:30--12:00  The Cascade Vulnerability Problem
          J. Horton, R. Harland, E. Ashby, R. Cooper,
          W. Hyslop, B. Nickerson, W. Stewart, and K. Ward

2:00--3:30: PANEL: The Federal Criteria
          Panelists: TO BE ANNOUNCED

4:00--5:00: DATABASE SECURITY:  Marv Schaefer, Session Chair
  4:00--4:30:   A Model of Atomicity for Multilevel Transactions
          Barbara Blaustein, Sushil Jajodia,
          Catherine McCollum and LouAnna Notargiacomo
  4:30--5:00:   Achieving Stricter Correctness Requirements in
        Multilevel Secure Database
          Vijayalakshmi Atluri, Elisa Bertino and
          Sushil Jajodia

5:00:   IEEE Technical Committee Meeting

6:00:   POSTER SESSIONS

WEDNESDAY
9:00--10:30: ANALYSIS OF CRYPTOGRAPHIC PROTOCOLS:  Yacov Yacobi, Session Chair
   9:00-- 9:30: Trust Relationships in Secure Systems
        -- A Distributed Authentication Perspective
          Raphael Yahalom, Birgit Klein and Thomas Beth
   9:30--10:00: A Logical Language for Specifying Cryptographic
        Protocol Requirements
          Paul Syverson and Catherine Meadows
  10:00--10:30: A Semantic Model for Authentication Protocols
          Thomas Woo and Simon Lam

11:00--12:00:   SYSTEMS: Virgil Gligor, Session Chair
  11:00--11:30: Detection and Elimination of Inference Channels
        in Multilevel Relational Database Systems
          X. Qian, M. Stickel, P. Karp, T. Lunt and
          T. Garvey
  11:30---12:00 Assuring Distributed Trusted Mach
          Todd Fine

12:00:  SYMPOSIUM ADJOURNS
```

- -

Symposium Registration: Dates strictly enforced by postmark.

Advance Member (to 4/12/93) $240*

Late Member (4/13/93-4/30/93) $290*

*Registration must include IEEE number to qualify.

Advance Non-Member $300
Late Non-Member $370

Advance Student $50
Late Student $50

Mail registration to:
Cristi Garvey
R2/2104
TRW Defense Systems Group
One Space Park
Redondo Beach, CA 90278
(310) 812-0566

****** ABSOLUTELY NO REGISTRATIONS BY EMAIL ******

Computers, Security and the Law

<kimble@minster.york.ac.uk>
Sat, 30 Jan 93 16:14:27

The University of York in the UK is running a two day conference on Computers, Security and the Law that may be of interest to the readers of COMP.RISKS. The programme for the conference follows. If you do not think this is a suitable place for this but know of somewhere that is perhaps you could forward it or let me know and I will do so.

FINAL PROGRAMME.
COMPUTERS: SECURITY AND THE LAW
31 March - 1 April 1993

The conference will be run by the Department of Computer Science in association with the Society for Computers & Law and the Licensing Executives Society .

The aim of the conference is to highlight some of the important legal issues that surround the use, and abuse, of computer technology in a way that should be accessible to the non-specialist, such as lawyers or computer scientists.

The target audience for the conference is senior management and those in both public and private sector organisations who wish to improve their knowledge about the legal aspects of buying, using or creating computer related products and services. The conference will be of interest to the police, the civil service, banks, insurance and building societies.

The programme will take place over two consecutive days. The first day will deal with the legal aspects of intellectual property rights, copyright and contract law as it relates to computer products and services. The second day will deal with the topics of computer crime and its prevention, security, data protection and privacy.

The conference dinner will be a Medieval Banquet at St William's College (founded in 1461). The keynote speaker will be Emma Nicholson, MP.

Proceedings of the conference will be published and be available to participants after the conference.

REGISTRATION AND FEES:

Delegates will be able to register for either of the two days separately if they wish. Fees: #275 for full conference, #165 for single day; a discount is available for early booking by 19th February 1993. (See application form for further details.

PROGRAMME: DAY ONE

0930 - 0950 Registration

0950 - 1000 Introduction. Chair: Dr Keith C Mander, Head of Department of Computer Science, University of York.

1000 - 1030 Overview of law relating to Intellectual Property Rights. Speaker: David Stanley, Licensing Executives Society.

Copyright Law, The Patent Law, The Law of Confidence, The Law of Designs, Trade Marks, Semiconductor regulations.

1030 - 1115 Intellectual Property Rights as they apply to computers. Speaker: John Sykes, Licensing Executives Society.

Hardware, software and firmware. Back-up copies, "Look and feel" - the limits to copyright protection, work created on a computer, work generated by a computer.

1145 - 1230 Acquisition of computers 1. Speaker: Geoff Allan, Independent Computer Consultant.

How does the acquisition process work?; documents involved - Invitation to Tender, Proposal, Specification; what are the legal ramifications and importance of these documents?

1415 - 1500 Acquisition of computers 2. Speaker: Dai Davis,
Society for Computers & Law.

The legal issues in acquisition contracts; payment triggers; bespoke software - escrow agreements, maintenance agreements.

1500 - 1545 Facilities Management Contracts. Speaker: Jane
Rawlings, Society for Computers & Law.

What is facilities management?; types of arrangements available; issues - software licensing and performance; response time, availability, confidentiality, employment, security and computer crime.

1615 - 1700 Review and discussion: a plenary session.
1900 - 2200 Conference Dinner: Keynote Speaker: Emma Nicholson, MP.

PROGRAMME: DAY TWO

0930 - 0950 Registration
0950 - 1000 Introduction. Chair: Dai Davis, Society for
Computers & Law.

1000 - 1045 Computer crime. Speaker: to be announced on the day.

Types of computer fraud, unauthorised access,, unauthorised modification, conspiracy to defraud, blackmail, fraud as theft, other offences.

1045 - 1130 "The Monday morning syndrome". Speaker: Dennis Jackson,
Computer Security Consultant, Staffordshire County Council.

The story of a real intrusion to a computer system and its world-wide ramifications.

1200 - 1245 Computer crime (Damage to programs or data).
Speaker: Dr Jan Hruska, Sophos Ltd.

What is a virus?; criminal damage; reckless damage; blackmail, common viruses.

1400 - 1445 Data Protection Act, Security & Privacy. Speaker:
Dr J N Woulds, Senior Assistant Registrar, Office of
the Data Protection Registrar.

Overview and Principles of the Act, legal requirements and constraints on computer users, supervision by the Registrar.

1445 - 1530 Security techniques. Speaker: John A Clark, CSE
Lecturer in Safety Critical Systems, University of York.

Physical, logical and procedural security; authentication and access control; accounting and intrusion detection; communications security; evaluation.

1530 - 1600 Review and discussion: a plenary session.

1600 Tea and depart.

FURTHER DETAILS FROM:

Conference Organiser: Francoise Vassie
Centre for Continuing Education
King's Manor, York, YO1 2EP
The University of York

Tel 0904 433900 Fax 0904 433906

or

E-Mail KIMBLE@UK.AC.YORK.MINSTER

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 31

Friday 5 February 1993

Contents

"Computer Blamed For Phone Jam"

<joe@cbcosmos.att.com>
Fri, 29 Jan 93 7:42:40 EST

from the 1/28/93 Columbus (Ohio) "Dispatch"

> by Ron Lietzke and Bruce Cadwallader
>
> A three-minute computer failure at an Ohio Bell central office disrupted phone service for 42,000 telephone lines in the Downtown business district for about 45 minutes yesterday morning. The computer problem cleared after a few minutes, but the disruption snowballed when a surge of callers seeking dial tones caused a telephone traffic jam of sorts, Ohio Bell spokesman David Kandel said.
>
> Outgoing and incoming calls on 15 Downtown prefixes were disrupted by the problem, which started at 9:42 AM. The Columbus police, the Franklin County Sherrif's Department, Columbus Public Schools, and state offices were among those disrupted by the outage, Kandel said.
>
> Callers in the affected prefix areas who dialed 911 could not reach Columbus police or the Franklin County Sherrif's office for at least 3 minutes. However, those agencies reported that they did not receive any complaints after the dial tones returned. "It was starting to clear itself within minutes, but because you're looking at such a huge volume of calls Downtown, it took the system time to recover," Kandel said. "The system was delivering a very, very slow dial tone."
>
> Problems started when one of two computer processors failed. The other took over, but it took about three minutes for it to retrieve the information from the failed processor, Kandel said. Ohio Bell technicians were working with the equipment manufacturer yesterday to determine what caused the processor to fail. It still was not working late yesterday. [...]
>
> Columbus police dispatchers reported having problems for about 30 minutes. Chief Deputy Robert Taylor of the sheriff's department said this radio room used cellular phones until the problem cleared. Neither department knew of any emergencies missed because of the computer problem. Columbus firefighters said they were receiving 911 calls throughout the period of disruption.

Two items of interest I note. One is that even a brief delay in grabbing data from the failed computer resulted in a large backlog. Perhaps the system was not designed to account for the large number of lines in downtown Columbus, which boomed during the 1980's. Phone systems tend to use less than state-of-the-art technology (to avoid many of the "bleeding edge" problems often noted here), but in this case, perhaps a faster processor or live mirroring of the data in question would have helped.

As to my second point, twice the article points out that nobody knew of any emergency calls that were missed, with the implication that no harm was done. Dead men tell no tales?

Joe Brownlee, Analysts International Corp. @ AT&T Network Systems 471 E Broad St, Suite 2001, Columbus, Ohio 43215 (614) 860-7461 joe@cbcosmos.att.com

BNFL prosecuted for unauthorised software changes

Martyn Thomas <mct@praxis.co.uk>
Thu, 4 Feb 93 15:48:16 GMT

According to Computing (4 Feb), British Nuclear Fuels Ltd is being prosecuted for making alleged unauthorised software changes to a safety mechanism on a shield door at Sellafield.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

Residues in a surplus bank computer

Fred Cohen <fc@turing.duq.edu>
Wed, 3 Feb 93 18:35:52 -0500

This one goes in the `When will they ever learn?' category:

I just got a call from a person who recently purchased a Unix based PC as junk from a bank, and low and behold, the computer was not cleaned before sale. How hard is it to break in? Not too! All you have to do is boot from a DOS floppy, run Norton Utilities or any similar tool, search for the `root:' part of the password file, and change that line to look like `root::0:1::/:'. Then you reboot from Unix and login as root with no password!

So that's too simple to be believed, but of course it works, and now comes the real problem. I am not sure it's illegal to use that data however you want! That's right, the computer crime laws don't cover computers that are not attached to any networks, aren't part of the banking system, etc. This system is no longer a banking computer, the data was sold along with the system to the new owner by the bank with no stipulations or warnings (as-is), and the new owner, as far as I can tell, has the right to use anything on the computer as their own.

It's a little upsetting that the bank didn't bother to do a secure deletion before giving all this data away (only about 120Mbytes worth of information on customers, etc.). How about the privacy of the customers of the bank? How about the EFT codes stored on-line! How about all the passwords that can now be guessed and exploited to enter the bank as if you were an employee? Oh well, anyone want to buy a used computer - no longer so cheap?

[Expletives deleted if there were expletives UNDELETED.
By the way, remember that the C2 Orange Book requirement is for deletion prior to initial assignment and reallocation. Somewhere there should be a requirement for deletion prior to permanent deallocation as well. PGN]

Re: Educational computer game banned (Shaun, RISKS-14.30)

<ghaas@informix.com>
Thu, 4 Feb 93 07:43:33 PST

With all due respect to Christina Kirby, the "Wizards" game is NOT a computer game. It is a pencil-and-paper game, like other adventure simulations. The students gain points by achieving goals in spelling (and perhaps other language-related tasks), and translate these points into progress around a game board. It bears a superficial resemblance to "Dungeons and Dragons," with magicians, wizards, a winged dragon, a pit -- symbols that some (fundamentalist) Christians equate with Satanism and/or disregard for Biblical symbolism. The symbols were the basis of the argument made against the game.

The teachers had two objections -- the issue of choice of instructional materials, and that of the way the District imposed the ban. One result of the uproar was a rewrite of the "Challenged Instructional Materials" policy. making the evaluation process much more accessible to the concerned public. Another was the motivation of a parent in the district who fought the ban to mount a (successful) run for a School Board seat last election, unseating an incumbent.

--Guy K. Haas (active in the MUSD since 1987)

Re: Clever Tactics Against Piracy (RISKS-14.30)

Gerd Meissner <100064.3164@compuserve.com>
03 Feb 93 04:28:01 EST

It might be interesting for readers who want to know more about the "Clever Tactics Against Piracy" (RISKS 14.30) that the story, including some technical details, was first published in the German news magazine DER SPIEGEL (#36, 1992, August 31st), titled "Trojanisches Pferd" (Trojan Horse). The company used a 12-digit key that looked like the serial number of the "free-demonstration coupon", which had to be printed out and sent back, to identify the pirated copies found on the "customers" machine and some details about the computer it was found on.

> [Mark Brader just reminded me in a different context
> of always looking a Trojan horse in the mouth. PGN]

Anecdotes Wanted on the Risks of Information Security

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Thu, 4 Feb 93 13:26:04 EST

I am seeking anecdotes of incidents where information security mechanisms or practices led to a problem (e.g., lost work or data, wasted time, down time, being locked out because of lost crypto keys or access tokens). I am also interested in descriptions of security features that are difficult to use and lead to problems. If you send me something, please indicate whether I can attribute it to you or you wish to remain anonymous.

Thanks,

Dorothy Denning denning@cs.georgetown.edu

Re: The FBI and Lotus cc:Mail (Joltes, RISKS-14.29)

Isaac Rabinovitch <ergo@netcom.com>
Sun, 31 Jan 1993 18:49:01 GMT

>Happily, the presenter said that Lotus refused to honor the FBI's request.
>Bravo!

Do not relax. So what if an official back door doesn't exist? Other federal agencies are more discreet than the FBI, and would consider "their" back door useless if any notice were taken of its existence. Furthermore, somebody is bound to see the profit in covertly adding a back door to a product and quietly selling it to individuals with a commercial interest in violation of privacy.

I checked with Lt. Colonel North, Admiral Yamamoto, and especially Captain Murphy, and they all agree: never assume a publically-accessible medium is secure just because it's encrypted!

ergo@netcom.com   Isaac Rabinovitch
{apple,amdahl,claris}!netcom!ergo   Santa Cruz, CA

The FBI and Lotus cc:Mail (Joltes, RISKS-14.29)

Roger D Binns <cs89rdb@brunel.ac.uk>
Mon, 1 Feb 93 11:47:57 GMT

: Happily, the presenter said that Lotus refused to honor the FBI's request.

Are you sure? Lotus could quite easily have honoured their request, and merely tell everyone they haven't. The FBI is happy, the consumer is happy. This brings to a mind a phrase 'ignorance is bliss'.

Roger

cs89rdb@brunel.ac.uk   Roger Binns   Brunel University - UK |

The FBI and Lotus cc:Mail

Bill Stewart +1-908-949-0705 <wcs@anchor.ho.att.com>
Tue, 2 Feb 93 12:52:36 EST

In RISKS 14.29, joltes@husc.harvard.edu reports that Lotus says that the FBI had asked them to place backdoors into Notes and cc:Mail, and they refused. Assuming that they told the truth, I'll second Dick's "Bravo!".

But one RISK here is that, without *sources*, it's hard to tell -
does Lotus provide sufficient documentation on file formats and encryption

algorithms that users can verify that the program does what it claims?

Bill Stewart, AT&T Bell Labs, Holmdel, NJ, wcs@anchor.att.com

> [Even WITH sources it can be hard to tell. Recall Ken Thompson's
> C-compiler Trojan horse in which there were no changes to the
> source code of either the C compiler or the UNIX login routine. PGN]

Re: The FBI and Lotus cc:Mail (Joltes, RISKS-14.29)

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Fri, 29 Jan 93 13:34:41 EST

In RISKS-14.29, Dick Joltes said the following about a presentation he attended on Lotus Notes and the response of the Lotus representative to a question about how the encryption was done:

> The presenter said that the data was considered very secure, so much so that the FBI had approached Lotus to ask that a "back door" be left in the software in order to give the Bureau a method for infiltrating suspects' filesystems. She said they were specifically targeting "drug dealers and other bad people."
>
> Given this backdoor, what was to stop the Bureau from inspecting confidential materials on any system? The risks seem obvious. ...

There are, in fact, very good controls to stop the FBI or any other law enforcement agency from doing this. They're called warrants. In order to execute a search and seizure on any system, the government needs to have a court order. To get a court order, they have to demonstrate that there is probable cause that a crime has been commited. Neither the FBI nor any other law enforcement agency is allowed to "infiltrate" someone's system and poke around to see what's there.

The "obvious" risk here is not from the government. If the government is unable to break through the crypto or get the key, they may be unable to obtain evidence needed to prosecute someone who has commited a crime. This is potentially a very serious problem, especially as records become more heavily computerized.

> Happily, the presenter said that Lotus refused to honor the
> FBI's request. Bravo!

Encryption of files and communications is going to make it much more difficult, and in some cases impossible, for law enforcers to get evidence needed for conviction. Unless we want a society with greater crime, we need to find some way of meeting both our needs for information security and our needs for law enforcement. Then we can cheer.

Dorothy Denning

Professor & Chair, Computer Science, Georgetown University

Re: The FBI and Lotus cc:Mail

<joltes@husc.harvard.edu>
Mon, 1 Feb 93 14:16:33 EST

Dorothy Denning, responding to my posting regarding cc:Mail, says:

> There are, in fact, very good controls to stop the FBI or any other law
> enforcement agency from doing this. They're called warrants. In order
...
> the FBI nor any other law enforcement agency is allowed to "infiltrate"
> someone's system and poke around to see what's there.

The key word here is "allowed." As we've seen with such scandals as Watergate and Iran-Contra, what is allowed by law and what is actually done sometimes are two different things. What is to stop an agency from conducting an initial covert search of a person or corporation's records, then requesting the warrant after they find questionable or illegal material?

Dorothy's comments presuppose that all operatives within all governmental bodies are completely honest. While I would say that a majority of these workers are honest, the risk that some are not makes the presence of known back doors in supposedly "secure" software a highly questionable situation.

> The "obvious" risk here is not from the government. If the government
> is unable to break through the crypto or get the key, they may be
> unable to obtain evidence needed to prosecute someone who has commited
> a crime. This is potentially a very serious problem, especially as
> records become more heavily computerized.

Certainly it is. However, we must evaluate whether the risks to the public at large outweigh the advantage of having such back doors available to legitimate authorities. What if the codekey sequence used to activate the alternative access method became known due to a security leak (disgruntled Lotus employee or government agent, espionage, etc)? Lotus would then need to issue a binary patch to change the codekey (at their expense, no doubt). Customer confidence in the product would sag and businesses would begin to question the security of their own supposedly encrypted software.

If I were running a business and knew that a product I was evaluating had a built-in back door, it would end my interest in the product.

> Encryption of files and communications is going to make it much more
> difficult, and in some cases impossible, for law enforcers to get
> evidence needed for conviction. Unless we want a society with greater
> crime, we need to find some way of meeting both our needs for
> information security and our needs for law enforcement. Then we can
> cheer.

My cheer was in regard to Lotus' refusal (well, they *said* they refused) to blindly install a security hole in their most successful product simply because a government agency said "please do it." Knowing that acquiescence to such a demand was a violation of the trust placed in Lotus products by their customers, they did the "right thing" and said "no."

I agree that some balance needs to be stuck, but the scales must not be tilted to the needs of law enforcement at the expense of the public. Given some recent incidents (such as "Operation Sun Devil," which nearly put a legitimate business into bankruptcy due to the actions of paranoid and uninformed agents) it seems obvious to me that few Federal agencies currently possess the basic skills needed to differentiate between criminals and "fringe groups" such as gamers and hackers whose participation in society is outside the "norm" of American experience.

The subject of "Computing and the Law" is one that is just beginning to make an impact on society, and both the public and the government need to feel through the tangle of issues that surround it. We must not make the mistake of infringing on privacy simply to deter crime, since this will establish legal precedents that could easily become Draconian in their use if unchecked.

Dick Joltes, Harvard University Science Center   joltes@husc.harvard.edu
Hardware & Networking Manager, Computer Services   joltes@husc.bitnet

---

Re: The FBI and Lotus cc:Mail

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Wed, 3 Feb 93 12:03:53 EST

Dick Jotes, responding to my response to his post on cc:Mail, says:

> The key word here is "allowed." As we've seen with such scandals as Watergate and Iran-Contra, what is allowed by law and what is actually done sometimes are two different things. What is to stop an agency from conducting an initial covert search of a person or corporation's records, then requesting the warrant after they find questionable or illegal material?
>
> Dorothy's comments presuppose that all operatives within all governmental bodies are completely honest. While I would say

I do not assume that everyone in government is totally honest. Rather, I acknowledge that the American system of government has extensive mechanisms to protect against abuses, including the illegality of breaking into someone's system or conducting a search without a warrant, Congressional oversight committees and hearings, and the use of the media to expose abuses.

> What if the codekey sequence used to activate the alternative access method became known due to a security leak (disgruntled Lotus employee or government agent, espionage, etc)? Lotus would then need to issue a binary patch to change the codekey (at their expense, no doubt). Customer confidence in the

> product would sag and businesses would begin to question the security of their own supposedly encrypted software.

Customer confidence is an important concern, but since we don't know exactly what the FBI requested of Lotus, we don't know what vulnerabilities might exist and whether businesses would accept whatever risks might be present.

> I agree that some balance needs to be stuck, but the scales must not be tilted to the needs of law enforcement at the expense of the public. Given some recent incidents (such as

The public needs law enforcement. This is not the public vs. law enforcement.

> "Operation Sun Devil," which nearly put a legitimate business into bankruptcy due to the actions of paranoid and uninformed

If you're referring to Steve Jackson Games, it was not part of the Sun Devil investigation (which was about toll fraud and credit card fraud).

> agents) it seems obvious to me that few Federal agencies currently possess the basic skills needed to differentiate between criminals and "fringe groups" such as gamers and hackers whose participation in society is outside the "norm" of American experience.

Please don't make such sweeping generalizations based on one case or even a few. There have been hundreds (probably thousands) of cases that have been handled extremely well.

> The subject of "Computing and the Law" is one that is just beginning to make an impact on society, and both the public and the government need to feel through the tangle of issues that surround it. We must not make the mistake of infringing on privacy simply to deter crime, since this will establish legal precedents that could easily become Draconian in their use if unchecked.

I agree that this is a difficult issue that needs to be sorted out. I also argue that we need to find ways to satisfy both our need to control crime and our need for privacy & security. None of these needs will be or indeed can be satisfied in an absolute way. The challenge is to find ways that keep the risks at acceptable levels.

Dorothy Denning

Re: The FBI and Lotus cc:Mail

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Thu, 4 Feb 93 16:39:43 EST

I talked with a knowledgeable person in FBI Headquarters whom I know and trust about the claim that they asked Lotus to put a "back door" into the encryption system of Notes. He was confident that Headquarters had not made any such request of Lotus and was surprised to hear about it. He did not know if someone in one of the field offices might have asked Lotus for help in conjunction with a specific investigation.

Dorothy Denning

Re: The FBI and Lotus cc:Mail

<joltes@husc.harvard.edu>
Fri, 5 Feb 93 9:16:39 EST

There should be additional information on its way to RISKS about this subject (from another source). Employees of Lotus were involved in meetings with the FBI held under the auspices of the EFF over the past 18 months. Several proposed bills were discussed and tabled. We have it from one of the employees who was actually involved.

It is not surprising that Dorothy's source knew nothing (if true) of the contacts. Stratification and compartmentalization within federal organizations is not uncommon, with the result that groups within the same agency do not know of the activities of others.

Dick Joltes joltes@husc.harvard.edu

With Regard to Lotus Notes and the FBI...

Peter Wayner <pcw@access.digex.com>
Tue, 2 Feb 1993 23:36:50 -0500

{This is the text of a letter to me from Ray Ozzie, one of the developers of Lotus Notes. He said it was okay to forward this to comp.risks to clarify the recent posting about the FBI's involvement with Lotus. I believe that the details of the interaction are much less ominous in this rendition and more importantly it comes from the head developer's mouth. -PCW}

The message entitled "The FBI and Lotus cc:Mail" is not entirely correct, although it is correct "in spirit".

As one of the developers of Notes, I have represented Lotus twice regarding FBI proposals. In the first (about 18 months ago), the FBI was trying to persuade Congress to pass a law requiring communication service providers to deliver the original plain text of messages entering their systems, in essence requiring us to install a back door. Lotus was not approached by the FBI - rather, the EFF learned of the bill and asked me to participate in a round-table discussion with lawmakers and others from the telecommunications and computer industries. The bill was tabled shortly thereafter.

Last year, we again participated in several discussions with the FBI related to a new proposal that would have required manufacturers of communication equipment and services to modify their products (in this case, Lotus Notes) to be able to, on demand and in a timely fashion and from a single access point, grant the FBI access to communications. This new law would not require us to install a backdoor, that is, they took the issue of encryption off the table, but would instead require us to install logic into our message routers to disable dynamic adaptive least-cost path routing and also to disable code that breaks messages into packets for transmission on different virtual circuits. It would also require us to put logic into the message routers to deliver copies of messages to a central monitoring point from anywhere in the network. This FBI plan has also been tabled.

If it weren't for the Electronic Frontier Foundation, we never would have had a chance to participate. EFF and the CPSR are providing a great service for our industry, which has a pitifully small lobbying presence in Washington. Neither Lotus nor Lotus Notes was singled out by the FBI, rather, I represented Lotus voluntarily in order to defend Lotus' commercial interests. Additionally, I was compelled to attend because I believe very, very strongly in my right to privacy as a US citizen.

On the other hand, the FBI has a very difficult job to do, and with the onslaught of technology, it fears that it may soon lose its longstanding authority to carry out court-ordered wiretaps. Valid wiretaps - ones that you would probably agree with. From their perspective, why can't a technical solution be found to what appears to be a technical problem?

From my perspective, though, the cat's out of the bag. It's already very easy for the average joe to do effectively unbreakable end-to-end encryption of messages on standard PC hardware. Passing laws won't stop bad guys from using encryption, so these laws will just have the effect of increasing the cost of every mail system, every PBX, every LAN router, every cellular phone, and so on. Not to say what the laws will do to your privacy.

Think about it. And then call the EFF.

Anyone can get your U. of Illinois transcript

Carl M. Kadie <kadie@cs.uiuc.edu>
Sun, 24 Jan 1993 17:47:45 GMT

If you are a student at U. of Illinois, you should know that anyone who knows your social security number and birthday can now see your official transcript. To add insult to injury, if someone does looks at your transcript, *you* will be charged a $5 transcript fee.

The administration building, room 100, now has three computer terminals. Anyone can walk up to one and type
 1) a social security number
 2) a birthday
 3) an address

If the social security number and birthday match a current student, that student's transcript will be send to the address and that student's account will be charged $5.

At the very least, check your university bill. It seems that your only protection is your ability to track down the destination address of an improperly send transcript (assuming the university keeps a record of these addresses).

- Carl Kadie   = kadie@cs.uiuc.edu =

Phone Company Cleverness

Jon Leech <leech@cs.unc.edu>
25 Jan 1993 21:00:58 GMT

Seen on page 2 (e.g. the part most people throw out) of this month's bill from Southern Bell:

```
  "Call RightTouch(R) service [to do various things such as
   disconnecting your phone or ordering extra-cost services]
   ....
   Please protect your access code: ####"
                 ^ actual 4-digit code printed here
```

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 32

Friday 5 February 1993

Contents

[TDR] Programmer Licensing

"Tansin A. Darcos & Company" <0005066432@mcimail.com>
Thu, 4 Feb 93 03:45 GMT

Al Underwood asked about the possibility of Government Computer Professional Certification, otherwise known as Programmer Licensing. A famous philosopher referred to it as "Guild Socialism," i.e. that in exchange for their group providing some needed service, their group must be the only one allowed to perform it. Doctors, Lawyers, Electricians, Plumbers and others got their practices set up so that any involvement in them by persons who are not licensed by their guild becomes a criminal offense. That some of these activities may be hazardous by persons not trained in the particular practice in question may be the reasoning behind the requirements, but in every case, the actual practice of licensing is used to protect those in that particular guild from competition. Doctors keep out people from foreign countries. Lawyers use it to keep people from dispensing information about minor matters such as bankruptcy, or use it as a club to threaten people, and so on.

I remember that New Jersey was planning to do this a couple of years ago. I made a big stink on any forum I could find in the computer world (I did not know of many Internet lists at that time, so I could only complain on one or two) and sent out messages on the BBS networks I could get access to, in order to warn people about this.

When certification is done at the mandatory level, i.e. you must have a license to practice the certified occupation or you can be charged with a criminal act, it gives to private parties the power of the State to decide what is or is not satisfactory performance. It can be prostituted in all sorts of ways depending on the political agenda of the people who are involved.

1. License fees could be anything from $10 to $2000 a year depending on what the board wants to set the fees at. If you can't afford the fee, that's too bad, you're out of the business.

2. License boards generally grandfather the law: anyone who claims to be working in that particular field at the time the law is in effect is granted an automatic license. Therefore the license rule serves to do just one thing: raise money for the licensing board and begin to weed out those who either weren't around when the licensing started or could not afford the fees. This can also be used as a hidden tax, by, for example, budgeting $100,000 for the license bureau, while setting the tax to take in $1.1 or $2.1 million, thus using the law to raise an extra 2 mil for revenue hungry state legislatures.

3. The license boards conceivably can decide what is or isn't valid practice in a particular occupation. A Programmer Licensing Board, or "Software Engineers Quality Control Board" or whatever it is called, can decide, for example, that the use of the "GOTO" is no longer permitted, or the COBOL ALTER, or some other language construct, and make use of the proscribed method grounds for someone to lose their license.

4. One state can set standards such that its requirements become effective beyond its borders. It's noted there is a man who is a lawyer in California who has to come back into DC to defend his license to practice over an issue that allegedly was settled, because if the DC Bar revokes his license all the other states will.

5. If someone writes opinions which are unflattering of a License Board or take an unpopular stance on an issue, the License Control Board can, using item 3 above, take someone's license away by changing the standard in a way that the person cannot meet it and thus loses his license. For a fictional example of how this could be prostituted into requiring almost everyone in a particular guild to become an indentured servant of a particular company, read the short story "Magic, Inc." by Robert A. Heinlein. It's usually in a combined story of "Waldo, and Magic, Inc," where two related short stories are combined.

6. A computer program is the creation of the mind of an individual, and as such is "a figment of the imagination" since a computer program has no physical apportation other than as bits on disk, which are no different from any other bits. As such, a computer program is a form of writing. I question whether a law requiring someone to have a license in order to write something would stand challenge in the United States on 1st Amendment grounds of prior

restraint. I do not know if someone has ever tried to license reporters in order to show that they know how to write and spell and use English correctly; whether such would withstand court scrutiny is an interesting question. But a law that allowed a reporter to lose his license if a government agency decided he is not qualified would be so offensive to the first amendment that a court wouldn't even consider arguments over the intended "improvement" of the reporters guild such a law would attain. Requiring reporters to know their subject matter in order to write about it would certainly make them better writers. It also would certainly be unconstitutional.

7. There is generally a shortage of talented computer people. A law requiring licensing of programmers (or 'software engineers' or whatever it is) would not fix the problem and would only exacerbate it and might make things worse since everyone currently working can be grandfathered, some places might have to hire incompetents because the supply of quality people is dried up.

8. Some companies have gone to training their own people in order to make up for a famine of supply. If the laws require that you can only enter the field after a four year degree from an accredited university, there goes the space for opening level people and the chance for a company to 'grow their own.'

9. Cutting people's appendixes for free is still 'practicing medicine'. Fighting a traffic ticket (where traffic offenses are still crimes) is still 'practicing law'. Doing these things for someone else, even if for free, is still performing a licensed occupation which is a crime. What does this do to the shareware world of people who write programs on spec for others to try and use and pay for if they like them?

10. A few years ago the Food and Drug Administration busted into a warehouse and seized thousands of gallons of contraband orange juice. Because it was unfit for human consumption? Because it was contaminated? Because there was a danger to the public? Because the agency didn't like the label on it and wanted that particular processor - Proctor and Gamble - to comply with a standard that it was not requiring of 300 other orange juice processors. When P&G said that if the EPA would evenly enforce the law on everyone they would go along, the EPA decided to seize the packages. What this has to do with the licensing of software people is slightly related to #9. If someone is writing software for a company and doesn't have a license, can the software be seized? If the person has a license where the program is made but not in other states? (You can't practice medicine or law or engineering in states not licensed.) If the program is transported from a state not requiring a license to create software to one where on is, can the product be seized for noncompliance? The product was produced by an unlicensed person in a state where licensing is required. In some states if you order a stock not registered in that state

    and then decide to change your mind and not buy it, the broker
    cannot force you to pay for it because of mandatory registration
    of stock issues. Could not the same thing be done for
    computer programs or the creators of same?

These and perhaps other points come up in the licensing of software professionals; the dangers to the people who make this stuff, and perhaps dangers to the public.

I have heard that the reason it was killed was because (1) the software industry didn't want it; (2) Bell Labs, in New Jersey, was upset when the estimated license fees for all of the people who worked there would cost the company more than $1,000,000.

Apparently some legislator in New Jersey proposed this law without asking anyone either in the industry or in its customers, if anyone even wanted it.

Paul Robinson -- TDARCOS@MCIMAIL.COM

[Also, see RISKS-13.13 and 15, CACM Inside RISKS Feb 91]

**** pointer-> Injured using Computer Pointing Device?: READ THIS ****

Pete W. Johnson <petej@garnet.berkeley.edu>
2 Feb 1993 04:03:04 GMT

This is a pointer to a basenote and discussion pertaining to computer pointing device injuries (mouse, trackballs, puck, stylus, etc.) in sci.med.occupational. For convenience I have included a copy of the basenote below. To follow net etiquette, please direct all responses to the basenote below in sci.med.occupational notesgroup ONLY.

=-=
(Copy of Basenote)

This note (which is being posted monthly) is for anyone that has been injured using a computer pointing device (mouse, trackball, puck, tablet, etc.). I have been assisting computer operators who have been injured using pointing devices for the past 4 years. I am now presently doing research at the University of California's (San Francisco and Berkeley's) Ergonomics Lab on the design of computer pointing devices with the goal of reducing injuries associated with their use. In order to do this, I need to collect information on pointing device design characteristics (button design, button force, device size, device shape, etc.) that are important in minimizing and/or reducing the physical stresses operators are subjected to. Some of this information will be collected through my laboratory research, but a major and important source of information has to come from operators like yourself. I need to collect all the information I can from computer operators that have been injured as a result of pointing device use.

In order to do this, I need your help. If you have been injured using a

pointing device, I would appreciate it if you would send me a note with
information pertaining to your injury. I would like the information e-
mailed directly to me (petej@garnet.berkeley.edu). The format I would
like the information sent to me is as follows, fill in as much as you
can:

 1) NAME: (optional)
 2) COMPANY: (optional)
 3) PHONE #: (optional)
 4) NUMBER OF HOURS SPENT IN FRONT OF THE COMPUTER PER DAY:
 5) PERCENTAGE OF TIME SPENT USING A POINTING DEVICE:
 6) MANUFACTURER OF COMPUTER AND MODEL NUMBER:
 7) POINTING DEVICE USED AT TIME OF INJURY: (Please be specific)
     a) MANUFACTURER
     b) MODEL OR PART NUMBER
     c) DESCRIPTION OF DEVICE
 8) PRIMARY SOFTWARE APPLICATION USED AT THE TIME OF YOUR INJURY
 9) TYPE OF INJURY
10) WHAT YOU THINK CAUSED YOUR INJURY
11) IF INJURY IS RESOLVED OR YOUR CONDITIONS HAVE IMPROVED, WHAT CHANGES
    WERE MADE (This is probably the most beneficial information)

    -

My intent is to enter this information into a database in order to
gather information and look for trends. Each month I will share
relevant information by posting a monthly summary in
sci.med.occupational similar to what has been done with keyboard
information. If you are presently experiencing problems, feel free to
call me (510/231-9405) and I will share with you what I know. I am also
open for suggestions, please post responses to this basenote or e-mail
me if you have any further suggestions or input.

If your company has internal bulletin boards, please post this note or
provide a pointer telling your co-workers about this basenote in the
sci.med.occupational newsgroup. I will be also be posting a pointer to
this basenote in comp.risks, comp.human-factors, and sci.med as well.

Finally, if you have any opinions or inputs on a particular pointing
device or pointing device design in general, send me a note or call me.
Our lab is assisting some of the major pointing device manufacturers
with the design of their pointing devices. If you have some inputs for a
particular company, I will be happy to direct them to the appropriate
person.

Thanks for your help.

Peter W. Johnson
                        (End of Basenote)

Suggestions for a hi-tech crime-investigators' seminar ??

Jim Warren <jwarren@autodesk.com>
Thu, 4 Feb 93 14:01:53 PST

I have been invited to give (or organize) a 4-hour seminar presenting civil liberties perspectives and concerns to a group of 40-60 high-tech criminal investigators on the first day of the HTCIA Northern California 3-day workshop in April (High Tech Criminal Investigators Association). They are expecting attendees from Nor Cal and from beyond. My understanding is that most of the members are sworn peace officers who are specializing in investigating high-tech crime; a minority are corporate and agency computer security officers. Most will attend the seminar (only one seminar per time-period).

I see it as an *outstanding* opportunity to
(a) open [more] communication channels between in-the-trenches law enforcement officials and civlibbies,
(b) learn more of their concerns and problems,
(c) enhance the chances of additional similar and expanded exchanges at future law-enforcement meetings through *nonconfrontational*, well-informed, candid discourse, and
(d) better inform law enforcement folks of the complexities, styles and trade-offs in "cyberspace," and their ramifications for law enforcement's legitimate and significant concerns.
[And -- heh! -- it will give "them" a chance to harangue "us" civlib types; equitable role-reversal for those cops who have entered the lion's den by attending any of the Computers, Freedom & Privacy conferences of the last several years.]

I have invited an attorney who is specializing in these issues to join me in organizing and presenting this seminar, and am in hopes that her organization will support her participation. She has been closely monitoring related legislation in Washington, DC, and has also been directly involved in a major computer-search case currently being litigated in Texas.

Query/request:
I have a number of ideas for topics and perspectives to present/cover, and have several documents I plan to provide as handouts. But, I am very-much interested in receiving suggestions and/or papers/handouts that might be appropriate for presentation/distribution at a regional meeting of high tech criminal investigators [long on meat; short on emotion and opinion, please].
Please forward comments, suggestions and copies (ideally e-copies for reformatting and printing in a combined handout, including a note permitting reproduction for this purpose). [Confidentiality of sources and suggestors will be protected, upon request.]

--jim   [forward or post elsewhere, as desired]
Jim Warren, 345 Swett Rd., Woodside CA 94062; 415-851-7075
jwarren@well.sf.ca.us -or- jwarren@autodesk.com
[for identification purposes only: founder and Chair, 1991 First Conference on Computers, Freedom & Privacy; a recipient, 1992 Electronic Frontier Foundation Pioneer Awards; "futures" columnist, MicroTimes; member, Autodesk Bd.of Dirs.]

Revised Computer Crime Sentencing Guidelines

Dave Banisar <banisar@washofc.cpsr.org>
Sat, 30 Jan 1993 15:12:11 EST

>From Jack King (gjk@well.sf.ca.us)

The U.S. Dept. of Justice has asked the U.S. Sentencing Commission to promulgate a new federal sentencing guideline, Sec. 2F2.1, specifically addressing the Computer Fraud and Abuse Act of 1988 (18 USC 1030), with a base offense level of 6 and enhancements of 4 to 6 levels for violations of specific provisions of the statute. The new guideline practically guarantees some period of confinement, even for first offenders who plead guilty.

For example, the guideline would provide that if the defendant obtained ``protected'' information (defined as ``private information, non-public government information, or proprietary commercial information), the offense level would be increased by two; if the defendant disclosed protected information to any person, the offense level would be increased by four levels, and if the defendant distributed the information by means of ``a general distribution system,'' the offense level would go up six levels.

The proposed commentary explains that a ``general distribution system'' includes ``electronic bulletin board and voice mail systems, newsletters and other publications, and any other form of group dissemination, by any means.''

So, in effect, a person who obtains information from the computer of another, and gives that information to another gets a base offense level of 10; if he used a 'zine or BBS to disseminate it, he would get a base offense level of 12. The federal guidelines prescribe 6-12 months in jail for a first offender with an offense level of 10, and 10-16 months for same with an offense level of 12. Pleading guilty can get the base offense level down by two levels; probation would then be an option for the first offender with an offense level of 10 (reduced to 8). But remember: there is no more federal parole. The time a defendant gets is the time s/he serves (minus a couple days a month "good time").

If, however, the offense caused an economic loss, the offense level would be increased according to the general fraud table (Sec. 2F1.1). The proposed commentary explains that computer offenses often cause intangible harms, such as individual privacy rights or by impairing computer operations, property values not readily translatable to the general fraud table. The proposed commentary also suggests that if the defendant has a prior conviction for ``similar misconduct that is not adequately reflected in the criminal history score, an upward departure may be warranted.'' An upward departure may also be warranted, DOJ suggests, if ``the defendant's conduct has affected or was likely to affect public service or confidence'' in ``public interests'' such as common carriers, utilities, and institutions. Based on the way U.S. Attorneys and their computer experts have guesstimated economic "losses" in a few prior cases, a convicted tamperer can get whacked with a couple of years in the slammer, a whopping fine, full "restitution" and one to two years of supervised release (which is like going to a parole officer). (Actually, it *is* going to a parole officer, because although there is no more federal parole, they didn't get rid of all those parole officers. They have them supervise convicts' return to society.)

This, and other proposed sentencing guidelines, can be found at 57 Fed Reg 62832-62857 (Dec. 31, 1992).

The U.S. Sentencing Commission wants to hear from YOU. Write: U.S. Sentencing Commission, One Columbus Circle, N.E., Suite 2-500, Washington DC 20002-8002, Attention: Public Information. Comments must be received by March 15, 1993.

* * *

Actual text of relevant amendments:

UNITED STATES SENTENCING COMMISSION
AGENCY: United States Sentencing Commission.
57 FR 62832

December 31, 1992

Sentencing Guidelines for United States Courts

ACTION: Notice of proposed amendments to sentencing guidelines, policy statements, and commentary. Request for public comment. Notice of hearing.

SUMMARY: The Commission is considering promulgating certain amendments to the sentencing guidelines, policy statements, and commentary. The proposed amendments and a synopsis of issues to be addressed are set forth below. The Commission may report amendments to the Congress on or before May 1, 1993. Comment is sought on all proposals, alternative proposals, and any other aspect of the sentencing guidelines, policy statements, and commentary.

DATES: The Commission has scheduled a public hearing on these proposed amendments for March 22, 1993, at 9:30 a.m. at the Ceremonial Courtroom, United States Courthouse, 3d and Constitution Avenue, NW., Washington, DC 20001.

Anyone wishing to testify at this public hearing should notify Michael Courlander, Public Information Specialist, at (202) 273-4590 by March 1, 1993.

Public comment, as well as written testimony for the hearing, should be received by the Commission no later than March 15, 1993, in order to be considered by the Commission in the promulgation of amendments due to the Congress by May 1, 1993.

ADDRESSES: Public comment should be sent to: United States Sentencing Commission, One Columbus Circle, NE., suite 2-500, South Lobby, Washington, DC 20002-8002, Attention: Public Information.

FOR FURTHER INFORMATION CONTACT: Michael Courlander, Public Information Specialist, Telephone: (202) 273-4590.

* * *

59. Synopsis of Amendment: This amendment creates a new guideline applicable to violations of the Computer Fraud and Abuse Act of 1988 (18 U.S.C. 1030). Violations of this statute are currently subject to the fraud guidelines at S. 2F1.1, which rely heavily on the dollar amount of loss caused to the victim. Computer offenses, however, commonly protect against harms that cannot be adequately quantified by examining dollar losses. Illegal access to consumer credit reports, for example, which may have little monetary value, nevertheless can represent a serious intrusion into privacy interests. Illegal intrusions in the computers which control telephone systems may disrupt normal telephone service and present hazards to emergency systems, neither of which are readily quantifiable. This amendment proposes a new Section 2F2.1, which provides sentencing guidelines particularly designed for this unique and rapidly developing area of the law.

Proposed Amendment: Part F is amended by inserting the following section, numbered S. 2F2.1, and captioned "Computer Fraud and Abuse," immediately following Section 2F1.2:

"S. 2F2.1. Computer Fraud and Abuse

(a) Base Offense Level: 6

(b) Specific Offense Characteristics

(1) Reliability of data. If the defendant altered information, increase by 2 levels; if the defendant altered protected information, or public records filed or maintained under law or regulation, increase by 6 levels.

(2) Confidentiality of data. If the defendant obtained protected information, increase by 2 levels; if the defendant disclosed protected information to any person, increase by 4 levels; if the defendant disclosed protected information to the public by means of a general distribution system, increase by 6 levels.

Provided that the cumulative adjustments from (1) and (2), shall not exceed 8.

(3) If the offense caused or was likely to cause

(A) interference with the administration of justice (civil or criminal) or harm to any person's health or safety, or

(B) interference with any facility (public or private) or communications network that serves the public health or safety, increase by 6 levels.

(4) If the offense caused economic loss, increase the offense level according to the tables in S. 2F1.1 (Fraud and Deceit). In using those tables, include the following:

(A) Costs of system recovery, and

(B) Consequential losses from trafficking in passwords.

(5) If an offense was committed for the purpose of malicious destruction or damage, increase by 4 levels.

(c) Cross References

(1) If the offense is also covered by another offense guideline section, apply that offense guideline section if the resulting level is greater. Other guidelines that may cover the same conduct include, for example: for 18 U.S.C. 1030(a)(1), S. 2M3.2 (Gathering National Defense Information); for 18 U.S.C. 1030(a)(3), S. 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft), S. 2B1.2 (Receiving, Transporting, Transferring, Transmitting, or Possessing Stolen Property), and S. 2H3.1 (Interception of Communications or Eavesdropping); for 18 U.S.C. 1030(a)(4), S. 2F1.1 (Fraud and Deceit), and S. 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft); for 18 U.S.C. S. 1030(a)(5), S. 2H2.1 (Obstructing an Election or Registration), S. 2J1.2 (Obstruction of Justice), and S. 2B3.2 (Extortion); and for 18 U.S.C. S. 1030(a)(6), S. 2F1.1 (Fraud and Deceit) and S. 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft).

Commentary

Statutory Provisions: 18 U.S.C. 1030(a)(1)-(a)(6)

Application Notes:

1. This guideline is necessary because computer offenses often harm intangible values, such as privacy rights or the unimpaired operation of networks, more than the kinds of property values which the general fraud table measures. See S. 2F1.1, Note 10. If the defendant was previously convicted of similar misconduct that is not adequately reflected in the criminal history score, an upward departure may be warranted.

2. The harms expressed in paragraph (b)(1) pertain to the reliability and integrity of data; those in (b)(2) concern the confidentiality and privacy of data. Although some crimes will cause both harms, it is possible to cause either one alone. Clearly a defendant can obtain or distribute protected information without altering it. And by launching a virus, a defendant may alter or destroy data without ever obtaining it. For this reason, the harms are listed separately and are meant to be cumulative.

3. The terms "information," "records," and "data" are interchangeable.

4. The term "protected information" means private information, non-public government information, or proprietary commercial information.

5. The term "private information" means confidential information (including medical, financial, educational, employment, legal, and tax information) maintained under law, regulation, or other duty (whether held by public agencies or privately) regarding the history or status of any person, business, corporation, or other organization.

6. The term "non-public government information" means unclassified

information which was maintained by any government agency, contractor or agent; which had not been released to the public; and which was related to military operations or readiness, foreign relations or intelligence, or law enforcement investigations or operations.

7. The term "proprietary commercial information" means non-public business information, including information which is sensitive, confidential, restricted, trade secret, or otherwise not meant for public distribution. If the proprietary information has an ascertainable value, apply paragraph (b) (4) to the economic loss rather than (b) (1) and (2), if the resulting offense level is greater.

8. Public records protected under paragraph (b) (1) must be filed or maintained under a law or regulation of the federal government, a state or territory, or any of their political subdivisions.

9. The term "altered" covers all changes to data, whether the defendant added, deleted, amended, or destroyed any or all of it.

10. A "general distribution system" includes electronic bulletin board and voice mail systems, newsletters and other publications, and any other form of group dissemination, by any means.

11. The term "malicious destruction or damage" includes injury to business and personal reputations.

12. Costs of system recovery: Include the costs accrued by the victim in identifying and tracking the defendant, ascertaining the damage, and restoring the system or data to its original condition. In computing these costs, include material and personnel costs, as well as losses incurred from interruptions of service. If several people obtained unauthorized access to any system during the same period, each defendant is responsible for the full amount of recovery or repair loss, minus any costs which are clearly attributable only to acts of other individuals.

13. Consequential losses from trafficking in passwords: A defendant who trafficked in passwords by using or maintaining a general distribution system is responsible for all economic losses that resulted from the use of the password after the date of his or her first general distribution, minus any specific amounts which are clearly attributable only to acts of other individuals. The term "passwords" includes any form of personalized access identification, such as user codes or names.

14. If the defendant's acts harmed public interests not adequately reflected in these guidelines, an upward departure may be warranted. Examples include interference with common carriers, utilities, and institutions (such as educational, governmental, or financial institutions), whenever the defendant's conduct has affected or was likely to affect public service or confidence".

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 33

Thursday 18 February 1993

Contents

Cable freeloaders

Tony Scandora 708-252-7541 <SCANDORA@cmt.anl.gov>
Mon, 8 Feb 1993 12:43:14 -0600 (CST)

Continental Cablevision of Hartford broadcast a special offer of a free T-shirt during last fall's Holyfield/Bowe fight (14Nov92). Unlike most pay-per-view broadcasting, this one did not show up through legitimate decoders. The ad and its 800 number only showed up when watched through illegal decoders. 140 freeloaders called the 800 number within minutes of the ad's broadcast. Continental sent the T-shirts by certified, return receipt mail, and then sent them a followup letter reminding them of the federal law (fines up to $10,000) and demanding a $2000 fine. [Chicago Tribune, 3 Feb 1993]

Tony Scandora, Argonne National Lab, 708-252-7541
scandora@cmt.anl.gov or scandora@anlcmt.bitnet

[Also noted by abg@beowulf.EPM.ORNL.GOV (Alex L. Bangs) in Newsweek, Feb 15, 1993 ("A Technical Knockout" -- Periscope) and mcclella@yertle.Colorado.EDU (Gary McClelland). Sorry for the long delay in getting this issue out. It was unavoidable. PGN]

Esperanto from a computer error

Philip Brewer <pbrewer@urbana.mcd.mot.com>
Mon, 08 Feb 93 08:36:36 CST

The following appeared in the November issue of _Esperanto_, the publication of the Universal Esperanto Association. (This is my translation from the original Esperanto.)

> Portugal: Esperanto from a computer error

> Hans Jankowski (German) was pleasantly surprised when a money-changing
> machine from the bank "Totta and Acores" in the Lisbon airport gave
> him his receipt in Esperanto. Because the Portuguese Esperanto
> Association was also surprised, Antonio Martins decided to explore.
> It seems that this was probably an error in setting up the computer:
> on installation of the ten-language system, someone mistakenly
> programmed Esp-eranto instead of the Spanish (esp-anol). So, no one
> congratulate the bank: they would be able to repair the "mistake"!

Their guess as to the origin of the situation certainly sounds plausible to me, although they apparently did not contact the bank to find out for sure.

Philip Brewer pbrewer@urbana.mcd.mot.com
Motorola Urbana Design Center ...!uiucuxc!udc!pbrewer Ho mia korv'

A "Handy" Risk for AirTravel?

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Sat, 6 Feb 1993 15:42:07 +0100

German newspapers report broadly on risks of hand-held telephones used in flight. Following a report of a new German weekly magazine FOCUS (some sort of Anti-Spiegel published since mid-January 1993, with some remarkably well-investigated articles on IT InSecurities), Germany's federal airtransport authority (Luftfahrt-Bundesamt, LBA in Braunschweig) admitted that major problems with passengers telephoning with "handy" mobile hend-held telephones have recently been experienced in some German airplanes.

Newspapers report that hand-held telephones have influenced flight instruments (e.g. indicating velocity) even in landing approach. An LBA manager responsible for analysis of flight systems' security mentioned a B737 approaching Hamburg airport under IFR conditions when slope indicator suddenly began to jump; the pilot interrupted descent and made another (successful) approach. In som. The LBA manager was quoted to say that if velocity indicators be adversely affected by some influence of such a "handy" telephone, the pilot may be tempted to diminish the velocity below the critical value, with catastrophic influence on the plane.

When contacted by me, this LBA manager refused some overdrawn citations but admitted that LBA sees serious problems and had warned carriers several times. Meanwhile, passenger instruction concerning emergency exits etc now also mentions risk of hand-held telephones which (according to some old German law) are not allowed to use in-flight. According to him, wires in planes are traditionally "hardened" against some electromagnetic induction; but the order of magnitude of such protection (about 3 Volt/meter) is, according to recent measurements of MBB (part of German Airbus, DASA) significantly lower than the 30 Volt/m which some hand-helds induce. Signal induction may even be worse as effects of reflections and resonances (which may develop in edges and channels below the cabin) may well enlarge the effect in a way hardly to measure.

In public debates, such new facts add to the criticism that some overly computerized systems (e.g. Electronic Flight Management Systems, Fly-by-Wire) may enlarge in-flight risks. But at least one more advanced technology may reduce the risk of electromagnetic radiation: German Airbus is preparing to replace one (of 3) wires for some part of A340 communication (at least experimentally) by Fly-by-Light connection; in such a system, risk will remain with opticouplers between electromagnetic and optic parts as well as with traditional non-optical computers but the lines near the passengers parts will become immune against electromagnetic effects.

Klaus Brunnstein (Univ Hamburg, February 6,1993)

PS: this year, some of you may have missed my traditional report from Chaos Conference. Luckily, I was unable to participate, because several participants independently informed me that NOTHING worthwhile to report happened. Participation was said to be significantly lower than ever before, and even some journalists which are CCC's good friends did not report this year. Moreover, due to very chaotic organisation, CCCs usual electronic articles were not available for FTP. "Downsizing" CCC seems to be in interesting contrast to US hackers (2600) which become more active, as visible from the Pentagon raids.

Released GSA Docs Slam FBI Wiretap Proposal (Banisar, RISKS-14.28)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Wed, 20 Jan 93 08:25:20 -0500

We knew there was some intelligence in Washington (contrary to popular belief), I have encountered many dedicated civil servants who actually understand the issues despite the pseudo-random efforts of transitory appointees. The excerpts I have seen of the GSA thoughts demonstrate this.

Actually, on reflection such a law might be a *good thing*. At the moment the country is in an economic slump and numerous encryption technology companies are struggling. Think of the benefits to them !

For the 1974 automotive model year the government passed the seatbelt interlock law that mandated fastening of the seatbelts in occupied front seats before the automobile could be started. This provided a windfall for a number of people: those who made the millions of new interlock devices and wiring as well as those who were paid to disconnect them.

Fortunately some cars were constructed in such a way that a simple connector disconnect under the seat would allow starting in any condition. Such forethought !

The simple fact is that such a law is unenforceable and will not have the desired effect (not that that has ever stopped Washington before), it is simply too easy to bypass by anyone who cares. We have had plenty of examples of how-to in both RISKS and PRIVACY (exercise is left to the student).

Not that a few miscreants won't be caught, stupidity is not confined to the law-abiding, but all such a law does is serve notice that conversations may be monitored (as they may be now) and a new industry will be born. Those in on the ground floor will make a few more millions from both sides and business will continue as usual.

One universal truth in the USA is that *every* new law, good or bad, needed or unnecessary means another piece of the pork barrel for someone. The line has undoubtedly already formed.

Padgett

Re: Tapping phones

Fred Cohen <fc@turing.duq.edu>
Sat, 6 Feb 93 10:15:46 -0500

I must strongly disagree that the government needs special capabilities for tapping phones, decoding transmissions, etc. built into these systems by the manufacturers. But perhaps my reasons are very different than the ones recently stated regarding CC:mail.

Everyone seems to be arguing the issue from a standpoint of the government's need to crack down on crime vs. the civil liberties of the citizens. I personally fall heavily on the civil liberties side, but I also think that historically, we give up civil liberties to fight crime and provide security. I find it very hard to understand why cryptography should be an illegal weapon while hand guns are legal, but then I can't understand how cigarettes and alcohol can be legal when marijuana and cocaine and penicillin and RU248 (238?) are illegal. The point, I guess, is that it is political power that determines legality and not rationality. Which brings me to my point.

I am concerned that the government acts unfairly toward some companies and against others based on their size, market share, political affiliations, etc. If the government approaches Lotus and not me to make a back door for them, I think they are unfairly supporting Lotus in favor of me. It is an implicit endorsement of Lotus! I want the FBI to offer me hard cash and government contracts in exchange for putting back doors in my software for them. In fact, I think we should require fairness to the extent that if the FBI wants back doors in any product, they have to make the same deal for all other products.

This is not a privacy issue, it is a business issue. We have the CSPR and the SPA and other such groups that essentially provide better business connections for people and support the positions of their constituents. If their constituents want to allow a 40 bit RSA to be claimed as `secure', they support it, even though technically speaking, this is trivial to break - in a matter of minutes - on a PC! None of these companies are working for our privacy, they are working for their profits. They don't provide secure encryption because there is no profit in it. If the FBI can't read these codes, it's probably not for lack of a back door - it's probably because of a lack of technical expertise and funding.

I am eager to hear some of you tell me that there is profit in security. What a bunch of malarkey! There may be a little profit in good security for a few select organizations, but the vast majority of the profit from security is from the perception and not the reality. I often hear companies tell me their cryptosystem is really good because it was approved by the NSA - they don't mention the words `for export'. People commonly buy wordperfect because of it's encryption capability, but this has never been secure in any way. In fact, they are buying the wordperfect cracking program from QUT to read files encrypted by employees who have since left. PKware sells authenticated PKzip capability, and people buy it because they want the perception of integrity, but it is easy to crack, an forged virus-infected zip files under their newest algorithm have already been shown after only a few weeks in widespread distribution.

Now about Lotus. In my limited personal experience with Lotus, I have found them to be sincere about providing the best protection they can in their products, subject to the time constraints placed on them by the market which values performance over almost everything else. I think they did the right thing by claiming to have refused to put in a back door, at least from a business standpoint. I also think that if the government offered enough money in exchange for the back door, Lotus would put it in. This is not a moral issue, it is a business issue.

SEMI-HUMOROUS-SEMI-SINCERE-REMARKS-ON

So if you are a private citizen who wishes to maintain privacy, or a criminal who wishes not to be caught, there are at least three lessons to be learned:

1 - Buy from a small sincere company (like mine) that will (for the right amount of money) provide source code, and then get that source code vetted by a different small sincere company (like mine) that will certify the algorithm, its implementation, and report on its adequacy. Small companies do this better because you probably need a real expert for the whole process, and

only the right small company will likely provide this to you. The second similar company provides you with the redundancy required for high integrity.

2 - Security costs time and money. If you aren't willing to suffer the consequences, you don't want security! Most people say they want the best security for the price and performance, but as most real experts know, you don't get much security unless you get a lot of security. The average high school level cracker can break almost every commercial security product in a matter of a few hours - most in minutes.

3 - The best encryption in the world won't make you very safe if you dial into CompuServe (NOTE I AM NOT CITING COMPUSERVE AS AN ACTUAL PERPETRATOR BUT RATHER AS A CONVENIENT NAME-RECOGNITION IDENTIFIER FOR THE LARGER CLASS OF SUCH SERVICES) from your PC to send the information. The FBI could easily provide the back door in the communications service to enter your PC from your remote connection and extract your keys, the plaintext of your message, or maybe even place the back door in your encryption package. Before you laugh at the suggestion, note that when a recently introduced communications service first came on the market, it `accidentally' transmitted private information from subscribers over the wire. If it happens accidentally, you know we can do it on purpose.

SEMI-HUMOROUS-SEMI-SINCERE-REMARKS-OFF

US+412-422-4134 Protection Experts US+907-344-5164
FAX US+412-422-4135 -OR- 907-344-3069 24 hours - 7 days

Re: Joltes Vs Denning

"Gary Preckshot" <Gary_Preckshot@lccmail.ocf.llnl.gov>
9 Feb 1993 12:50:46 U

For all the fur that's in the air, the participants in this discussion give naive trust to the assumption that "there's all this crime the FBI has to stop" without ever considering whether you could reduce the amount of crime by changing the law. It's a classic risk, and it has been exploited by Hitler, Mussolini, Bismark, Saddam Hussein, and Torquemada, to name a few. You state it thus, filling in the blanks to suit your particular needs:

"Our cause is just, therefore we must ......"

Nonsense. Damn little deserves this kind of credulity, certainly not the performance of the FBI, the DEA, and the Federal Government. The Joltes-Denning twain argue nits about how to stem a legal trickle while we are inundated by breaches of reason.

Gary

Mobile phones: "too secure"?

Marc Horowitz <marc@Athena.MIT.EDU>
Sun, 07 Feb 93 01:14:11 EST

`The Sunday Times', 31 January 1993. Main section, p. 12. (Home News)

SPYMASTERS ORDER REDESIGN OF `TOO SECURE' MOBILE PHONES by Christopher Lloyd

[Cartoon of a ridiculous mobile handset with various antennaea and dishes protruding. It is being held by a dismayed, purple-suited, man whilst a sign reads: "New! GCHQ-approved mobile phone".]

The next generation of mobile telephones has proved so secure against tapping that it is to be made less safe on the advice of the intelligence services. The phones, based on coded digital technology, will have their technology modified so that spies can continue to eavesdrop on private conversations.

The changes, ordered by a European Community (EC) telecommunications committee in Brussels, are being made at the insistence of European governments, including Britain's. They fear that surveillance operations against drug barons, the criminal underworld and foreign powers could be undermined.

Digital mobiles phones, based on a system called GSM, are already replacing standard analogue networks across the world. They are equipped with a sophisticated scrambling code called A5, offering protection from interception equivalent to many military systems.

It is this code that is to be replaced by one called A5X, to allow undercover eavesdropping to continue.

Last week a Department of Trade and Industry spokesman confirmed changes were being introduced to make it easier for security agencies - ranging from GCHQ, the British government's listening post near Cheltenham, to the FBI in America - to eavesdrop.

"Alternative coding is being developed for the reasons you have outlined," he said. "There is a general desire for this among the governments of Europe."

The department, which issues export licenses for the phones, is particularly concerned that the original A5 technology should not be sold to countries that may adapt it for military applications.

In America, the FBI has voiced similar concern. Nestor Michnyak, spokesman for the FBI headquarters in Washington, said that digital technology was advancing so fast that counter-surveillance was in danger of being undermined.

"We are trying to get companies and manufacturers to work with us to allow us to maintain the surveillance operations we have undertaken since the late 1960s," he said. "All we are asking is to be able to continue to do what we are currently doing and we want the same access we are having now."

Manufacturers of GSM mobile phones will be forced to adapt products to work with the new codes. Motorola, one of the leading makers of the digital mobile handsets, complained that costs may rise as a result.

"We are flying blind here," said Larry Conlee, the assistant general manager of Motorola's European cellular division. "The GSM system has ended up more secure than it should have been for the commercial market and now we're trying to recover from it."

Vodafone, Britain's largest analogue mobile phone company, which has already installed 250 GSM base stations covering 50% of the UK population, said its network will need to be adapted to accept the new codes.

"Government authorities have made it known that they don't want this high level of encoding," said Mike Caldwell, the spokesman for Vodafone.

Caldwell said the problem with the original system was that it would take security services weeks rather than minutes to decode the conversations they wanted to bug. Despite the changes, it will be still virtually impossible for any amateur eavesdropper to intercept calls made on the digital mobile phones.

===============

Transcript of an article in New Scientist, 30 Jan 1993

Spymasters fear bug-proof cellphones
(Barry Fox, Bahrain)

One of the jewels of Europe's electronics industry, the new all-digital cellular phone system GSM, may be blocked from export to other countries around the world by Britain's Department of Trade and Industry. The DTI objects to the exports because it believes the encryption system that GSM uses to code its messages is too good. Sources say this is because the security services and military establishment in Britain and the US fear they will no longer be able [to] eavesdrop on telephone conversations. Few people believe GSM needs such powerful encryption, but the makers of GSM complain that the DTI has woken to the problem five years too late.

At MECOM 93, a conference on developing Arab communications held in Bahrain last week, many Gulf and Middle Eastern countries sought tenders for GSM systems, but the companies selling them could not agree terms without the go-ahead of the DTI. Qatar and the United Arab Emirates want to be first with GSM in the Gulf, with Bahrain next. GSM manufacturers are worried that the business will be lost to rival digital systems already on offer from the US and Japan.

The Finnish electronics company Nokia, which is tendering for Bahrain's GSM contract, says "There is no logic. We don't know what is happening or why." A DTI spokeswoman would only say that exports outside Europe would need a licence and each case would be treated on its own merits.

The GSM system was developed in the mid-1980s by the Groupe Special Mobile, a consortium of European manufacturers and telecommunications authorities. The technology was supported by European Commission and the GSM standard has now been agreed officially by 27 operators in 18 European countries.

GSM was designed to allow business travellers to use the same portable phone anywhere in Europe and be billed back home. This is impossible with the existing cellphone services because different countries use different analogue technology.

The plan was for GSM to be in use across Europe by 1991, but the existing analogue services have been too successful. No cellphone operator wants to invest in a second network when the first is still making profits. So GSM manufacturers have been offering the technology for export.

Whereas all existing cellular phone systems transmit speech as analogue waves, GSM converts speech into digital code. Foreseeing that users would want secure communications, the GSM designers built an encryption system called A5 into the standard; it is similar to the US government's Data Encryption Standard. British Telecom was involved in developing A5, so the British government has special rights to control its use.

To crack the DES and A5 codes needs huge amounts of computer power. This is what alarmed the FBI in the US, which wants to be able to listen in to criminals who are using mobile phones. It also alarmed GCHQ, the British government's listening post at Cheltenham which monitors radio traffic round the world using satellites and sensitive ground-based receivers.

The DTI has now asked for the GSM standard to be changed, either by watering down the encryption system, or by removing encryption altogether. This means that GSM manufacturers must redesign their microchips. But they cannot start until a new standard is set and the earliest hope of that is May.

Any change will inevitably lead to two different GSM standards, so robbing GSM of its major selling point -- freedom to roam between countries with the same phone. Manufacturing costs will also rise as new chips are put into production.

PLCs : Request for information

Pete Mellor <pm@cs.city.ac.uk>
Sat, 6 Feb 93 19:00:50 GMT

As part of a research project, I would like to find out about Programmable Logic Controllers (PLCs), of the sort frequently used for real-time control of industrial plant.

I require information about the hardware and software, any fault-tolerant architectural features, methods of program development, reports on their use, etc.

Information would be particularly welcome from anyone who has worked with PLCs, but any odd stories or references would be useful.

The result will probably be a project report (or two) on the application of
PLCs in the control of safety-critical systems. This report will be in the
public domain, but if requested I will treat sources as confidential and
not attribute the information in the report.

Many thanks. Please address any responses to me personally, not to RISKS.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

User interface at the checkout stand

"Rob Slade, DECrypt Editor, 604-984-4067" <roberts@decus.arc.ab.ca>
6 Feb 93 20:13 -0600

About two months ago I was permitted to accompany my wife on an expedition to the fabric store. Our final transaction, involving a credit card, was a source of no small confusion to the clerk at the till. He punched all the requisite buttons, but was unhappy with the result. Finally, though, he punched the transmit button. Apparently he was no happier with this new result, since he (mentally) ran over the process again before again punching the transmit button.

Still unhappy, he asked help from a co-worker, who quizzed him on the process. Satisfied that he had no, in fact, made an error, *she* punched the transmit button, and was no happier than he with the result. The manager, was brought in, and was still not any happier after she (the manager) had punched transmit. The situation was resolved when someone remembered to turn on the printer attached to the "swipe" unit.

I was reminded of this yesterday. Why? The credit card statement came with, you guessed it, four copies of the same billing.

Risks? The unit apparently was indicating an error, but did not give any indication as to what that error was. The procedure had a "fault", but was allowed to proceed without a vital component. (The printed receipt, signed by the customer, is, in fact, the only legal proof of the transaction. yes, I do know that the existence of the credit card record is a "presumption of evidence" of the transaction.) Finally, even though the transaction was only entered once, the unit still submitted four confirmed "billings", with only the transmit key being hit again. I find it odd that the transaction, having been transmitted, would not be cleared from the "till-side" unit in order to prevent such accidental duplicates.

Where's the fire?

Jim Carroll <jcarroll@jacc.com>
Mon, 8 Feb 1993 08:22:14 -0500

On the evening of Feb. 2nd my wife and I were woken up by sounds out on the street. My wife struggled out of bed, looked through the venetian blinds, and screamed at me to put on my glasses and come to the window.

The house across the street was on fire. This was no, small, contained fire : the entire, complete structure was up in flames. I was quoted in the press days later as saying that the flames were over fifty feet high; I still don't think this is an exaggeration.

It was a stunning and disturbing site : so much so, that we have slept only fitfully since then. The house was completely destroyed. Fortunately, the owner escaped.

What makes it all the worse is that it quickly became apparent that the fire department was not responding! For what seemed like an eternity, the fire burned out of control, with only a lone police officer on the scene. Eventually, the fire department arrived and began to do their work. As the neighbours congregated in shock outside, the story began to circulate that 'it took the fire department 22 minutes to get here', and that 'they went to the wrong address'.

It turns out that when the operator at 911 received the call, Birchwood was punched into the computer. The system listed Birchwood Heights Drive first, a street a good 5 miles away! from our location. Tragically, the operator selected that location, and a full response team of 6 pumpers and trucks was sent. Meanwhile, the fire on Birchwood Drive continued to rage out of control.

My neighbour across the street called three times, since it became evident that something was wrong when the fire department was not there within five minutes (being only about 1 mile away.) They realized their mistake within 10-12 minutes, after the third call (and after obviously seeing that there was no fire on Birchwood Heights Drive!)

The Mississauga Fire Department has apologized to the owner of the destroyed property (estimates of loss are $1/2million or higher), and has promised to review it's dispatch procedures.

Surely the system can be programmed to provide a second confirmation for streets that are phonetically similar? Surely something can be done with the system configuration to avoid this easy but tragic mistake?

Jim Carroll, J.A. Carroll Consulting, Mississauga, Ontario, Canada
jcarroll@jacc.com +1.416.855.2950

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 34

Monday 22 February 1993

Contents

And You thought Your Computer Chat Was Private

Marty Leisner 71348 <leisner@eso.mc.xerox.com>
Sat, 13 Feb 1993 14:06:39 PST

In the February 7, 1993 NY Times (sunday) on page 32 they had an article (about 10 column inches) detailing privacy issues with email.

They talked about Oliver North's message in 1986 to his aide Ronald Sable:

"Oh Lord, I lost the slip and broke one of the high heels.   Forgive please.
Will return the wig Monday".

The article quotes Paul Saffo (Institute for the Future) talking about "we have yet to establish the conventions for e-mail).

marty   leisner@eso.mc.xerox.com   leisner.henr801c@xerox.com
Member of the League for Programming Freedom

Friendly Spies

Peter Wayner <pcw@access.digex.com>
Mon, 22 Feb 1993 11:12:37 -0500

Fans of encryption and those who merely fan the fires of debate about encryption's inherent threat/value will want to dig up Peter Schweitzer's new book _Friendly Spies_ just published by Atlantic Monthly Press. He includes many different details about covert intelligence operations directed against US corporations by cold war allies. Time and time again he says, foreign governments conspire with foreign companies to steal US technology and economic secrets.

He mentions that France and Germany and many other countries require US Companies to "register" the encryption key for reasons of national security. All of the American transmissions are monitored and the data is passed on to the local competitors. Companies like IBM finally began to routinely transmit false information to their French subsidiary just to thwart the French Secret Service and by transitive property of economic nationalism, French computer companies.

The lessons? Key registration in the world hurts American corporations. Cryptography protects the creators and thwarts those who seek to copy innovation.

-Peter Wayner

The "Information America" service

<Brian.Randell@newcastle.ac.uk>
Wed, 17 Feb 93 12:18:22 GMT

A colleague has just shown me an article about an online service called "Information America". The article is (possibly justifiably) alarmist in tone - and I cannot vouch for its factual accuracy. The article appeared in issue 8 of a (strange, to me at least) magazine called Mondo 2000, published some time in 1992 - the publisher's address is given as PO Box 1071, Berkeley, CA.

Let me say no more about the article or the magazine, but just provide soc.roots/ROOTS-L readers some illustrative quotes from it:

"BIG BROTHER ISN'T DEAD, HE'S JUST SUBCONTRACTING

If you have a modem, a home computer and can afford $95 an hour fees you too
can access Information America's online computer database, cross indexing the
Postal Service's National Change of Address file (NCOA), major publisher and
direct marketing companies' client information, birth records, drivers'
license records, phone books, voter registrations, records from up to 49
governmental agencies, and more. Information America boasts up to date
information on over 111 million Americans, 80 million households, and 61
million telephones.

If you are not scared yet you should be. Because complete strangers can
find out where you live, tracing you through extensive relocations even if
they have only a last name, or a state, an old address or telephone number.
....
Not until recently has information like this been commercially available in
a single database, specifically with law enforcement, private
investigators, bounty hunters and lawyers in mind. Information America is
the first accessible service to make use of previously collected data for
the express purpose of providing up-to-date whereabouts and personal
profiles of as many Americans as possible.
....
People finder is made up of four services: SKIP TRACER, TELEPHONE TRACKER,
PERSON LOCATOR and PEOPLE FINDER MULTITRACK
.....
SKIP TRACER traces a person's moves or verifies the current address when
all you have is an old address. You will enter the person's name, street
number, street name, and either the zip code or the city/state. If your
subject is in IA's files a profile will be provided that includes the
address he moved to (or current address), phone number, length of
residence, and more. You may also request a list of ten of the person's
neighbours. A profile on the current resident at your subject's old address
and up to ten neighbours there may also be available.
....
TELEPHONE TRACKER tracks down the owner of a telephone number... If a match
is found, you may look at a profile of that individual/residence and a
listing of up to ten neighbours.
....
PERSON LOCATOR helps you locate a person when specific address information
is not available. Enter the person's name and indicate whether you wish to
conduct a search by city, state(s), zip or nationwide. Person Locator will
compile a list (up to 300 names for nationwide and up to 100 names for
individual state searches) that match the information entered..... When you
find the right name, you may request a profile and neighbour listing for
that individual.
.....
PEOPLE FINDER MULTITRACK helps you find multiple people during one search.
Search results are available the following business day.
....
IA's clients are mostly lawyers and paralegals working at large legal
firms, but the FBI is also a major IA client.
....
IA has existed for at least three and a half years, but has remained
relatively unknown to the public.
....

To market its database services, IA seems to have adopted a grass-roots
kind of approach. IA employs liaison in major metropolitan cities whose job
it is to research and contact prospective clients lawyers, for example. I
am unaware of any advertising in specialist journals.
...."

Discussions of the potential dangers of a service like this would be better addressed to the splendid Usenet newsgroup comp.risks - to which my colleague is addressing a separate message about Information America. However it seems to me that the service might be of legitimate interest to a number of soc.roots/ROOTS-L readers (for example, those carrying out aextensive "one-name studies"), hence my posting this message. Brian Randell

PS I reiterate - I have no personal knowledge of Information America, and cannot vouch for the accuracy or fairness of the Mondo 200 article from which I have quoted.

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,
NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

"Telephone Service Cut Off"

"Lin Zucconi" <Lin_Zucconi@lccmail.ocf.llnl.gov>
18 Feb 1993 09:06:10 U

The Valley Times (Feb.18) reported that telephone service was cut off for more than 4 hours to about 37,000 phone lines in Livermore, CA including "911" and operator "O" lines. The article said that "the significance (of the malfunction) was in having three prefixes that can't reach emergency phone lines.... The phone company [Pacific Bell] was stymied in correcting the problem because diagnostic tests of the equipment told technicians that there was no problem....Technicians eventually located the problem in a call processor computer tape and replaced the malfunctioning tape." Luckily for those of us that live here, this is a relatively low crime area and no serious crimes occurred during the outage. Some banks compensated by letting in only a few customers at a time because they were concerned that their alarm systems wouldn't be able to call police.

Computer delays response to fatal fire

Lauren Wiener <lauren@reed.edu>
Sat, 20 Feb 93 10:49:25 -0800

>From the Oregonian, Saturday, Feb. 20, 1993, p.B1:

"Computer delays response to fatal Bonny Slope fire", by James Mayer

It takes seven minutes for the alarm to reach Tualatin Valley Fire & Rescue
because of a glitch that sends it to the office that dispatches Portland Fire
Bureau units instead of to the proper agency in Washington County

[BACKGROUND: Multnomah County is the county that contains the City of Portland. Suburban Washington County adjoins it to the west. Multnomah County is oddly shaped, and small slices of it here and there are served by suburban agencies instead of the corresponding Portland agency. I live in one of those places, and when I moved into my present house in 1980 it took the telephone company two days to find me and sort out who was responsible for hooking up my telephone service. Which fortunately was not an emergency.]

A computer error added seven minutes to the time it took firefighters to reach a 68-year-old woman trapped in her burning Bonny Slope home last week.

Mildred Smith died of smoke inhalation suffered in a pre-dawn Feb. 12 blaze at her home at 12401 NW Thompson Rd.

A neighbor telephoned 9-1-1 to report the fire at 2:40 AM, but firefighters from Tualatin Valley Fire & Rescue were not dispatched until 2:47 AM because a computer error sent the original call to the wrong place.

Eugene Jacobus, Washington County deputy medical examiner, said it would be hard to determine whether the dispatching delay made a fatal difference. Firefighters were also delayed by steel-bar security doors when they reached the remote house north of Cedar Mill, 5 and 1/2 minutes after finally getting the call for help.

"It's really hard to say, but certainly a delay of that magnitude is going to make a difference, Jacobus said. "You can be relatively sure that any delay, whether two or seven minutes, is going to rob an individual of some ability to be resuscitated."

By Friday, officials had traced the problem to the computerized telephone switching system at Portland's 9-1-1 center on Kelly Butte.

Fire and US West Communications officials say a "reloading" of some computer software by US West inadvertently changed the way the 9-1-1 system routed calls for a very small number of callers.

"We're still looking to find out how that happened," said Jim Haynes, US West spokesman.

Tapping the new digital car phone systems

John W. Sinteur <fourcnl!sinteur@relay.nluug.nl>
Mon, 22 Feb 1993 12:14:53 -0800

The following appeared in the Automatiseringsgids in The Netherlands last week. The Automatiseringsgids is a weekly newpaper-like magazine on information technology in the Netherlands. My comments are in [... -JS] I tried to translate literally, any mistakes are mine, but not intented as such. The author of the article gave me permission to send RISKS a translated version of his article. ...

I think most comments on what's in the article are already made before, I just wanted to let you know what's happening over here in Europe... -John

GSM cannot be tapped. (Automatiseringsgids, 19 Feb 93)

The Ministry of Justice is negotiating with PTT Telecom to figure out which way Justice, Police and Security Services can listen in on subscribers of the new digital car phone system (GSM). The government is now discussing the option of tapping conversations at the central PTT switchboards. [PTT Telecom is the sole provider of telecom infrastructure in the Netherlands -JS]

GSM is protected by personal subscriber smart-cards and complex algorithms, well enough to stop professional eaves-droppers. Security officials fear that this will be welcomed by criminal organisations, who can communicate through this system without fear of being tapped.

[The article does not mention exactly which 'algorithms'. Public key perhaps? If anyone really knows, please tell us -JS]

Since GSM will be used throughout Europe, it is especially useful for criminals operating internationally.

Secret and Police Services in Europe are trying to convince their Ministries of Internal Affairs of the need to force GSM providers to adapt their services to make tapping possible. The German government is talking to two GSM providers, DBP Telekom and Mannesmann/PacTel, to persuade them to cooperate and implement a tapping option. British Telecom and Vodafone in Great Britain are also discussing this problem with the government. [GSM] providers are thinking about this problem and are trying to find a solution for all of Europe.

[end of article]

[sinteur@fourc.nl John W. Sinteur, 2:512/48 (fidonet)]
[Snail: Jade str 28, 2332 RT Leiden, The Netherlands]

A quick request for opinions

Fred Cohen <fc@turing.duq.edu>
Fri, 12 Feb 93 19:15:43 -0500

I am writing a book about artificial life, and have some examples of programs that automate distribution of software in LANs, implement distributed databases, etc. They are all written in the Unix shell, and involve a few lines of code that automatically copy the programs between machines to automate the distribution process. It has come to my attention that there may be substantial objection to this idea and I am asking people in this forum for their opinion.

Each program includes explicit safeties to prevent copying to machines where operation is not authorized by the root, and they are designed not to spread outside of particular directories. The code is very obvious (only a few lines of shell script after all), and the book includes explicit warnings not to remove safeties or use on any machine where you don't have permission.

Questions:

1 - why not provide this in the book?
2 - what risks do you see in it?
3 - are you an admin or a user?
4 - do you think there is value in including these examples?
5 - do you think the advantages of examples outweigh any risks?
6 - do you think that the versions that optimize their own behavior by
    `evolving' improved forms should not be included - if not why not?

Please Email me your responses ASAP, as the book goes to press in a few weeks. Also, if you DO NOT want your comments included in the book (no names will be used) tell me. Otherwise, I will feel free to include any comments I find particularly enlightening. FC

London Ambulance Service

<Brian.Randell@newcastle.ac.uk>
Fri, 19 Feb 93 12:55:43 GMT

The London Ambulance Service Crisis reported to RISKS earlier has been absent from the UK press for a while, but now it seems likely to burst forth again. The attached article is reprinted in its entirety from (UK) Computer Weekly, 18 Feb, 1993. Cheers. Brian Randell

Report to confirm (pounds)1m 999 systems blunder (by David Evans)

LONDON Ambulance Service made a fatal blunder when it bought a (pounds)1m untested computer system to handle 999 calls, an official inquiry will reveal next week. Union leaders have already blamed the system for contributing to the deaths of at least four patients.

Around 800,000 emergency calls are handled by the capital's ambulance service each year. But after a spate of incidents, in which calls were lost and emergency victims suffered long delays before ambulances arrived, the system was abandoned.

Now an official report into the fiasco, demanded by health secretary Virginia Bottomley, is expected to be scathing in its criticism.

Since last November an independent panel has been looking at the circumstances surrounding the purchase of the system, bought when a previous computer-aided dispatch module crashed. Yet after just a few months of use the replacement was similarly suffering from calldata overload.

Questions raised by the report will include why Aldershot-based Systems Options was chosen as the main soft-ware supplier when it had no previous experience in providing dispatch systems to the ambulance sector.

Jim Pedroza, Systems Options' founder, has consistently refused to talk to the press. His networked solution based on Apricot workstations and servers contrasts markedly with mini-based systems favoured by other emergency services.

According to sources working close to the inquiry team, one conclusion is that a replacement computer-aided dispatch system will now take years, rather than months, to implement. It will also confirm that the Systems Options solution is wholly unfit for the task.

Said one London ambulance source: "What we're talking about here is an official stamp of condemnation. Not enough attention was paid to the project, and the lack of expertise in choosing the system was completely unacceptable."

The outcome of the report has been delayed to allow for the publication this week of the Tomlinson report on London hospitals.

Since the system was ditched, the service's chief John Wilby has resigned and control room staff have reverted to manual methods of dispatching crews.

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,
NE1 7RU, UK Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

DCCA-4 Call for Papers

Teresa Lunt <lunt@csl.sri.com>
Mon, 22 Feb 93 10:07:56 -0800

Below is the Call for Papers for the 4th IFIP Working Conference on Dependable Computing for Critical Applications. The conference aims to promote research that considers different aspects of dependability, including security, safety, reliability, and availability, in a common framework, with emphasis on high assurance.

Call for Papers:

4th IFIP Working Conference on Dependable Computing for Critical Applications
January 4-6, 1994, Catamaran Resort Hotel, San Diego, California, USA

Increasingly, individuals and organizations are becoming critically dependent on sophisticated computing systems. In differing circumstances, this dependency might for example center on the continuity of service received from the computing system, the overall performance level achieved, the real-time response rate provided, the extent to which catastrophic failures are avoided, or confidentiality violations prevented. The notion of dependability, defined as the trustworthiness of computer service such that reliance can justifiably be placed on this service, enables these various concerns to be subsumed within a single conceptual framework with reliability, availability, safety and security, for example, being treated as particular attributes of dependability.

The fourth IFIP Working Conference on Dependable Computing for Critical Applications aims at bringing together researchers and developers from academia, industry and government for advancing the state of the art in dependable computing. Papers are sought in all areas of dependable computing, including but not limited to models, methods, algorithms, tools and practical experience with specifying, designing, implementing, assessing, validating, operating and maintaining dependable computing systems. Of particular, but not exclusive, interest will be presentations which address combinations of dependability attributes, e.g. safety and security or fault-tolerance and safety, through studies of either a theoretical or an applied nature.

Submitting a Paper: Six copies (in English) of original work should be submitted by 30 June 1993, to the Program co-Chair:

Dr. Gerard Le Lann
INRIA - Project REFLECS
BP 105   Tel: +33.1.39635364
78153 Le Chesnay Cedex   Fax: +33.1.39635330
France   E-mail: Gerard.Le_Lann@inria.fr

Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper should include a short abstract and a list of keywords indicating subject classification. Papers will be refereed and the final choice will be made by the Program Committee. Notification of acceptance will be sent by September 24 1993, and camera-ready copy will be due on November 12, 1993. A digest of papers will be available at the Conference, and hardbound proceedings will be published after the Conference as a volume of the Springer-Verlag series on Dependable Computing and Fault-Tolerant Systems.

Important Dates:
Submission deadline: June 30, 1993
Acceptance notification: September 24, 1993
Camera-ready copy due: November 12, 1993

General Chair
F. Cristian, Univ. of California, USA

Program Cochairs
G. Le Lann, INRIA, France
T. Lunt, SRI International, USA

Local Arrangements/Publicity Chair
K. Marzullo, Univ. of California, USA

Program Committee
J. Abraham, U of Texas at Austin, USA
A. Avizienis, UCLA, USA
D. Bjoerner, UNUIIST, Macau
R. Butler, NASA, USA
A. Costes, LAAS-CNRS, France
M-C. Gaudel, LRI, France
V. Gligor, U of Maryland, USA
L. Gong, SRI International, USA
H. Ihara, Hitachi, Japan

J. Jacob, Oxford U, UK
S. Jajodia, George Mason U, USA
J. Lala, CS Draper Lab, USA
C. Landwehr, NRL, USA
K. Levitt, U of California Davis, USA
C. Meadows, NRL, USA,
J. McLean, NRL, USA
M. Melliar-Smith, UCSB, USA
J. Meyer, U of Michigan, USA
J. Millen, MITRE, USA
D. Parnas, McMaster U, Canada
B. Randell, U of Newcastle upon Tyne, UK
G. Rubino, IRISA, France
R. Schlichting, U of Arizona, USA
J. Stankovic, U of Massachusetts, USA
P. Thevenod, LAAS-CNRS, France
Y. Tohma, Tokyo Inst. of Technology, Japan

Ex-officio
J-C. Laprie, LAAS-CNRS, France
IFIP WG 10.4 Chair

Call for papers, Technology and Society

<m16805@mwvm.mitre.ogr>
Tuesday, 16 Feb 1993 20:08:04 EST

CALL FOR PAPERS
TECHNOLOGY: WHOSE COSTS?...WHOSE BENEFITS?

Areas of Concentration:
Computers and Communications, Health Care, Energy and the Environment

The International Symposium on Technology and Society 1993 (ISTAS '93)
The International Symposium that links Technology and Social Effects

Sponsors:
The Institute of Electrical and Electronic Engineers Inc. (IEEE)
Society for the Social Implications of Technology
The IEEE National Capital Area Council
The IEEE Technology Policy Conference Committee

Washington DC October 22-23, 1993

Technology is constantly changing the our world. New ways of doing things bring benefits undreamed-of just a few years ago. These technologies also have their price. The costs can be financial, but also less freedom, more risks, more stress. How do we balance benefits and costs? Do those who enjoy the benefits bear their fair share of the costs? How can we determine a fair share? If we can, and don't like the results, what do we change? Is the Government always the best way to change things?

ISTAS '93 invites significant contributions on these issues from a wide spectrum of scholarly and concerned individuals. The contributions can be papers, proposals for a session or panel of invited experts, or proposals for "poster" or discussion sessions. Please send a 100 word summary for papers or a 1000 word proposal for sessions, to the General Chair

Dr. William J. Kelly, Attn. IEEE, MITRE Corporation, m/c Z568, 7525 Colshire Drive, McLean, VA 22102 E-mail: wjkelly@mitre.org

Deadline for Submission:	March 12, 1993
Notification of Acceptance:	April 12, 1993
Camera Ready Copy:	June 30, 1993

For information call Jackie Hunter (703)-803-8701

Privacy Digests

Peter G. Neumann <neumann@csl.sri.com>
Mon, 22 Feb 1993 13:13:37 -0800

Periodically I will remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry higher-level discussions in which risks to privacy are a concern.

* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@cv.vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@cv.vortex.com".

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Dennis G. Rears. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to comp-privacy@pica.army.mil and administrative requests to comp-privacy-request@pica.army.mil.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be appropriate for you to read both, depending on the strength of your interests and time available.

PGN

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 35

Tuesday 23 February 1993

Contents

Seeing red over valentine envelopes

luis fernandes <elf@ee.ryerson.ca>
Sat, 13 Feb 93 20:46:50 EST

The following appeared in the Feb. 13, 1993 issue of the "Toronto Star":

Edmonton(CP)-- It's that time of year again when love is in the air and Canada Post is seeing red. Red envelopes, that is. That's because the computerized mail sorting machines, which can process 33,000 letters an hour, have trouble reading addresses off the red envelopes popular for Valentine Day greetings, a Canada Post spokeswoman says. "We in Canada have some of the most technically advanced machinery in the world," Teresa Williams says. "And while it's not impossible for them to read red envelopes, some of them can present a bit of a challenge." If your valentine card hasn't arrived, it may have been delayed in the mail-sorting process, William says. A reminder for next year: white envelopes should be used instead. "Or put a white sticker on a red envelope," Williams suggests.

Meanwhile Hallmark Cards Inc., based in the United States, is complying with a U.S. Postal Service request to stop producing dark-colored envelopes over the next couple of years. U.S. machines can't read them either.

KIO diskettes stolen from the Spanish Government

"(Miguel Gallardo)" <gallardo@batman.fi.upm.es>
Wed, 10 Feb 1993 15:52:04 UTC+0100

During the night of 5 February 1993, 18 diskettes were stolen from the Ministry of Economy and Taxes in Madrid, Spain. All the diskettes contained information of international funds transferred by Kuwait Investment Office (KIO) since 1988.

The situation of this large group of chemical, building and real estate companies in Spain is very complex, because many of them are in bankruptcy, the Spanish Government paid a lot of money for this industry support, there are thousands of people losing their jobs, and present managers of KIO in Spain demanded old jobs at the Court, because of money fraud and political corruption.

Javier De la Rosa, Fouad K. Jaffar and Mohamed al Sabah are the names related with it that appear every day in several press items that compare their management with Michael Milken (convicted), John H. Gutfreund, Donald M. Feurstein (Salomon Inc) and other Securities & Exchange Commission affairs in USA. But they control many journalists here, thanks to the singer Julio Iglesias' ex-manager, and now Javier De la Rosa's speaker [spokesman?], Alfredo Fraile.

The Government Ministry, Carlos Solchaga, told the press that he thinks the goal of the thief is to sell this information to the press, and to discredit HIM. He advised journalists not to buy this interesting digital information, because legal prosecution will be ordered if anything is published.

On the other side, Javier De la Rosa told the journalists that there is a mafia in Spanish bureaucracy that stole the diskettes. But this is not a clever idea because it is not necessary to steal something that can be easily diskcopied.

What is much more interesting is that KIO has nothing to say, and that a Spanish Justice refused to accept its demand because there was not enough information enclosed. It seems that they did not find a computer expert able enough to look for financial scandal data in computers and back-ups, now owned by them.

IMHO, everybody has too many things to hide in this sad story.

Miguel A. Gallardo Ortiz, PX86 Engineer UNIX&C freelance working on RSA crypto
Fernando Poo, 16 (Proyecto X86) E - 28045 Madrid (Spain)
Tel: (341) 474 38 09 - FAX: 473 81 97 E-mail: gallardo@batman.fi.upm.es

Citibank outage

Marty Leisner 71348 <leisner@eso.mc.xerox.com>
Tue, 23 Feb 1993 08:03:35 PST

"Software Problem Halts Citibank's Automatic Tellers for 4 Hours" -- Sunday NY Times, page 43 Metro, February 14. 1993 About 7 column inches

Citibanks 1200 ATMs went down (refused to dispense cash or complete transactions) from 10AM to 2 PM on Saturday because of "a software glitch" when new software was being installed...

marty leisner@eso.mc.xerox.com leisner.henr801c@xerox.com

Japanese Bank Hit By Phone Fraud

John Mello <jmello@igc.apc.org>
Tue, 23 Feb 93 14:20:38 PST

The Boston Business Journal, February 1993

A Boston branch of the Daiwa Bank Ltd., the 25th largest bank in the world, was victimized by prison inmates with a gift for social engineering, according to the Boston Business Journal. The inmates placed collect calls to the Daiwa switchboard, identified themselves as telephone repairmen, and said they could fix the company's telephone problems by being connected to an outside line. Once connected to an outside line, the cons made long-distance calls, sticking Daiwa with the tab. Some of the calls were to sex hotlines.

Hospitals in the Boston area were some of the first victims of this form of phone fraud, the newspaper reported. Inmates treated at the hospitals would memorize employees' names or use the names of physician's who appeared on TV to con operators into giving inmates access to outside lines. Once the operators got wind of what was happening, though, the hospitals were able to clamp down on the problem. One inmate, impersonating a doctor who appeared on TV the previous day, gave himself away by referring to himself by title "doctor." The operator knew the physician always identified himself by his first name. the last thing the jailbird heard before the operator hung up on him was, "I suggest you speak to the warden about that."

Long Distance..Is the next best thing to praying there

Paul Robinson <tdarcos@access.digex.com>
Tue, 23 Feb 1993 13:39:44 -0500 (EST)

>From the {Washington City Paper} of Feb 19-25, page 18:

News of the Weird by Chuck Shepard:

In January, Israel's national telephone company initiated a fax service that transmits messages to God via the Wailing Wall in Jerusalem. In May, the Roman Catholic Church will unveil a high-tech confessional at a trade show in Vincenza, Italy, that will accept confessions by fax. And in December, a sect of Orthodox Jews in Brooklyn, NY began selling its members special beepers so they will know instantly when the Messiah arrives on earth."

And there is precedent for a response, I guess:
"Your Majesty, I have a message from God for you." - Judges 3:20

Paul Robinson -- TDARCOS@MCIMAIL.COM

[Hopefully, the Messiah will not arrive on the Sabbath, although there might be a question as to whether the beeper is actually being USED as long as it does NOT trigger. Confessions by EMail should be easy to set up. L.A. has long had drive-through churches; I suppose services via on-line interactive multimedia X-window conferencing cannot be far behind. But watch out for a hi-tech Allah McGordo bombshell in virtual reality. PGN]

re: _Friendly Spies_ (Wayner, RISKS-14.34)

"Sean Matthews" <sean@mpi-sb.mpg.de>
Tue, 23 Feb 93 09:34:39 +0100

Consider this a balancing comment on economic risk of incorporating american technology (it is also tangentially relevant to the original discussion about export restrictions on US cryptographic technology).

I don't doubt that the French, German or British intelligence services carry out occasional industrial espionage for their local industries (certainly, I have seen reports of British intelligence doing this in the British press).

However, to balance this (least anyone think from the above that the US is somehow more virtuous in these things, and does not behave in such an underhanded, ungentlemanly, or even, dare I say it, nefarious, manner) I should point out that there are, or at least were, when I still lived there, regular complaints in the British press from firms trying to sell technology that contained US made components to, say, China, only to find, first, that the US department of trade prohibited the sale on strategic grounds, and second, that identical technology was suddenly no longer strategic when it was offered by some US company that had mysteriously heard about the British deal, and was able to close it instead.

Sean

Re: The "Information America" service

John Pettitt <jpettitt@well.sf.ca.us>
Tue, 23 Feb 1993 16:54:41 GMT

Information America does a lot more than is described in the post (I have not seen the Mondo article yet). I know one of their sales people (well ex she quit just before christmas). Their prime selling strategy to lawyers seems to be in competition with Lexis, Nexis (sp?) and Dialog (all large online database services).

The idea is that the lawyer (or more correctly a paralegal) can research case law on line in a fraction of the time it would take in the law library. They have all US court cases on line (local & federal).

I don't think there is any "dark' intent in the lack of publicity for IA, more that they just don't see value in advertising to people who are not going to buy their service.

As to the other services they provide, what is the problem ? We live in an information society. If you don't want people using and tracking information, don't give it to them (i.e., go live some place where there are no phones or credit cards).

[P.S. I am CEO of a direct response marketing company so I'm biased :-)]

John

> [I presume there will be comments about a person's not having to give the information to them for it to be there -- whether it is right or wrong! Subsequent discussion might better belong in the PRIVACY groups noted in RISKS-14.34. PGN]

MIT's on-line Student Information Services (SIS)

"Jonathan I. Kamens" <jik@aktis.com>
Wed, 10 Feb 93 18:19:20 -0500

(Re: "Anyone can get your U. of Illinois transcript" in RISKS-14.31)

MIT recently put on-line a new service, SIS, through which students can access data in the registrar's database, including both personal and confidential data about their own status and general data such as course schedules.

SIS is worth mentioning here, in response to Carl Kadie's message about problems with a similar system at the University of Illinois, because (in my opinion) SIS is a good example of system designers taking security issues seriously enough and doing a good job of meeting security needs.

In order to use SIS to access personal data, a user must first register an "extra" password with the Kerberos database. The program that registers this password does so by transmitting it to the Kerberos server in encrypted form (using a key derived from the user's main Kerberos principal, for which he already has a password) so that it isn't exposed to the network.

The assumption that led to the extra-password requirement is that people already have the mindset that it's OK to share their accounts (i.e., their main Kerberos principal password) with other people, so that name/password pair is not sufficient authentication. The documentation about SIS, and the prompting that takes place when the user chooses an extra password, makes it very clear that this password should be treated more securely by the user, and that if the user sees fit to give it to others, that user is giving those others access to his personal data in the registrar's database.

Once the user has registered for an extra password, he still can't access personal data in the registrar's database immediately. A notification is mailed, by U.S. Mail, to the address for the user in the registrar's database. About a week after that notification is received by the user, the password actually becomes active and the user can access personal data on-line.

Obviously, this second safeguard is to protect against the possibility of a user registering another user's extra password. The notification mailed to the user explains in detail what it's about, and tells the user whom to contact if he *did not* register an extra password.

I suspect that an extra password does not become valid if the paper mail notification is returned by the post office (i.e., is not successfully delivered to the user). Granted, the time given for the notification to be returned by the post office probably isn't sufficient for all failed delivers, but I think that the probability of a notification not being delivered properly to someone whose extra password was illicitly registered by someone else is sufficiently low that this is not a concern.

Once a user's extra password becomes valid he must type this password each time he wants to use the SIS service to access personal data (and he must already have valid Kerberos tickets for his main principal). The Kerberos tickets thus acquired are used to establish a Kerberos-authenticated network connection to the machine on which the registrar's database resides. Furthermore, the session key created while establishing that connection is used to encrypt all personal data sent over the network.

There is one more safeguard to prevent security breaches of the database. The SIS protocol does not allow for direct modification of the database on the SIS server. Most data in the system can't be modified through it at all; instead, users must talk to the registrar directly to effect changes. The data that *can* be modified is mostly MIT directory information, e.g., term address and phone numbers, and when a user requests modifications to that data, the modifications are stored and manually eyeballed for sanity by the registrar before actually being fed into the system.

Finally, just in case there is some possibility that someone might manage to break into the database machine (although it's pretty fortress-like in its configuration :-), that machine is not actually the "home location" of the registrar's database. It's a copy that is updated by SneakerNet (a tape carried from the registrar's office) regularly. The registrar's computer is

on a subnet that is isolated from most of the campus network (and that is
certainly more paranoid about who gets to connect to it than the rest of the
campus network).

As you can see, I think that the people who designed and implemented
SIS did a good job of meeting security concerns. Their only mistake
was using Motif for the UI :-).

Jonathan Kamens Aktis, Inc. jik@Aktis.COM

---

re: Tapping Phones (Cohen, RISKS-14.33)

"Mark W. Schumann" <mark@whizbang.wariat.org>
Sat, 20 Feb 1993 14:24:03 EST

Fred Cohen <fc@turing.duq.edu> writes in RISKS v14n33:

! 3 - The best encryption in the world won't make you very safe if you
!dial into CompuServe (NOTE I AM NOT CITING COMPUSERVE AS AN ACTUAL PERPETRATOR
!BUT RATHER AS A CONVENIENT NAME-RECOGNITION IDENTIFIER FOR THE LARGER CLASS OF
!SUCH SERVICES) from your PC to send the information. ...

You're perpetuating a security scare that has no basis in fact.

Prodigy, the latter service you mention, requires the use of its own front-end program on your PC. You cannot use Prodigy without it. Since this front-end program executes on your PC, it does have the potential for the abuse you mention. I personally do not use Prodigy in part because of this security loophole.

On the other hand, other communication services, such as Compuserve, do not have this questionable "feature" at all.

You dial Compuserve from your PC with a communications program of your choice. At all times the contents of your memory and hard drive are under the complete control of your CPU and communications program.

You are probably thinking of the "Quick B" transfer protocol which appears to allow Compuserve to "take over" your PC to run both ends of a file upload/download. (A similar sequence occurs with the popular ZMODEM protocol.) This is not really so; Compuserve actually sends only an ENQ (05) character to the PC, which is interpreted by your comm program as a request to begin a file transfer. Again, the PC's memory and hard drive are still under the control of your own comm program, not Compuserve. Most comm programs, such as Telix and Crosstalk, can be configured to ignore ENQ and require the PC user to execute the transfer command manually.

Bottom line: No online service can cause your PC to execute code that is not in the PC's memory space, Prodigy notwithstanding.

Mark W. Schumann/3111 Mapledale Avenue/Cleveland, Ohio 44109-2447 USA
Domain: mark@whizbang.wariat.org CIS:73750,3527

1st ACM Conference on Computer and Communications Security

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Tue, 9 Feb 93 11:29:05 EST

******* 1st ACM Conference on Computer and Communications Security *******
Nov 3-5 1993, Fairfax, Virginia

Sponsor: ACM SIGSAC
Hosts: Bell Atlantic and George Mason U

In cooperation and participation from:
International Association of Cryptologic Research
IEEE Communications Society TC on Network Operations and Management
IEEE Computer Society TC on Security and Privacy

CALL FOR PAPERS

Topics of interest
==================

The purpose of this new conference is to bring together researchers and practitioners of computer and communication security. The emphasis is on the security requirements of the industrial and commercial sectors, e.g. telecommunications, finance, banking, etc. The primary focus is on high quality original unpublished research, case studies and implementation experiences. We also encourage submission of papers addressing the social and legal aspects of security. Conference proceedings will be published by ACM. Selected papers, with suitable revisions, will be considered for publication in upcoming special issues of the Communications of the ACM and IEEE Communications Magazine. Topics of interest include:

Communications & Information Security: Theory and Techniques

Access Control
Audit
Authentication
Authorization
Cryptanalysis
Cryptosystems
Crypto. Prtcls
Database Sec.
Digital Signatures
Formal Models
Hash Functions
Integrity
Intrusion Detection
Randomness
Viruses and Worms
Zero Knowledge

Applications,Case Studies & Experiences

Cellular and Wireless
Electronic Commerce
Enterprise Security
LAN Security
Network Firewalls
Open Systems Security
Security APIs
Security Arch.
Security Mgmt.
Smart Cards
Telecom. Sec.
WAN Security

Social and Policy Issues

Cryptographic standards   Legal Issues
Information Priv.   Tech. Export

Instructions for Authors
========================

Authors should submit five copies of their papers to Ravi Ganesan at the address below by May 15, 1993. Papers should not exceed 7500 words (approx. 15 single spaced pages of 11pt), and should not have been published or submitted else where. As the review process will be anonymous, names and affiliations of authors should appear only on a separate cover sheet. Authors will be notified of review decisions by July 15, 1993. Camera ready copies of accepted papers are due back by August 15, 1993 for inclusion in the Conference proceedings.

Program Committee
=================

Victoria Ashby, MITRE   Steve Bellovin, AT&T Bell Labs.
Whitfield Diffie, SUN Microsystems   Taher El Gamal, RSA
Deborah Estrin, Univ. of Southern CA   Joan Feigenbaum, AT&T Bell Labs.
Virgil Gligor, Univ. of Maryland   Li Gong, ORA Corp.
Richard Graveman, Bellcore   Sushil Jajodia, George Mason U
Paul Karger, GTE   Carl Landwehr, NRL
E. Stewart Lee, Univ. of Toronto   Giancarlo Martella, Univ. of Milan
Michael Merritt, AT&T Bell Labs   Jonathan Millen, MITRE
Clifford Neuman, USC Info. Sci. Inst.   Steven Rudich, CMU
Rainer Rueppel, R3 Security Engg.   Eugene Spafford, Purdue Univ
Jacques Stern, DMI-GRECC   Michael Wiener, BNR
Yacov Yacobi, Bellcore

Organizers
==========

General Chairs

Dorothy Denning   Raymond Pyle
Georgetown U   Bell Atlantic
Reiss 225   7th Floor, 11720 Beltsville Drive
Georgetown, DC 20057   Beltsville, MD 20705
denning@cs.georgetown.edu   rpyle@socrates.bell-atl.com

Program Chairs

Ravi Ganesan   Ravi Sandhu
Bell Atlantic   George Mason U
7th Flr, 11720 Beltsville Drive   ISSE Dept.
Beltsville, MD 20705   Fairfax, VA 22030
ravi@socrates.bell-atl.com   sandhu@sitevax.gmu.edu
Ph#: (301) 595-8439

```
 Proceedings Chair and Treasurer        Local Arrangements Chair

 Victoria Ashby                      Catherine Hoover
 MITRE                             George Mason U
 7525 Coleshire Drive,                 Center for Professional Development
 McLean, VA 22102                     Fairfax, VA 22030
 ashby@mitre.org                     Ph#:(703) 993-2090
```

Call for Papers: Computer Security Applications Conference

Marshall D. Abrams <abrams@mitre.org>
Mon, 22 Feb 93 15:30:48 EST

```
       CALL FOR PAPERS AND PARTICIPATION

       Ninth Annual Computer Security
         Applications Conference


            December 6 - 10, 1993
         Orlando Marriott Internation Drive
              Orlando, Florida
```

The Conference
  The Information Age is upon us, along with its attendant needs for protecting private, proprietary, sensitive, classified, and critical information. The computer has created a universal addiction to information in the military, government, and private sectors. The result is a proliferation of computers, computer networks, databases, and applications empowered to make decisions ranging from the mundane to life threatening or life preserving.

   Some of the computer security challenges that the community is faced with include:

    * To design architectures capable of protecting the
      sensitivity and integrity of information, and of assuring
      that expected services are available when needed.

    * To design safety-critical systems such that their software and
      hardware are not hazardous.

    * To develop methods of assuring that computer systems
      accorded trust are worthy of that trust.

    * To build systems of systems out of components that have
      been deemed trustworthy.

    * To build applications on evaluated trusted systems without
      compromising the inherent trust.

    * To apply to the civil and private sectors trusted systems
      technologies designed for military applications.

* To extend computer security technology to specifically
  address the needs of the civil and private sectors.

* To develop international standards for computer security
  technology.

This conference will attempt to address these challenges. It will explore a broad range of technology applications with security and safety concerns through the use of technical papers, discussion panels, and tutorials.

Technical papers, panels and tutorials that address the application of computer security and safety technologies in the civil, defense, and commercial environments are solicited. Selected papers will be those that present examples of in-place or attempted solutions to these problems in real applications; lessons learned; original research, analyses and approaches for defining the computer security issues and problems. Papers that present descriptions of secure systems in use or under development, or papers presenting general strategy, or methodologies for analyzing the scope and nature of integrated computer security issues; and potential solutions are of particular interest. Papers written by students that are selected for presentation will also be judged for a Best Student Paper Award. A prize of $500, plus expenses to attend the conference, will be awarded for the selected best student paper (contact the Student Paper Award Chairperson for details, but submit your paper to the Technical Program Chairperson).

Panels of interest include those that present alternative/controversial viewpoints and/or those that encourage "lively" discussion of relevant issues. Panels that are simply a collection of unrefereed papers will not be selected.

INSTRUCTIONS TO AUTHORS:

Send five copies of your paper or panel proposal to Ann Marmor-Squires, Technical Program Chairman, at the address given below. Since we provide blind refereeing, we ask that you put names and affiliations of authors on a separate cover page only. Substantially identical papers that have been previously published or are under consideration for publication elsewhere should not be submitted. Panel proposals should be a minimum of one page that describes the panel theme and appropriateness of the panel for this conference, as well as identifies panel participant and their respective viewpoints. Send one copy of your tutorial proposal to Daniel Faigin at the address given below. It should consist of one- to two-paragraph abstract of the tutorial, an initial outline of the material to be presented, and an indication of the desired tutorial length (full day or half day). Electronic submission of tutorial proposals is preferred.

Completed papers as well as proposals for panels and tutorials must be received by May 18, 1993. Authors will be required to certify prior to June 19, 1993, that any and all necessary clearances for public release have been obtained; that the author or qualified representative will be represented at the conference to deliver the paper, and that the paper has not been accepted elsewhere. Authors will be notified of acceptance by

July 31, 1993. Camera ready copies are due not later than September 18, 1993.
Material should be sent to:

Ann Marmor-Squires   Daniel Faigin
Technical Program Chair   Tutorial Program Chair
TRW Systems Division   The Aerospace Corporation
1 Federal Systems Park Dr. P.O. Box 92957, MS M1/055
Fairfax, VA 22033   Los Angeles, CA 90009-2957
(703) 803-5503   (310) 336-8228
marmor@charm.isi.edu   faigin@aero.org

Ravi Sandhu
Student Paper Award
George Mason Univ.
ISSE Dept.
Fairfax, VA 22030-4444
(703) 993-1659
sandhu@gmuvax2.gmu.edu

Areas of Interest Include:

Trusted System Architectures
Software Safety Analysis and Design
Current and Future Trusted Systems Technology
Encryption Applications (e.g., Digital Signature)
Application of Formal Assurance Methods
Risk/Hazard Assessments
Security Policy and Management Issues
Trusted DBMSs, Operating Systems and Networks
Open Systems and Composted Systems
Electronic Document Interchange
Certification, Evaluation and Accreditation

Additional Information
    For more information or to receive future mailings, please contact
the following at:

Dr. Ronald Gove   Diana Akers
Conference Chairman   Publicity Chair
Booz-Allen & Hamilton   The MITRE Corporation
4330 East-West Highway   7525 Colshire Dr.
Bethesda, MD 20814   McLean, VA 22102
(301) 951-2395   (703) 883-5907
gover@jmb.ads.com   akers@mitre.org

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 36

Weds 24 February 1993

Contents

Third Conference on Computers, Freedom, and Privacy, CFP 1993

Bruce R Koball <bkoball@well.sf.ca.us>
Wed, 24 Feb 1993 11:05:46 -0800

There's still time to register for CFP'93! A number of spaces in this limited-attendance event are still available, so act now!

The Third Conference on Computers, Freedom and Privacy, 9-12 March 1993
San Francisco Airport Marriott Hotel, Burlingame, CA

The sessions in the main program include:

* ELECTRONIC DEMOCRACY

* ELECTRONIC VOTING
* CENSORSHIP AND FREE SPEECH ON THE NET
* PORTRAIT OF THE ARTIST ON THE NET
* DIGITAL TELEPHONY AND CRYPTOGRAPHY
* HEALTH RECORDS AND CONFIDENTIALITY
* THE MANY FACES OF PRIVACY
* THE DIGITAL INDIVIDUAL
* GENDER ISSUES IN COMPUTING AND TELECOMMUNICATIONS
* THE HAND THAT WIELDS THE GAVEL
* THE POWER, POLITICS AND PROMISE OF INTERNETWORKING
* INTERNATIONAL DATA FLOW

The conference will also offer a number of in-depth tutorials
on subjects including:

* Information use in the private sector
* Constitutional law and civil liberties
* Investigating telecom fraud
* Practical data inferencing
* Privacy in the public and private workplace
* Legal issues for sysops
* Access to government information
* Navigating the Internet

INFORMATION
For more information on the CFP'93 program and advance
registration call, write or email to:

CFP'93 INFORMATION
2210 SIXTH STREET
BERKELEY, CA 94710
(510) 845-1350
cfp93@well.sf.ca.us

A complete electronic version of the conference brochure with more detailed descriptions of the sessions, tutorials, and registration information is also available via anonymous ftp from sail.stanford.edu in the file: pub/les/cfp-93

[SEE ALSO RISKS-14.21 (with an address correction in 14.26). PGN]

2nd Conf. on Computers, Freedom, & Privacy-written & elec. proceedings

"Lance J. Hoffman" <hoffman@seas.gwu.edu>
Thu, 4 Feb 93 16:58:10 EST

The written proceedings and the electronic written proceedings of the Second Conference on Computers, Freedom, and Privacy, sponsored by the Association for Computing Machinery and held March 18-20, 1992 in Washington, D. C. are now available.

To obtain the written proceedings, contact the ACM Order Department, P.O. Box 64145, Baltimore MD 21264, 1-800-342-6626 or 1-410-528-4261 (MD, AK, and outside US). The ACM order number is 533921. The price is $15.00 for ACM members and $26.00 for others.

To obtain the electronic proceedings, make an ftp connnection to ftp.gwu.edu and login as "anonymous". Get file CFP2S00, which has a table of contents describing the other files CFP2S01, CFP2S02, ..., CFP2S11. Get these files if you desire them.

Professor Lance J. Hoffman, Dept of Electrical Engineering and Computer Science
The George Washington University, Washington, D. C. 20052
(202) 994-4955 fax: (202) 994-0227 hoffman@seas.gwu.edu

Educational Loan Services -- ELSI

Steve Hoffman 24-Feb-1993 0959 <hoffman@xdelta.enet.dec.com>
Wed, 24 Feb 93 07:27:00 PST

My mother recently received several telephone calls from an organization called Education Loan Services Inc (ELSI), of Braintree, Massachusetts. Neither she nor any other family member had ever heard of ELSI -- an organization that reputedly acts as a student loan clearing house, and as I have inferred from my conversations with them, as a collections agency.

The callers asked for her (Marie) or for my wife (Kelly) concerning a student loan. (Both my wife and I have had student loans. Mom predates the modern concept of a student loan :-) Mom, being computer-literate and quite familiar with the more typical computer snarls, naturally assumed it was a computer error and that it concerned either Kelly or me -- she naturally assumed the ELSI database had not been updated to indicate that both of our student loans had been paid.

After an extended conversation with a representative of ELSI, I found they were "cold calling" anyone with a name that matched those on their loan paperwork, and further, that the match with Kelly's name was (apparently) a fluke. Further, the only way they claimed they could confirm that they had a mistake was for me to provide them with Mom's social security number.

ELSI refused to accept any other information from me -- length of time at address, differences in surnames, attendance at other schools, etc -- concerning the parties (not) involved, nor could they provide any information on the cosigners of the student loan they claimed they were calling on.

When my mother called ELSI back, a (different) ELSI representative indicated that it appeared to be a simple mix-up on the area code, and that her portion of ELSI did not have direct access to the ELSI folks placing the outbound calls. (Which we found rather surprising.) Interestingly, a different ELSI representative had told me that ELSI was calling people based on directory services information -- and not based on a mixed-up telephone number on the loan paperwork.

This situation strikes me as having multiple risks. I could have provided ELSI with a bogus social security number for Mom. (I declined to provide any number.) If ELSI could validate the social security number -- and I am quite certain they could, via any one of several credit bureaus -- they would have already known that mom wasn't a match. (And then why did they call?) Such an organization could also easily be illicit -- "scavenging" either for social security numbers or worse, scavenging payments from the parents of former students -- parents who might unknowingly send an ELSI-like organization a payment or two to keep their child from `defaulting'.

Steve Hoffman   hoffman@xdelta.enet.dec.com

Phone problems: "...Phone Jam" (RISKS-14.31) and a new problem

<warner@ohio.gov>
23 Feb 1993 20:15:07 -0400 (EDT)

One of the major causes of the long time to get the data from the failed computer is that phone switches have a lot more 'state' that they did in the past. For example, the State of Ohio Centrex (where I work in the telecom office) is served by the switch which failed. We have somewhere over 20,000 lines (I don't keep up with the details.) In the past we had to configure options like Call Forward No Answer and Call Forward Busy with written service orders. But now each line has an option called Call Forward No Answer Universal (At least the name is close!) which allows someone at the phone to specify the number to Call Forward Busy to. This can be changed at any time. Therefore in the case of a switch failure you can not just return to the "standard" configuration, but must load a lot of 'state' information from the failed computer.

This type of state is becoming more common in "fancier" features. It makes it much easier to manage a large number of phones! Features like call forwarding, which also require the switch to remember a number, are becoming more and more common.

The State of Ohio phones were dead from about 14 minutes or so. This likely affected the Franklin County Ohio Highway Patrol Post's (and General Head Quarters) public numbers also.

Also, in yesterday's Columbus Dispatch it looks like Ohio Bell lost another one:

The Columbus Dispatch, Wed Feb 17, 1993 Page 3 C (Metro Section)
(Small article at the bottom in Columns 1 & 2)

"Blown Fuse disrupts phone service"

A blown fuse in the Ohio Bell switch serving 54,768 telephone lines in Worthington disrupted service throughout the day yesterday. Repairs were expected to be completed last night. Ohio Bell Spokesman Keith Jameson said 911 and other emergency numbers remained in operation, although getting a dial tome within the affected area was slow. Calling into the area was difficult most of the day, since Ohio Bell purposely blocked 75 percent of incoming calls while repairs were under way. Jameson said that strategy enabled people within the area to make calls. By 5 PM, the company had reduced blocked incoming calls to 50 percent. The switch shut down at about 10:30 AM, when at least one fuse blew, but Jameson said there may be other problems with the switch. The problem was not weather related, he said.

William "Bill" Warner, III (N8HJP), State of Ohio - Telecommunications
2151 Carmack Rd, Columbus, OH 43221 (614)466-6683 warner@ohio.gov (Internet)

MIT's on-line Student Information Services (Kamens, RISKS-14.35)

<smb@research.att.com>
Wed, 24 Feb 93 12:21:43 EST

>In order to use SIS to access personal data, a user must first register an
>"extra" password with the Kerberos database. The program that registers this
>password does so by transmitting it to the Kerberos server in encrypted form
>(using a key derived from the user's main Kerberos principal, for which he
>already has a password) so that it isn't exposed to the network.

But has the Kerberos protocol been beefed up yet to guard against password-guessing attacks?

As Michael Merritt and I noted in our critique of Kerberos (Winter Usenix, 1991, Dallas), Kerberos is vulnerable to password-guessing. An intruder, from anywhere on the Internet and without any authentication, can request ticket-granting tickets for any user. These are encrypted with a key derived from the user's password. But guessing at passwords is an old game -- and one that succeeds, with ~25% probability, against typical UNIX system passwords. Kerberos is somewhat more secure, since it permits passwords to be longer than 8 characters, but I'm unaware of any study that's been done to find out if people actually take advantage of this.

Granted, such attacks may not succeed against any particular student. But against a collection of students, the odds are pretty good that some will be vulnerable.

I've seen proposals to strengthen Kerberos against such attacks, but I don't know if these have been deployed yet. And there are protocols that prevent any password-guessing attacks, even by eavesdroppers (i.e., Lomas et. al, 1989 SOSP; Bellovin and Merritt, 1992 Oakland Symposium).

My point here is not to criticize the designers of SIS. All things considered, they seem to have done a very good job; the only other safeguard I can think of would be to notify the student of any new uses of the SIS account. Rather, I'm trying to point out that secure systems can't be built on weak foundations. Intruders don't go through security; they go around it.

--Steve Bellovin

Kerberos and password-guessing attacks

"Jonathan I. Kamens" <jik@aktis.com>
Wed, 24 Feb 93 18:14:16 -0500

> From: smb@research.att.com
> Date: Wed, 24 Feb 93 12:21:43 EST
>
> But has the Kerberos protocol been beefed up yet to guard against password-guessing attacks?

Yes.

The most recent release of MIT Kerberos Version 4 includes kadmin protocol enhancements to allow for the rejection of weak passwords, and code on the server to check and reject weak passwords.

I don't know if any V4 vendors have incorporated changes like this into their products; I suspect it will happen eventually if there is enough demand for it.

Furthermore, MIT Kerberos Version 5 supports optional preauthentication. MD5 on the user's password, Smart Card technology, or some other technique (the code is pretty abstract, so new preauthentication types can be added relatively easily) is used to create a "magic cookie" which is passed to the server along with the TGT request. If the cookie is wrong, the server won't give the user a TGT to decrypt. Preauthentication can be required or optional on a principal-by-principal basis.

MIT V5 doesn't yet have weak-password rejection in it, but the hooks for it are there, and it will be added before the first official (i.e., not beta test) V5 release.

I don't think DCE Kerberos has preauthentication in it right now, and I don't think they plan to add it before the first official DCE release (If you want them to, and you're a member of the OSF, then let them know!). I don't know whether or not DCE Kerberos has weak-password rejection in it.

It is true that both V4 and V5 are still vulnerable to network eavesdropping weak-password attacks, since an eavesdropper can watch for a TGT on the network and try to decrypt it once it arrives, even if he doesn't know the preauthentication magic cookie which convinced the server to send the TGT. However, weak-password rejection makes the risk of an attack of this sort minimal, and it is not vulnerable on an entire-Internet scale like the attack which Steve mentioned.

(Thanks to Ted T'so, tytso@mit.edu, for confirmation of much of the information above about V5.)

Jonathan Kamens   jik@Aktis.COM

Re: Tapping Phones (Schumann, RISKS-14.35)

Fred Cohen <fc@turing.duq.edu>
Wed, 24 Feb 93 07:51:07 -0500

I must disagree [with the statement] that I am creating an unrealistic security scare. In fact, even if you are running Kermit from a PC, there are ways for remote sites to inject commands/code into your machine. The same is true for many PC-based telnet, FTP, and Xmodem protocols. Here is a real example:

An FTP program was commonly used at one university to transfer information between user PCs and a file server. One day, someone noticed files appearing on their computer that shouldn't have been there. On subsequent investigation it was found that the FTP protocol allowed remote users to send files into the PC whenever the PC was setup to do outgoing transfers. It turns out that this is one of the most popular - public domain - FTP packages around. At this one site, a password was added to the process to prevent exchange when the other party did not know the password - but - they did a poor job of it, and someone discovered a trivial way to get past it within a few days.

Another?:

The well known attack where you transmit characters to a remote terminal that tell the terminal to store a sequence of characters and play it back can be exploited to attack remote computers running terminal emulators that are accurate. If you run Kermit, you may find that the VT emulations are good enough to do the job. That's right - even if you are simply logged in typing commands, you can be had if the attacker is good enough at it and your package is a true emulation. In fact, when you login, you usually even tell the remote site what kind of terminal you are emulating, thus easing it's attack burden.

Another?

X-windows without the magic cookie allows remote users to watch what is being displayed on your screen over the network. Most X setups are insecure in this way - at least most of the ones I have seen.

Another?

Well - I'll hold off for now awaiting your response. My point still seems to hold - encrypting links is not adequate to prevent access to your data - encryption without good computer security is generally not adequate - the government or anyone else willing and able to go to the trouble can get you by exploiting the places you login to - it is not patently safe to login to on-line information services, even if you don't run their software. - FC

Re: On-line services (lack of) security (Schumann, RISKS-14.35)

Bill Seurer <seurer+@rchland.ibm.com>
Wed, 24 Feb 1993 13:45:09 -0600 (CST)

"Mark W. Schumann" <mark@whizbang.wariat.org> writes in RISKS 14.35

>Prodigy, the latter service you mention, requires the use of its own front-end
>program on your PC. You cannot use Prodigy without it. Since this front-end
>program executes on your PC, it does have the potential for the abuse you
>mention. I personally do not use Prodigy in part because of this security
>loophole.

Oh boy, let's kick Prodigy around some more. Long ago when I was a Prodigy subscriber and the rumors of Prodigy's uploading of stuff it shouldn't started I did some experiments the results of which were posted here. I proved (as best I could) that the rumors were probably unfounded and based on Prodigy's method of allocating disk space without clearing it of previous data first. Some other people who contacted me had done similar experiments with similar results.

>On the other hand, other communication services, such as Compuserve, do not
>have this questionable "feature" at all.

America On-Line, TSN, and probably others also have special communication programs that you must use. Other services which do not REQUIRE a specific comm program nonetheless OFFER one that usually improves use of the service. Genie (for sure, Aladdin) and Compuserve (vague memory from years ago) both do.

>You dial Compuserve from your PC with a communications program of your choice.
>At all times the contents of your memory and hard drive are under the complete
>control of your CPU and communications program.

Yeah, but how do you know that the authors of PC-TALK, Qmodem, or whatever don't have a special hook in them that when you call up Compuserve it doesn't (semi-seriousness on) upload all your pitiful Tetris scores so the FBI can blackmail you? Or heck, maybe Microsoft has modified Windows or DOS to append juicy data to the end of files opened for uploading somehow. Maybe the FBI knows that the authors of Qmodem use Turbo C++ (or whatever) and have had Borland modify the compiler to insert this surreptitious uploading code into the comm program automatically when it is compiled. Maybe AMI has modified this BIOS to do something like this. Who can you trust?

(paragraph about QUICKB deleted)

>Bottom line: No online service can cause your PC to execute code that is not
>in the PC's memory space, Prodigy notwithstanding.

Not true as I have already shown.

In any case, any service that tried something like this would be committing corporate suicide. People would notice that their modems were uploading all this data if by no other means than the Send Data light on their modem and the hard disk access light and doubtlessly one of them would figure out what was happening.

Even at high speeds with top notch data compression it still takes a long time to transfer any significant amount of data. Maybe "they"

could somehow work it into the background so whenever your modem sent
data you wanted it to a little bit extra would get mixed in but that
seems pretty pointless.

- Bill Seuer   Language and Compiler Development   IBM Rochester, MN
  Internet: BillSeurer@vnet.ibm.com   America On-Line: BillSeurer@aol.com

Re: request for opinions on Artificial Life (Cohen, RISKS-14.34)

"Bill Humphries, Data Husbandry Flunky" <humphrie@ssc.wisc.edu>
Wed, 24 Feb 93 13:41:18 -0600

I understand that most AL research is done by writing AL programs which run on a virtual computer. The practice is analogous to hacking E Coli which can only live on a particular medium which is not availiable outside the lab's petri dish.

I have no problem with people publishing code, even code which could be put to 'sinister' ends (such as PGP). The author is not responsible for the actions of the reader or end-user.

If you want to provide some sort of security, perhaps you can make a proprietary virtual machine which you distribute with the code in your book.

The code would then only run on the virtual machine. This could provide some way of at least tracking the spread of malevolent AL programs.

Obviously this is not a perfect solution, but hey, what that guy from NASA says, this isn't a risk free world.

Bill Humphries <humphrie@ssc.wisc.edu> : U. Wisconsin Economics : 608-262-4543

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 37

Thursday 4 March 1993

Contents

Power Outage Locks Up Jail System

Jennifer Smith <jds@hardy.math.okstate.edu>
Fri, 26 Feb 93 19:59:44 CST

NEW SOFTWARE FAILS TO FIX JAIL'S COMPUTER SYSTEM, by Judy Kuhlman, Daily Oklahoman, 26 Feb 1993

An attempt by Oklahoma County officials to fix their troubled jail's malfunctioning computer system failed Thursday. Prisoners remained locked inside their cells for the fourth consecutive day in the $54 million, 12-story jail that opened in November 1991, Oklahoma County Sherrif J.D. Sharp said. "Everything is just like it was. The computers are still down. We have an open facility. Some doors are locked open and others are locked closed, both inside and outside the facility," Sharp said. Twenty-two jailers were trapped from 10 am to 6:30 pm Monday inside a jail control room when the controlling computer shut down following a five-minute power outage. Guards since then have been manually opening and closing the prisoners' cell doors, Sharp said.

Computer software purchased by jail officials at a cost of $4,836 and installed Thursday did not fix the jail's problems, Capt. James Rouse said.

Oklahoma County commissioners had an emergency meeting Wednesday to approve the purchase of that computer diagnostic equipment and to consider additional equipment needed to deal with the county's latest jail crisis. Officials were not certain what caused the computers to shut down, Oklahoma County engineer Ted McCourry said. "We're taking it one step at a time. But every time we round one corner, we run into another problem. Slowly but surely we're getting it back. But we will still need outside help," Rouse said. The technician who built the computer system is supposed to fly into OKlahoma City from Denver today to assess the problem and recommend a solution, Sharp said. "I'm extremely frustrated. I have never seen anything like it. It is a real touchy situation here," Sharp said. Sharp said there was no danger of prisoners escaping. "We have called in extra people and are taking extra precautions which I cannot talk about at this time," Sharp said.

Commissioners have also authorized the purchasing agent to immediately go out for bids for a power-surge protector, expected to cost about $80,000, to prevent electrical surges and a battery back-up system for the computers that could cost an estimated $500,000. McCourry said the power-surge protector and back-up system was never included in the original jail plans and specifications. Commissioner Shirley Darrel asked the purchasing agent to find out who took the surge protector out of the specifications and why it was taken out in the first place.

Sharp has said the problems might have been averted if the county jail had been provided with a back-up system or a power-surge protector.

McCourry said the jail has a back-up generator to supply power in the advent of a power outage. The computer back-up system would act as a third source of power for computers.

County Clerk John Garvey has also suggested the sheriff hire a full-time computer expert.

[This is, I believe, the same "escape-proof" jail that had 2 escapees within a month of its becoming operational. Having computer-controlled doors with not even a surge protector, not to mention no one in the state running the system, is unfortunately quite typical. Jennifer Smith jds@math.okstate.edu]

[We previously reported the effects of a failure of automatic jail-doors in El Dorado, California, in 1988. PGN]

Hacker disables cancer database

<Jonathan.Bowen@prg.ox.ac.uk>
Thu, 25 Feb 93 14:16:52 GMT

Following is an abridgement [by JB and PGN] of an article that appeared in the Home News section (page 4) of the Guardian newspaper in the UK on 25 Feb 1993:

> A schoolboy computer hacker caused chaos when he dialed into a vital database at a Brussels-based centre for cancer research and treatment. Paul Bedworth allegedly ran a rogue program that generated 50,000 phone calls, and caused the computer system at the European Organisation for the Research and Treatment of Cancer to "crash". In the process, Mr. Dedworth, now 19 and a student of artificial intelligence at Edinburgh university, left the centre with a 10,000 pound [c. US$14,000] phone bill. His trial is in progress.

Jonathan Bowen, Oxford University Computing Laboratory

> [A Reuters story noted by "Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> says Bedworth also broke into the British Telecom telephone network, a Lloyds Bank computer, and the Financial Times of London. PGN]

Smells like Green Spirit...

Jeffrey S. Sorensen <sorenj@rpi.edu>
Fri, 26 Feb 1993 14:42:03 GMT

In the Jan/Feb issue of _Health_ magazine p. 53:

> Talk About Paying Through the Nose
>
> Bill-collection agencies in England began lacing their invoices with a product containing androstenone, a chemical secreted from men's armpits and groins that is known to be a sex attractant in some species. In one preliminary study, mailed invoices treated with the product resulted in a 14 percent higher payment rate than untreated bills.

and from the Art of User Interface design:

> The Less Care She Got, The Less She Cared
>
> A patient in Manchester Royal Infirmary in England was found unconscious after she mixed up the nurse's call button with the one to give herself more painkiller and pressed the latter button impatiently for several minutes.

Jeffrey Sorensen   sorensen@ecse.rpi.edu

Evacuation plan, generators fail in World Trade Center blast

"Jay Elinsky" <elinsky@watson.ibm.com>

Sat, 27 Feb 93 20:43:30 EST

The New York Times, in its morning-after coverage of yesterday's huge explosion in the World Trade Center garage in downtown Manhattan, reported that the blast destroyed the complex's operations center and severed cooling lines for the emergency generators. The result was that there was no organized leadership in evacuating 50,000 people down the stairwells of the 110-story twin towers, and the ventilation system was unable to suck out smoke. As of tonight, the toll stands at 5 killed, 2 missing, and over 1,000 injured.

The former director of the agency that runs the center said that studies in the mid-80's showed it could withstand a car bomb. "'They said you could sustain a car bomb', he said. 'What they didn't tell us was you couldn't sustain it if it was perfectly placed.'"

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

[NOTE ADDED 1 MAR 1993: Maybe my submission was a bit hasty. Today's Times says that the Port Authority *did* know in 1985 that a car bomb could disable building systems, but they decided not to implement the recommended changes because of the expense. Jay]

[An old story, eh? Security is almost always considered too expensive until AFTER the disaster. An 3 March 1993 AP report suggests that that the closure would last for at least a month, and the city of NY speculated that the "initial disruption is costing $100 million daily" with second-order costs per day increasing daily. PGN]

Bank account problems

Jeremy Epstein <epstein@trwacs.fp.trw.com>
Mon, 1 Mar 93 09:39:04 EST

According to a Washington Post article last week, the Resolution Trust Corporation [the federal agency charged with cleaning up failed savings & loans] generated incorrect data on Form 1099s [that's the form that tells the Internal Revenue Service how much interest you earned for the year, so you pay tax on it].

According to the article, there have been some serious glitches, including a woman whose 1099 reported $152,000 in interest, rather than the $3,000 she actually earned. Other statements were off by a factor of 100 or more. According to the article, the IRS was not sent the erroneous figure, although about 2000 customers of the failed Trustbank received incorrect notices.

The error occurred because "of a computer tape mishap" according to an RTC spokesman. No further details on the mishap were provided.

As more and more data is submitted to the IRS electronically, and the IRS does more and more electronic cross-checking, it's easy to see how people could have received automatic dunning notices for underreporting their income, had the erroneous data been sent to the IRS. I wonder whether the IRS's analysis software (or auditors) would have noticed that for many people, the amount of interest reported was highly unlikely given their historical tax data and income.

Jeremy Epstein, Trusted X Research Group, TRW Systems Division
Fairfax Virginia +1 703/803-4947 epstein@trwacs.fp.trw.com

The White House Communication Project

David Daniels <0004381897@mcimail.com>
Thu, 25 Feb 93 16:25 GMT

FYI... HERE'S SOME GRIST FOR THE MILL!

>Date: Tue, 23 Feb 1993 22:55:18 GMT
>Sender: Computers and Society ARPA Digest <COMSOC-L@AUVM.BITNET>
>From: Shellie Emmons <sme46782@uxa.cso.uiuc.edu>
>Organization: University of Illinois
>Subject: The White House Communication Project
>
>I am currently involved in a research project that is trying to aid the
>Clinton Administration in making effective use of computer-mediated
>communication to stay "in touch" with the public. Our coordinator has
>gotten in touch with Jack Gill, Director of Electronic Publishing and
>Public Access Electronic Mail for the Clinton Administration, and he
>(Gill) has embraced the efforts of the research group to lend a helping
>hand to this task. Some questions he has posed to the researchers include
>the following:
>
> (1) When you get thousands of messages a day, how do you
> respond effectively?
> (2) How do you make a public e-mail system inclusive
> and accessible?
> (3) What would happen if e-mail became the primary
> mode of(mediated) access to government?
>
>We would appreciate any insights and suggestions of possible solutions to
>these questions.
>
>Shellie Emmons sme46782@uxa.cso.uiuc.edu

[Respond to Shellie. I sent a noted several weeks ago to Jack Gill,
but have heard nothing. I presume he is absolutely swamped. PGN]

Re: your permanent record

Richard A. Schumacher <schumach@convex.com>
Thu, 25 Feb 1993 02:43:22 GMT

Forwarded to protect another's privacy.

>Some weeks ago, conversation on AFU turned to the existence of
>'permanent records' for grade school and high school students.
>It turns out that the state of OHIO has been keeping computerized
>records of Ohio primary and secondary students. The local paper
>has exposed this mess in the past week. I quote from the
>_Columbus Dispatch_:

> Virtually all school districts are sending 93 categories of
> information about each of Ohio's 1.8 million primary and
> secondary school students to 25 regional data centers.

> The information is linked to a student identification
> number, which the state says should be the student's social
> security number. The computer data include test scores,
> disciplinary action, medical details including pregnancy,
> race, handicaps and family income. [...]
> Princeton [a Cincinnati HS] supplies the state with
> statistics that do not identify students, but has never
> given information linked to names or identification numbers.
> As a result, the state has threatened to cut off the
> district's funding, beginning with it's April payment of
> about $288,000.

> Princeton and other school are suing the state based on the
> Federal Privacy Act. [...]
> Many districts don't even tell parents or students they are
> sending information about students to the state.

>[many sordid details deleted for brevity]

>Ohio has also kept a database of accusations of child abuse
>with 200,000 names on it. Ohio's population is about
>11,000,000. It was, until recently, impossible to find out
>if you were on the list, and who accused you, and impossible
>to get your name removed. If you worry at all about due
>process, facing your accuser, etc., don't bother to move here.

>I considered posting this information to COMP.RISKS or
>COMP.SECURITY.PRIVACY, but I didn't care to be "Jolted" by the FBI or CIA.

New York Telephone's newest dis-service

Jeffrey S. Sorensen <sorenj@rpi.edu>
Mon, 1 Mar 1993 19:50:09 GMT

In the Feb '93 "Hello" notice distributed with our monthly phone bill is an informative little piece about CIRCUIT 9(sm) This service "allows business subscribers to identify a caller's ``billing'' telephone number, even if the number is not published in the telephone directory."

CIRCUIT 9 services are assigned to 910 exchanges in the 212 and 718 area codes,
920 elsewhere in NY State, and 880 in area code 900.
Note that the CIRCUIT 9 exchange 880 is actually a fee-per-call 900, which have
long had the ability to receive calling number information.

Here's the juicy section:

There are important limitations on the ways in which businesses that obtain your phone number through CIRCUIT 9 Service may use this information. For example, they may use your number to route or screen calls, or to obtain billing information about your account with them.

However, subject to certain exceptions [?!], businesses that obtain your phone number through CIRCUIT 9 Service may not use your number to establish telemarketing lists or to conduct outgoing telemarketing calls without your consent. [!?]

If you believe a business has misused the information they obtained through CIRCUIT 9 Service, you may call a special toll-free number. Call 1-800-729-8924 Monday through Friday 9am to 5pm.

The notice goes on to tell you that you can have these calls blocked by calling you service representative, but doing so will also block exchanges 394, 540, 550, 970, and 976 and the area codes 700 and 900. I guess privacy is an all or nothing...

Further, the notice ends stating "Because CIRCUIT 9 service uses a different technology [?] from Call ID, the restrict options [mandated by the PSC] (per-call and all-call restrict) used to prevent number delivery through Call ID cannot be used to prevent number delivery through CIRCUIT 9 service."

I am beyond confused at this point. What do they mean "certain exceptions?" What constitutes my "consent?" It almost seems NY Tel is admitting they have had an utter disregard for our privacy in the past and are just writing us to say they will continue in the same vein in the future.

I wonder what horrible punishments will rain down upon and business that I report to their 800 number...

Jeffrey Sorensen sorensen@spl.ecse.rpi.edu

Phone Company Writes to a Public Telephone

Mark Brader <msb@sq.com>
Tue, 2 Mar 1993 01:49:00 -0500

warren@itexjct.jct.ac.il writes in comp.dcom.telecom:

> The August 14 edition of Yerushalaim (a Jerusalem local newspaper)
> contains a copy of a letter that Bezeq, the Israeli telco, mailed to a
> phone booth which it owns.
>

> The form letter is addressed to "Bezeq, Inc." at the address at which
> the phone booth is located (155 Costa Rica Street), and informs the
> subscriber that while in the past, its bill was computed by reading a
> meter, which made it impossible to obtain a listing of calls made,
> this will now be possible (at a fee, of course, something that Bezeq
> did not mention to the phone booth).
>
> The letter-carrier delivered the letter by placing it inside the phone
> booth.
>
> Bezeq responded that the program that sends out mailings will be
> corrected. The phone booth was unavailable for comment.

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

Cohen/Radatti on Unix and Viruses

Pete Radatti <radatti@cyber.com>
Wed, 3 Mar 93 14:16:47 EST

The widely circulated paper by J. David Thompson entitled "Why Unix is Immune to Computer Viruses" has been attracting controversy. Due to this controversy and the concern that this paper may be providing a false sense of security to the Unix community, Doctor Fredrick B. Cohen and Peter V. Radatti have published refuting papers. These papers are too long to post here, however they are available upon request. Make your request by fax, email or post and copies can be returned by fax or post. Email copies are not available.

Address post to:
Peter V. Radatti, C/O CyberSoft, 210 West 12th Avenue
Conshohocken, PA. 19428 USA

FAX requests to: +1 (215) 825-6785

Email requests to: radatti@cyber.com

Thank You, Peter V. Radatti

London Ambulance Service - the Report

<Brian.Randell@newcastle.ac.uk>
Sat, 27 Feb 1993 10:21:29 GMT

On Friday 26 February the UK national newspaper The Independent covered the just-released report on the London Ambulance Service debacle very fully - it was the main story on the front page (entitled "Report Prompts Departure of Ambulance Boss"), with three more stories taking up a significant fraction of page 3. These are entitled "Manager's `created an atmosphere of mistrust'", "[Secretary of State for Health] Bottomley condemns `catalogue of errors'", and "Father grieved for asthmatic son who died in his arms". The first of these three has the most detail, and is quoted below in its entirety.

Brian Randell

==========

The London Ambulance Service Crisis

MANAGERS "CREATED AN ATMOSPHERE" OF MISTRUST,
By Susan Watts, Technology Correspondent, The Independent, 26 February 1993

It would be hard to paint a more damning picture of failed management than that which emerged from the inquiry into the London Ambulance Service yesterday. The report said that the LAS management "created an atmosphere of mistrust" with its over-aggressive style, born in part out of the desperation to put right decades of poor performance.

The LAS made "virtually every mistake in the book" when implementing its "ambitious" (pounds)1.5m computer system, one of the three-strong inquiry team said. The computer-aided dispatch (CAD) system was seen as the only hope the service had to put right its poor response times in dealing with emergency calls. But the software was "not complete, not properly tuned, and not fully tested", the report said.

The inquiry team was set up after the CAD system broke down on 26 and 27 October last year, then collapsed a second time on 4 November, forcing controllers to revert to pen and paper to dispatch ambulances.

Managers took a high risk, "misguided" decision to have the CAD system up and running in one phase. The system was developed and installed in "an impossible timetable", the report said. The final system had known technical problems, and the people who would have to use it were not properly trained to do so. The team concluded that LAS management ignored advice to this effect "from many outside sources".

One of the team members, Paul Williams, said management had concentrated on getting the best price for its computer system rather than one which would be best for the job. He said he would have expected a system of this kind to have cost at least twice as much as the LAS computer. The report said there was "no evidence of key questions being asked about why the [final] bid was substantially lower than other bidders". The report questioned the apparent lack of accountability within the service itself, and upwards to managers at regional level. This was exacerbated by the LAS operating at arm's length from its health authority, which meant it was not subject to checks from regional managers.

The team said that although the computer system did what it was supposed to do, the design had "fatal flaws" that together would lead to all the symptoms of a systems failure. It found that System Options, the software company which supplied the system, had never before dealt with a system this large and complex. "We believe that they [the software supplier] rapidly found themselves in a situation where they were out of their depth.

The team believes that some parts of the failed software system can be salvaged, although chunks of the applications software may need to be substantially rewritten.

The report refutes earlier statements from the LAS that the two disastrous days in October had been exceptionally busy. The number of calls was in fact only a little above average. It was only when ambulances failed to arrive, and duplicate calls came in, when things got out of hand.

LAS board members appeared to have been given a "misleading impression" about progress with the computer system and regional members seemed to have been given even less of an idea what was going on within LAS.

Last year's crisis prompted the resignation of John Wilby, the chief executive of the service. Yesterday, South West Regional Health Authority revealed that it had already decided to remove Mr Wilby from his post, having first raised fears over his performance at a meeting with him six months before the computer breakdown.

Jim Harris, LAS chairman, denied that this might have put pressure on Mr Wilby to produce results. But the report concluded that "an important factor was almost certainly the culture within LAS of `fear of failure'."

Professor Marion Hicks, the health authority's chairman, said Mr Wilby was given a limited time to improve, but by mid-October "the decision had been taken to terminate his contract". This would have gone ahead in November if the LAS board had not been taken over [sic] by events, and Mr Wilby's voluntary resignation.

Non-executive LAS board members who remain are Roddy Braithwaite, Victor Paige, Mary Spinks, Janet Preston and Stephen Miles. The executive committee comprises Martin Gorham (chief executive), Alan Kennedy (acting director of operations), Simon Young (director of finance) and Bernadette el-Hadidy (director of human resources).
[Ends]

The front page story leads with a report that the chairman of the LAS, Jim Harris has resigned, and repeats the union claim that up to 20 deaths resulted from ambulance delays, but states that this allegation is hotly denied by management, adding that: "Yesterday's document shies away from linking deaths directly with ambulance delays caused by the computer crash. It said an examination of 26 cases at coroners courts since November 1991 showed that the LAS had not been blamed for a single death. Two cases are outstanding."

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,
NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923 FAX +44 91 222 8232

Bank machine glitch leaves users poorer, but empty-handed

Randal Schwartz <merlyn@ora.com>
Sun, 28 Feb 93 12:37:14 -0500

>From The Oregonian, Sunday, 28 Feb 93:

Bank machine glitch leaves users poorer, but empty-handed

For thousands of people last week, automatic tellers charge their
accounts without dispensing money

>From staff and wire reports

Customers who used an automatic teller machine in U.S. Bank's Exchange system Thursday morning may want to take a close look at their next monthly statement to make sure everything adds up.

Thousands of Oregon ATM users who tried to withdraw money between 4 a.m. and 10:30 a.m. Thursday came up empty-handed, even though the machine's faulty computer software subtracted the money from their accounts anyway. A U.S. Bank spokeswoman assured that all accounts would be corrected by Tuesday.

Mary Ruble, corporate spokeswoman for the Portland-based company, said the bank has what is called a redundant computer system that keeps track of all transactions and has passed the information to all banks who have customers who have been affected.

Ruble said Saturday that 18,000 transactions in Oregon, Washington, Idaho, Nevada and California were affected Thursday.

"We are aware of the problem but we haven't been able to clear them all up yet," Ruble said."We've shifted people from other responsibilities to speed up the correction process."

John Kresge, vice president and manager of the U_S_ Bank's ATM network, said the problem started when the bank was modifying the software in its main computer in Portland. The computer links U.S. Bank with The Exchange, a huge electronic clearinghouse that coordinates ATM deposits and withdrawals for customers of banks throughout the Northwest.

The glitch affected only non-U.S. Bank customers who tried to make transactions from U.S. Bank's ATM machines, Kresge said. It is not known which banks were affected the most.

To safeguard from any account discrepencies [sic], Ruble recommends that ATM users keep their receipts and compare them with their monthly statements. Problems should be reported to the customers' individual banks.

Kresge said all accounts will be properly credited, whether or not customers noticed the problem.

"I hope there isn't too much anxiety out there," Kresge said. "I am certain each one of those transactions will be reversed. We have an army of people looking at it. They are manually going through all the transactions and making corrections and reversing any charges that may have occurred."

Randal L. Schwartz / Stonehenge Consulting Services (503)777-0095
merlyn@ora.com (semi-permanent)

Does Publisher's Clearinghouse Use Information America?

Jane Beckman <jane@stratus.swdc.stratus.com>
Mon, 1 Mar 93 18:02:49 PST

I read the article on "Information America" with great interest, as it would explain a great deal of things that have bothered me, wondering how certain individuals got particular information.

In the first instance, we received a phone call from a law enforcement agency looking for a "Mark Frates." This individual has become known to us, as arrest warrants, letters from lawyers, etc. have arrived on a regular basis, to be returned "Not here." Since his last name matches the previous owners' name, we assume he (and his several aliases) is their son. But HOW, I wondered, did they get OUR phone number? We moved into a house formerly owned by his parents, but our phone number was not connected to the Frates. Apparently, someone has used this, or a similar, service, trying to track this guy down.

But the most worrying piece of mail came from the lowly Publisher's Clearing House. It was the standard hype, with "you may be the winner..." and all, but it had a worrying piece of personalization. "Although you have not ordered anything from us since 1982..." In the time in between, my husband had moved five times, and had not even renewed the original subscription. Somehow, Publisher's Clearinghouse had tracked him across the country, and from Washington State to California, through the course of several moves, and had paired him with a magazine subscription from ten years before. Impressive tracking capability for a junk mailer! Especially one who, by implication, must have files on most of the residents of the U.S. Imagine what someone with more interest in you could do...

Jane Beckman [jane@swdc.stratus.com]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 38

Sunday 7 March 1993

Contents

6th Int'l Computer Security and Virus Conf

Richard W. Lefkon <dklefkon@well.sf.ca.us>
Thu, 4 Mar 1993 12:52:02 -0800

SIXTH INTERNATIONAL COMPUTER SECURITY & VIRUS CONFERENCE and Exposition
sponsored by DPMA Fin.Ind.Chapter in cooperation with
ACM-SIGSAC, BCS, CMA, COS, EDPAAph, ISSAny, NUInyla, IEEE Computer Society
Box 894 Wall Street Station, NY NY 10268 (800) 835-2246 x190

FINANCIAL FIRMS OPEN MEETING THURSDAY ON TRADE CENTER RECOVERY

To address the technical side of network and computer terrorism recovery while information systems personnel are interested, a special public forum of industry leaders has been scheduled for next Thursday March 11, entitled, "Trade Center Crisis Recovery." The in-depth panel will include eight industry representatives - from four affected financial firms that successfully resumed business after Friday's disaster, and four suppliers that helped them.

The panel will be housed in next week's Sixth International Computer Security & Virus Conference at the Madison Square Garden Ramada, co-sponsored by the eight computing and networking societies.

With damage estimates already in the multi-billions, Sally Meglathery, Electronic Security Head for the New York Stock Exchange and a scheduled panelist, warns financial data keepers: "Review [your] restart recovery procedures to be sure that you have adequate backup to recover from an attack."

Other than state and federal offices, the main corporations inhabiting the famed skyscraper are indeed banks (First Boston, Sumitomo, Dai-ichi), brokers (Dean Witter, Shearson, Salomon, Mocatta and the Commodities Exchange) and insurance companies (Hartford and Guy Carpenter). Each type will send a representative, as will some service firms.

William Houston, Eastern Region Head for Comdisco Data Recovery, notes that "This is the second time in three years an electrical disaster has completely shut down" the famed twin skyscraper. His firm helped rescue the computer, networking and "back office" operations of two dozen downtown firms in response to the August 13, 1990, electrical substation fire.

"We have some major customers in the Towers," notes Houston, "and while preserving their anonymity I intend to plainly tell the Thursday audience just what worked this time and what didn't."

Michael Gomoll, an executive with competitor CHI/COR Information Management, says the terrorist act will have three key results: "Direct loss of revenues, effects on global markets and businesses, and concerns of the business insurance profession." Ironically, CHI/COR, a firm specializing in disaster recovery, was itself assaulted by the crippling Chicago flood of April 13, 1992. As part of his presentation, Gomoll intends to explain how cable conduits played an important role in both disasters.

Last fall, the conference now hosting this "Trade Center Crisis Recovery" roundtable, received what now seem prophetic words in its greeting from Mayor David Dinkins: "As the telecommunications capital of the world . . . we are also extraordinarily susceptible to the various abuses of this technology."

Another irony has to do with the "Meet the Experts" reception at the Empire State Building Observatory following the forum. In previous years, the hosting conference has had its skyline reception at Top of The World, located within the Trade Center. That spot will not open this month.

also extraordinarily susceptible to the various abuses of this technology."

Problem with PLC Software

"Lin Zucconi" <lin_zucconi@lccmail.ocf.llnl.gov>
3 Mar 1993 16:50:50 U

People using Modicon 984 Series programmable controllers with Graysoft Programmable Logic Controller (PLC) software Version 3.21 are advised to contact Graysoft (414) 357-7500 to receive the latest version (3.50) of the software. A bug in Version 3.21 can corrupt a controller's logic and cause equipment to operate erratically. PLCs are frequently used in safety-related applications. Users often assume that if their "logic" is correct then they are ok and forget that the underlying logic is implemented with software which may not be correct.

Lin Zucconi zucconi@llnl.gov

Mass electronic scanning of UK international telexes from London

James Faircliffe <I_USERID_4@prime1.central-lancashire.ac.uk>
Fri, 26 Feb 93 17:30:55

[Originally in Computer Privacy Digest Sat, Volume 2 : Issue: 021,
27 Feb 93, contact comp-privacy-request@PICA.ARMY.MIL. PGN]

A few months ago, a well-respected British TV documentary show (might have been 'World in Action') discovered that all out-going telexes from the Uk were electronically scanned by British Telecom (the main phone company) personnel, supervised by the security services. Direct scanning by the security services would have been illegal. They were looking for words like 'terrorist' & 'bomb', but the civil liberties implications are far-reaching. Obviously, this could affect the privacy of American telexes to the U.K.

J.F. Faircliffe. i_userid_4@uk.ac.uclan.p1

`Untested' Risk Management System for Nuclear Power Stations

Anthony Naggs <AMN@vms.brighton.ac.uk>
Thu, 4 Mar 93 13:10 GMT

Headline: Sacked expert fears nuclear safety risk
Byline: Paul Brown, Environment Correspondent (The Guardian, 4 March 1993)

A computer system created to make Britain's nuclear reactors safer could fail at a vital moment because it has not been tested properly, according to the man who designed it.

Bob Hodson-Smith, who has been sacked by a company commissioned by Nuclear

Electric to design a back-up safety system for nuclear power station controllers, says the system might not perform adequately at precisely the moment it was needed because "bugs" had not been removed from the programming. He has expressed his fears to Nuclear Electric, the state owned company that runs [all commercial] nuclear power stations in England and Wales. It is understood that the company is seriously concerned at the implications.

The firm which sacked him, Active Business Services (ABS), of Sheffield, has described his fears as irrational. But Mr Hodson-Smith says: "I could no longer live with the fact that safety might be compromised and I had done nothing to warn anyone."

The Safety Related Plant Status Monitoring System, as Nuclear Electric describes the system, has been in operation at a Magnox power station at Oldbury-on-Severn in Gloucestershire for aa year. Similar computer systems are being brought into operation at Dungeness A in Kent and Hinkley Point A in Somerset.

Status, as the system was called, was designed to prevent the kind of accidents that occurred at Three Mile Island nuclear power station in the United States and the Piper Alpha oil platform disaster. In both cases shift workers faced with a breakdown in equipment switched to substitute systems, unaware that they had been taken out of service by a previous shift.

Status was designed to prevent this happening. Staff log into the computer every item of safety-related equipment in the nuclear station, so operators can see at a glance whether it is in proper working order. Safety at nuclear stations relies on all vital equipment being duplicated at least twice so any defective equipment can be bypassed.

Mr Hodson-Smith's alarm is based on the belief that the computer system might be relied on in times of emergency when "bugs" in the programming had not been removed. In memos he warned ABS that he was not satisfied the system was safe, and urged the company to inform Nuclear Electric of his fears.

In a memo to ABS managing director, Paul Sellars, he said he was aware he would be "fired" if he published the information but "I am not prepared to present a false picture to Nuclear Electric. I believe that what is being done with the Status project is not morally tenable."

Mr Hodson-Smith said he was not prepared to supply the newer Advanced Gas Cooled Reactor [AGR] (at) Hinkley Point B with a similar system unless Nuclear Electric were fully informed of the potential difficulties with Status at the other stations. He insisted that the system be thoroughly debugged, which could only be done by writing a technical manual explaining the system and cross-checking it. This had not been done.

In a memo he said that if it was a computer system for a bank "it would be acceptable to stick together a functionally complete version, install it and hope it was right. If it failed then it can be fixed as required. However, it is simply not acceptable to do this for a nuclear power station control room system related to safety."

Mr Sellars, managing director of ABS, responded by suggesting that Mr

Hodson-Smith consult a psychiatrist, Dr James Conway in Sheffield. Dr Conway's view of his patient was that "he exhibited symptoms of anxiety and overwhelming worry which would be understandable ... if his fears were well-founded. He believes there is little communication with the management at present."

In a letter Mr Sellars told Mr Hodson-Smith that the Status system would not become fully operative until fully tested. "The company does recognise the nature and extent of its responsibilities."

The company and Mr Hodson-Smith remained at loggerheads. He was subsequently dismissed, and has begun an action for unfair dismissal.

Mr Sellars said: "Mr Hodson-Smith had a very good brain but his behaviour has become irrational. He was not involved in the commercial area. He had become impossible to manage." Mr Sellars said there were no bugs in the system, which was being fully tested. Technical manuals on how the system was constructed were being written and would be provided to Nuclear Electric.

Mr Hodson-Smith has sent papers detailing his fears to the three nuclear stations involved and Nuclear Electric is studying them.

Nuclear Electric emphasised that the computer system had not yet been fully integrated into the control system for the reactors. Safety had therefore not been compromised.

Nuclear Electric said that the system was a management tool for checking equipment. In the case of an emergency the reactor would be shutdown automatically, independently of the Status system.

[A few of the risks covered: reliability of risk management systems; risk of bringing a system into disrepute by the actions of disruptive staff; risk of using a system for a year before full testing and manuals are complete; ...
Anthony Naggs, Software/Electronics Engineer, PO Box 1080, Peacehaven,
East Sussex BN10 8PZ UK +44 273 589701 amn@vms.brighton.ac.uk

Re: Evacuation plan, generators fail in World Trade Center blast

Scott E. Preece <preece@urbana.mcd.mot.com>
Thu, 4 Mar 93 14:20:50 -0600

| [An old story, eh? Security is almost always considered
| too expensive until AFTER the disaster... PGN]

Now let's be fair. How many other buildings got the same advice and have not been bombed? What is the expected benefit, over all major buildings, of ensuring against an event with probability x?

In any case, what difference would it have made? It would made the evacuation a little smoother and less traumatic, but I doubt it would have saved any lives or gotten the buildings re-opened any sooner.

Managers are always paid to decide how much risk is acceptable when weighed against how much expense. There is always some level of disaster against which you are not protected (suppose it had been a nuclear device). Maybe their decision was rotten and they just lucked out in not having a much larger loss of life; on the other hand, maybe their decision was pretty good and they had really bad luck in the placement of the bomb coupled with really good luck in not having any coincident problems to raise the death count. I don't know enough to know whether they acted correctly; I doubt that either the author of the note or the moderator know, either.

scott preece, motorola/mcg urbana design center, 1101 e. university, urbana,
il 61801 uunet!uiucuxc!udc!preece preece@urbana.mcd.mot.com 217-384-8589

Re: Where to buy emerg. stairwell lightbulbs? (Carlson, RISKS-14.37)

Joel Kolstad <kolstad@cae.wisc.edu>
Tue, 2 Mar 93 15:45:18 cst

>Help keep my building from suffering from 'World Trade Center Syndrome'
>(lack of emergency lighting)... Point me in the right direction please!

From the news I've seen, I got the impression that the emergency lighting was controlled by a central computer somewhere, although each separate light/battery pack had a little bit of intelligence of its own. However, whoever programmed the emergency light microbrains had a panic routine that just sat around trying to re-establish contact with the main controller if the main controller had blown up. But apparently it skipped the programmer's mind that, if the main controller had blown up, it just might be a good idea to turn on the emergency lights.

Does anybody know if this is true? If so, it's some really poor programming! Perhaps comp.risks would be a good place to take this.

---Joel Kolstad

Re: Does Publisher's Clearinghouse Use InfoAm? (Beckman, RISKS-14.37)

Karl Kraft <karl@ensuing.com>
Thu, 4 Mar 93 12:01:56 -0800

More likely, they use a service called National Change of Address. A well-known company will (for a fee), update a mailing list to reflect any changes in address in the last three years.

The well-known company? The United States Postal Service.

Karl Kraft karl@ensuing.com

Re: Smells like Green Spirit... (Sorensen, RISKS-14.37)

Barry Salkin <bsalkin@nyx.cs.du.edu>
Fri, 5 Mar 93 09:39:26 GMT

> A patient in Manchester Royal Infirmary in England was found unconscious
> after she mixed up the nurse's call button with the one to give herself more
> painkiller and pressed the latter button impatiently for several minutes.

It is usual practice with Patient Controlled Analgesia (PCA) to have a lockout on the syringe driver, so that the patient cannot give themselves repeated doses without sufficient time between them. This not only prevents overdoses, but also means one bolus (dose) of painkiller has time to act before the patient is able to give themselves another dose, so that if the first dose is effective, the second, later, dose will not be administered by the patient.

However, if the syringe driver wasn't set up with the time lockout .....

Barry.   bsalkin@nyx.cs.du.edu or zchag12@ucl.ac.uk

Re: The White House Communication Project (RISKS 14:37)

Joseph T Chew <jtchew@Csa3.LBL.Gov>
Fri, 5 Mar 93 08:09:15 PST

Regarding Bill Clinton's electronic mail, Shellie Emmons <sme46782@uxa.cso.uiuc.edu> asks, as reported here by David Daniels <0004381897@mcimail.com>:

> (1) When you get thousands of messages a day, how do you
>   respond effectively?

Same way you respond to thousands of letters or phone calls a day: delegate it to staff members who are trusted to (at least) winnow out whatever wheat there may be and respond to the chaff with a polite virtual form letter. There are 480 minutes in a working day; even assuming that our energetic Mr. C. puts in more than an 8-hour day, he clearly isn't going to give even a cursory acknowledgement, much less a thorough reading and thoughtful reply, to thousands of messages.

If any good ideas are received, he could take a "That'll teach 'em to suck eggs!" approach: have the White House staff find some aide or advisory-panel opening and invite his tormentor to work toward analyzing and implementing the idea. Citizens who envision government policymakers as putting in a six-hour day in a brandy-and-cigars atmosphere will learn their lesson right quick. :)

> (2) How do you make a public e-mail system inclusive
>   and accessible?

Figure out how to ape Minitel in the context of our technological and cultural base? Ignore the problem entirely, given that the older means of communicating with the government will remain available?

> (3) What would happen if e-mail became the primary

> mode of(mediated) access to government?

The Golden Age of Unix Nerds, that's for sure. :) Seriously, one needs some analysis of the modes currently used before this question can be answered. Again, perhaps the key would be to deliberately keep the older modes available: mail, irate phone calls to one's Congressperson, riding through the Rose Garden on horseback and shouting at the upstairs windows, whatnot. With all due respect to the people who are afraid of disenfranchising the computer-illiterate, I can't see the new medium drastically changing the way the government receives input, unless the individual representatives and staffers *choose* to ignore other forms of input, from letters to phone calls to lobbyists.

The real RISK, of course, is that the President would discover Usenet News!
:)
Joe

Re: The White House Communication Project (Daniels, RISKS-14.37)

Randall Davis <davis@ai.mit.edu>
Thu, 4 Mar 93 19:57:21 est

>From: Shellie Emmons <sme46782@uxa.cso.uiuc.edu>
>I am currently involved in a research project that is trying to aid the
>Clinton Administration in making effective use of computer-mediated
>communication to stay "in touch" with the public. ...

There are a number of confusions tangled up in this message; I'll summarize. Ms. Emmons is an undergraduate the UIUC who was asked by a professor to set up an email list for a research project. She posted a message about the project to three newsgroups (comp.human-factors, comp.society, comp.mail-misc), suggesting more by the description than is entirely correct, and called it "The White House Communication Project", even tho it has no official connection to the White House. The name of the project will be changed. Jack Gill is not the name of the White House person who is involved in efforts to get email running there.

Any email that does go to an address used by Media Affairs Office of the White House is printed out and handed to the folks who handle ordinary White House mail; those folks add that letter to the other fifteen thousand (15,000) letters that the White House gets every day. Eventually someone may reply (via US Mail) to the message in exactly the manner that they reply to all of their hardcopy mail.

There are a number of organizations trying to help the government use email, one of them is a consortium of researchers led by the MIT AI Lab.

The original message above is of course an example of a computer risk: the ability to attract a considerable amount of attention and excitement in a very short period of time; the medium amplifies the message.

Randall Davis, Associate Director, AI Lab

Clinton/Gore technology policy

Bill Gardner <wpg@ethics.med.pitt.edu>
Sun, 28 Feb 93 13:57:32 EST

This is a comment on the technology policy statement announced by Clinton and Gore on 2/22/93. The policy initiatives include the substance of the National High Performance Computer Technology Act that Gore had previously sponsored in the Senate (e.g., S. 1067 in the 101st Congress). Central to that act and the new initiative is the National Research and Education Network (NREN), a plan to increase the bandwidth of the internet and develop software for its utilization. I am concerned that the technology policy does not adequately address privacy or other concerns about the social implications of computing, including concerns raised by its proposed initiatives.

In the hearings on the High Performance Computing Act, medical informatics was one of the applications envisioned for the NREN. It's also part of the Clinton technology policy. The (brief) discussion of medicine in the 2/22 statement is interesting:

> "This information infrastructure -- computers, computer data banks, fax machines, telephones, and video displays -- has as its lifeline a high-speed fiber-optic network capable of transmitting billions of bits of information in a second....
>
> "The computing and networking technology that makes this possible is improving at an unprecedented rate, expanding both our imaginations for its use and its effectiveness. Through these technologies, a doctor who needs a second opinion could transmit a patient's entire medical record -- x-rays and ultrasound scans included -- to a colleague thousands of miles away, in less time than it takes to send a fax today."

Well, imagine that ("Hey Sue, lookit chromosome 17 on this guy from the Farber! 20 bucks at 7 / 5 sez he's malignant in 5 years. Bet he hopes his insurer never sees this, har har."). Without having any expertise here, I find it plausible that network consults using computerized medical records would have many benefits for patients. But it's also clear that implementing a network-mediated record system that provided secure confidentiality would be a challenging engineering task. I mean social as well as computer engineering, it's the communication among people that is problematic here.

I find much to like in the technology policy, so I would love to be proven wrong. Unfortunately, I see little evidence that privacy has sufficient priority in the current policy or the former High Performance Computing Act. I would appreciate hearing from others whether the policy adequately covers other aspects of socially responsible computing. The technology policy ought to include a statement of ethics concerning computerized information. I also believe that the NREN should follow the example of the NIH's Human Genome Project, which devotes 5% of its research budget to a program for studies of the Ethical, Legal, and Social Implications of human genetic research.

William Gardner, Psychiatry Dept, School of Medicine, University of Pittsburgh
Pittsburgh, PA 15213 412-681-1102 wpg@ethics.med.pitt.edu FAX:412-624-0901

Cellular Phreaks & Code Dudes

John Stoffel <john@wpi.WPI.EDU>
Thu, 4 Mar 1993 18:15:08 -0500

I picked up the premiere issue of a new magazine called "Wired" which
is trying to spread the word about the Digital Revolution. And
editorial blurb from the inside page is repeated here:

============
WHY WIRED?

Because the Digital Revolution is whipping though our lives like a Bengali typhoon - while the mainstream media is still groping for the snooze button. And because the computer "press" is too busy churning out the latest PCInfoComputingCorporateWorld iteration of its ad sales formula cum parts catalog to discuss the meaning or context of SOCIAL CHANGES SO PROFOUND their only parallel is probably the discovery of fire.

There are a lot of magazines about technology. "Wired" is not one of them. "Wired" is about the most powerful people on the planet today - THE DIGITAL GENERATION. These are the people who not only foresaw how the merger of computers, telecommunications and the media is transforming life at the cusp of the millennium, they are making it happen.

OUR FIRST INSTRUCTION TO OUR WRITERS: AMAZE US.

Our second: We know a lot about digital technology, and we are bored with it. Tell us something we've never heard before, in a way we've never seen before. If it challenges our assumptions, so much the better.

So why not now? Why "Wired"? Because in the age of information overload, THE ULTIMATE LUXURY IS MEANING AND CONTEXT.

Or put another way, if you're looking for the soul of our new society in wild metamorphosis, our advice is simple. Get "Wired".

-LR [jfs: Louis Rossetto]

You can reach me at 415-904-0664 or lr@wired.com
================

Along with this they had an interesting article on "Cellular Phreaks and Code Dudes" by John Markoff (markoff@nyt.com), which discusses how the latest rage of Silicon Valley hackers is Cellular phones. He gives an example of how two phreaks hacked into an OKI 900 cellular phone and some of the features they discovered:

  o how to use it as a cellular scanner.

o the manufacturer's interface so you can attach the phone to a portable computer.

o one of the phreaks wrote some software to track other portable phones as they move from cell to cell, this allows him to display the approximate locations of each phone since he knows the geographical locations of each cell.

o having the phone watch a specific number, and when that number is used, pick up and by using a simple sound activated recorder, you've made an instant bugging device! Maybe all the spies in Common Market who were worried about having point to point encryption on cellular phones didn't think of this trick?

I found this article to be worth the cost of the magazine, as it ties in directly with RISKS readers here have been talking about. Now if it is this easy to hack this phone, how hard would it be to hack into the general cellular phone service machines, those that handle the passing of phones from cell to cell?

The down side was the really annoying format, which seems to be "Techno-babble-obnoxious" with arbitrary changes in typeface, orientation, etc as you flip through pages. I felt that this detracted from the overall look of the information they were trying to present, making it harder to assimilate. I'd be interested in talking to anyone else who has read this magazine too.

John

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 39

Tuesday 9 March 1993

Contents

Bruce Nuclear Plant - Potential Safety Problem

David Levan <ac401@freenet.carleton.ca>
Mon, 8 Mar 93 13:54:20 EST

Article From Ottawa Citizen, March 8, 1993 by Canadian Press.

> Ontario Hydro Cites Safety Reasons For Reducing Power Production At Bruce Nuclear Plant
>
> Power production has been reduced at Ontario Hydro's largest electrical generator so that engineers can solve a potential safety problem, a utility spokesman said Sunday. Hydro began 'derating' the units at the Bruce nuclear plant to 60 per cent Friday after learning the safety margin in the event of

a reactor accident was slimmer than expected, said Tony Tidbury manager of reactor safety. 'This is not a problem in the reactor right now,' said Tidbury. 'It would only change in the event of an extremely, unlikely accident,' would be a huge leak of heavy water - which cools the reactor's radioactive fuel, Tidbury said. The Lake Huron nuclear plant produces about 20 per cent of Ontario's electricity but Hydro spokesman Geoff McCaffery said the cut shouldn't be a problem."

David Levan, DLSF Systems Inc., 189 Knudson Drive, Kanata, Ontario Canada
K2K 2C3 ac401@freenet.carleton.ca (613) 592-8188, fax (613) 592-2617

Steve Jackson Games/Secret Service wrapup

Eric Haines <erich@eye.com>
Tue, 9 Mar 93 10:25:35 -0500

[Eric Haines, erich@eye.com, sent me a Houston Chronicle article by Joe Abernathy, a sometime contributor to RISKS, which Eric found in the electronic mail magazine "Desperado" ("no, it's not a magazine about hacking"). "There can be justice in the world, after all..." EH. I cannot include the long copyrighted article here, but have excerpted from the beginning, as follows. It's a good article. Alas, no date. But Joe may still be available at Joe.Abernathy@houston.chron.com if you want to dig up the whole thing. Also, see RISKS-9.95,96;10.01,ff. for the earlier history. PGN]

Steve Jackson Games/Secret Service wrapup
By JOE ABERNATHY Copyright 1993, Houston Chronicle [no date given]

AUSTIN -- An electronic civil rights case against the Secret Service closed Thursday with a clear statement by federal District Judge Sam Sparks that the Service failed to conduct a proper investigation in a notorious computer crime crackdown, and went too far in retaining custody of seized equipment. The judge's formal findings in the complex case, which will likely set new legal precedents, won't be returned until later. [...]

The judge's rebuke apparently convinced the Department of Justice to close its defense after calling only ... one of the several government witnesses on hand. "The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave any concern as to whether (legal) statutes were involved. We know there was damage," Sparks said in weighing damages.

The lawsuit, brought by Steve Jackson Games of Austin, said that the seizure of three computers violated the Privacy Protection Act, which provides First Amendment protections against seizing a publisher's works in progress. The lawsuit further said that since one of the computers was being used to run a bulletin board system containing private electronic mail, the seizure violated the Electronic Communications Privacy Act in regards to the 388 callers of the Illuminati BBS.

The testimony described by Joe was rather strange. Agents testified that there was no criminal connection, they were not even trained in the Privacy Protection Act, and it took them only an hour to discover the true nature of the situation. The Electronic Frontier Foundation spent over $200,000 bringing this case to trial. The legal ramifications are considerable. Perhaps someone from EFF will contribute an analysis to RISKS, although many EFFers (and I) are at Computers, Freedom, and Privacy 93 this week. Don't hold your breath, but perhaps we need to wait for the judge? PGN

`Interrupt' by Toni Dwiggins

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 9 Mar 93 16:14:33 PST

> Toni Dwiggins, Interrupt, Tor Books, Tom Doherty Associates, 317pp., 1993, ISBN 0-312-85345-9, only in hardcover at present, US$19.95.

A terrorist whose computer handle is `Interrupt' plots to take down the public switched telephone network. For telephone system techies and lovers of good techno-mysteries, this is a well-written and compelling book that you will find intriguing. There are lots of good plot twists. A marvelous first novel by Toni Dwiggins, it is well written and well researched.

Short Course on Software Safety?

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Tue, 09 Mar 93 09:49:58 -0800

I am trying to assess the potential interest in my teaching a short course (a week or less) on software safety at the University of California, Irvine this summer. Topics could include basic system safety principles, management of safety-critical software projects, human error and the design of the human-machine interface, system and software hazard analysis, software engineering practices for safety-critical systems (software requirements analysis, design for safety, and verification of safety), and risk assessment.

Would such a course interest you? Which of the above topics would be of the most importance to you?

Nancy Leveson nancy@ics.uci.edu

> [Please reply directly to Nancy, not to RISKS. We do not normally run prospecti for courses. However, this potential offering is so closely related to the charter of the Risks Forum that it seems essential to include it. Besides, Nancy has been a subscriber from volume 1 number 1 on and carries our entire akashic record in her head. PGN]

Ohio student database under legal attack

Tim McBrayer <tmcbraye@thor.ece.uc.EDU>
08 Mar 1993 10:47:02 -0500 (EST)

An article, entitled "School files: Dangerous data?" appeared as the headline article in the 8 March 1993 _Cincinnati_Enquirer_. It discusses Ohio's Education Management Information System (EMIS), used to store demographic, attendance, program, summer school, achievement and proficiency testing, and post-graduation records of all public school attendees in Ohio. The complete set of data to be recorded was listed. This includes family income information, reason for leaving school (transferred schools, drug abuse, pregnancy, etc.), and extracurricular activities (including those not(!) related with school, such as 4-H or Scouting). Information is indexed either off of a Social Security number (a RISK in itself), or off of a school district-supplied ID number. Students switching school districts and not using their SSN will have a new number assigned to them. Students with multiple ID numbers, I assume, are cross-indexed--but the article was unclear on this point.

The EMIS system was proposed in 1989 and set to begin operation in July, 1991. The legality of the system was challenged that month by a Cincinnati-area school district (Princeton), and EMIS was declared illegal on Jan. 9, 1992. The Ohio legislature then passed a law (House Bill 437) on April 30, 1992, nullifying the previous ruling. A new suit, filed by Princeton and others, was filed Oct. 2, 1992, accusing the state of violating federal privacy laws. This suit is up for decision in Hamilton County Common Pleas court this month.

Several of the well-known RISKS of large databases were brought up in the article, which are quoted below.

"Reliability is just one of the concerns about EMIS that led Princeton City School District to sue the state. 'Our concern is that kids do make mistakes, and here's a record that never disappears.' said Richard Denoyer, Princeton superintendent. 'If a kid drinks a beer, that could be in there forever.

'You used to give your Social Security number on your check at the grocery store,' Denoyer said. 'People don't do that anymore. They know that (with the number) you can get into where you shop, what you buy, even how much money you have in the bank.'"

(...)

"Some say any number that can identify a student is too much.

'There's this whole industry of data brokers and private eyes who make a living obtaining (personal) information,' said Evan Hendricks, editor and publisher of _Privacy_Times_, a newsletter on privacy issues. If they want it badly enough, they're not above bribing an employee or impersonating a school official to get it, he said. 'That information isn't available if there's no name attached.'

'When you've got that much information linked together, that increases the risk,' the ACLU's Goldman said. 'This would just be a huge challenge (to hackers): ''Let's look at Johnny's grades.'' '

A couple of other interesting RISKS-related comments in the article were:

"...over 50% of the requests (into the FBI's criminal database--TJM) are non-law enforcement, typically from employers and licensing boards."

"This information (driver's license records) is now a public record and state governments are bringing in a hefty revenue selling mailing lists."

The article also mentions a similar system in Texas, and says the Texas system has not been challenged on privacy grounds.

Tim McBrayer, Computer Architecture Design Laboratory,
University of Cincinnati tmcbraye@thor.ece.uc.edu (513) 556-0904

Royal Bank client cards

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
08 Mar 93 07:12:17 EST

A report in the Monday, 8 March 93 Globe and Mail newspaper Report on Business by John Partridge raises questions about privacy and security: "Numbers the Royal doesn't keep secret."

According to the report, the Royal Bank of Canada sometimes allows its market-research firms to have not only the names, addresses, telephone numbers, sex, and age of selected customers but also their client-card numbers.

Critics argue that releasing these card numbers could lead to fraud; e.g., criminals with knowledge of the numbers etc. could fraudulently obtain new "replacement" cards and enter new personal identification numbers (PINs) at the customer's home bank.

Defenders argue that the likelihood of success of such ploys is negligible.

Royal Bank spokesperson Denise Curran is quoted as saying that the Bank supplies card numbers because they include coded information such as "geographic indicators" that help the market researchers cross-tabulate results.

However, four other major Canadian banks refuse to provide client-card numbers to market research firms.

The Consumers' Association of Canada objects to all banks' providing outsiders with customer information of any kind without the client's permission. The Royal Bank argues that because its market research is for its own internal use, it does not need to ask for such permission.

Michel E. Kabay, Ph.D., Director of Education,
National Computer Security Association

Royal Bank Client Cards

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>

09 Mar 93 08:14:39 EST

John Partridge reports in the Globe and Mail newspaper's Report on Business for Tue 9 Mar 93, that the Royal Bank of Canada has cancelled its practice of releasing client card numbers to its market research firms.

Tony Webb, senior vice-president of personal financial services, said, "No doubt must be allowed to remain in the minds of our customers."

Jacqueline Singh, VP of marketing, said, "...there are other ways ... to get the geographic data ... for them [the researchers] but also keep client numbers confidential." She added, "Our feeling is that if there is one more piece of information we can keep confidential, then we absolutely should and must."

Political->Personal risks (WTC/NYC)

Stephen Tihor <TIHOR@ACFcluster.NYU.EDU>
08 Mar 1993 14:35:58 -0400 (EDT)

Readers from outside the NY area should be aware that the World Trade Center was built and is operated by the Port Authority of New York and New Jersey. This bi-state agency has some surprising powers to ignore local and even many state laws and regulations. The building grossly violates local NYC building and fire codes.

This is not without some advantages. The city building codes mandate specific practices which have high labor costs during construction and prevent the use of many modern construction techniques even good ones. It is unclear if the WTC could have been built under traditional codes at all. Of course the safety systems used, while not to code might have have adequate "diversity" in location and conduit routing to survive. The basic structural design seems to have stood up quite well. But there are a number of cases where the ability to ignore local code resulted in bad choices.

For example self-contained battery operated trickle-charged lighting systems in halls and emergency stairs are present in also evey other large building.

The NYC Fire Department has repeatedly stated that they would not be able to properly respond to a fire above the tenth floor given the building's design. (Inadequate high pressure feed system, lack of separately routed conduits for external power supplies to the fire fighting substations throughout the building etc.

Re: World Trade Center blast

<frank@rnl.com>
Tue, 9 Mar 93 11:07:11 EST

In regards to the bombing at the World Trade Center, the news reports and comments made at the various news briefings seem to indicate that the emergency lighting was run off the backup generators only, there were no batteries in the emergency lights in the stairwells. Among the reasons given was the high cost of maintainance of the batteries.

Something which has been troubling me since the bombing and that I haven't seen discussed anywhere was the vulnerability of the broadcasting system. The World Trade Center has most of the antennae for the New York area. On the day of the bombing I was home with my kids who were watching TV at the time. All the stations except a local PBS station, ch.21, which broadcasts from here on Long Island and ch 2, CBS, which kept a backup antenna on the Empire State Building were knock off the air and most weren't back on until much later that night. I couldn't help but think about all the years of watching those emergency broadcast messages and wondering how they figured to keep broadcasting through an emergency with no backup broadcast facilities.

As a side note it was interesting to see what ch 2, the CBS station did with their one time New York monopoly. They kept to there regular schedule, The Wizard of Oz aired unopposed. Actually given the events of the day it wasn't such a poor choice. I wonder if they got to increase there advertisement rates for the night?

Frank Caggiano, R.N. Limited, Stony Brook N.Y.
fcaggian@rnl.com ..!uupsi!itpd4!frank

Re: Evacuation plan, generators fail in World Trade Center blast

"Jay Elinsky" <elinsky@watson.ibm.com>
Mon, 8 Mar 93 11:25:50 EST

In RISKS-14.38, Scott Preece suggests that the impact of the World Trade Center bombing would not have been significantly reduced if the Port Authority had acted on a study that showed the garage to be vulnerable to a car bomb. He also suggests that neither I nor the moderator know enough to question the Port Authority's decisions.

Well, I read the newspaper. The blast and its aftereffects have been covered very extensively in the local press. I've drawn the following conclusion: If the basement levels had contained only parking, plus the structural components needed to keep the buildings sitting on top, then the situation would be very different. Evacuation would have taken place in lighted, clear stairwells rather than pitch-dark, smoke-filled stairwells, and hundreds of smoke inhalation injuries would have been avoided. Most of the people who were killed, Port Authority employees who were in offices or a lunchroom on the garage level, would have been elsewhere and would still be alive. The job of getting the buildings ready for reoccupancy would be simplified, because the air-conditioning plant wouldn't be buried under rubble.

I DON'T know how much it would have cost to retrofit the buildings to move everything out of the basement.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

Emergency lighting: intelligent? Why? (Kolstad, RISKS-14.38)

<chaz_heritage.wgc1@rx.xerox.com>
Tue, 9 Mar 1993 08:29:15 PST

In RISKS-14.38 Joel Kolstad writes:

>...emergency lighting... controlled by a central computer ... each separate light... pack had a little bit of intelligence of its own... the emergency light microbrains had a panic routine...trying to re-establish contact with the main controller if the main controller had blown up...if the main controller had blown up, it just might be a good idea to turn on the emergency lights<

Non-maintained emergency lighting normally consists per unit of a lamp, a battery stack, a changeover relay and, in most cases, a trickle-charger for the batteries. Supply current keeps the relay in the 'charge batteries; lamp off' position. If it (or the relay's coil or connections) fails, the relay's spring carries the contacts to the 'lamp on' position. Restoration of supply current returns the unit to the 'charge batteries; lamp off' state. The device's control system is therefore, within the usual limits, fail-safe.

I cannot imagine any good reason to replace this old, tested, cheap and reliable system, in which each unit is independent of the others, with something interconnected and allegedly 'intelligent', particularly since the latter seems in the WTC's case (if the above allegation is true) to have neatly evaded the fail-safe principle.

>...it's some really poor programming!<

Safety equipment should not, IMHO, ever require 'programming'. Its operation should be based on simple principles of physics (preferably basic mechanics), and upon as few of them at once as is possible, and its condition and readiness should be easily subjected to inspection at any time. Otherwise it eventually ceases to be safety equipment at all, and becomes another hazard.

Most of the basic safety devices (e.g. Otis' elevator safety mechanism, Fermi's gravity control-rods or Westinghouse's vacuum brake) were invented long ago and cannot now be 'improved' by the addition of 'features' since any added complication can only reduce reliability, their most desirable characteristic. Adding the wild variable of 'programming' seems most unlikely ever to benefit anyone except the programmer and salesfolk involved. I wonder how many airpeople would buy a computer-controlled parachute...

Mystified, Chaz

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 40

Tuesday 16 March 1993

Contents

Garage door burglaries

"Chuck Payne -- Quad/Tech S&R -- Ext. 7976" <CPAYNE@corp.qgraph.com>
11 Mar 1993 14:07:21 -0500 (CDT)

The newspapers in Milwaukee reported an interesting case this morning.

An installer of automatic garage door openers has been arrested, pending being formally charged of burglary. He is accused of recording the electronic code settings on the automatic garage doors he installed, and then returning some time later and opening the garage doors electronically. He has been accused of an entire string of burglaries, and stolen goods were apparently found in his home. In some cases, the garage door was opened and the inside door to the rest of the house was unlocked, or else it was pried open.

Sounds like it might be a good idea to change the code settings on your garage door opener if it was installed by someone else, or even serviced recently.

Charles D. Payne, Safety Engineer, Quad/Tech International, Div. of
Quad/Graphics Inc., Sussex, Wisconsin 414-246-7976 cpayne@corp.qgraph.com

MCI 800 problem

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>
10 Mar 93 13:28:00 EST

Some time ago, my parents (who live in another state) decided that, if they were going to hear their grandchildrens' voices, they needed to get a personal 800 number from MCI. The personal 800 scheme works like this: each household is assigned a unique 800 number (I'm told), and an access code (4 digits). As a precaution against abuse, when you dial the 800 number you get a message telling you to enter your code. Only callers who enter the correct code get connected, so no massive dialing scheme advertising holiday resorts (etc) can exploit the users' willingness to pay for incoming calls.

I promptly programmed my parents' number and the code on adjacent buttons of my phone and left it at that. I would just hit the first button, wait for the announcement (voice-mail style) and hit the second button. This worked, until a little over a month ago. At that point, after I hit the second button I was asked to wait, and an operator came on the line and asked for my code. The first time this happened, I refused to give the code (since I had forgotten it (!)). A moment later, it apparently showed on the operator's console, and I was put through.

I thought this was an aberration, but at no time after the first event was I able to get directly through, without talking to an operator. I thought their equipment might not be able to handle the high speed dialer, so I relearned the code and punched it in myself. Still no go. I tried from my office. Same thing.

Finally, last week, I managed to get the operator to switch me to a technical representative. This individual and I discussed what was happening, and the rep told me that he knew of another case where much the same thing had happened. I then asked if they had changed or upgraded their system software lately. Long pause. "Why yes, we did, just about a month ago."

I suggested they check things out, and was promised a report. Well, a couple of days later the system WORKED! And it has not failed again since. I have not received a report (nor a consulting fee from MCI), but I suspect that MCI's upgrade of their personal 800 system included some, uh, 'features' of which they weren't aware. They may have gone back to the old software, or they may have just fixed MY problem. I don't know which. But I am certain that the origin of the problem had to do with a programming error in MCI's hardware/software, and this raises the issue of other errors that might be out there.

Should MCI employ beta testers? That would be my suggestion. They could pay people like me to make trial calls at, say, 3:00 AM CST, just to make sure the system worked as advertised. Hey, in a world where most people can't program an MS-DOS .BAT file, you need to check!

Andrew Marchant-Shapiro, Sociology and Political Science Depts., Union College
Schenectady NY 12308 518-370-6225 marchana@gar.union.edu marchana@union.bitnet

System Dynamics of Risks

Bill Park <park@netcom.com>
Sun, 14 Mar 93 13:20:34 -0800

From: dyurman@igc.apc.org
Subject: System Dynamics of Risks
Newsgroups: sci.systems

System Dynamics of Risks: Risk Perceptions, Mental Models, Circuit Breakers

There have been a number of postings about risk and public acceptance of risks from various technologies, e.g. nuclear, chemical, etc. I think it's worth reviewing some of the basics about risk perceptions. This posting is based on the following references for those who wish to develop their own conclusions.

"Perceptions of Risk," Slovic, Paul, _Science_, 4/17/87. Vol 236, pp. 280-285.

"The Fifth Discipline," Senge, Peter, Doubleday, 1990.

"Technological Risk," Lewis, H.W, Norton, 1990.

This posting is done in "bullet" form so that I can show attribution to source by concept. Almost all of the material in this post comes from one or more of the sources noted above. I have merely condensed some of the key ideas.

Senge's work on system dynamics does not mention risk perceptions, per se, rather, in any great detail. I have applied his tools for thinking about system dynamics to risk perceptions.

Finally, if I have made any errors in representing the work of these authors, they are unintentional. I would appreciate clarifications where necessary.

OBJECTIVES - Slovic

* Provide a basis for understanding and anticipating public perceptions of hazards. [Note: Senge - risk perceptions are mental models.]

* Improve communication of risk information among technical experts, lay people, and decision makers.

BACKGROUND - Slovic

* The development of chemical and nuclear technologies has been accompanied by the potential to cause catastrophic and long-lasting damage to the earth and to the life forms that inhabit it.

* The mechanisms underlying these complex technologies are unfamiliar and incomprehensible to most citizens. The most harmful consequences of these technologies are such that

learning to mitigate or control them is not well suited to management by trial-and-error. The public has developed increasing levels of dread of the unknown consequences of complex technologies.

* The public is well aware that economic and political pressures during the design process in complex systems may lead to systems being built and operated near the edge of the safety envelope. [Senge - Eroding goals]

* Some systems, once built, represent such significant investments that it is nearly impossible to walk away from them regardless of risks. [Senge - Yesterday's solutions are today's problems.] Example, nuclear waste resulting from the balance of terror associated with nuclear weapons.

* Those who are responsible for human health and safety need to understand the ways people think about and respond to risk. Perception and acceptance of risks have their roots in social and cultural factors and not in science.

* The result is that some risk communication efforts may be irrelevant for the publics for which they are intended because the "publics" have hidden agendas. Also, the public may be raising the issue of risk to human health and the environment as a surrogate for other social, economic, or political concerns.

* Risk perceptions are mental maps composed of attitudes, beliefs, assumptions, and judgements. Following is an example of the "Not in my back yard," or NIMBY mental map.

[Senge - reinforcing, vicious loops.]

- Attitude: government science is not trustworthy

- Belief: government serves special interests, not the public

- Assumption: you can't fight city hall

- Judgement: whatever it is the government is proposing to do, get it out of my back yard.

* Disagreements about risk perceptions do not change as a result of better data becoming available and being disseminated to the public. People have a hard time changing their opinions because of the strong influence initial impressions, or pre-existing biases, have on the interpretation of new information. Also, the method of presenting the new data, e.g. as mortality or as survival rates, can alter perceptions of risk.

* Generally, the gap between perceived and desired risk levels suggests that people are not satisfied with the ways the market or regulatory agencies have balanced risks and benefits. Generally, people are more tolerant of risks from activities seen as highly beneficial, but this is not a systematic relationship.

* The key factor regarding acceptance of exposure to risk appears to be the degree to which a person chooses that exposure in return for a perceived level of benefits. The relationships between perceived levels of benefits and acceptance of risks are mediated by factors such as familiarity, control, potential for catastrophic consequences, and equity.

* In the case of nuclear power people's deep anxieties are linked to the history of negative media coverage. Also, there is a strong association between public attitudes about nuclear power and anxieties about the proliferation of nuclear weapons.

Accidents as Signals - Slovic

* The impact of accidents can extend far beyond direct harm. An entire industry can be affected regardless of which firm was responsible for the mishap.

* Some mishaps cannot be judged solely by damage to property, injuries, or death. Some events, like Three-Mile Island (TMI), can have ripple effects on public perceptions of risks leading to a more hostile view of complex technologies in general.

* The signal potential of an event like TMI, and thus its social impact, appears to be related to how well risks associated with the event are understood. The difference in perceptions between a train wreck and a nuclear reactor accident is that the wreck is seen as a discrete event in time while the reactor problem is regarded as a harbinger of further catastrophic mishaps. The relationship is between degree of unknown dread of the consequences of the accident and the degree of subsequent irrational fears of future catastrophes.

Risks & Benefits - Slovic

* Firms conducting risk assessments within the framework of cost - benefits analyses often fail to see the "ripple" effects of worst case scenarios.

* For example, Ford Motor Co. failed to correct a design

problem with the gas tank of its Pinto compact care. A cost - benefit analysis indicated that corrections costs greatly exceeded expected benefits from increased safety.

* Had Ford looked at public risk perceptions of auto fires in crashes, the analysis might have highlighted this defect differently.

- Public perceptions of auto crashes regarded the risk of fire as a very high order problem involving considerable dread.

- Ford ignored potential higher order costs such as damage claims from lawsuits, damaged public reputation, lost future sales, and diminished "good will" from regulatory agencies.

Risk Perception & Mental Models - Senge

The logic of mental models with regard to risk perceptions is illustrated by the following notes:

1. Senge - Structure influences system performance

IF: structure influences system performance, and;

IF: mental models - attitudes, beliefs, assumptions, judgements - are part of the structure;

THEN: Mental models influence system performance. Risk perceptions are mental models because they are based on social and cultural factors such as attitudes, beliefs, assumptions, and judgements

2. Senge - The easy way out usually leads back in.

IF: culture is the dominant collection of shared mental models operating in society, and;

IF: risk perceptions, which are mental models, have their roots in social and cultural factors, and not in science;

THEN: some risk communication efforts based solely on scientific data will fail since they do not address mental models which are the basis for risk perception.

3. Senge - The harder you push the harder the system pushes back.

IF: both our private and shared mental models are
always flawed and can get us into trouble when
they are taken for granted, and;

IF: levels of dread, in terms of perceived risk of
complex technology, are reinforced by irrational
fears caused by the unknown but potentially
catastrophic effects of new technologies;

THEN: inappropriate mental models about complex
technologies may be reinforced, rather than
mitigated, by additional "marketing" efforts
to promote new technologies.

Charting Mental Models About Risk - Senge

Variables are defined as elements in a system which may act or be acted upon. A variable can move up or down in terms of intensity, duration, absolute or relative values, etc., but it's movement is measurable.

Slovic - There are four areas in which variables are defined for mental models at work in shaping risk perceptions. Following each variable definition is a list of factors which further define them.

* The degree of voluntary acceptance of the risk, e.g. drinking coffee (caffeine) v. second hand smoke. (who makes the decision for exposure to the risk)

- Controllable?

- Consequences not fatal for individuals or groups?

- Equity in choice, degree of exposure?

- Low risk to future generations?

- Risks easily reduced or mitigated by individual choices?

- Risk decreases over time as more knowledge becomes available?

* The level of dread of the unknown the person has about the risk, e.g. thermonuclear war v. car accident. (obliteration of the collective v. individual survival)

- Totally uncontrollable; e.g. Pandora's box?

- Catastrophic results?

- Consequences fatal?

- No equity or choice, random exposures to risks?

- High risks to future generations?

- Risk increases over time regardless of what is known about it?

* The amount of knowledge the person has about the risk and especially its consequences, e.g. inhaling pesticide residue v. drinking alcoholic beverages. (imprecise science v. known, quantifiable data)

- Risks / consequences observable by trial and error, experimentation, or measurement?

- Those exposed realize the dangers?

- Effects / consequences separated in time and space, e.g., harm to future generations?

- Risks known to science, or exist in realm of "folklore?"

* The degree of control the person has to prevent the consequences of system failure, e.g., riding on a snowmobile v. working in a coal mine. (individual control v. collective control)

- Consequences known, capable of quantification?

- Effects immediate?

- Risk well known and understood by the public and science?

- Solutions to mitigate risks work?

General Notes on Risks and Human Factors -- the Latent Failure Syndrome - Lewis

* Numerous functions and services in large, complex systems may be dependent on unrelated events. Large, technologically complex systems have "latent" failures within them. These are failures which are only apparent under a specific set of often obscure triggering conditions. Examples include;

Nuclear	Three Mile Island, Chernobyl
Space	Challenger shuttle explosion
Industry	Bhopal

Environment   Exxon Valdez oil spill

*   While these disasters all have apparent triggers, in fact, these failures are virtually never the result of a single fault.

*   The risks of large system failures, with accompanying catastrophic consequences, accrue to the system as a whole rather than to individual components.

*   Pressures during the design phase [eroding goals] may lead to systems being built to operate near the edge of the safety envelope.

*   Logical redundancy is compromised by a lack of physical redundancy. For example, separate communication channels are carried in the same conduit.

Application of the "Latent Failure" Syndrone -- nuclear/chemical waste cleanup

1. Senge - Today's problems come from yesterday's solutions

   IF: public anxieties [mental models] about nuclear technology are linked to dread of thermonuclear war, and;

   IF: existing nuclear wastes are the by-products of weapons' production processes;

   THEN: the public will extend it's original perceptions [mental models] to cover processes involving the management of the wastes even though the cleanup is designed to neutralize them.

2. Senge - The cure can be worse than the disease

   IF: the public has an intuitive grasp of the "latent failure syndrone" with regard to complex technologies, e.g., nuclear weapons production, and;

   IF: the public's mental map include a paradigm that "things blow up,"

   THEN: the public will assume that the perceived risks of cleaning up waste from nuclear weapons production are no different than for the activities that created the bombs in the first place.

Comments welcome, especially on ways to make distinctions between risk perceptions about nuclear weapons v. risk perceptions about management of nuclear wastes. Are there any?

Dan Yurman, PO Box 1569, Idaho Falls, ID 83403
dyurman@igc.apc.org 3641277@mcimail.com

Facing the Challenge of Risk and Vulnerability in Information Society

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Sat, 13 Mar 1993 15:54:46 +0100

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING
Working Group 9.2 - Social Accountability of Computing

Announcement of Working Conference:
"Facing the Challenge of Risk and Vulnerability
in an Information Society"
to be held at Namur, Belgium, 20-22 May 1993

The event is jointly organised by IFIP-WG9.2 and the "Cellule Interfacultaire de Technology Assessment" (CITA), F.U.N.D.P., Namur and sponsored by the Belgian National Scientific Research Fund (FNRS) and the Ministry of the French Community.

1) Background

There has been much work done on the technical aspects of risk and vulnerability within computer systems, and on what can be done to reduce risk and alleviate the consequences. Less attention has been paid to the risks to which society is exposed and its vulnerability in the age of information technology.

The problems of risk and vulnerability are not new (and aspects of risk may even sometimes be considered to be necessary for society) but the size, complexity and global reach of computer systems means that the issues raised have acquired a much greater urgency.

The conference is an important opportunity to bring together many specialists to address specific problems. The scope of the conference is quite specific: careful analysis of the concepts of risk and vulnerability, particular experiences of both individuals and organisations, as well as professions and other institutions of society, and responses to find new ways of meeting these challenges.

2) Main themes of the Conference

- Analysis of Vulnerability and Risk: Theoretical papers which seek to analyse the nature and types of risk in society and the ways in which society is vulnerable.

- Vulnerability of the Employee and Citizen

- Vulnerability of the Manager and Organisation: Papers that are based on case studies which increase our understanding of the risks faced by people and organisations.

- Professional Responses

- Societal Responses: Papers which address the question: What can be done? through such means as legislation and the legal system, insurance, codes of ethics, codes of practice, education, etc.

3) Structure and Organization of the Working Conference

Day#1: Thursday May 20, 1993: 9.30 a.m., Plenary
BERLEUR Jacques (University of Namur, B), on behalf of IFIP-WG9.2:
  Risk and Vulnerability in an Information and Artificial Society
BEARDON Colin & HALES Mike (Brighton University, UK):
  Whose Risk? Whose challenge? Questions of Power and
  Vulnerability in a Designed World
VAN LIESHOUT Marc & MASSINK Mieke (University of Nijmegen, NL):
  Constructing A Vulnerable Society

Thursday May 20 p.m.: Workshops on Concepts/Health Care/Access Capabilities

  Workshop on Concepts:
LAUFER Romain (HEC Graduate School of Management, F):
  The Social Construction of "Major Risks"
NAULLEAU Daniel (Equipe Informatique et Societe, F):
  The New Vulnerability. Some Ideas to Face it.
YOUNG Lawrence F. (University of Cincinnati, USA):
  A Jurisprudential View of Information Technology (IT)

  Workshop on Health Care:
BAKKER Albert R.(BAZIS Foundation, NL):
  Dependency of Healthcare Organisation on their Information System
LOUW Gail (University of Brighton, UK):
  The Use of Web Analysis in the Introduction of Nursing
  Information Systems

  Workshop on Access Capabilities:
DUTTON William (Annenberg School for Communication, USA):
  Electronic Service Delivery and the Inner City:
  Community Workshop Summary
WHITEHOUSE Diane (University of Toronto, CDN):
  I.T. and Disability

Thursday May 20 Late p.m.: Participants are invited to write their
  two best ideas on "sand plates".

Day#2: Friday May 21, 1993 9.30 a.m.: Plenary

BRUNNSTEIN Klaus (University Hamburg, D):
Paradigms of IT and Inherent Risks
LOBET-MARIS Claire, in collaboration with KUSTERS Benoit, (CITA, University
of Namur, B):
Risks and Vulnerability in New Inter-Organizational Systems
OWEN Jenny, BLOOMFIELD Brian & COOMBS Rod(CROMTEC,University of Manchester,UK):
Information Technology in Health Care: Tension and Change
in the UK National Health Service

Thursday Friday 21 p.m.: Workshops Health Care/Organisations/Tentative Response

Workshop on Health Care:
NGUYEN NAM Tien, PRINTZ Yves, SAADAOUI Sanae & NICOLAY A.(CITA,
University of Namur, B):
Benefits and Risks Assessment of Computerized Health Cards:A Case Study
SCHOPMAN Joop (University of Innsbruck, A):
Information Technology's Ideology Makes its Use Risky

Workshop on Organizations:
NILSSON Peter (Swedish National Audit Bureau, SW)
How to Reduce IS Risk in the Public Sector? A Survey
ZETTERQVIST S (Church of Sweden Education Centre, SW)
The Need of Education on Managerial Level for an
Ideological and Member-Based Organization Due to the
Change in Legal Requirements and to the I.T.
Implementation

Workshop on Tentative Responses:
UNDERWOOD Alan (School of Information Systems, Brisbane, AUS):
Certification in the Australian I.T. Profession
VAN HOUTTE Paul (CRID, University of Namur, B):
People Risks Related with Informatic Services
Professions and Professional Liability Insurance

Friday 21: p.m. during Workshops: Selection, amongst individual ideas
(see "Sand Plates" of Thursday p.m.), of the best "group ideas": groups are
invited to write "Silver Plates".

Friday May 21, 1993: 6.00 p.m. Plenary
The 2nd IFIP-WG9.2 NAMUR AWARD will be granted to Riccardo PETRELLA, Head of
the FAST Programme (CEC, DGXII), for his outstanding contribution with
international impact to the awareness of social implication of information
technology.

Friday May 21, 1993 Evening: Conference dinner

Day#3: Saturday May 22, 1993:

Saturday May 22: 9.30 a.m. Plenary
COUMOU C.J. (Computer Security Consultants, NL):
Using Risk-Analysis as a Tool for Decision Making.

Experiences from Real Life
HOLVAST Jan (Stichting Waakzaamheid Persoonsregistratie, NL):
Vulnerability and Privacy: Are We on the Way to a
Riskless Society?

Saturday a.m., during Workshops: Selection, amongst group ideas (see "Silver Plates" of Friday p.m.), of the "GOLDEN IDEA"

Saturday May 22 p.m. Plenary: "AGORA":
Presentation and selection of the "GOLDEN PLATE" on "How to face the Challenge of Risk and Vulnerability in an Information Society?" Recommendations by the Workshops.

4) Date and Place
The Working Conference will start on Thursday May 22nd, 1993 at 9.30 a.m. (Welcome at 9.00) and end on Saturday 24th, at 4.00 p.m.

The Conference will take place on the premises of the Facultees Universitaires Notre-Dame de la Paix, Namur - Belgium.

Participants arriving on Wednesday p.m. will be welcomed at the "Centre de Rencontres", 53 Rue de Bruxelles, B-5.000 NAMUR (five minutes from the Namur Railway Station), from 6.00 to 8.00 p.m.

5) Registration
A registration form is included. Participants are kindly requested to complete and return it before April 15th at the latest.

The Registration Fee is BEF 5.500: it includes attendance at all conference sessions, abstracts, coffee-breaks, lunches, cocktails and the conference dinner. It is to be paid into the account 350-0000001-23 (Banque Bruxelles Lambert) of the Facultees Universitaires Notre-Dame de la Paix, Namur with the mention "cpo 9202- IFIP May Conf." The amount must be in Belgian francs, all bank charges excluded. Eurocheque or American Express are also accepted, if you prefer this means of payment. There will be no refund for cancellations not received before May 10th, 1993.

6) Accommodation
You may receive a list of hotels from the Conference address (below). As hotel rooms in Namur are limited, you are well advised to book your hotel room as soon as possible. The Organizing Committee cannot be held responsible for difficulties encountered in case of late booking, although we shall do our best to help you.

7) Conference Address:
For all further information, please contact:

Jacques BERLEUR, B,
IFIP-WG9.2 Chairman
FUNDP, Rue de Bruxelles 61, 5000 Namur, Belgium
Tel: +32.81.72.40.00

Fax: +32.81.72.40.03
Email/UUCP: jberleur@info.fundp.ac.be
/Bitnet: jberleur@bnandp51

8) Programme Committee:
Jacques Berleur, Chair,
Colin BEARDON, UK
Paula GOOSSENS, NL
Romain LAUFER, F
Peter NILSSON, Sw
Ton WESTERDUIN, NL
Luc WILKIN, B

9) REGISTRATION FORM
(Please use capital letters):

First Name:
Surname:
Company, Organization:
Mailing Address:
City:
Postal Code:
Country:
Phone: Fax:
Email:

I will attend the Conference
- date and hour of arrival:
- date and hour of departure:
Registration fee
- paid at FUNDP (cpo 9202)
- International cheque (to the name of J.BERLEUR)

Signed:
Date:

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 41

Wednesday 17 March 1993

Contents

Automated Teller Machine network problems in New Jersey

Joel A. Fine <joel@postgres.berkeley.edu>
Wed, 17 Mar 93 12:47:12 -0800

According to CBS news, the national network of Automated Teller Machines went on the blink earlier today (3/17/93). Apparently EDS's main computer center in New Jersey was damaged in last week's blizzard, and the backup computer center was temporarily being occupied by companies forced out of the World Trade Center as a result of the bombing.

What a nightmare, to be the administrator of a system like this, and
to have to plan for the possibility of both a bombing and a blizzard.
No wonder designing fail-safe computers is hard!

- Joel Fine joel@cs.berkeley.edu

[That is what contingency planning is all about! PGN]

ATM problems in California East Bay

"Lin Zucconi" <lin_zucconi@lccmail.ocf.llnl.gov>
16 Mar 1993 10:38:53 U

``East Coast Storm Freezes Some [San Francisco] East Bay ATMs''

An article in the March 16, 1993 Livermore/San Ramon, CA "Valley Times" stated that a roof collapse in a Clinton NJ computer data center operated by EDS prevented many San Francisco East Bay residents from accessing their ATM accounts over the weekend. The article said that "the data center...provides the technological power that runs about 5,000 of the nation's 87,000 automatic teller machines, including dozens in the East Bay." By Monday afternoon, EDS hadn't restored full power to its ATM network leaving local bankers scrambling for ATM alternatives. EDS has a back up system but it is being used by other financial companies that suffered outages as a result of the Feb. 26 bombing of the World Trade Center.

Quote from Larry Kurmel, executive director for the California Bankers Association: "You tend to take these things [operating ATMs] for granted until something like this happens. Then you realize these [ATM] systems are subject to random events."

Lin Zucconi zucconi@llnl.gov

Buy IBM and get fired

Ross Anderson <rja14@cl.cam.ac.uk>
12 Mar 93 15:51:24 GMT

The press in Britain this morning has been full of stories about Taurus. This was a share dealing system in which the London stock exchange and local institutions had invested some 400 million pounds (600 million dollars). It didn't work and a review showed that there was no reasonable prospect of it working; it seems that it just got too complex to cope with.

It has now been written off and the chief executive of the stock exchange `resigned' today.

A fair bit of the previous press criticism centred on the security, which was designed by IBM and was apparently rather difficult to manage. As far as one can tell from the press reports, it used their `common cryptographic architecture' of 4753s for central control, DES cards in PS/2's for terminal security, and smartcards for personal key management. Coopers and Lybrand, the systems integrators, have also got a fair bit of stick (they sponsored Eurocrypt 91, or so I seem to recall).

It will be interesting to see if this marks a turning point for bankers' attitude to crypto technology. Up to now, it has been hard to sell things like formal methods or elliptic curves to men in suits, as DES in steel boxes was what they were comfortable with.

Future systems however may well use public key algorithms, and maybe even electronic wallets which distribute the security processing entirely into smartcards.

In that case, expect further entertainment, as some of the complexity will be pushed into the settlement process, or the arbitration system, or the key management mechanism; and the lack of relevant systems experience will exact its pound of flesh in one way or another.

Our head of department remarked that such fiascos can be compared to the civil engineering disasters of the nineteenth century such as the collapse of the Tay bridge. Civil engineers eventually got their act together, but there was a long learning process in which they worked out how to structure their approach to large problems and combine the maths with the project management in a way that worked.

Watch this space!

Ross

new meaning to "program blowing up"...

David Honig <honig@ruffles.ICS.UCI.EDU>
Wed, 10 Mar 93 21:07:31 -0800

>From the Fall 1992 issue of Intervue,
the Intergraph customer newsletter:

Next time Mohammed A. Salameh is trying to find a parking
place for his van, he should use BombCAD...

--------begin article-----------

MANCHESTER, England. Royal Ordnance Security Services is using a new software package, BombCAD, as the basis for assessing the security level of a site and predicting the effects of an explosion within or outside a structure.

BombCAD was developed using MicroStation PC CAD software to produce sophisticated #D models of the structure under analysis. If a building was designed using CAD, BombCAD is able to use the original database containing information on the overall site and building construction to produce a computer model. [...]

Using Intergraph's modeling capabilities, Royal Ordnance can create credible scenarios for any property or installation and determine the likely effects of an explosion, in terms of structural damage and human injury. The range of effects of each simulated explosion is displayed graphically on the 3D model and reproduced as supporting evidence in a written report.

According to Andrew Quinn of Royal Ordnance, "We've already carried out studies for four clients: two for risk assessment, one for the design of a new building, and the fourth for modification of an existing structure. Most clients, for obvious reasons, do not wish to be identified. However, one example that is public knowledge is Manchester Airport. We carried out a number of 'what-if' scenarios and were able to provide the airport information on evacuation routes, risk areas, and general safety programs."

No anonymity for Canon copiers?

Brad Mears [I-Net] <bmears@gothamcity.jsc.nasa.gov>
Tue, 16 Mar 1993 14:17:53 -0600 (CST)

The most recent issue of Popular Science had a small sidebar concerning new copier technologies that are being used to combat counterfeiting. According to Canon, their new color copiers include two mechanisms to prevent people from copying currency.

The first is rather innocuous - the copier can recognize many different currencies and will print a blank image rather than a fake bill. No obvious risks here.

The second mechanism is a bit more threatening. According to the story, which I quote without permission -

> "Each copier embeds a code into the copied image, which is impossible to see. A special scanner extracts the code and a computer program then furnishes the copier's serial number, allowing identification of the registered purchaser of the machine."

As a means to combat counterfeiters this may be very useful. Unfortunately, it is also useful for tracking down people who report government waste, publishers of underground newsletters, and others who may have a legitimate need to remain anonymous. Plus, it seems a bit too much like the Eastern bloc countries who used to require registration of typewriters.

Brad Mears bmears@gothamcity.jsc.nasa.gov

Re: Steve Jackson Games

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 17 Mar 93 14:45:48 PST

This morning's news notes that Steve Jackson Games was awarded $50,000. [See RISKS-14.39 for the Rest of the Story.]

Re: System Dynamics of Risks (Yurman, RISKS-14.40)

"John (J.G.) Mainwaring" <crm312a@bnr.ca>
Wed, 17 Mar 1993 15:56:00 +0000

I found that the posting by Dan Yurman on the perception of risks really helped clarify some issues. I had not previously encountered the phrase "level of dread" in risk analysis, and it seems particularly useful. In statistical analysis, death in a car accident seems to be an atomic concept, so we focus on what will save the most lives. In every day experience, death in car accidents happens both often enough and seldom enough that we become somewhat hardened to the possibility. Death by fire in a car accident happens less often, but summons such a level of dread that we see it differently; we feel that "nobody should have to die that way". We are likely to respond "irrationally" and demand that cars be made safe from fire even if spending the same amount of money in some other way would save more lives.

However, the point that "Some systems, once built, represent such significant investments that it is nearly impossible to walk away from them regardless of risks. [Senge - Yesterday's solutions are today's problems.]" does not seem to be borne out by: "Example, nuclear waste resulting from the balance of terror associated with nuclear weapons."

I would say that "nuclear waste ..." has become such a risk that we cannot walk away from it, whatever the cost. Perhaps the point would be better made as "Coal, oil and nuclear powered electricity generating plants represent such an important investment that it would be nearly impossible to walk away from them regardless of the risks they present".

As he argues so well later on, nuclear waste disposal has become a very unpopular topic because of its association with nuclear weapons. We have no investment in existing stockpiles of waste, and it would be easy to just say that no one has room for it in their back yard, we'll just ignore the problem. In this case, informed recognition of the risk has led to an understanding that we must continue to invest in solutions to the existing problems, even though it might seem cheaper to just walk away from them.

Re: 'Untested' Risk Management System for Nuclear Power Stations

Anthony Naggs <AMN@vms.brighton.ac.uk>
Wed, 10 Mar 93 12:15 GMT

Following up on my previous posting, The Guardian today (10 March 1993) published a letter from George Jenkins, (Generation Director at Nuclear Electric), commenting on the article thus:

The headline "sacked expert fears nuclear safety risk" (4 March) will have concerned some readers, and the prominent article underneath suggested that the Status computer system ". . . might be relied on in times of emergency when 'bugs' in the programming had not been removed." May I make three facts absolutely clear?

First, the computer system in question is a stand-alone management information system. It is not connected to our reactor safety and control systems at all. Indeed, if you were to visit any of the nuclear plants where it is being tested (as your reporter was invited to do), you would see at a glance that it is not even located on the reactor operator's desk, and forms no part of his control process.

Second, if it were to be removed, switched off, or even fail during operation, it would not have the slightest effect on reactor safety. The main reactor safety systems at all UK nuclear power stations are hardwired, and do not depend at all on computer software.

Third, any such computer system is subject in any event to rigorous checking and validation, independent of its manufacturers. That's what we're doing. If it fails to meet our standards of reliability - among the highest in the world - then it will simply be rejected.

Anthony Naggs, Software/Electronics Engineer, (and virus researcher)
Phone: +44 273 589701 Email: amn@vms.brighton.ac.uk

Re: `Untested' Risk Management System for Nuclear Power (Naggs, 14.38)

T. Kim Nguyen <kim@jts.com>
Wed, 10 Mar 1993 16:55:34 -0500

> [A few of the risks covered: reliability of risk management systems; risk of bringing a system into disrepute by the actions of disruptive staff; risk of using a system for a year before full testing and manuals are complete; ...]
> Anthony Naggs, Software/Electronics Engineer, PO Box 1080, Peacehaven,
> East Sussex BN10 8PZ UK +44 273 589701 amn@vms.brighton.ac.uk

[Naggs'] note at the end appears to be very biased against the whistle blower: "risk of bringing a system into disrepute by the actions of disruptive staff" is not quite the way I would have put it. The company is behaving much like NASA did when problems with the shuttle's O-rings were discovered: instead of fixing the problem, the company is attempting to discredit the safety-minded individual and is attempting to sweep the problem under the rug. Yes, the whistle blower may have been "disruptive", but only to the extent that he was forced to publicly announce the system's problems because of the management's refusal to acknowledge even the possibility of a problem existing.

T. Kim Nguyen, Document Imaging Systems, JTS Computer Systems Ltd., Toronto
kim@jts.com k.nguyen@ieee.org uunet.ca!jts.com!kim kim@watnow.uwaterloo.ca

Electronics on Aircraft

rob horn <horn%temerity@leia.polaroid.com>
11 Mar 1993 18:20:31 -0500 (EST)

The FAA is opening an investigation into the risks of interference from portable electronic devices on airplanes. The previous investigation was 6 years ago, with the final report issued Sept 16, 1988. It concluded that the risk was small and that portable electronics could safely be used. The new investigation should issue an interim report in October and final report in July 1994.

The reasons given for a new investigation are:

1) The number of devices in use has grown substantially. Some problem reports identified dozens of devices in use at the time of the problem.

2) The shrinking size and low-voltage electronics of modern avionics are potentially more vulnerable to EMI

3) Aircraft contain more composites. The previous examination was only for metal skinned aircraft. The metal provides substantial EMI protection.

4) There have been reports of interference from portable electronics.

From the limited number of reports there is a clear and substantial danger from cellular phones. These have been determined to be the cause of one third of all suspected EMI. They are also the most dangerous. Despite the prohibition on use in flight, people are observed to use the phones during takeoff and landing. This is the worst time for interference because the aircraft is most sensitive to navigation and control interference at this time.

The airlines may move more quickly. They are already authorized to impose any restrictions that they feel appropriate. Given the incident reports there is a potential that cellular phones may be prohibited from carry-on baggage (as are other hazardous materials).

EMI problems should make software people feel right at home. It is like spaghetti code. Every single wire and conductor is an antenna and resonator. Every chip a potential transmitter. All of these interact with each other to add or cancel. To minimize EMI you want the sum effect to be the least efficient antenna/transmitter possible.

Fortunately, this does not conflict with the real design goals and most of the wires are already very inefficient. The problem is tracking down the occasional exception that is transmitting too much noise.

Rob Horn   horn@temerity.polaroid.com

International Card Fraud

<rmoonen@ihlpl.att.com>
Wed, 10 Mar 93 09:30 GMT

> [Ralph notes that this is not directly a COMPUTER RISK,
> but it is interesting anyway. PGN]

This week German shops and gas-stations have banned Dutch customers who wish to pay with their credit card. In particular Euro-card users were duped by this. The reason was that a recent study by fraud-prevention units in the Netherlands noted a sharp increase in credit-card-fraud.

Unsuspecting customers at German gas-stations got into trouble when the only means they had to pay was their credit-cards. They could still withdraw cash from ATMs with their cards however. It's interesting that because of the easy ways to commit fraud with a credit card, now the Germans have decided the Dutch customers are the perpetrators.

This case makes me think of the red-lining of phone-booths in inner-city areas with a high ethnic population. The phone company reasoned that as these areas showed a high calling-card abuse rate, they shouldn't be allowed to call certain countries.

--Ralph

Re: Garage door burglaries (Payne, RISKS-14.40)

<king@ukulele.reasoning.com>
Tue, 16 Mar 93 10:41:18 GMT

<> An installer of automatic garage door openers has been arrested, pending
<> being formally charged of burglary.

This is not a particularly new risk.

People have always been exposed when they hired locksmiths. Locksmiths must be licenced and bonded for this reason, in most states. Indeed, despite these precautions one hears about a case of locksmith burglary now and again.

There are, however, two new features to the risk:

* You can change the code easily. Most people can't hire a locksmith to change their lock and then change the key themselves.

  This change is in the customer's favor, but he needs to do it.

* I would not be surprised to read about a burglary ring that builds a device to detect and record garage door opener codes. Jog around town wearing what appears to be a personal stereo while people are coming home from work in the evening, and when you get home read the tape, jot down your codes,

and burgle away the next day.

There are ways of dealing with this, such as time-dependent codes, but i don't expect to see them coming to a garage door near me anytime soon.

Re: Computer Controlled Parachutes (Heritage, RISKS-14.39)

Robert Vernon <bob@pta.pyramid.com.au>
Wed, 17 Mar 1993 18:38:38 +1000

> I wonder how many air people would buy a computer-controlled parachute...

In fact computer controlled parachute deployment is possible.

Traditionally a parachutist manually deploys his main parachute. If that fails then he follows a set procedure to release the main and deploy the reserve parachute. Mains usually open but sometimes they don't, so every parachutist must be trained in reserve procedures. Yet over the years the most common reason for death has been to simply fail to deploy the reserve when needed. In a high stress situation some people just seem to forget all their training.

So the Automatic Activation Device (AAD) was invented. These work on the rate of change of air-pressure. If you are descending too fast at a set height, then your parachute is deployed regardless. Note that an AAD is a backup only. You are not supposed to ever be low enough to need one and they should only fire if for some reason you don't or can't deploy. The mechanical models have always been regarded as too unreliable, too bulky and too expensive for experienced jumpers use so AADs have mostly been installed on student equipment.

A new microcomputer controlled model called a Cypres answer most of the normal complaints. They are reliable, accurate, and small. And they have extra features like automatically adjusting for zero altitude.

Until recently most experienced jumpers still refused to attach even this AAD to their own equipment. "No way will I risk it firing at the wrong time". Then last December a highly experienced (10000+ jumps) US jumper died when he was knocked unconscious in freefall. His rig had been given to him as demonstration gear and it had a Cypres installed. His last comment in the plane was supposed to be "I might have to wear it but they can't make me turn it on". After this death, the waiting list for a Cypres went from 2 weeks to 18 weeks and jumpers who wouldn't be seen dead with an AAD started talking seriously about installing one.

The RISK: I'm not sure there is one. The Cypres sounds too good to be true. Anyone who has one won't die. Yet I keep feeling that that is the risk. They are supposed to be a backup but I am afraid that people will slowly put less emphasis on reserve procedures and rely on this device working. One day it won't and the jumper will not know what to do. There is a lot of discussion in the Skydiving community about this topic at the moment.

Bob V!

Yet another White House address

<TDARCOS@MCIMAIL.COM>
Wed, 17 Mar 1993 12:17:50 -0500 (EST)

Comp Privacy <COMP-PRIVACY@PICA.ARMY.MIL>,
Risks in computing <RISKS@csl.sri.com>, libernet@dartmouth.edu,

MCI Mail announced yet another E-Mail address for messages to be sent to the White House. It stated in the note that messages sent to the address would be sent as paper mail to the White House via the USPS, rather than as E-Mail.

The implication, since the usual charge for individual messages is 50c for the first 500 characters, that this could conceivably be something that the White House is paying for, since MCI Mail permits "autoforwarding" of a message sent to a mailbox to be sent to a fax number, another E-Mail address or a Paper Mail address.

If MCI is doing this to encourage MCI Mail subscribers to send messages, then messages from users on Internet will almost certainly either bounce or not be sent.

I encourage people on Internet to try sending a message to the address supplied by MCI Mail for messages to the White House to see what happens.

I guess that's all I need to say.

OH YES! You need the E-Mail address, don't you? :)

0005895485@MCIMAIL.COM

Paul Robinson -- TDARCOS@MCIMAIL.COM

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 42

Tuesday 23 March 1993

Contents

Her Majesty's Government's missing millions

Pete Mellor <pm@cs.city.ac.uk>
Fri, 19 Mar 93 10:59:52 GMT

BBC Radio 4 news this morning (19th March 1993):

Sir John Bourne, head of the Government Audit office, stated that an audit of the Social Fund had revealed that (pounds) 37 million could not be accounted for. It appeared that 16 million of this could be ascribed to the "usual" errors in inputting data to the computer system. The other 21 million was "lost" due to the incorrect operation of the computer system itself.

The Social Fund is used to make "one-of" payments to people receiving social benefit, e.g., for the purchase of an essential item such as a cooker. The failure occurs when such people move from one area to another: the system does not transfer the record of the payment they have received to the new area, and the money appears to have been "lost". It is expected that it will be possible to trace most of the money.

A Labour MP who chairs one of the Social Benefit committees (sorry, name and committee not recorded) stated that this sort of problem is all too frequent, and is due to computers having been introduced too rapidly into government departments, and to the advice of the government's own computer experts having been ignored.

[No further details available at present.]

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

What a fragile, interconnected world we live in!

David Daniels <0004381897@mcimail.com>
Mon, 22 Mar 93 00:04 GMT

NY Times, 3/20 from Dallas, 3/19...

> The collapse of the snow-laden roof of a computer center in Clifton, NJ, last Saturday also brought down 5,000 ATM's nationwide, causing particularly serious problems in California and Illinois. The situation has left the banking industry and its customers wondering about their growing reliance on such machines.
>
> Some of the questions concern the planning for such emergencies. The computer center's crisis plan called for it to move to a backup site in North Bergen, NJ, operated by a company that supplies such disaster-recovery services. That plan was thwarted because the center was filled with other computer operators who had been displaced from the World Trade Center by last month's bombing.

Technological Manipulations in Political Advertising

David Daniels <0004381897@mcimail.com>
Sun, 21 Mar 93 05:35 GMT

NSF Press Release 93-24, 8 March 1993, contact Mary Hanson (202) 357-9498

RESEARCHERS UNCOVER "ETHICALLY SUSPECT"
TECHNOLOGICAL MANIPULATIONS IN POLITICAL ADVERTISING

Most Americans are aware of the potential impact of political ads on their voting behavior; but many may not realize that a significant percentage of ads they see on television have been technologically manipulated to create a false or misleading impression. Researchers supported by the National Science Foundation (NSF) analyzed 2,000 ads from the 1952 through the 1992 campaigns -- primarily at the presidential level -- and found that nearly 15 percent of them were deliberately distorted.

"We think we've identified a substantial problem that has implications for the political process," said Lynda Lee Kaid, director of the Political Communication Center at the University of Oklahoma, who is leading the pilot project. "The technology provides an opportunity for candidates to perhaps abuse the trust that the voters have in our political process."

Along with a panel of ethics experts, Dr. Kaid has analyzed the ways in which modern computer and audio-video technologies have been used to create ethically suspect television spots in political campaigns. Her analysis uncovered a variety of manipulation techniques, including speeding-up or slowing down an audio track to make a candidate's voice seem either God-like or whiny, and distorting video images. Such manipulations, Kaid said, were more likely to appear in negative ads than in positive ones.

According to Kaid, distorting video images has become an increasingly popular technique which she considers ethically "dangerous." "Many of these new technological devices make it possible to alter images in a way that is not perceptible to the human eye when they're viewed on television." For example, footage can be edited so that a candidate's comments are taken completely out of context or are used with other footage to portray an entirely different meaning than originally intended. Kaid pointed out that, while manipulation techniques are often used in many kinds of advertising, "we believe it's a particular problem in political advertising because it has become the major way in which candidates communicate with voters."

Kaid hopes her research will be used as a defense against unrecognized manipulation of voter opinion. "We're trying to help voters and the public recognize these techniques, so they can make better judgments and become informed consumers of political ads." She plans to create an educational videotape with her research findings.

In subsequent research phases, Kaid hopes to conduct experimental studies to determine the extent to which voters are actually misled by manipulation techniques, or whether they are capable of recognizing the distortions when they see them. "We'd like to develop a direct link between the technological distortions and the actual voter decision-making process so that we can show whether or not these techniques really do result in an abuse of the political process."

According to Rachelle Hollander, NSF program director of Ethics and Values Studies, the research findings point to the need to systematically examine the impact of political ads on voter behavior, and thus on public policy-making. "We need to start thinking about how new communications technologies can influence and persuade...but also can mislead," she said.

Conspiracy trial ends in `Surprise' acquittal

<Jonathan.Bowen@prg.ox.ac.uk>
Fri, 19 Mar 93 18:19:51 GMT

The Thursday 18th March 1993 issue of The Independent newspaper covers the acquittal of a teenage hacker in the UK in some depth. A front page article includes the following:

> Conspiracy trial ends in `Surprise' acquittal
> Hacker penetrated MoD [UK Ministry of Defence]
>
> The teenage hacker acquitted yesterday of conspiracy charges under the Computer Misuse Act 1990 gained access to Ministry of Defence computers holding confidential information. ...
> The print-outs show confidential telephone numbers and information about the US network and missile bases linked to the US Army. ...
> Police officers involved said they were "surprised" by yesterday's verdict. The Computer Crimes Unit was eager to prosecute this first major trial under the new legislation. [sic]

Page 4 includes a full page article on the subject in which it is estimated that the annual bill to British business of computer fraud is 1.1 billion UK pounds (c. $1.5B).

A leading article on page 25 states:

> If Mr Bedworth's acquittal sets a prededent, it will make an ass of the Computer Misuse Act 1990. The Act was drafted specifically in order to close loopholes that had previously allowed people to do legally what he did.

Jonathan Bowen, Oxford University Computing Laboratory

RISKS of brain interference

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
19 Mar 93 10:57:25 EST

This morning the Globe and Mail (Canada) reported that Fujitsu of Japan is working on a brain-wave interface for computers. According to The Times of London, company spokesperson Michael Beirne said, "Our goal is to create an intuitive computer that can pick up your thoughts even as you walk around a room." The Globe and Mail summary claims that the researchers are currently working on distinguishing thoughts of "up" from those of "down" to move a cursor.

RISKS participants will easily think of some fascinating problems ahead of the researchers and of society as this technique evolves. For example, in the 1956(?) movie, "Forbidden Planet," space-farers approach an unknown planet and are warned away by the lone inhabitants (an elderly man and his--naturally--nubile and short-skirted daughter). He shows the

visitors the remains of the original people who had lived on the planet.
The Krell were masters of technology and even devised a mechanism for
giving life to the thoughts of sentient beings. Unfortunately they suddenly
disappeared without a trace shortly after this technology was introduced.
Some crewmembers try the device out and create little dancing women for
their amusement. Then disaster strikes: invisible monsters turn crewmen
into hamburger every night, leaving bent stairways and huge footprints.
Eventually, a dying man croaks out the clue: "Monsters," he says, "monsters
from the id."

So what will happen to the brain-wave sensitive user interface when the
ostensible desire to do productive work on a certain file for that nasty
boss is overridden by the subconscious desire to delete the file?

And if the R&D folk really are working on pattern recognition for mental
vocalization, will this lead to pattern recognition of unconscious
mentation? Are we headed for telepathy machines? Mind readers?

What fun! Expect an increase in the volume of email in RISKS-L.

Michel E. Kabay, Ph.D., Director of Education
National Computer Security Association

Interference on airplanes

<sullivan@geom.umn.edu>
Sat, 20 Mar 93 14:14:31 CST

The March 13th issue of The Economist has a short article on interference by
passengers' electronic devices on aircraft control systems. It mentions "a
Boeing 747-400 that weaved from side to side until two laptops ... were turned
off" and Nintendos "confusing the automatic direction-finder" of a DC10.
Possible causes include plastic composites used in airplane construction, and
lower-voltage electronic systems. Electronic devices used by passengers "near
the front of an aircraft appear to be most disruptive". [Maybe we should
banish business class to the back of the plane.] There are also reports of
interference "triggering anti-lock brake systems" in German cars, and causing
Japanese robots to "run amok".

[Another article in the same issue discusses the failure of the London
Stock Exchange's computer trading system, Taurus.]

-John Sullivan@geom.umn.edu

Virus Catalog update/New VirusBase

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Tue, 23 Mar 1993 17:29:37 +0100

The new version of Virus Test Center' *Computer Virus Catalog* is now available
for ftp (ftp.informatik.uni-hamburg.de). The following files may be downloaded:

INDEX.ZIP the new index file (INDEX.293), listing all
283 viruses in 5 platforms yet described
AMIGAVIR.ZIP the cumulative AMIGAVIR files, now describing
77 AMIGA viruses (15 new ones)
MSDOSVIR.ZIP the cumulative MSDOSVIR.files, now classifying
156 MSDOS viruses and trojans (32 new ones)
MACVIR.ZIP the cumulative MACVIR files; no update since
July 1992 (.792) as no new viruses were found
ATARIVIR.ZIP the old AtariVir files (20 viruses) not updated
as we have no new viruses for analysis.

The single UNIX virus (AT&T Attack) will be sent on request (on ftp soon).
In the new MSDOSVIR.293 file, the following new PC viruses are classified:

10_past_3 (2), Adolf, Alabama, Chemnitz, Exe_Bug (2), Flip, Hey_You,
Kampana=Spanish Telecom (2), Minimal (15), Techno, VOID_POEM, V-163
and V-Sign/CANSU.

Moreover, characteristic features of viruses generated by the following authoring packages are also classified:

PS-MPC and VCL.

As announced last year, the new *machine readable CVC version* called CVBASE is also available for downloading: cvbase-293.zip. CVBASE allows to display all CVC entries (in total 288, on Amiga, Atari, Mac, MsDos and the single UNIX virus), under option VIRUS, but also gives an OVERVIEW and STRAIN relationship about All (about 2,200) viruses in the CARO/VTC collections (using CARO naming scheme) as well as the VTC collection on Amiga (77), Atari (20), Mac (35) and Unix (1). From STRAIN, one may read available CVC entries.

Any suggestions how to improve this version are welcome

Klaus Brunnstein (U-Hamburg, Virus Test Center, March 22,1993)

Buy IBM and get fired - a response (Anderson, RISKS-14.41)

"Todd W. Arnold" <tarnold@vnet.IBM.COM>
Tue, 23 Mar 93 13:18:20 EST

In an earlier posting, Ross Anderson discusses the cancellation of the Taurus project in the UK. The information he presents, some from the UK media, is misleading and in some cases incorrect.

This gave a rather unfair appraisal of IBM security products. In fact, this part of the system was finished, installed, and tested. I've been asked to post the following "official" description of the situation, so everyone knows what really happened.

"The overall Taurus project was managed by the London Stock Exchange with Coopers and Lybrand and other consultants in a number of key management positions; with a range of contractors involved in sub-projects modifying and enhancing the Stock Exchange systems.

A US software house was meant to be providing a new custody application and IBM provided a market-leading security infrastructure. The shelving of the overall TAURUS project is for reasons unconnected with IBM's role.

IBM's involvement has been as subcontractor for the TAURUS Message Security system. This leading-edge development exploited IBM ICRF host cryptography, OS/2, smart cards, and PS/2 cryptography and signature verification technology to deliver an outstandingly secure method of transferring data between member firms and the Stock Exchange.

The development was successfully completed last summer, then rigorously acceptance-tested by the Stock Exchange. IBM installed the system across 200+ separate financial institutions, completing on time in February against an aggressive schedule."

I've been told that the massive complexity of the back-end settlement systems was a major factor in the collapse, but I don't really know all the details.

(Note that the "signature verification technology" mentioned above is dynamic signature verification, a biometric technology -- not public key digital signatures. RSA public key functions are also available in TSS, but that's not what was used in Taurus.)

Todd W. Arnold, tarnold@vnet.ibm.com, IBM Cryptographic Facility Development, Charlotte, NC

Disclaimer: This posting represents the poster's views, not those of IBM

[I normally suppress all disclaimers and cover them blanket-wise in the masthead. This one is intriguing, because the posting explicitly contains an "official" description, which would seem to disclaim the disclaimer! PGN]

Re: Buy IBM and get fired (Anderson, RISKS-14.41)

<Bennet_Yee@PLAY.TRUST.CS.CMU.EDU>
Thu, 18 Mar 93 14:53:41 EST

We should not disparage physical security just because we can't sell our pet methodologies. Physical security is a necessary component of any security system. Private keys must be stored -- and _used_ -- in a secure environment where there is no risk of exposure. Formal methods and elliptic curves are orthogonal to the need for steel boxes.

+Future systems however may well use public key algorithms, and maybe even
+electronic wallets which distribute the security processing entirely into
+smartcards.

Regardless of whether we use public key or private key, we still need the ability to perform secure processing with the secret key. Be it a computer room with armed guards, a giant steel box, or other forms of tamper-proof hardware, -some- of the bank's computation must be secure. Whether we use public key or private key is again orthogonal to physical security needs.

Smart cards may appear attractive for many applications, but they do not suffice for handling the case of trying to ``distribute the security processing entirely into'' them. Even if we assume that they have sufficient power to run public key cryptosystems, a problem remains: we still can't always trust the balance on a smart card. Today's smart cards don't provide any physical security; their users do. The implicit assumption is that users of smart cards carry their smart cards with them at all times, and can keep the secrets/data kept within their smart cards from being exposed/modified. Malicious users, on the other hand, have plenty of opportunity to tamper with their smart cards. Keys may be exposed, balances may be changed -- there are no privacy and integrity guarantees with malicious users.

Not being able to keep balance information in smart cards means that there must be servers where such information is kept. Central servers mean that our electronic wallets do not really hold electronic currency but serves only as an ID card.

Chaum's digicash fixes some of the tampering problems by using cryptography, but it really is not much better than a checking system -- receivers of the digicash must contact a centralized server to verify that the digicash hasn't been previously spent before committing a transaction, or otherwise risk the digicash ``bouncing''; digicash is not really transferable except through centralized servers, since the need to trace its transfer path for duplication detection diametrically opposes the need for anonymity.

What are the risks? Mainly that of attitudes that we as scientists/professionals should avoid. We shouldn't jump on technological bandwagons. Public key cryptosystems, electronic wallets and smart cards, formal methods, etc, are powerful, useful tools, but they are no panacea. We must be careful in evaluating exactly how much can be done with them. Just because DES-in-steel-boxes may seem old and ``clunky'', there were good reasons for using it, and we had better think things through before we start dreaming about (or ``selling'') alternative technologies for the future.

Bennet S. Yee Phone: +1 412 268-7571 Email: bsy+@cs.cmu.edu
School of CS, Carnegie Mellon, 5000 Forbes Ave, Pittsburgh, PA 15213-3891

RISKS Backlog

RISKS Forum <risks@csl.sri.com>
Tue, 23 Mar 93 17:04:47 PST

Thanks to all of you who diligently respond to RISKS topics. There is a big backlog of items at the moment, particularly on garage door burglaries and computer controlled parachutes! Some of these items are drifting in relevance or otherwise requiring a little extra thought on whether to include them. Contributors must be patient. You may also note that I cannot reply to every message. I try to take care of all REQUEST mail and new topics, but occasionally the load of incremental comments on already marginal material becomes overwhelming. Thank you for your patience. The Management [PGN]

Eleventh Intrusion Detection Workshop

Teresa Lunt <lunt@csl.sri.com>
Tue, 23 Mar 93 16:08:59 -0800

ELEVENTH INTRUSION DETECTION WORKSHOP
CALL FOR PARTICIPATION

A two-day workshop on intrusion detection will be held at SRI International in Menlo Park, California on May 27-28, 1993, the Thursday and Friday following the 1993 IEEE Symposium on Research in Security and Privacy in Oakland, California. This will be the eleventh in a series of twice-yearly intrusion-detection workshops. The workshop will run from 9am until 5pm on Thursday, and 9am until 2pm on Friday.

The workshop will consist of several short presentations as well as discussion periods. If you have any progress to report on an intrusion-detection project or some related work that would be appropriate for a short presentation, please indicate the title and a paragraph describing your proposed talk on the form below. You can also indicate there your suggestions for discussion topics. Of course, you do not have to make a presentation to attend; all are welcome!

If you and/or your colleagues wish to attend, please RSVP using the form below. You may email the completed form to Liz Luntzel at luntzel@csl.sri.com, or send it by post. There is a $100 charge for the workshop. This fee includes lunches in SRI's International Dining Room. Please make your check out to SRI International and mail it to Liz Luntzel, SRI International EL-248, 333 Ravenswood Ave, Menlo Park CA 94025 USA. For other questions, please call Liz at 415-859-3285 or send her a fax at 415-859-2844 or email at luntzel@csl.sri.com.

SRI is located at 333 Ravenswood Avenue in Menlo Park. The workshop will be held in room IS109, which is in the International Building. If you wish instructions on how to get there, indicate that below.

-------------CUT HERE AND RETURN TO LUNTZEL@CSL.SRI.COM-------------

ELEVENTH INTRUSION DETECTION WORKSHOP

Yes! I will attend the Intrusion-Detection Workshop May 27-28 at SRI.

[Please complete the following:]

Name:

Title:

Affiliation:

Address:

_

PLEASE SEND ME INSTRUCTIONS for getting to SRI and parking.   YES |_|
[by email or SnailMail, as appropriate]

[Indicate one:]
I [will/will not] be willing to present a talk.

[Please complete the following:]

Title of Talk:

Abstract:

Suggestions for Discussion Topics:

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 43

Wednesday 24 March 1993

Contents

Dutch computer hacker arrested under new Dutch Law

<rmoonen@ihlpl.att.com>
Wed, 24 Mar 93 10:00 GMT

The "Volkskrant", a leading Dutch newspaper carried an article last saturday about the latest computer hacker arrest in the Netherlands. It was the first arrest made under the new Dutch Computer Crime Law. The hacker was arrested while sitting at a terminal in the computer room of the Amsterdam University. When the police arrived late in the afternoon, he was supposedly caught red-handed. A couple of hours later, the police searched his parents house, and confiscated some equipment and papers. The hacker was arrested last year also, but no charges were brought against him at that time. This time he probably will have a harder time getting out of it, because of the new law. It is unclear what charges he was arrested on exactly, or what he was doing at the time of his arrest. Watch this space for more news.....

--Ralph Moonen

Minnesota phone fraud

"Riley Vic" <riley_vic@msmail.src.honeywell.com>
24 Mar 1993 10:19:07 -0600

The Majority Leader of the Minnesota House of Representatives has just resigned amid disclosures that his son and nephew obtained his access code for the state long distance service. The service involves calling an 800 number and entering a personal code for making long distance calls related to state business. Although the son and nephew reportedly made less than $50 worth of calls themselves, they shared the codes with their friends. The total bill is now estimated at around $85,000 worth of calls. For now, taxpayers appear to be liable for the bill.

Victor Riley, Honeywell Systems and Research Center, Minneapolis
riley@src.honeywell.com

Beacon article-fu: The Mark Lehrer Case (RISKS-14.14 follow-up)

David Lehrer <71756.2116@compuserve.com>
23 Mar 93 14:55:45 EST

Akron Anomaly BBS trial issue:

Distributed with permission of The Akron Beacon Journal, David Lehrer

Police Say They Were Taking a Byte out of Crime. Munroe Falls Man Was Arrested for Having X-Rated Pictures on His Computer Bulletin Board; His Parents Believe the Sting Operation Was Politically Motivated.
Akron Beacon Journal (AK) - MONDAY March 22, 1993
By: CHARLENE NEVADA, Beacon Journal staff writer

[For those of you interested in following up on the strange developments in the Mark Lehrer case, previously discussed in RISKS-14.14 by his father, David Lehrer, the entire Akron Beacon article is obtainable from the CRVAX RISKS: directory in a file named RISKS-14.43LEHRER, or from David. PGN]

Re: Conspiracy trial ends in ... acquittal (Bowen, RISKS-14.42)

Olivier MJ Crepin-Leblond <o.crepin-leblond@ic.ac.uk>
Wed, 24 Mar 1993 10:32:29 +0000

I think what needs to be mentioned is the reason why he was acquitted (or at least, the reason that journalists propagated): "He was addicted to hacking".

That, I find, is the weakest explanation I have ever heard about a crime. Just
imagine a society where serial killers are acquitted "because they are
addicted to killing" !

While, IMHO, a prison sentence would have been tough on Mr. Bedworth; a fine,
or some sort of community service would have been welcome. Why have laws, if
they are not properly applied ?

Olivier M.J. Crepin-Leblond, Digital Comms. Section, Elec. Eng. Department
Imperial College of Science, Technology and Medicine, London SW7 2BT, UK
Internet/Bitnet: <foobar@ic.ac.uk> - Janet: <foobar@uk.ac.ic>

Re: Conspiracy trial ends in ... acquittal (Bowen, RISKS-14.42)

Peter Debenham <PPXPMD@ppn1.nott.ac.uk>
24 Mar 93 15:29:34 GMT

This posting creates a slightly false impression by not giving the grounds that the acquittal was acquired on. The court deemed that Mr Bedworth's behaviour was uncontrollable by him due to a total addiction to hacking. In other words he was unable to form the "guilty mind" that is necessary to get a conviction in a British court on such charges. Very much like an acquittal on any other charge due to being unable to know what you are doing (be the cause mental illness, temporary effect from prescribed drugs etc).

Despite the Independent's leader, no new precedent has been set has been set in this case. It is just the application of a well established piece of British law to a new statute.

Peter Debenham, Physics Dept., University of Nottingham, UK. NG7 2RD
P_Debenham@ppn1.nott.ac.uk   + 602 515151 x8323 (wk)   +602 730487 (hm)

Re: Buy IBM and get fired, response (Arnold, RISKS-14.42)

<Ross.Anderson@cl.cam.ac.uk>
Wed, 24 Mar 93 12:55:03 GMT

In reply to this:

(1) My primary source was `Waiting for Taurus' by J Green-Armitage in Computer Weekly March 4 1993 pp 28 - 29. This article states that the considerable delays and cost overruns were due to a number of problems, including the security subsystem, management hassles and regulatory delays. To quote the article `IBM must accept a modicum of blame because it needed an extra three months in 1992 to finish its solution'.

This article appeared a few days before the project was cancelled and the chief executive of the stock exchange resigned.

(2) There will be a lot of lawyers picking over this disaster. Two hundred banks and brokers have lost over half a billion dollars between them, and IBM

seems to be one of three possible defendants (the others are Coopers and the Stock Exchange itself).

If, as IBM now say, their system was finally signed off a few days before the project meltdown, then they may get lucky. But they're obviously still worried. Why else did they not just keep quiet and let the matter die? If they hadn't tried to argue the matter, my initial posting to sci.crypt would have been forgotten by now.

Ross Anderson

Risks of automatic signature inclusions

<tada@Athena.MIT.EDU>
Tue, 23 Mar 93 22:43:39 -0500

In his article on IBM's security for the Taurus project, Todd W. Arnold, tarnold@vnet.ibm.com, IBM Cryptographic Facility Development, Charlotte, NC wrote:

>I've been asked to post the following "official" description of the situation
  [...]
>Disclaimer: This posting represents the poster's views, not those of IBM

To which PGN added:
>   [I normally suppress all disclaimers and cover them blanket-wise in the
>   masthead. This one is intriguing, because the posting explicitly
>   contains an "official" description, which would seem to disclaim the
>   disclaimer! PGN]

There are all sorts of risks present. Perhaps IBM should be expanding its signature verification software to verify that you really want to add a particular signature to your posting?

There are semantic and syntactic risks too. The word "official" is surrounded by quotes, indicating that perhaps it doesn't retain the normal meaning.

Or perhaps Todd's final line was in OO syntax. The message "disclaimer" meaning denial, repudiation, is being sent to the text string denying the authority of the posting. Computers routinely know what to do with double negatives which humans tend to contract into a single negative.

One speculates whether PGN will append a message, "I normally suppress all humor except my own. This one is intriguing, ..." :-)

-michael j zehr
    [Zehr Gut. Even though we are coming up on 1 April,
    I will not append anything to Michael's message. PGN]

Smart card/electronic cash security (Re: Yee, RISKS-14.42)

Niels Ferguson <Niels.Ferguson@cwi.nl>
24 Mar 93 10:57:50 GMT

[Was: Buy IBM and get fired, Bennet Yee]

I'm not sure what 'digicash' you are talking about. The smartcard based electronic cash system that Chaum's _company_ DigiCash is marketing does not require any on-line processing during payment. The payment protocol uses a commit-challenge-response structure which can eliminate the need for on-line communication with a central server. In contrast to other smartcard based systems there is no system-wide 'master' key stored in a tamper-resistant box at each shop. The recipient can validate the money by a simple signature verification using a public key. The system does rely on the tamper-resistance of the smartcards for security; if anybody 'breaks' a smartcard and extracts all the keys, then this will allow a limited amount of fraud.

The use of master keys in many smartcard based applications is of course a serious risk. If the master key is ever compromised for any reason, then the whole system collapses. It is questionable if storing such a master key in thousands of tamper-resistant boxes is secure enough. Especially for electronic cash applications, the fraud potential once the master key is known is unlimited.

There are several other purely cryptographic systems for electronic cash. The early systems were indeed on-line to prevent a user from spending the same piece of money twice. Later systems achieve an off-line payment protocol without any compromise regarding the privacy. (For more details, see the Chaum-Fiat-Noar paper of Crypto '88.) All of these systems do NOT require any tamper-resistant device anywhere, except in the central bank. The security depends only on the cryptography used. Up to now these kind of systems have not been used due to their complexity and inefficiency. Recent improvements have lead to systems which are much more efficient and simpler.

There is a general construction to make any of these systems transferable. With electronic cash the transferability is less important than with physical payment systems; it only takes a phone call to hand in the received money and withdraw some new cash. The transferability has some disadvantages, one of which is that the size of the money (in bits) MUST grow as it is passed from one user to another. Another disadvantage is that any user can always recognise any piece of money that passed through her hands, which reduces the level of privacy.

The current state of affairs is that electronic cash without tamper-resistant user devices is technically feasible. We are considering implementing one of the newer protocols to provide electronic payments via e-mail.

Niels T. Ferguson, CWI, Amsterdam, Netherlands   e-mail: niels@cwi.nl

Re: RISKS of brain interference: not as tabloid as you'd think

David Honig <honig@ruffles.ICS.UCI.EDU>
Tue, 23 Mar 1993 19:58:41 -0800

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com> wrote in RISKS-14.42,

> This morning the Globe and Mail (Canada) reported that Fujitsu of Japan is
> working on a brain-wave interface for computers. ...

Actually its been known for some time that activity in a certain piece of your brain reliably predicts eye and motor movements, by as much as 1/3 second. This is of interest both to human factors people (the military has been interested in this for faster response for firing missiles by a jet pilot) and philosophers; Daniel Dennett writes of this in his recent tome, _Consciousness Explained_, which came out last year. Dennett is a cognitive-and-neuroscience-aware philosopher (a rare and precious thing) at Tufts I believe.

Software Warranties [longish]

Paul Robinson <tdarcos@access.digex.com>
Mon, 8 Mar 1993 00:19:52 -0500 (EST)

A split version of this message has been sent to the Ethics-L list. It will be sent as one long message to the Risks List.

A user who did not put his E-Mail address in his message,
wrote the following on the Ethics-L list (ETHICS-L@vm.gmd.de) :

> Should the author of shareware be held liable for possible
> damages caused by the use of their product, and if so to
> what extent? Should a shareware author be held liable for
> the performance of their product in every hardware and software
> configuration?

First off, I'm not a lawyer but I do know a little about the laws relating to the operation of a business in general.

What you are (in general) referring to are the laws relating to warranty and "fitness of purpose". These laws place the general burden of operation for a product upon the manufacturer or seller, subject to whatever provisions they warrant; and in addition, each state has some laws of its own relating to warranty protection.

In general, a manufacturer is supposed to provide a product which meets the "fitness of purpose" test, i.e. an iron should heat and it be warm enough to press clothes. It should not explode when plugged in, nor should the person be electrocuted when touching any metal parts. If the person is burned by touching the face plate, that's a consequence of misuse of the product for which the manufacturer is not responsible.

If one makes a program to do accounts payable, it should accept transactions, print checks and keep a list of checks it printed, among other things. It should not crash when started, it should not damage other programs or files on the system, it should be able to print checks without printing 50 pages of garbage (and wasting 50 checks). If the person's checks are ruined because they put them in upside down, or the printer jammed, that's a consequence of misuse of the product for which the manufacturer is not responsible.

What the law should do is hold the manufacturer of a piece of software responsible for (1) any bugs he knew about (2) any failure to test under reasonable conditions of the market place, i.e. running without a printer, with printer unconnected, without a floppy disk inserted, and make sure it can recover without damage. Also a program would be expected to refuse to run under conditions it can't handle, for example, on any version of DOS less than 2.0, or under MS-Windows except in DOS mode, or whatever. If it requires VGA it should quit with a message if one isn't present. If a program requires a 286 or better, running it on an 8086 should issue a message and it should quit to the operating system, not crash or lockup the machine.

These, and perhaps other requirements, are reasonable minimum standards by which a program should be required to act. Under no circumstances should a program damage other program's files, nor should it be damaging to the hardware (unless the hardware is extremely delicate and can be damaged simply by misprogramming, such as with the older Hercules Graphics boards). Is it reasonable to assume that someone should have known that something should be done a certain way? Crashing and damaging other people's files are evidence of negligence. If this is the result of other programs contributing to it, that's another issue.

However, holding a software manufacturer liable for damages is going to be difficult. I ain't seen a program publisher who didn't put down a laundry-list of disclaimers, exclusions and warranty negations, even up to the point of declaring the software to be "as is". That's a legal term meaning the seller makes no representations about the particular item at all; in the context of computers it could be anything from a fantastic product that does everything you can imagine and even fulfils needs that you haven't even realized you had, to a worm that slags the motherboard and roaches the hard drives, then procedes to jump to other computers via the modem and network cards and do the same.

There is legal precedent in where a man was placed on trial for doing exactly that; he put in a program patch that destroyed everything in sight when he was removed from the payroll. I believe that man is now having an extended vacation with free room and board as a guest of the People of the State of Texas.

> Should the author of shareware be held liable for
> damages caused by the use of their product, and if so to
> what extent? Should a shareware author be held liable for
> the performance of their product in every hardware and software
> configuration?

> If they can then it is unlikely that they ever could write
> program and not get sued. Should a shareware author be treated
> differently if they make their living off shareware?

Technically a person can be sued if they provide a software package for free;

technically anyone can be sued for anything at all; whether someone else can win and collect from them is another thing altogether. If the seller is some guy who makes, say $5,000 a year or less selling programs, nobody is going to sue him because he probably doesn't carry Errors & Omissions insurance and he's judgement proof, meaning there's no money for the shyster to go after even if he does win.

Now let's say some large company, with assets is found. Using the term from the vernacular, let's call them "Deep Pockets Software, Inc." Since many companies are only incorporated in their home state, you have to sue them there; unless they are doing business in other states (and merely providing programs to a multistate distributor such as Egghead, Babbages, Waldenbooks, GTSI, Comp USA, or Micro Center in the area of retail stores, and Cost Plus, Programmers Shop, Dustin Discount Software or 47th Street Computer in the Mail Order arena, does not necessarily constitute "doing business") you might not be able to get service upon them. You might be able to sue the seller, but if the company simply put the software out on racks and people buy it, or simply put a description in a catalog, there may not be grounds for a claim against the seller since they've made no promises. If the in-store seller makes it possible to try the program on their machine first, then the claims are even weaker.

Also, contributory negligence comes into play: You look stupid when the defense attorney asks, "Did you have recent backups of your computer system's files? Aren't you aware you're supposed to have backups? Did you not read the message on the package that said 'Do not install this program without backing up everything'?" In some states, if the plaintiff (the one suing) is even 1% at fault, (s)he gets nothing.

> For example: A shareware author writes a disk defragmentation
> software which is tested and works perfectly on several computer
> setups. A person gets the software and runs it on their computer.
> The software destroys several important files which cost the person
> a large sum of money. Should the person be able to sue the author
> of the software?

First of all, even if the buyer of the software patched the program so that it was defective, an ran it despite no backups, and then saw his hard disk mangled, he can still sue the (1) maker of the hard drive (2) seller of his computer (3) seller of the software (4) manufacturer of the software (5) company that made the car that drove him there, etc.

The question at hand is whether he can collect damages from any of these parties. He can always sue even if he has no case at all; whether he can collect damages is another thing altogether.

You have to look at (1) the purpose of the product at hand (2) intended audience of the product (3) potential damage which can be caused by the product and (4) is this something the manufacturer could have foreseen?

There are disk defragmenters sold for many different computers, including VAX systems. I'll review this for MS DOS systems as I have more familiarity with those.

The purpose of a disk defragmenter is to reduce the number of separate segments of a file which are stored on a disk, presumably down to one contiguous set of segments for each file. As such, a defragmenter program works at the lowest level of the file system, even manipulating the File Access Table on an MSDOS computer. This places it in the class of Maintenance programs, of a level of dangerousness as a computer virus. (In fact, you have to disable any virus checking software to run this sort of thing because it has to have WRITE ACCESS to the FAT table of the hard disk.) This is probably the most dangerous class of user accessible programs around.

The best method for constructing a disk defragmenter is to (1) move one or more file block(s) to an empty spot to either make the space contiguous for a file or to open up empty space in front of a file in order to make it contiguous (2) update the fat table with the new location (3) do the next block.

What this does is ensure that the FAT table, the most critical part of the system, is updated when the information changes. You don't update the FAT table until AFTER you move the file. This way, the worst that can happen - a reboot, a power failure - the file system is still intact and no damage is done even if the process dies half-way through.

Now, the question at hand is what type of damage occurred, and why it happened. First, if the manufacturer failed to tell people to take precautions (1) disable virus checkers (2) disable disk caching (3) disable multitasking (4) disable TSRs or anything that keeps a file open (5) run the program from the DOS prompt, then there would be cause to raise negligence.

In fact, if someone wrote a disk defragmenter to run under MS-Windows, or failed to tell people to shut it down, first, I'd assume that to be almost automatic negligence. (In fact, I think people should be told to remove MS Windows before attempting to get any serious work done. Not just remove it from memory, remove and erase it from their system, but that's another story. :))

Now, the question comes up about why the user didn't have a backup of that critical file or files. Floppy disks sell for 53c each at a computer store or less for anything up to 1.44 meg. (I just bought 100 of them from the local store, which sells them for 17c each. If I wanted to go in and buy just one, it would have been 17c plus tax.) There is no excuse for failing to have critical files backed up.

The user can raise the issue that he did not know this. Well, if the program showed a screen stating these facts and asked if the user wanted to continue, and he did, there would be a hard time proving that the user didn't know.

Let's go further; let's say the user ran the defragmenter, and he does have his files backed up, but it trashes everything because of a bug in the system. Then, he could have a case for liability to the extent necessary to pay the cost of reparation of damages, i.e. the amount of work needed for restoring his system. Considering that a diskette takes about one minute to read, plus maybe 30 seconds to change disks, the time value of someone to restore a system, plus perhaps lost time discovering files had been damaged, would be what they could expect, if it was reasonable for this to be expected. Perhaps the maximum liability might be $1 per megabyte damaged. But this would be for every system damaged.

If a manufacturer does not state what his program should not be run on (for example, IDE or MFM or SCSI or ESDI disks, or whatever), or does not warn of the consequences of use (you must make sure you have current backups, you have to disable TSRs, you have to turn off MS-Windows) then they have a problem.

The question is reasonableness: what could be reasonably expected to happen in ordinary use? If the manufacturer discovers, after 100,000 copies have been shipped, that there is a bug that if the defragmenter is run between 11:59 pm and midnight, on the last day of the year on an IDE drive it will damage the FAT table and exit, it would then be liable for anyone injured by this until the public had knowledge of this. Sending a letter to every owner of the package along with a correction is one way, but the real question is whether they knew about the problem or could reasonably foresee it.

The question of a company's liability for erroneous software is more-or-less all moot because nobody provides warranties for software. But, this may change as software usage becomes so prevalent that these days of "caveat emptor" (let the buyer beware) stops being tolerated for software packages. Then the question of what warranty protection the buyer is entitled to comes into question. Also, the "standing" of a software company with respect to what type of work it does is also a question to be answered.

The "standing" of a company depends on whether it claims to be professional or technical. A professional does not guarantee the work he does, but he does guarantee that he meets the minimum standards set by the industry he works in, or by law or both. For example, a doctor, a lawyer, an engineer all adhere to the "professional" doctrine: you meet the minimum educational qualifications needed to be licensed, i.e. you at least know how to do the work in question. When a professional operates, in the absence of negligence, he is not liable if his actions fail to fix the problem, as long as his technical qualifications are intact. That's why you can't sue a lawyer if your side loses. You still have to pay an architect for his drawings even if you don't like the way the building looks.

On the other side is the technical person. He does not guarantee his experience, but he does guarantee the technical performance of his work. For example, a construction company will use the required materials and workmanship to construct a bridge according to the architect's specifications. If the bridge fails, as long as the materials and workmanship were satisfactory to complete the task as described, the builder isn't liable. He may have just graduated from hod carrier to owner of a construction company, but he does guarantee he will follow the requirements and not use materials of less quality than is required for the task.

In the Software industry, we are attempting to exclude both classifications of qualification: we do not claim to have the professional background (in some cases, the people who are in the industry cannot do so; many of them may not even have the qualifications), so we cannot stand on professionalism, i.e. we can't guarantee our ability to do the work. And because we can't know that

the programs will work, nor can we guarantee we know what the best methods
there are out there, we can't guarantee the product. Since we cannot
guarantee our qualifications, and we can't guarantee our product, places that
make computer programs are refusing to guarantee {anything}.

I think the ability to do this will be limited in the future as common
practice and legislation force the makers of software to take some
responsibility for their creations. Incidents like the attempt by the State
of New Jersey a couple of years ago to license programmers is one such
foretaste of things to come.

Paul Robinson -- TDARCOS@MCIMAIL.COM

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 44

Monday 29 March 1993

Contents

The FORTRAN-hating gateway

"Joe Dellinger" <joe@montebello.soest.hawaii.edu>
Fri, 26 Mar 93 23:04:46 HST

Several months ago we started noticing that (now and again) the network connection to the mainland would become very very slow; this would continue for 10-15 minutes or so, then all would suddenly be well again. A while after this started happening a coworker of mine complained to me that the connection to the mainland _never_ worked anymore. It seems that he had some FORTRAN source that he needed to copy to a machine on the mainland, but he never could because "the network wouldn't stay up long enough for the ftp to complete".

Yes, it turned out that the network outages happened whenever he attempted to ftp that _particular_ FORTRAN source file to the mainland. We next tried compressing the file; it copied just fine then (but unfortunately the machine on the mainland had no uncompress program, so it was still no go). Finally we "split" his FORTRAN program up into very small pieces and sent them one at a time. Most of the pieces would copy without trouble, but a few would either not go at all or only go after many _many_ retries.

Examining the troublesome pieces, we found they all had one thing in common: they contained comment blocks that began and ended with lines consisting of nothing but capital C's (his preferred FORTRAN commenting style). At this point we started sending e-mail to the network gurus on the mainland asking for help. Of course, they wanted to see an example of our un-ftp-able files, so we mailed some to them... but our mail never got there. Finally we got the bright idea of simply _describing_ what the unsendable files were like. That worked. :-) [Dare I include in this message an example of one of the offending FORTRAN comment blocks? Probably better not!]

Eventually we were able to piece together the story. A new gateway had recently been installed between our part of campus and the connection to the mainland. This gateway had GREAT difficulty transmitting packets that contained repeated blocks of capital C's!!!! Just a few such packets would occupy all its energies and prevent most everything else from getting through. At this point we complained to the gateway manufacturer... and were told "Oh, yes, you've hit the repeated C's bug! We know about that already.". Eventually we solved the problem... by buying new gateways from another manufacturer. (In the manufacturer's defense I suppose an inability to propagate FORTRAN programs might be considered a feature by some!)

Call for the Class of '88

Ed Ravin <eravin@Panix.Com>
Mon, 29 Mar 1993 18:03:17 GMT

I Found the squib below on the Prodigy service --

QUIRKS   Offbeat Computer News

Mary Bandar recently turned down an invitation to attend kindergarten with others born in '88. "Boy, wouldn't those kids ever be surprised when they see me coming to school," Bander, 104, told the Associated Press. "Why would they want me? I know the ABCs yet. And I can count to 10," said the Winona, Minn, resident, who was born in 1888.

> Sister Mary Donald Miller, superintendent of Winona Area Catholic Schools, told the AP that the mix-up occurred when school officials instructed a computer to search for the names of people born in '88.

The RISKS aware person might ask a few more questions-- which computer was the school using? Where is this central database of all the people in Winona, Minnesota? Who puts the data into it, and who decides who else can pull the data out?

I expect that as we approach the millenium, we'll see a lot more of these "off by a century" errors.

Ed Ravin eravin@panix.com philabs!trintex!elr +1 914 993 4737

If they mention flying saucers, they're out to get you

Christopher Maeda <cmaeda@ERNST.MACH.CS.CMU.EDU>
Sun, 28 Mar 93 12:29:15 EST

Date: Tue, 23 Mar 1993 14:33:00 BST
Subject: if they mention flying saucers, they're out to get you
From: Derek Cooper <RCAA000@maple.cc.kcl.ac.uk>

From the London Times today (I did check that it's not April 1st!)-

> Officers in Warrington Cheshire fed up with people listening in to their messages, broadcast that a flying saucer had crash-landed in a field & gave details of where to find it.
>
> Radio messages about a huge glowing spacecraft were broadcast with the warning "Do not approach. It may be radioactive." The warning was followed by directions to the field in Appleton. The eavesdroppers arrived within minutes, expecting to see little green men. They were arrested instead.
>
> Police said that 5 people had been reported to the Crown Prosecution Service for telecommunications offences. Scanning devices that can pick up police radio messages are widely available but using them to listen to police transmissions is an offence.

[I have seen this on several groups. There is a question whether it is actually illegal if you are merely listening, as opposed to doing something about it. PGN]

Computer problems at Empire Blue Cross

Robert Wentworth <rhw@hoh-1.att.com>
Mon, 29 Mar 93 15:47:43 EST

From a NY Times article (3/29/93, p. A1,B2) on financial and management problems at NY state health insurer Empire Blue Cross/Blue Shield:

Empire was forced to write off $50 million that had gone uncollected or unbilled because of computer problems dating to the mid-1970's, according to an internal report obtained by The New York Times.
 One glitch involved a computer system that could not understand bills of $100,000 or more. A $103,000 charge, for example, would be interpreted as only $3000, and the smaller amount would be billed to the client. That failure occurred 29 times and cost Empire $3 million, the report said.

[Management comments about such problems being ancient history and Empire's real problems lying elsewhere.]

Still, the computer problems persist. An expensive new electric system for handling claims --- being developed by a former board member --- was expected to be finished about 18 months ago, but is not likely to be completed until later this year. Empire has invested $17 million in that venture.

Fantasy Baseball Journal Virus

<ega@neptune.att.com>
Thu, 25 Mar 93 08:37 EST

As baseball season is upon us, those who belong to fantasy leagues begin to devour all available material about players, statistics, injuries, and so on. One such supplier of these needed facts and opinions, The Fantasy Baseball Journal, recently apologized for a particularly buggy issue. They attribute the printing errors to a "so-called virus that has seeped onto our computer network." This is not so startling, as we all know this kind of thing can happen. What is startling is the claim in the FBJ that "if [the virus] is the problem, then that's solvable." Perhaps these baseball statisticians are smarter that we thought...

-- Ed Amoroso, AT&T Bell Labs

Reported procedural problems with TCAS, from sci.aeronautics

Lorenzo Strigini <strigini@iei.pi.cnr.it>
Fri, 26 Mar 93 14:38:45 MET

From: ak336@cleveland.Freenet.Edu (John Dill)
Newsgroups: sci.aeronautics
Subject: TCAS Glitchs
Date: 25 Mar 1993 14:48:47 GMT
Organization: Case Western Reserve University, Cleveland, OH (USA)
NNTP-Posting-Host: slc10.ins.cwru.edu

I've been a controller at the Cleveland ARTCC for 22 yrs. I've always welcomed the arrival of any new procedure or technology that can enhance our ability to safely separate air traffic. TCAS has proven to be one such aid. However, a problem has been discovered which has the potential to be disastrous.

Here is the problem:
Aircraft "A" is climbing to an assigned altitude of 23,000' (as an example), while aircraft "B" is descending to an assigned altitude of 24,000'. The two a/c are on converging courses and their combined verticle closure rate is high, in this case we'll say about 6000' fpm. TCAS (on each aircraft) does what is called a coordinated interrogation, meaning the equipment talks back and forth and decides on the best resolution. Of course, the TCAS has no way of knowing the aircraft are intending to both level off 1,000' apart, so it issues a resolution advisory (RA) to both flight crews telling them to INCREASE their respective rates of climb and descent. This is in direct conflict to the controllers clearances. Only after the controller notices the mode c readouts deviating from the assigned altitudes is he aware of a problem. (actually, the frightcrews (pun intended) are required to inform the controller that they are responding to a TCAS RA, but due to frequency blockage, other duties, etc. this may not happen. Upon seeing the deviation, the controller attempts to have the aircraft return to their assigned altitudes.

There have been several incidents similar to this fictional one. The loss of separation has been severe (as little as 200') and resulted from the crews confusion on who's instructions to follow. In the past few weeks, the FAA has issued directives to all controllers to NOT attempt to countermand a TCAS RA. By following only the TCAS RA, it is felt that the separation, even though less than standard, will be sufficient.

John

Dutch hacker in jail for another month

Hans van Staveren <sater@cs.vu.nl>
Thu, 25 Mar 93 9:53:23 MET

The so-called hacker, the twenty-year-old Ronald O., whom we caught on one of our PC's doing things as yet unknown at Delft University, will be in temporary custody (or whatever the correct English term for that is) for 30 more days. This is to give the police more time to gather evidence.

According to the papers, forged credit cards were found while searching his home, and that also will not help his case. He is supposedly unwilling to answer any questions at this point, but is charged with crimes that could send him to jail for a maximum of four years.

Although I am definitely not suggesting he is a nice guy, somehow I have some difficulty connecting this nervous kid in our room with a sentence of four years. I hope that being the first to be caught under the new law, and in the act to boot, is not going to give him too much extra attention from law officers.

Never forget the RISK of someone dying to try out his new toy. This goes for hackers and law enforcement personnel alike.

Hans van Staveren, Vrije Universiteit, Amsterdam, Holland

Correcting computer information held on you

Peter Debenham <PPXPMD@ppn1.nott.ac.uk>
26 Mar 93 13:36:39 GMT

Over the past couple of weeks it has been pleasant to see the dangers of faulty information held on computer being acknowledged in Britain. Under the Data Protection Act (1986) in this country a Data Protection Registrar was set up to monitor uses of computers to store personal information and to be an independent source of help to get faulty data corrected.

Recently a television advert has been running showing clips of actors mentioning problems that can happen with computer systems (My building society thinks I died three years ago, According to my bank I have a criminal record etc.) finishing with the address of the Data Protection Registrar and a voice-over saying that if you have problems with faulty information held on you to contact him. People in other countries might like to know that it is possible to for officialdom to acknowledge risks of faulty information.

Peter Debenham, Physics Dept., University of Nottingham, UK. NG7 2RD
+ 602 515151 x8323 (wk) +602 730487 (hm) P_Debenham@ppn1.nott.ac.uk

Re: Conspiracy trial ends in ... acquittal (Bowen, RISKS-14.42)

Anthony Naggs <AMN@vms.brighton.ac.uk>
Thu, 25 Mar 93 23:39 GMT

Drawing on a variety of newspaper and magazine articles I hope I can sketch a slightly wider picture of the case. The best overall article I have seen is in this week's New Scientist, (27 March 1993), which I recommend for further reading.

A little terse I'm afraid, but here is my precis:

On 26 June 1991 British police arrested 3 men who had been cooperating in hacking a number of university, government and commercial computer systems across the world. Individually they used the handles "Gandalf", "Wandaii" and "Lizard", collectively they called themselves the "Eight Legged Groove Machine". They left messages to system managers on some hacked systems signed "8LGM" or "Eight Little Green Men".

They did not meet, or even know each others real names and addresses, until they were introduced by the arresting officers, but discussed hacking, passwords and vulnerable systems on bulletin boards and hacked systems.

Karl Strickland, 22, of Liverpool and Neil Woods, 26, of Oldham in Lancashire were charged with conspiracy to dishonestly obtain telecommunications services, having pleaded guilty they are waiting to be sentenced.

Paul Bedworth, then 18, of Ilkley in West Yorkshire was charged with two counts of conspiracy under the Computer Misuse Act, and one of conspiring to dishonestly obtain telecommunications services.

It is interesting that the Crown Prosecution Service chose to charge Bedworth with conspiracy, rather than a simpler charge of unauthorised access to/modification of a computer system. This decision was the foundation of the acquittal, requiring the prosecution to demonstrate that he had a "guilty mind" at the time of the hacking.

In court Bedworth's solicitor, (lawyer to you US folks), claimed that the case was a show trial, and brought in a psychiatric expert who described Bedworth as having a "nonchemical dependence" on using a computer.

It is hard to see how a compulsion to use computers, or even to hack, can be adequate grounds for acquittal, indeed the judge quite clearly directed the jury to disregard this. Nevertheless the jury returned not guilty verdicts on all charges. It is impossible to know their reasoning, as it is a criminal offence to publish any details of the jurors deliberations.

Much of the press, including the New Scientist article, represent this as setting a legal precedent. Firstly, this doesn't make sense, because nobody can say what the supposed precedent is. Secondly, only the ruling of a judge can do this, (subject to appeal to a higher courts, ..).

In this case we can do little but accept that our jury system has again demonstrated it's unpredictability. Though this is of little consolation to those institutions who suffered expensive tampering with their systems, and had to foot tens of thousands of pounds of phone bills, due to the actions of these men.

Anthony Naggs, Software/Electronics Engineer, (and virus researcher)
Phone: +44 273 589701   Email: amn@vms.brighton.ac.uk

Re: Software Warranties (Robinson, RISKS-14.43)

Geoff Pike <pike@snake.CS.Berkeley.EDU>
Thu, 25 Mar 93 23:21:36 -0800

> ...places that make computer programs are refusing to guarantee {anything}.
>This is as it should be. The risk is not that software might not work; the
>risk is that people blindly assume that it worked, is working, or will work.

A mildly related thought is that the following sort of problem will frequently rear its ugly head in the near future: An engineer (or architect, etc.) screws up and is sued, but the problem is traced back to a faulty piece of third-party software that he or she used. Now the court must try to untangle the liabilities, a process that will require detailed technical knowledge that no judge or jury is likely to have.

Geoff Pike (pike@cs.berkeley.edu)

Akron BBS Sting Update 3 (See RISKS-14.43)

David Lehrer <71756.2116@compuserve.com>
27 Mar 93 11:40:58 EST

The following is an editorial published in the Akron Beacon Journal on Wednesday, March 24, 1993. This editorial is copyrighted by the Akron Beacon Journal, and commercial use or resale of this article is forbidden. Permission to post this editorial in its entirety has been generously granted by Mr. David B. Cooper, Associate Editor.

MUNROE FALLS CARRYOUT
Akron Beacon Journal (AK) - WEDNESDAY March 24, 1993, A14

The Fourth Amendment to the Constitution was written to safeguard ordinary citizens against unreasonable search and seizure. Recently, however, law-enforcement officials have taken to seizing possessions of convicted and suspected criminals, particularly drug dealers.

In the case of 23-year-old Munroe Falls resident Mark Lehrer, police confiscated a sophisticated, $3,000 computer setup, programs and disks on the suspicion that he might be letting kids look at dirty pictures. That charge was never proved. In fact, it appears that police received only one or two complaints about his computer bulletin board, none from area parents. Lehrer contends a clerical error put the pornography into files accessible to all the bulletin board's users, not just adults. Police enlisted a 15-year-old, falsified his identity for a membership and then helped the teen call up a possibly offending program.

But, when the Summit County grand jury refused to indict the University of Akron computer whiz on the original charges, Munroe Falls police filed other charges based on the possibility that some of the programs in Lehrer's private collection contained pictures of minors.

Lehrer did plead guilty to a misdemeanor charge of 'attempted possession of criminal tools' -- his computer -- based on those subsequent charges.

No one downplays the seriousness of crime in our society, whether it's in the suburbs or inner cities. None argue that children should be able to view pornography.

But in the absence of compelling evidence that Lehrer was trying to peddle child porn to kids, either at the outset of this case nine months ago or now, it could appear that the police acted hastily in confiscating the computer. Such actions invite questions as to whether the police were protecting against a child pornographer or using the intimidating powers of the police and judicial system to help themselves to a nice hunk of expensive machinery. dl

Virginia voters & Social Security Numbers

Jeremy Epstein <epstein@trwacs.fp.trw.com>

Thu, 25 Mar 93 10:49:49 EST

In a copyrighted story, the March 24 Washington Post includes an article describing a ruling by the 4th Circuit Court of Appeals that Virginia's law requiring a SSN to register to vote is unconstitutional.

The decision is being hailed by civil rights groups as a victory for the 4 million Virginians who are registered to vote. Because voter roles are public information, registering to vote is equivalent to publishing your SSN. The judges wrote "The harm that can be inflicted from the disclosure of a Social Security Number to an unscrupulous individual is alarming and potentially ruinous.... The statute at issue compels a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy."

A spokesperson for the Virginia Attorney General's office said they have not decided whether to appeal the ruling.

The case was brought by Marc Alan Greidinger, a 29-year-old Fredricksburg lawyer (who represented himself) after he was denied the right to register to vote because he refused to reveal his SSN. Greidinger said that during the lawsuit he gave his SSN who was able to get his current balance on two loans, last payment dates, and university transcripts.

It is not believed that the ruling will affect other state agencies (such as motor vehicles) which require SSNs, because those are not considered public records.

The article mentions help from the Public Citizen Litigation Group (one of the Ralph Nader organizations), and quotes the legal director for the ACLU, which was not involved in the case.

[I guess the "good guys" won one!]

SSN in the news

Chris Phoenix <chrisp@efi.com>
Thu, 25 Mar 93 09:50:54 PST

Our local "News Radio 74" has a feature called "the Osgood File" in which Charles Osgood talks for several minutes. This morning his topic was Social Security numbers. He said a little, but missed some very important points.

He talked about the invasions of privacy that were possible with someone else's SSN, but said only one or two sentences about possible loss of money. He mentioned that cards used to say "Not to be used for ID purposes" and don't say that anymore, but did not talk at all about which uses are actually illegal. He talked about a lawyer in Virginia (?) who sued the election officials because they required his SSN to register to vote and then sold the lists to special interest groups. But he did not say anything about all the other abuses that happen, and especially did not give any advice on how to reduce your risk.

I was disappointed with the report. He could have given some very useful information about our rights and the danger of SSNs, but aside from a closing comment about "Remember, if they've got your Social Security number they've got your number!" there was almost nothing in the report that was actually useful to a listener.

Chris Phoenix chrisp@efi.com 415-286-8581

Court Bans SSN Disclosure

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 26 Mar 1993 17:21:41 EST

PRESS RELEASE, March 26, 1993

"FEDERAL APPEALS COURT UPHOLDS PRIVACY: USE OF SOCIAL SECURITY NUMBER LIMITED
CPSR Expresses Support for Decision"

A federal court of appeals has ruled that Virginia's divulgence of the Social Security numbers of registered voters violates the Constitution. The Court said that Virginia's registration scheme places an "intolerable burden" on the right to vote.

The result comes nearly two years after Marc Greidinger, a resident of Falmouth, Virginia, first tried to register to vote. Mr. Greidinger said that he found it nearly impossible to obtain a driver's license, open accounts with local utilities or even rent a video without encountering demands for his Social Security number.

Mr. Greidinger told the New York Times this week that when the State of Virginia refused to register him as a voter unless he provided his Social Security number he decided to take action. He brought suit against the state, and argued that Virginia should stop publishing the Social Security numbers of voters.

This week a federal appeals court in Richmond, Virginia ruled that the state's practice constituted "a profound invasion of privacy" and emphasized the "egregiousness of the harm" that could result from dissemination of an individual's SSN.

Computer Professionals for Social Responsibility (CPSR), a national membership organization of professionals in the computing field, joined with Mr. Greidinger in the effort to change the Virginia system. CPSR, which had testified before the U.S. Congress and the state legislature in Virginia about growing problems with the misuse of the SSN, provided both technical and legal support to Mr. Greidinger. CPSR also worked with Paul Wolfson of the Public Citizen Litigation Group, who argued the case for Mr. Greidinger.

In an amicus brief filed with the court, CPSR noted the long-standing interest of the computing profession in the design of safe information systems and the particular concerns about the misuse of the SSN. The CPSR brief traced the history of the SSN provisions in the 1974 Privacy Act. The brief also described how the widespread use of SSNs had led to a proliferation of banking and credit crime and how SSNs were used to fraudulently obtain credit records and federal benefits.

CPSR argued that the privacy risk created by Virginia's collection and disclosure of Social Security numbers was unnecessary and that other procedures could address the State's concerns about records management.

This week the court of appeals ruled that the state of Virginia must discontinue the publication of the Social Security numbers of registered voters. The court noted that when Congress passed the Privacy Act of 1974 to restrict the use of the Social Security number, the misuse of the SSN was "one of the most serious manifestations of privacy concerns in the Nation."

The Court then said that since 1974, concerns about SSN confidentiality have "become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits, or Social Security benefits, order new checks at a new address, obtain credit cards, or even obtain the person's paycheck."

The Court said that Virginia's voter registration scheme would "compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote."

The Court held that Virginia must either stop collecting the SSN or stop publicly disclosing it.

Marc Rotenberg, director of the CPSR Washington office said, "We are extremely pleased with the Court's decision. It is a remarkable case, and a real tribute to Marc Greidinger's efforts. Still, there are many concerns remaining about the misuse of the Social Security number. We would like to see public and private organizations find other forms of identification for their computing systems. As the federal court made clear, there are real risks in the misuse of the Social Security number."

Mr. Rotenberg also said that he hoped the White House task force currently studying plans for a national health care claims payment system would develop an identification scheme that did not rely on the Social Security Number. "The privacy concerns with medical records are particularly acute. It would be a serious design error to use the SSN," said Mr. Rotenberg.

Cable News Network (CNN) will run a special segment on the Social Security number and the significance of the Greidinger case on Sunday evening, March 28, 1993. The Court's opinion is available from the CPSR Internet Library via Gopher/ftp/WAIS. The file name is "cpsr/ssn/greidinger_opinion.txt". The CPSR amicus brief is available as "cpsr/ssn/greidinger_brief.txt".

CPSR is a national membership organization, based in Palo Alto, California. CPSR conducts many activities to protect privacy and civil liberties. Membership is open to the public and support is welcome. For more information about CPSR, please contact, CPSR, P.O. Box 717, Palo Alto, CA 94302, call 415/322-3778 or email cpsr@csli.stanford.edu.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 45

Thursday 1 April 1993

Contents

Formation of new society/discussion group

Pete Mellor <pm@cs.city.ac.uk>
Thu, 1 Apr 93 11:10:10 BST

Society for the Promotion of Ergonomically Reasonable Measurement
Peter Mellor, 1st April 1993

This is to announce the formation of the above-named Society.

Aims:

1. To resist the use of meaningless scales of measurement.

2. To improve the friendliness of information systems.

3. To resist imposed uniformity.

4. To counteract official nonsense with unofficial nonsense.

5. To have a good piss-up at least once a year.

6. Err...that's it.

Discussion of Aims:

There is a regrettable tendency today to make everything more friendly to computers, and less friendly to people. Even some recent changes which were intended to make calculations easier for humans have had unfortunate effects.

For example, when measuring the height and weight of people, is it more meaningful to say:

> "Pete Mellor is 1.880 metres tall, and weighs 79.378 kilogrammes stripped."

or:

> "Pete Mellor is 6' 2" tall, tips the scales at 12 and 1/2 stone, and looks quite striking in a pair of tight-fitting flared jeans."?

Supporters of the aims of the Society would all agree that the second of these descriptions is easier to grasp, and conveys far more information that is likely to be of interest than the first.

The Society therefore supports the use of scales of measurement that are scaled to people. So, for instance, the inch (length of top joint of thumb) is more informative than the millimetre when doing anything on a small scale. Going up one level of scale, the foot (distance from big toe to heel) and yard (distance from tip of nose to end of middle finger of outstretched arm) have served architects and furniture makers well for centuries. The metre, by comparison, is too large for small work, and too small for large. Nobody ever uses the decimetre or decametre anyway, so most of the metric system is immediately redundant. Similar remarks apply to grammes and kilogrammes versus ounces and pounds.

The scales of measurement that have evolved with us are the ones that we find most natural to use. This applies even when it comes to measuring new things, like software. The Society therefore promotes the measurement of source code in hands (applied vertically up the side of a pile of print-out, in the same way that the height of a horse is measured).

The Biblically minded may use the cubit for medium-scale measurement, otherwise the use of the rod, pole or perch is recommended.

The system of units that the Society favours will be known as the "ton, furlong, fortnight" system.

Political Allegiance:

In the UK, the society will seek the support of the Rainbow Alliance, and the personal patronage of Screaming Lord Sutch and Cynthia Paine.

In Italy, it is hoped that La Cicciolina will be persuaded to sponsor us.

In other countries, all suggestions welcome.

Diversity:

Any Eurocrap aimed at doing away with our essential differences is deprecated.

For example, in the UK pillar boxes and telephones should be red, in Germany they should be yellow.

The Society believes that books written in Britain should be spelt according to the Oxford Dictionary. Americans who do not wish to follow this standard are encouraged to use Mencken. The Society fully supports the Academie Francaise in its attempt to prevent its fine language from being corrupted by either American or English. In fact, it would like to see the Germans doing more, such as reintroducing Gothic script. The same goes for the Welsh, Irish, Russians, etc.

The intention is to cause a fragmentation of knowledge across language boundaries. Since there is already far too much information around for anyone to use sensibly, this would be entirely beneficial.

Any academic who really wants to know what is going on in artificial intelligence at the University of Beijing should have the dedication to learn Mandarin Chinese!

Membership:

The fee is 17s. 6d. per annum, payable to: "P. Mellor Ethanol Supplies Ltd."

Annual meetings will be held in the King's Head, Upper Street, Islington, London, where beer is still sold at 1 pound 16 shillings per pint.
(Dates to be arranged to suit members.)

Paid-up members may charge for consultations on any matter regarding measurement, provided fees are quoted in the appropriate national currency, e.g., a UK member should quote a consultancy rate in guineas per fortnight.
(Any attempt to quote in ECUs will result in immediate expulsion.)

Other points:

The use of metric sizes of nuts and bolts in the UK should be discontinued
in favour of Whitworth.

Aeroplane prices should be quoted in the currency of the country of origin.
For example, British aeroplanes should be sold at so many pounds sterling per
hundredweight, like everything else of a comparable size.

If this causes a problem in purchasing an A320, it is recommended that the
individual bits be bought independently from the various members of the Airbus
Industrie consortium in the appropriate national currencies and that these are
assembled by the buyer, rather like the purchase of a motorcycle in "kit"
form.

Since the Society opposes the use of acronyms, anything that you might have
thought the initial letters of the Society's name might have spelt is
irrelevant.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: Turn of the century date problems (Ravin, RISKS-14.44)

Steve Peterson <peterson@fs.fs.com>
Mon, 29 Mar 93 18:24:35 CST

In a humorous vein, I've regularly proposed a "programmer's cruise" that would
depart on December 30, 1999. The cruise would be 30 days long and would come
with the following guarantees:

* The ship would be be controlled by mechanical or simple electric
  controls -- no computers in the loop.

* The crew would be tested on their ability to navigate via dead reckoning
  and celestial navigation.

* It's route would avoid going under established routes for airliners and
  would stay out of the normal shipping lanes.

* It would be impossible for anyone on-board to be contacted from the shore.

* Anything else that could be done to avoid date-related failures.

Given the spate of date-related failures, I'm starting to give it serious
consideration.

Steve Peterson, FOURTH SHIFT Corporation, 7900 International Drive,
Bloomington, MN 55425 USA 612 851 1523 peterson@fs.com

Daylight Savings Time hampers police

Debora Weber-Wulff <dww@math.fu-berlin.de>
Wed, 31 Mar 1993 08:55:52 GMT

The "Tagespiegel", a Berlin daily, carried an article on Monday describing the problems encountered switching from Middle European Time to Middle European Summer Time on Sunday. It seems that the Bavarian Police Computer System was caught unawares, and responded by closing down. "Inpol", which stores all information about persons the police are looking for, as well as having connections to the car and stolen car registries and other databases, just stopped.

From 3 a.m. on no checks could be made at the borders or for stopped cars, except for alcohol tests. A dragnet action, scheduled for 4 a.m. was carried out despite the data loss, but only resulted in 16 arrests for DUI. The cause of the error was still being feverishly searched for as the paper went to press. [no update in Tuesday's papers, so they must have found it ;-)]

Debora Weber-Wulff, Professorin fuer Softwaretechnik, Technische Fachhochschule, FB Informatik, Luxemburgerstr. 10, 1000 Berlin 65 GERMANY

Computer does the right thing -- shuttle launch scrubbed

Pete Mellor <pm@cs.city.ac.uk>
Thu, 1 Apr 93 10:05:37 BST

An item on BBC news a few days ago described how the latest shuttle launch was aborted when the control computers closed down the main engines 3 seconds before lift-off.

It was reported that the system had detected a stuck fuel valve.

If so, this appears to be a case of a computer system doing the right thing for once, and probably saving the lives of the astronauts.

Does anyone have any more information on the incident?

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

More on Minnesota Legislature phone fraud

Steve Peterson <peterson@fs.fs.com>
Tue, 30 Mar 93 11:24:27 CST

There was an item a couple issues ago about a phone fraud case in the Minnesota Legislature. Events since then may be of interested to RISKS readers.

As reported previously, the Majority Leader of the Minnesota House of

Representatives (the second most powerful position in the House) hid an $85,000 phone fraud problem for several months.

The fraud occurred because the Majority Leader's son revealed his father's access code to the state phone system to a few of his friends, who then told it to others, and so on. The system was set up to allow users to dial in on an 800 number, enter the code, then dial any number.

Once the fraud was publicly revealed the scandal has grown and the leadership of the DFL (the Minnesota Democratic party) has been working overtime on damage control. Already there are articles in the local press (normally supporters of the DFL) suggesting that they has become "too arrogant" in its power.

Since the discovery of the fraud the following has occurred:

* The Majority Leader was forced to resign from his post.

* There has been an effort by the Democrats to shift the blame to MCI, who is the Legislature's long distance provider. The Republicans, sensing a political opportunity, are battling efforts to shift the blame.

* The House suspended its rules to approve an amendment to Minnesota's Open Meeting act, which restricts what types of public business can be conducted in private. The amendment adds the Legislature to the list of public bodies which are affected by the law, which is a step that many have felt desirable for years.

The case has recently taken a turn into the realm of privacy law. The Ramsey County Attorney (the county in which the state Capitol is located) yesterday issued a grand jury subpoena for the detailed phone records of every member of the House. Many members are opposed to this on the grounds that communications between them and their constituents are privileged. State law is unclear on the issue and it is likely that the subpoena will be challenged in court. Separately, the House Speaker has asked the District Court to rule on whether she can release the records.

In addition to the investigation by the County Attorney, State Attorney General Hubert H. Humphrey III has opened a criminal investigation into the matter.

Steve Peterson, FOURTH SHIFT Corporation, 7900 International Drive,
Bloomington, MN 55425 USA 612 851 1523 peterson@fs.com

Re: Call for the Class of '88 (Ravin, RISKS-14.44)

Jonathan Rice <rice@tamarack.cray.com>
Wed, 31 Mar 93 14:02:13 CST

The local paper had a bit more information. I believe that the database in question was one maintained by the church that Mary Bandar belongs to, in which she is listed by consent. This does not seem to be the usual bugbear of huge and ill-controlled government databases.

More interesting to me from a RISKS perspective is that the clerk who generated the form letters to potential kindergarteners actually *typed* "1988" -- it was the program itself that accepted but discarded the leading digits, without notice. Sorry, no idea what software was in use.

Jonathan C. Rice | rice@zizania.cray.com | ...uunet!cray!rice

Re: Correcting computer information ... (Debenham, RISKS-14.44)

Pete Mellor <pm@cs.city.ac.uk>
Tue, 30 Mar 93 11:27:56 BST

Further to the mailing by Peter Debenham <PPXPMD@ppn1.nott.ac.uk> in RISKS-14.44:

> Recently a television advert has been running showing clips of actors
> mentioning problems that can happen with computer systems ...

It is interesting that the government is embarking on a publicity campaign now. I do not recall a comparable campaign when the act first came into force, though this may be due to erasable memory chips between the ears. DP professionals certainly had it drawn to their attention by poster campaigns and training sessions provided internally by large computer manufacturers, but I don't *think* there were any TV ads.

> Under the Data Protection Act (1986) in this country a Data Protection
> Registrar was set up to monitor uses of computers to store personal
> information and to be an independent source of help to get faulty data
> corrected.

This poses certain risks for computer users. Suppose that I keep the following information on-line for my own reference:

a) Names and addresses of professional contacts.

b) Notes on their research interests.

c) Names and birthdays of members of their families. (It might be good for business if I sent their kids birthday cards! :-)

d) Comments such as: "This guy is an idiot. Don't get into any more projects with him!"

As I understand it, I am not required to register as a data holder if I merely keep type a) data. I am *probably* required to register if I keep b), and more so if I keep type c).

In any case, it is extremely unlikely that I would be prosecuted for failing to register unless I were foolish enough to keep type d) data and also to supply a copy of my file to someone who passed it back to the person about whom I had written nasty comments.

The University keeps computer files with staff and student records. Naturally it is registered and every employee or student has the right to see the information held and demand that it be corrected if it is error. (In fact, hard copies are posted to staff periodically to remind them to update their records, e.g., change of address.)

What about e-mail, though? Suppose I send a piece of vitriolic e-mail about a particular student to another member of staff (not that I would, of course! :-). Am I in breach of the Act by sending the e-mail? Am I in breach of the Act if I keep an on-line copy? Is the recipient in breach by filing an on-line copy, and if the recipient keeps one but I don't, am I still liable? Is the recipient in breach while it resides in the destination mail-box before it is read? Are we both covered by the fact that the University is registered? (In fact I *think* the Act requires registration of particular systems.)

Regardless of whether we should register or not, does every student in the University have the right to read every e-mail memo about them sent between staff if these have been stored on-line? If comments are felt to be unfair, should the student be able to demand that the record of past correspondence be toned down even though the vitriolic original was read and acted upon long ago, or would it suffice simply to print and file a hard copy of the memo and delete it from the on-line file, thereby removing it from the terms of the Act?

I am not thoroughly familiar with the wording of the Act, but I suspect the answers to some of the above questions are far from obvious.

Does anyone know how successful the Act has been in terms of prosecutions for unregistered holding of data or justified demands for corrections? Have any test cases established precedents for the points I have raised?

Perhaps a publicity campaign should be aimed at holders of data who might be unwittingly breaking the law (as was the earlier campaign at the time the Act came into force).

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Re: Dutch hacker in jail for another month (from: Hans van Staveren)

<rmoonen@ihlpl.att.com>
Tue, 30 Mar 93 08:26 GMT

->According to the papers, forged credit cards were found while searching his
->home, and that also will not help his case. He is supposedly unwilling to
->answer any questions at this point, but is charged with crimes that could
->send him to jail for a maximum of four years.

Don't forget that when he was arrested the previous time, he also was unwilling to answer any questions. This gives a good motive for 'nailing' this

guy. The credit cards shouldn't be much of a problem for him, because
possession of them is not as big an offense as actually using them, and that's
hard to prove.

->Although I am definitely not suggesting he is a nice guy, somehow I have some
->difficulty connecting this nervous kid in our room with a sentence of four
->years. I hope that being the first to be caught under the new law, and in the
->act to boot, is not going to give him too much extra attention from law
->officers.

I'm afraid that being the first will only make for a harsh trial, to set an example. It's not only the first time a hacker will go to trial under the new law, it's also the first time one was caught red-handed. A sentence of four years will not only ruin those four years for him, but the rest of his career will also be in severe danger. I hope the judge has done his homework on computers though...

(Trials in the Netherlands do not work with juries, which might be to his advantage, because in this case, the parties involved will at least know what they are talking about...)

--Ralph Moonen

Credit and Avis rent a car re-visited

Boyd Roberts <boyd@prl.dec.com>
Tue, 30 Mar 1993 18:49:43 +0200

On returning from my US vacation yesterday, I found a strange letter asking me to contact my old bank whose accounts I'd closed more than a year and a half ago. On calling the bank today, they tell me that an Avis car rental was billed to my old VISA card I had with then, although I'd charged it to another card when I made the rental. The a/c number they used was the one used on the application form. Must be yet another benefit of having an Avis ``Wizard Card''.

So, this begs the question: Will any random digit sequence work as long as the leading digits point to a real bank? [Not if they do a real-time check. PGN]

This is just another problem caused by renting from Avis. The last time I did it, their data on me was misused and cost me some US$2000 through fraudulent `telephone' transactions of which I've only recoved half of, some 6 months later.
Boyd Roberts boyd@prl.dec.com

Little green sting (saucers, Cooper/Maeda, RISKS-14.44)

Joseph T Chew <jtchew@Csa3.LBL.Gov>
Tue, 30 Mar 93 13:54:21 PST

A reading from RISKS-14.44...

> [I have seen this on several groups. There is a question whether it
> is actually illegal if you are merely listening, as opposed to doing
> something about it. PGN]

Might as well indulge my sense of the obvious by inserting, "...under UK laws." I don't know if they subscribe to the idea, as we do in the US, that most things heard on the air may be listened to and even acted upon with impunity. (Newsies with a police/fire scanner take advantage of this, for instance.) According to my faulty memory of possibly obsolete US broadcast law, *disclosing* the contents of non-broadcast transmissions is the no-no.

--Joe

Re: The FORTRAN-hating gateway

Phil Karn <karn@qualcomm.com>
Tue, 30 Mar 93 14:58:06 -0800

I had a very similar problem last year with the SLIP link to my house. Every time I tried to FTP the individual files making up the infamous PC game Wolfenstein 3D, the transfer hung at the same point in one particular file. A compressed archive of the same files went over fine.

Investigation showed that the offending data sequence was a long string of ascii '+' characters. This is the default "command escape" character on a modem with the Hayes command set. To escape from data mode to command mode, you send '+++' preceded and followed by at least a second of idle time. But I *wasn't* triggering the command escape. The modem stayed in data mode. It just corrupted my packets.

The modems in question were Motorola/Codex 3260 FASTs, which support DTE speeds up to 115.2 kb/s. It seems that at such a high link speed, whatever special processing the modems do on the '+' character (e.g., restarting a timer) takes more than one character time. So if you send too many '+' characters in a row the modem's fifo eventually overflows.

The workaround was to change the command escape character to 128, which effectively disabled the in-band escape feature, and to use DTR to control the modem state. Not only is this completely reliable, it's faster too. And it avoids Hayes' stupid patent on the "+++" sequence, a worthwhile goal in itself.

Phil

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 46

Tuesday 6 April 1993

Contents

Sound of the Fury: Sub-liminal highway monitoring...

Peter Wayner <pcw@access.digex.com>
Mon, 5 Apr 1993 18:00:02 -0400

The April 5th 1993 edition of the Washington Post contains a short item describing how AT&T is modifying some of the technology it developed for submarine warfare to smooth traffic flow on the highways. They are currently testing the system on the New Jersey Turnpike where they've installed "SmartSonic" sensors that ... ``measure the speed of passing vehicles by listening to their individual sounds or `acoustical signatures' just as they have been used to listen to other submarines.''

The RISKS? The system will supposedly control ramp access and offer alternative, less-congested routes. This means we are effectively replacing a low-level system with one that is high-level and if not drive-by-wire, at least navigate-by-wire. I have no ideas whether the highways obey/mimic differential equations that are potentially chaotic, but I hope they will check these things out.

Naturally, the privacy arguments about electronic tollbooths apply to this situation. I can imagine the 21st century crook on the lam (and lambs avoiding the crook): he hacks his carburetor chip to change the distinctive signature of his car. Or better yet, he hacks his DSP-controlled sonic-muffler to change the signature regularly. Gotta love technology... The 21st century is going to be a great one for nerds like us.

[Must be sub-laminal? PGN]

Computer company helps students with fake IDs

<FPHAASE@delphi.com>
05 Apr 1993 20:45:31 -0400 (EDT)

This article appeared in the New Orleans Times Picayune on Thursday, April 2. It in interesting to note that a software company unknowing helped these teenagers in their escapade.

Four 16-year-old students were issued misdemeanor citations by Slidell (a suburb of New Orleans) police for unlawful use of a license. Apparently they had made phony driver licenses using one of the student's father computer and a desk top publisher program. The driver licenses were from the states of Minnesota, Wisconsin and Washington. The 4 students would manufacture these IDs and sell them for $30. The students were all honor students from one of the local high schools.

The police seized a computer disk, a cutting board and a lam

Mangled zip code leads to collection agency

Ken Hoyme <hoyme@src.honeywell.com>
Tue, 6 Apr 93 10:12:18 CDT

Here is a classic example of the screw-ups that can happen when a simple number gets mangled in a computer database.

I am a member of the Columbia House CD Club. The way such clubs work is you get a bunch of (nearly) free CDs at the beginning of your membership, with an obligation to purchase a certain number within a specified time. They reserve the right to bill you for unpurchased CDs if you do not fulfill the obligation.

Last Summer, the US Post Office gave us a new zip code (the population in our community had grown to the point where this was necessary). I sent a change of address form in with the change (55369 -> 55311). After this, their monthly mailings stopped. Last week, I received a letter from a collection agency due to my unfulfilled agreement. The address was so incredibly mangled, I am amazed that the post office was able to route it. The zip code had only one digit right (54762). The city and street names were mangled as well. Apparently their data entry operator damaged the record when entering the change of address.

My guess is that Columbia House attempted to send their bulk-class mailings to this mangled address and never got them routed (or a proper response to the "Address Correction Requested" notation). I don't suppose the Post Office spends a lot of time trying to route misaddressed bulk mail. Rather than trying to send me anything by 1st class mail, they turned it over to a collection agency to make this attempt. Seems pretty inefficient, since the cost of the collection agency has to be more than a 1st class letter.

Finally, I called Columbia House's 1-800 (toll-free) number to clear this up. The operator corrected the address on-line, but made the comment that he had to make sure that the change 'took'. Apparently they have experienced regular problems with entering an address change, only to have the system not actually make the change to the database record. They either have a software or training problem there.

The simple change of two zip code digits led to far more chaos than it should.

Ken Hoyme, Honeywell Systems and Research Center, 3660 Technology Dr.,
Minneapolis, MN 55418 (612)951-7354 hoyme@src.honeywell.com

NREN WRAP [Joe's Final Houston Chronicle NII Story]

Joe Abernathy <Joe.Abernathy@houston.chron.com>
Thu, 1 Apr 93 14:54:12 CST

NREN Wrap -- This is my last story for the Houston Chronicle. It is to appear on April 4, 1993. Please feel free to redistribute it for any non-commercial use.

To those of you who have provided so much help these past four years, thanks. It's been a real education. I've accepted the job of Senior Editor-News at PC World magazine, and I'll still be writing the Village Voice Technocracy column, so I hope you'll all stay in touch. My new contact information is P.O. Box 572390, Houston, Texas 77257-2390, joe@blkbox.com.

By JOE ABERNATHY
Houston Chronicle Staff Writer

The specters of class struggle and international economic warfare are casting a shadow over administration hearings on how to build a sophisticated national computer network. Billed as an engine of job growth, a central concern is emerging that the ``data superhighway'' promised by Vice President Al Gore and President Bill Clinton during the campaign could produce a large underclass of ``information have-nots.''

Based on an emerging global computer network known as the Internet, which links up to 12 million people in more than 30 nations, the National Research and Education Network (NREN) is a decade-long project of former Sen. Gore. Gore envisions a future in which oceans of data, including libraries of movies, books and other creative works, would be readily avail able to every home. In selling a $5 billion spending plan focused on the network in 1992, Gore held forth the image of classrooms without walls, sophisticated medical collaborations, and globally competitive small businesses. ``The NREN is at all odds the most important and lucrative marketplace of the 21st century,'' he said in a recent statement.

But in trying to make it work, it has become apparent that the NREN remains in many ways a captive of its privileged institutional heritage. Some Americans don't even have telephone service, and many still don't have computers with which to access the net.

Two congressional hearings were held in late March concerning the National Information Infrastructure, and a bill has been introduced that would take up where Gore's 1992 High-Performance Computing Act left off _ bringing the net to classrooms, small business and other potentially disenfranchised Americans. Clinton's budget includes an additional $489 million over six years for the network. And while the regional Bells, newspapers and other information giants have been struggling for years over the future of the medium, congressional insiders say that with the in creased attention, a resolution seems likely to be found during the current session of Congress.

``What I think is really getting squeezed out is that there hasn't been a genuine, public interest, bottom-up grass roots voice. It's a huge, huge issue,'' said Marc Rotenberg, director of the Washington offices of Computer Professionals for Social Responsibility, the primary champion of civil rights in the new electronic medium. ``It's about people, it's about institutions, it's about who gets to connect and on what terms.''

Observers also fear that the rush to wield the network as an economic weapon could produce dramatic incursions into free speech and other civil liberties.

``I'm very concerned that the rhetoric about national competitiveness is transforming itself into a new cold war,'' said Gary Chapman, director of CPSR's 21st Century Project in Cambridge, Mass. ``The concerns of intelligence and other federal agencies including NASA has been to look at technology resources that are not related to military security but to economic benefits as being things that have to be protected by Draconian measures of security.''

Recent disciplinary actions at NASA Ames Research Center in Northern California seem to support Chapman's concerns. Up to eight of the 11 scientists disciplined in December were targeted because of their participation in politically oriented, international discussion groups hosted on the Internet computer network, according to documents ob tained by the Houston Chronicle under the Freedom of Information Act, along with subsequent interviews of NASA Ames personnel.

``Some people there were accused of dealing with foreign nationals about non-classified technology issues,'' said Chapman, whose organization also has made inquiries into the matter. ``NASA said the U.S. has to protect its technology assets because of the global environment of competitiveness.''

The issues are even simpler for Raymond Luh, a subcontracting engineer fired by NASA. Luh, an American of Chinese ancestry, feels that his career was destroyed simply because he joined in one of the thousands of political discussions aired each day over the Internet. ``I feel I have been gravely wronged by NASA,'' Luh said. ``I cannot possibly seek employment elsewhere. My reputation as a law- abiding citizen and a hard-working researcher has been tarnished almost beyond repair.'' NASA refused to comment on the matter.

According to FOIA documents provided by NASA's Office of the Inspector General, Luh was fired when ``a document containing Chinese writing was found in (Luh's computer). ... Investigation determined that Luh's office computer held a large volume of files relating to his efforts to promote Most Favored Nation trade status for the People's Republic of China. ... Luh was not authorized to use his computer for this activity.''

To Luh, however, he was only one of the chorus of voices that joined in a fiery debate surrounding fallout from the Tiananmen Square massacre. He wasn't trying to make policy _ he was exercising intellectual freedom, in his spare time.

``That's a very dangerous and disturbing kind of trend,'' said Chapman. ``The parallel is with the Cold War and transforming the modes of thinking and the practices of these agencies into new forms of control, even in the absence of militarily significant enemies. We'll start think ing about the Japanese or whatever Pacific Rim country you want to pick as being `enemies,' and intellectual commerce with these people will be a matter of economic security. ``The freedom of expression aspect of that is very critical. We want to make sure that this is a system in which people can express themselves freely without repercussions.''

Observers fear that Luh may be only the first such casualty as federal agencies and special interest groups reshape the Internet into their own model, carving up a pie estimated to be worth $3.5 trillion.

While Gore's vision implies the construction of a high-speed, high-tech fiber optic network, a number of counter-proposals are being floated.

The Electronic Frontier Foundation -- which earlier made a name for itself with a successful court challenge to the conduct of the Secret Service in a hacker crackdown -- is focusing on building a less powerful, less costly network that could reach more people, more quickly. ``Our central concern is that we get from debate to doing something,'' said Jerry Berman, EFF director.

EFF's approach _ endorsed by Rep. Edward J. Markey, D-Mass. _ is to build an ISDN (Integrated Services Digital Network) service atop the telephone network, making a modest level of digital computer transmission available quickly to every home. The more sophisticated fiber optic approach implied by Gore's NREN could be implemented as time and money allow. But few voices have been heard backing ISDN.

``The current state of the discussion is turmoil and chaos,'' said the CPSR's Rotenberg. ``It's a mistake to place too much emphasis on any technological configuration. A lot of that energy and those resources would be better spent talking about users and institutions rather than technology and standards. This is like trying to explain railroads in the 18th century or cars in the 19th century. Here we are in the 20th century, and we know something big is happening right under our feet and we know it has something to do with these new telecommunications technologies.

``None of us knows where this is going to take us, but I think people should have some sensitivity to the prospect that the future world we're going to live in is going to be shaped in many ways by the decisions we make today about the information infrastructure.''

Danny Dunn, Automatic House, Automatic Electric Post Office

Jerry Bakin <jerry@amex-trs.com>
Fri, 2 Apr 93 13:00:21 MST

Can you see the irony in this situation? Here, the intelhouse usenet list, a group interested in "intelligent" houses, and automated process control cannot even get the net traffic automated and must return to a human tended process! How can we rely on the intelligent houses we build? More like a house of cards....

Jerry Bakin.

> Bone-weary from travel and working 150 hours in two and a half weeks,
> the intelhouse mailing list administration wizard comes back into his
> office, blows the dust off of his aged keyboard, and urges his fingers
> back to their less-exhausted nimble selves. Quickly invoking mail, he soon
> discovers that in his absence wicked site administrators and fools in
> charge of Usenet mail maps have wrecked havoc on his precious mailing
> list. Yes, after all the spells, incantations, and perl scripts, a few
> site administrators had managed to bounce mail in a fashion not only
> non-RFC-compliant, but also so dastardly as to have never before been
> inflicted on his system. If only he hadn't spent the weekends working on
> excising an evil hardware demon from a large justice system computer, and
> his weekdays trying to promote his company's talents to a large maker of
> plastic money, he could have countermanded the errant mail going to
> hundreds of innocent mailing list readers. He could have eliminated the
> terror and confusion and misery needlessly inflicted on those people,
> after all, it was he that the wicked site administrators were after.
>
> Nevermore, he swore. Instead, he would personally see to it that his

> forwarding scripts would not inadvertently pass on these bounce messages
> to innocent bystanders. He lamented that it meant less timely delivery of
> mail, in that he would personally read each item and post only those of
> utility to all readers. Yes, he would become one of those dreaded wizards
> with incredible power at his fingertips. He would become ... a
> MODERATOR!
>
> Yes, readers of this mailing list, mail will cease to flow as quickly as
> it has in the past. It will pass a human's (??) eyes before being sped
> on its way. But for a worthy cause ... truth, justice, and the intelligent
> way!

Teenage Hackers

Jim Haynes <haynes@cats.UCSC.EDU>
Sat, 3 Apr 93 18:37:28 -0800

Saw this in the first quarter 1993 issue of "Miracles in Trust" the newsletter of the Perham Foundation. In a lengthy chronology of West Coast wireless developments there is this item.

July 1911: In Los Angeles, teenaged radio amateur operators, trained at Los Angeles Polytechnic High School, intercept and disclose collusion over the Catalina wireless circuit involving the Hearst newspapers, with much attendant publicity and a criminal prosecution later dismissed. The Wireless Association of Southern California, of over 200 young Los Angeles amateurs, forms as a result of the incident. It operates a 2kW spark transmitter using the call sign ALA.

Re: if they mention flying saucers, they're out to get you

Ian Phillipps <ian@unipalm.co.uk>
Fri, 2 Apr 93 13:50:27 BST

I don't know the name of the law, but in England, yes, it is an offence. There is no assumed right here to listen to anything on the radio waves. So if you realise that what you're listening to is not either a broadcast, licensed amateur or CB operator, you must stop listening.

Not a lawyer etc.etc.etc.

Ian Phillipps, Unipalm Ltd, 216 Science Park,   Phone +44 223 420002
Milton Road, Cambridge, CB4 4WA, England.   Phax +44 223 426868

[Brinton Cooper <abc@BRL.MIL> noted that the UK has a strange concept of civil liberties -- they seem to subordinate them to the needs of the state. Within their system, there may well be no question at all. PGN]

Re: if they mention flying saucers, they're out to get you

Olaf Titz <olaf@bigred.ka.sub.org>
Thu, 1 Apr 1993 23:03:00 +0200

I don't know about Britain, but in Germany it has been in fact illegal to listen, using whichever device, into frequencies not assigned to broadcasting services. This rule was overturned by the German Supreme Court about two years ago.

For every piece of telco equipment that is operated in Germany, a permission has to be obtained (usually by the manufacturer) from a telco authority. This permission could be granted with the provision to obey certain rules, whose violation constituted a criminal offence in itself. (One of the rules on every permission for radio equipment has been not to listen into non-broadcast waves.) The latter rule was turned down for the reason that the telco authority could in effect determine what was illegal and punishable, a power that rests exclusively with the Parliament. But the fact that even a pocket receiver has to be "licenced" remains.

Olaf Titz comp.sc.student karlsruhe germany olaf@bigred.ka.sub.org
uknf@dkauni2.bitnet s_titz@ira.uka.de 49-721-60439

Re: If they mention flying saucers, ... (Maeda, RISKS-14.44)

Robert VanCleef <vancleef@garg.arc.nasa.gov>
Thu, 1 Apr 93 11:11:39 PST

... my brother-in-law is a German airlines pilot. He has often discussed the difference between American and German laws on monitoring the airways. In Germany you must have a license to listen! He discusses their use of tracking vehicles to listen for leakage from illegal receivers and their active pursuit of violations.

Bob Van Cleef vancleef@george.arc.nasa.gov
NASA Ames Research Center (415) 604-4366

Re: The FORTRAN-hating gateway (Karn, RISKS-14.45)

Nick Andrew <nick@kralizec.zeta.org.au>
3 Apr 1993 08:54:58 +1000

I encountered a similar problem whilst attending Uni. New X.25 concentrators had been installed to speed up terminal access to the H*neywell mainframe in the central computer room. Every so often, all terminals would crash. After experiencing it a few times, I realised that they were crashing at a particular point in _my_ session. I was reading one of the online manuals.

I eventually narrowed it down to a simple sequence of 4 lowercase 'n's ... just like nnnn nnnn ... the gateway could NOT send or receive this sequence in a single packet. Unfortunately, nobody told that to the author of the online manual.

The concentrators were eventually replaced with Ungermann-Bass terminal
servers. No further gotchas have been reported.

Nick.

Kralizec Dialup Unix (Public Access), Zeta Microcomputer Software
P.O. Box 177, Riverstone NSW 2765

Hayes Sequence Triggered (FORTRAN-hating gateway, Karn, RISKS-14.45)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Thu, 1 Apr 93 22:32:06 -0500

Sounds more like the the modem was skating the HAYES patent by using the TIES (time-independent escape sequence) promoted by a competitor. This eliminates the "guard time" of 1 second that is an essential part of the patent. TIES proponents state that accidental triggering is statistically unlikely 8*)

Padgett

ps Turning off the "in band" sequence & using DTR I can understand, but
128 (80h) is just as likely as "+" (2Bh) in a binary file unless the
Motorola firmware interprets it as "none".

Re: Correcting computer information ... (Mellor, RISKS-14.45)

Roger D Binns <cs89rdb@brunel.ac.uk>
Tue, 6 Apr 93 18:26:44 +0100

My university department (Brunel - computer science) gets around some problems in what I regard as a devious way. They do not wish for students to see what their exam marks (ie percentages) are (grades are ok). By law, any data holder has 40 days to provide data on request. The department only keeps electronic copies of the records for 40 days, hence preventing any student from seeing them.

Quite what the ethics and reasoning behind all this are, I'll leave to others.

Roger Binns cs89rdb@brunel.ac.uk Brunel University - UK

Re: Dutch hacker in jail for another month

<rmoonen@ihlpl.att.com>
Fri, 2 Apr 93 10:07 GMT

It might be interesting to note that in another article in the 'Volkskrant'
the designer of the new Dutch Computer Crime Law was quoted as saying:

> [The fact that this hacker's custody was prolonged with 30 days]
> requires the judicial order to be severely shocked. Hacking a
> university computer does not fulfill that requirement.

Prof. Dr. H. Franken, who designed the law, also said that the law was not meant to be used against students who where merely playing around with computer systems, but was targeted for organised crime, and big-time fraud. Franken himself is an honorary member of the 'Time-Wasters' a hackers-club based in Eindhoven.

University officials have said that damages to their systems are small, but it is also said that he used their computer so hack other systems. We'll just have to wait and see what happens.....

--Ralph

Internic Registration Services Security Compromised

Mark Boolootian <booloo@framsparc.ocf.llnl.gov>
Fri, 2 Apr 1993 15:53:14 -0800 (PST)

From: Jim Lick <jim@pi-chan.ucsb.edu>
Message-Id: <199304022302.AA13439@pi-chan.ucsb.edu>
Subject: Internic Registration Services Security Compromised
Date: Fri, 2 Apr 1993 15:02:39 -0800 (PST)

INTERNIC REGISTRATION SERVICES SECURITY COMPROMISED

April 2, 1993

In what must be a great embarrassment to NSI officials, security at the Internic host for Registration Services was compromised on the second day of official service to the Internet community. Through a series of accidents, a user of their ftp service was able to access directories normally off-limits to anonymous ftp services.

As a result of this access, the user was able to obtain a copy of the system's /etc/passwd file that could be used to decode passwords of users on the system through the use of a password cracking program. The user was also able to access system logs, including a log of anonymous ftp transactions by users around the world.

In the course of this investigation the user was able to find numerous other security holes including world-mountable filesystems. Although no further action was taken, these holes would enable a malicious hacker to easily penetrate the system.

An Internic admin was in the process of fixing the security holes at the time of this release.

The Internic Registration Services is funded by NSF to administer registration of network numbers, domain names, autonomous system numbers, and other functions crucial to the operation of the global Internet.

Note: This is NOT an April Fool's Joke.

Call for Papers, PSAM II (System-Based Models)

<lavine@aero.org>
Thu, 01 Apr 93 12:21:44 PST

PSAM - II

An International Conference Devoted to the Advancement of
System-Based Methods for the Design and Operation of
Technological Systems and Processes

March 20-24, 1994
San Diego Hilton Beach and Tennis Resort

The purpose of PSAM is to provide a forum for the presentation of scientific papers covering both methodology and applications of system-based approaches to the design and effective, safe operations of technological systems and processes. These include nuclear plants, chemical and petroleum facilities, defense systems, aerospace systems, and the treatment and disposal of hazard wastes. The objective is to share experience to the benefit of all industries. Some of the topics within the scope of the meeting are:

- software dependability
- computerized control systems and operator aids
- automatic fault detection and diagnosis
- AI in support of process safety management

Send four copies of a summary (800-1200 words, single-space) to the Technical Program Chairman, George Apostolakis, by May 13, 1993. Full papers will be October 10, 1993.

Professor George Apostolakis
Mechanical, Aerospace, and Nuclear Engineering Department
38-137 Engineering IV, UCLA
Los Angeles, CA 90024-1597

310-825-1300, 310-206-2302 (fax)

For more information, contact Charlie Lavine, The Aerospace Corporation, lavine@aero.org, 310-336-1595.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 47

Wednesday 7 April 1993

Contents

Another Mystery for the San Francisco Muni Metro

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 6 Apr 93 08:46:58 PDT

Just after 1 p.m. on Sunday afternoon, April 6, a San Francisco Municipal

Railway car (1228) was headed for the car barns when it crashed into the rear of another car (1304) that had stalled in the Twin Peaks Tunnel. 15 people wound up in the hospital. It took all night to clear the wreckage, and full service began again only on Monday morning. The causes of the stall and of the crash were still unknown.

The signal system and the safety controls are as follows:

 * An `automatic' speed-control system has three speeds, 10, 27, and 50 mph.
   [Apparently ZERO is not considered a speed.]

 * A cab-signalling system informs the operator of the maximum permissible
   speed, red for 10, yellow for 27, green for 50.

The controls were thought to be `foolproof', because the car automatically slows or stops if the operator exceeds the maximum indicated speed. There are also impedance bonds in the tracks that are supposed to determine whether the track ahead is clear.

The operator of car 1228 is named Johnny Wong. Three possible scenarios were suggested:

1. Wong or someone else had disconnected the cab-signalling system, which would bypass the speed controls. [This is allegedly not easy to do, and has various voice protocols associated with it.]

2. There might have been a failure of the track-signal system, which would have made car 1304 invisible to the control systems.

3. Human failure was also mentioned, although in the absence of the first two scenarios, that does not seem to make much sense.

[Source: An article by Carl Nolte in the San Francisco Chronicle, 6 Apr 1993, pA1, following up on the previous day's reportage.]

Well, the next day's report begins with this paragraph: The crash

> ``... was the result of the operator deliberately disabling the safety system so that he could speed up his train, sources close to the investigation said''.

The investigation continues. Stay tuned for any further revelations.

[Source: article by Phillip Matier and Andrew Ross, SanFranChron, 7 Apr 1993, p. A1]

> [By the way, the "Another" in the subject line is because I was reminded of the Ghost trains that plagued the Muni Metro repeatedly beginning about ten years ago. PGN]

Columbia and Discovery shuttle problems

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 7 Apr 93 08:57:49 PDT

On 22 March, Columbia's main engines were shut down three seconds before lift-off, because of a leaky valve.

On 5 April, Discovery's launch (STS-56) was aborted eleven seconds before lift-off. Early indications pointed to a valve in the main propulsion system. In this case, the engines had not yet been ignited. (There had been an earlier one-hour delay at nine minutes before launch, due to high winds and a temperature sensor problem.)

[Source: San Francisco Chronicle, 6 Apr 1993, p.A2]

A computer glitch is now being blamed for the 5 April delay. Computer data had indicated that the valve had not closed. ``However, engineers believe that the valve closed properly and a bad circuit might be to blame.`` That is, the computer was in error in reporting the valve status.

[Source: AP item in the San Francisco Chronicle, 7 Apr 1993, p.A3]

Shuttle launch aborted by computer error...

Jim DePorter <jimd@SSD.intel.com>
Wed, 7 Apr 1993 01:38:34 GMT

[...]
The real reason for sending this is that the reporter said "since it is a bug in the computer software it will be easy to fix and the shuttle will be able to launch in the next 24 hours". Seems the expectations of fixing something as 'simple' as software are set way to high. I understand the idea behind the statement: If the problem was in the valve the shuttle could be delayed for more then 24 hours, while all you need to do to fix software is fix the code and reload the 'application' (possibly by floppy disk (-8).

The risk has to do with people having a little knowledge. Not to long ago software was a big and nebulous idea to most reporters. Now everyone has certain ideas about how software actually works, which in most cases is actually wrong (heck I know people who still have trouble understanding the difference between ram space and disk space).

STS-56 abort

Paul Robichaux, NTI Mission SW Dev Div <robichau@lambda.msfc.nasa.gov>
Wed, 7 Apr 93 08:43:58 CDT

<< this was originally posted on sci.space.shuttle by Ken Hollis of the Kennedy Space Center <> [...]

STS-56 abort at T-20 seconds (or thereabouts, maybe 16 seconds per my GLS DD?) was called today because of the GLS (Ground Launch Sequencer). It detected that the MPS (Main Propulsion System) High Point Bleed valve (PV22) closed indicator did not come on as expected.

PV22 is a monostable, normally closed, helium pneumatically actuated valve on a line attached to the LH2 17" manifold. This 17" manifold is the line that goes between the ET (External Tank) and the main engines to supply LH2 to the engines. The high point bleed line is situated in the Orbiter at the "high Point" of that manifold. The LH2 manifold between the ET and the Orbiter looks like an inverted "U". One end of this manifold goes down to the bottom of the LH2 section of the ET (as opposed to the LO2 section at the top of the tank), the other end goes down towards the engines. Since LH2 is very cold, just about any temperature rise will tend to let it gas off. The high point bleed allows any gasses / bi-phase liquid that may accumulate at the top of this U to be siphoned off overboard, where it is sent to the flare stack & burned. It only takes a couple of seconds for this valve to be closed before a gas pocket forms in this section of line, so the valve must be open as close to lighting the engines as possible so that the engines don't ingest a hydrogen bubble. Believe it or not, this still simplifies the operation of the LH2 system with the engines & loading the tank. The lines in the aft for the MPS / SSME system are commonly referred to as "a plumbers nightmare".

During the "terminal count" at about T-20 seconds, the open command is removed. Since this is a "monostable" valve, if there is no helium supply or no power to the solenoid that lets helium to the valve, the valve will close. GLS then verified at about 16 seconds (per my last DD) it is closed and everything is fine. Today the Open indicator went from ON to OFF (indicating it cycled) but the Closed indicator never went from OFF to ON (indicating it did indeed close) thus causing the abort. A downstream temperature transducer went from cold to very warm also indicating that the valve closed, but GLS does not check that temp ducer. A 48 hour scrub-turnaround has been called contingent on relying on the temp ducer rather than the Close indicator. Last I saw the indicator was not still working. It would be easy to say the it is a microswitch failure on the valve, but it could be quite a few things wrong (as always on the Orbiter) and further troubleshooting will have to be performed in the aft to figure out exactly what the problem is.

Any problems after T-31 seconds is an abort for the day. No more holds are available.

Ken Hollis INTERNET: HOLLIS@TITAN.KSC.NASA.GOV SPAN/HEPnet: KSCP00::HOLLIS

``Organized Crime Gets into Phone Fraud''

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 7 Apr 93 8:59:44 PDT

A new survey by John Haugh's Telecommunications Advisors, Inc., claims that technically sophisticated organized-crime rings are annually defrauding U.S. businesses and telephone companies of $4 billion in long-distance calls. 70.3 percent of the almost 700 companies surveyed reported they had been hit by toll fraud at least once in the past five years, with an average loss of $125,000 [inferentially, I conclude, per company rather than per hit]. Haugh predicted that 35,000 companies will be victimized this year. [That multiplies out to $4.375 billion for the year if the past average holds true.] [Source: An article by John Eckhouse, San Francisco Chronicle, 7 Apr 1993, p. D1]

An interesting bug for users of "at"

Dave Parnas <parnas@triose.eng.McMaster.CA>
03 Apr 1993 19:13:18 -0500 (EST)

If you look in the manual for "at" you will see that one of the recommended ways of using it is to have each at job schedule a new one a day or a week or a month later. Some find this easier than editing the /cron file or they may not have authority to do that.

I regularly use this trick to schedule a daily backup of my files onto a tape that I always leave in my tape unit. Last year in April it stopped working. I thought perhaps there had been some kind of outage or bug and simply restarted it.

This year I noticed that when it ran (early this morning) and try to schedule tomorrow morning's backup, at gave the message "too late". I thought it might have been some problem caused by a series of power outages we had yesterday but then I noticed it was also happening on two other machines.

I did some experimenting and found that at would not schedule any jobs from 0200 to 0259. A few hours later I understood.

Tomorrow morning there is no 0202 (the time that schedule my backup) because of the switch to EDT. We will go directly from 0159 to 0300.

I read the manual and there is no indication in the manual that any such check is made. It says you can use any time between 0000 and 2359. This is clearly a case of incomplete documentation.

Is it a case of the author of at being too clever, or me being too stupid?

I think it a nice example of how subtle can be the error that leads to a failure. It never occurred to me that they would be checking for that missing hour. They probably never thought of someone having a regularly scheduled call for 0202.

However, there is something even nicer. If it skips the run in the spring, shouldn't it run it twice in the Fall? I checked my records and it doesn't do that. Even though the clock is going to drop back it schedules the run for the next day. Now, is that a bug? If so whose?

A question of documentation!

Dave

RISKS of Complacency (DOS 6.0)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Thu, 1 Apr 93 21:09:21 -0500

Yesterday I went down to the local Babbages for a copy of DOS 6.0 with expectation of a similar experience as when 5.0 was purchased. Well the box was the same size but that was about it. (What do you expect for US50.00 anyway).

It seems that MS-DOS now comes much like an automobile or cable television: the base price doesn't include the options.

Inside the two-inch-thick box was a slim volume (321 pages vs 668 pages in the DOS 5.0 manual) mostly on the new "features" (as in "that's not a bug, its a feature" 8*) and three high density disks (and a coupon for low density - one of many coupons).

Well, I can say this much, its not really for monochrome laptops, its not really for XTs, the commands are not consistent, and it has its share of bugs, but seems ok otherwise.

Towards the end of the book you find a set of coupons: the first asks you to send in US24.95 + US5.00 for shipping + tax. This gets you the "Microsoft MS-DOS 6.0 Resource Kit" which includes the "MS-DOS 6.0 Technical Reference", and a set of "supplemental disks" which include things like COMP, EDLIN, EXE2BIN, and LCD.CPI which were left out of 6.0 (everyone in Redmond must like to wait on EDIT and has an active matrix laptop in their Porche).

If you are using STACKER, for US5.00 you can get a conversion utility for DBLSPACE & possibly repeat my experience (on my venerable but 100% compatible XT clone, WD controller, & ST-225, attempting to use DBLSPACE resulted in a "Divide Overflow" half-way through the conversion & left the machine unbootable even from floppy - had to reboot with a lesser DOS version and clean off all of the DBLSPACE files to recover - happened more than once so no fluke).

Speaking of DBLSPACE, when formatting a 360k floppy with /S, you now get three hidden files and have only 180k free: seems DOS 6.0 grew a bit and now puts 50+k of hidden DBLSPACE.BIN on the floppies too.

There is an anti-virus tool from Central Point but by now every virus-writer in the world knows how to turn it off with a high function of Int 10, 16, or 21h (haven't tried it but was told by a reputable source). Even so there is yet another coupon at the end of the book requesting another US19.90 for two updates, one "now" (they knew it was obsolete already ?) and one in 3-4 months. Actually cheap compared to the (pounds)29.90 they expect from UK residents (includes VAT).

What really got me is the lack of a simple environmental variable to turn of the color in the utilities for a monochrome display. I told SETUP to use monochrome but this ended when SETUP (which also informed me that an "incompatible disk compression" was present - nope) was done. For EDIT, /B is the switch and /NOHI helps. DEFRAG wants /BW, MSAV allows /BW but

/MONO works better (you can go out for lunch while the memory scan runs
on an XT).

Now there are alternatives to cubic money. You can download the supplemental
file (DOS6SUPP.EXE) from the MS BBS in Washington (206.936.6735), all 480+k
of it & the BBS does support 9600 baud but do not confuse it with v42,
v42bis, or MNP. 33 bad blocks (a record) during the download but my
trusty Supra, 16550 chips, and Procomm+/Zmodem (plugs) handled it ok.

The Anti-Virus update can be downloaded from 503.531.8100 - not on the
coupon but on page 277 - probably Central Point.

In short, the product has the feel of "not ready for prime time" but it
did appear in the first quarter '93 (last day actually - well Egghead
had it the day before).

A final note: I did try to call Microsoft tech support about things
encountered (90 days "free" support is available starting with the first
call). I got through to the lady who took serial numbers (and started the 90
day timer) quickly enough only to be informed after that I was 86th in line &
could expect a 90+ minute wait. Not an 800 call. From Florida to Washington.
No thank you. (At least they told me 8*).
Padgett

Using your company's E-mail for private purposes

Omer Zak <XLACHA1@WEIZMANN.weizmann.ac.il>
Wed, 07 Apr 93 01:40:22 +0300

At present, companies have the right to require their employees to use
company computers, including E-mail access, only for company business.
Employees who participate in the Internet discussion groups may violate
this restriction. Then they incur the risk of harassment if they ever
fall out of favor and/or hold unconventional political beliefs.

The remedy?
Next time you accept a job, negotiate (along with your salary and fringe
benefits) the right to use your company's E-mail also for private purposes,
subject to reasonable limits (which are based ONLY upon quantity of mail
send and received) and the understanding that the time you spend on
private E-mail is your time, not company time.

Companies have the right to control the use of computers which belong to
them. On the other hand, they are required to compensate you for your
work in their behalf (in the form of salary etc.). So considering E-mail
access to be another fringe benefit will solve the problem.
--- Omer

Re: Personal letters

Paul Robinson <tdarcos@mcimail.com>
Wed, 7 Apr 1993 03:03:09 -0400 (EDT)

On < Mon, 29 Mar 1993 13:24:37 (PST) > In Comp Privacy 2-11,
Steven Hodas <hhll@u.washington.edu>

> If I send a personal letter to someone do they have the right to
> disclose it to others without my consent?

No. The Copyright act of 1978 and later amendments gave statutory protection at the federal level for the first time to unpublished works.

> Does this vary state by state?

No. Prior to the 1978 law, an unpublished work was subject to the protection of the common law of the state in question. The new law expressly excludes states from having any jurisdiction over unpublished works and voids any "common law copyright" which might have existed. All works are automatically protected under federal law.

> If it's prohibited, is it a civil or a criminal issue?

Civil.

> If it is permitted doesn't that suggest that we have greater privacy
> protection for electronic communciation because the ECPA would prohibit
> that kind of disclosure?

I think you are confusing things. The ECPA gives to Electronic mail the same protections which are available for telephone conversations - the protection against interception by third parties or the use of intercepted E-Mail by law enforcement personnel without a warrant, i.e. what the laws against wiretapping and recording of telephone calls, the ECPA provides to the same extent to E-Mail.

The ECPA does not apply to the sender or recipient of the message. It only applies to anyone who may see a message prior to its delivery to the designated mailbox or delivery point. It applies to the E-Mail providers who carry the message and to anyone who delivers it.

I am also posting this to the Risks Digest for a reason which has to do with another issue which almost no one has noticed. As of April 1, 1988, the United States became a member of the Berne Union for the Protection of Literary Works. This treaty is most famous as the reason companies would simultaneously publish a book in Canada in order to obtain protection under the Berne Convention.

As of four years ago, that process was no longer necessary because the U.S. is now a member of the Berne Union. The most significant issue under Berne (I refer to this as "It Berne's me up") is that there are no formalities or requirements of notification in order for a work to obtain copyright protection.

What this means is that copyright notices became totally optional after

April 1, 1988 for all works first published on or after that date. In theory, if you obtained a computer program from someone which simply had his name and address on it, and wanted to use it, you would have to find out if the person who wrote it wanted anything to license it. You can be sued, and lose, and the other party can collect damages, even though the work has no indication of copyright notice.

I live just outside of Washington, DC and the Copyright office is just a 20 minute train ride away. A frightening fact is that despite the treaty having been around for more than four years, the Copyright office still does not have copies of the text of the treaty. They have copies of the Phonolog Convention (for protection of sound recordings) and they have copies of the Universal Copyright Convention (which instituted the C in a circle copyright notice.) But Berne is conspicuously absent. It makes me wonder what things are stated in this treaty that are so bad that nobody wants people to know what it says. (The last time I tried to get a copy was about a year ago, but that still was 3 years after implementation and the Copyright Office STILL did not have copies of the text of the treaty. It makes me wonder why.

Just remember this little piece of information. A treaty, once ratified by the Senate, has the force and effect of an amendment to the Constitution of the United States and can override its provisions. Think about that some time.

Paul Robinson -- TDARCOS@MCIMAIL.COM

Re: Hayes Sequence Triggered (Peterson, RISKS-14.46)

Ron "Asbestos" Dippold <rdippold@qualcomm.com>
Tue, 6 Apr 1993 20:43:37 GMT

risks@csl.sri.com writes:
>ps Turning off the "in band" sequence & using DTR I can understand, but
> 128 (80h) is just as likely as "+" (2Bh) in a binary file unless the
> Motorola firmware interprets it as "none".

In general, most modems treat anything above 127 as ignore. Having been bitten by the triple plus sequence even with the Hayes guard time (back when I used rn, for instance, and was '+'ing through articles...) I learned to turn this off very early.

Groupware (non)security query

"Rob Slade, DECrypt Editor, 604-984-4067" <roberts@decus.arc.ab.ca>
6 Apr 93 18:41 -0600

I am looking for experiences, anecdotes and comments relating to security, or the lack thereof, in "groupware" applications and systems. This material will become part of an article to be published later this spring. Any replies that I wish to quote I will contact the author first.

For those replying from the newsgroups, I would appreciate copies to
roberts@decus.ca and rslade@sfu.ca for backup.

Vancouver Institute for Research into User Security   Canada V7K 2G6
ROBERTS@decus.ca Robert_Slade@sfu.ca rslade@cue.bc.ca   p1@CyberStore.ca

Legal Net Monthly Newsletter

Paul Ferguson <fergp@sytex.com>
Wed, 31 Mar 93 16:31:09 EST

Opinion, editorial and news worthy submissions are currently being (sought and) accepted for a new start-up electronic news journal. This monthly compilation will be called 'The Legal Net Monthly Newsletter' and will focus on the legal and ethical aspects of computer networking. Legal Net Monthly will be a non-biased, open forum electronic newsletter keeping in step with the networking environment of the '90's and will be availble by E-Mail subscription.

Legal Net Monthly is aiming to release it's first issue on May 1st, 1993. Articles on the following topics are especially welcome:

- Defining "Criminal Mischief" on the Nets
- Authoring/Distributing Computer Viruses: Legal Implications
- Legislative news around the world

Send all submissions, subscription requests and correspondence to:
fergp@sytex.com

Paul Ferguson, Network Integration Consultant, Centreville, Virginia USA
fergp@sytex.com   sytex.com!fergp   1:109/229 (FidoNet)

*** Injured Using a Computer Pointing Device?: Read This ***

Pete W. Johnson <petej@garnet.berkeley.edu>
5 Apr 1993 06:45:52 GMT

This is a pointer to a basenote and discussion pertaining to computer pointing device injuries (mouse, trackballs, puck, stylus, etc.) in sci.med.occupational. For convenence I have included a copy of the basenote below. To follow net etiquette, please direct all responses to the basenote below in sci.med.occupational notesgroup ONLY.

(Copy of Basenote)

This note (which is being posted monthly) is for anyone that has been injured using a computer pointing device (mouse, trackball, puck, tablet, etc.). I have been assisting computer operators who have been injured using pointing devices for the past 4 years. I am now presently doing research at the

University of California's (San Francisco and Berkeley's) Ergonomics Lab on the design of computer pointing devices with the goal of reducing injuries associated with their use. In order to do this, I need to collect information on pointing device design characteristics (button design, button force, device size, device shape, etc.) that are important in minimizing and/or reducing the physical stresses operators are subjected to. Some of this information will be collected through my laboratory research, but a major and important source of information has to come from operators like yourself. I need to collect all the information I can from computer operators that have been injured as a result of pointing device use.

In order to do this, I need your help. If you have been injured using a pointing device, I would appreciate it if you would send me a note with information pertaining to your injury. I would like the information e-mailed directly to me (petej@garnet.berkeley.edu). The format I would like the information sent to me is as follows, fill in as much as you can:

1) NAME: (optional)
2) COMPANY: (optional)
3) PHONE #: (optional)
4) NUMBER OF HOURS SPENT IN FRONT OF THE COMPUTER PER DAY:
5) PERCENTAGE OF TIME SPENT USING A POINTING DEVICE:
6) MANUFACTURER OF COMPUTER AND MODEL NUMBER:
7) POINTING DEVICE USED AT TIME OF INJURY: (Please be specific)
   a) MANUFACTURER
   b) MODEL OR PART NUMBER
   c) DESCRIPTION OF DEVICE
8) PRIMARY SOFTWARE APPLICATION USED AT THE TIME OF YOUR INJURY
9) TYPE OF INJURY
10) WHAT YOU THINK CAUSED YOUR INJURY
11) IF INJURY IS RESOLVED OR YOUR CONDITIONS HAVE IMPROVED, WHAT CHANGES
    WERE MADE (This is probably the most beneficial information)

My intent is to enter this information into a database in order to gather information and look for trends. Each month I will share relevant information by posting a monthly summary in sci.med.occupational similar to what has been done with keyboard information. If you are presently experiencing problems, feel free to call me (510/231-9405) and I will share with you what I know. I am also open for suggestions, please post responses to this basenote or e-mail me if you have any further suggestions or input.

If your company has internal bulletin boards, please post this note or provide a pointer telling your co-workers about this basenote in the sci.med.occupational newsgroup. I will be also be posting a pointer to this basenote in comp.risks, comp.human-factors, and sci.med as well.

Finally, if you have any opinions or inputs on a particular pointing device or pointing device design in general, send me a note or call me. Our lab is assisting some of the major pointing device manufacturers with the design of their pointing devices. If you have some inputs for a particular company, I will be happy to direct them to the appropriate person.

Thanks for your help.
Peter W. Johnson

(End of Basenote)

FTCS-23 ADVANCE PROGRAM

<kaaniche@tsf.laas.fr>
Wed, 31 Mar 93 19:53:31 +0200

FTCS-23:The 23rd Annual International Symposium on Fault-Tolerant Computing
Diagora, Centre de Congres de Labege, Toulouse, France, June, 22-24, 1993

To receive a hardcopy of FTCS-23 Advance program [or a complete version of the on-line announcement, which was much too large for RISKS], please contact
Mohamed Kaaniche: LAAS-CNRS,7 avenue Colonel Roche, 31077 Toulouse, France
Tel: +(33) 61 33 64 05, Fax: +(33) 61 33 64 11
Email: Mohamed.kaaniche@laas.fr

[The full announcement is also in the CRVAX.SRI.COM RISKS archives CD RISKS: with the file name RISKS-14.FTC . PGN]

FTCS is the world's most important forum for the presentation and discussion of state of the art developments in dependable computing systems. This year's program features 60 regular papers, 5 practical experience reports, 6 software demonstrations and one panel. This program is the result of a very stringent selection process carried out by the international Program Committee on more than 300 submissions. The regular paper sessions cover a breadth of topics from concurrent error detection to software-implemented and application-based fault-tolerance, from theoretical issues in modeling to field measurement of fault- tolerant system dependability, from testing to fault injection. The opening plenary session will be devoted to practical experience reports on two safety-critical, software intensive systems currently in operation: the digital fly-by-wire systems of the Airbus family of airliners, and the speed control system of the Paris subway. The panel will discuss the limits in dependability, and the software demonstrations will encompass tools for hardware and software dependability evaluation.

Exhibitors from both industrial and academic communities will present commercially available products, advanced prototypes and tools relating to the conference theme. An exhitors' forum will offer technical presentations relating to the exhibited products, prototypes and tools.

The symposium participants will be given the opportunity to attend a pre-symposium review of the research conducted at LAAS-CNRS, as well as joining post-symposium technical visits of Aerospatiale, CNES and Matra Marconi Space.

On Monday June 21, a welcome reception will be organized at Hotel Capoul. On Tuesday June 22, the Mayor of Toulouse will give a reception in the famous "Salle des Illustres", followed by a concert at the Jacobins Cloister. On Wednesday June 23, the traditional excursion will be to Albi, home town of the famous painter Toulouse-Lautrec, followed by a banquet.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 48

Wednesday 7 April 1993

Contents

Re: Shuttle Failure Blamed On Computer Glitch (RISKS-14.47)

"Kriss A. Hougland" <hougland@enuxhb.eas.asu.edu>
Wed, 7 Apr 1993 11:35:21 -0700

From all the information on the shuttle delay, the situation seems to be:
A faulty sensor or broken wire that monitors that status of a valve.

So far, I have heard that the problem is still a computer glitch. This is not correct. The software performed as required. The solution to the problem is:

1) find and fix the problem -- I would speculate a very $$$ option

2) update the software to override the situation -- quick and easiy, but very risky if the problem is the valve.

It looks like people are fixing hardware problems in software again. There is a classic risk of overriding hardware problems with software while introducing the ability to do the override correctly, or by a nasty side effect by the program (oops -- I was using that variable to turn on the engines!)

I hope at NASA, they are willing to assume the risk of correcting hardware problems in software. (NASA does have some good brains so I think they are taking a very educated guess from the telemetry.) I would hate to see another shuttle go up in flames (sorry about the pun).

Safety-Critical Software, special issue of IEEE Software

<jck@neptune.cs.virginia.edu>
Wed, 7 Apr 93 16:20:35 EDT

CALL FOR ARTICLES IEEE SOFTWARE
SAFETY-CRITICAL SOFTWARE

A forthcoming special issue of IEEE Software will focus on safety-critical software development. The theme of the special issue is to document recent achievements and current challenges in both research and application of safety-critical software technology. Papers are solicited that report recent research results, both theoretical and experimental. Similarly, papers are solicited that document the best current practices, experience with these practices, and the major outstanding problem that the applications community sees.

Original articles are sought on relevant topics including (but are not limited to):

o Experience in safety-critical applications development in areas such as avionics, nuclear power system, and medical devices.
o Results of experiments in any area related to safety-critical software development.
o Significant challenge areas whose definition and motivation arise from practical experience.
o Development methods, processes, and standards designed for safety-critical software.
o Specification and verification techniques.
o Dependability assessment and modelling.
o Tools and environments supporting safety-critical software development.

Submitted papers must not have been previously published nor be under consideration for publication elsewhere. To be considered for the special issue, please send eight copies of the complete manuscript to either of the guest editors:

John C. Knight	Bev Littlewood
Department of Computer Science	Center for Software Reliability
University of Virginia	The City University
Thornton Hall	Northampton Square
Charlottesville	London, EC1V 0HB
VA 22903, USA	UK
(knight@virginia.edu)	(b.littlewood@city.ac.uk)

Submission deadline is June 15 for IEEE SOFTWARE

London Ambulance Service Inquiry Report (long)

<Brian.Randell@newcastle.ac.uk>

Wed, 24 Mar 1993 12:58:12 GMT

[Brian noted that his reason for sending this to RISKS was that, unlike the previous postings, this one is AUTHORITATIVE. He also wanted to give a clear impression of the scope and level of detail of the computer-related parts of the report, and of how they fitted into the report as a whole. PGN]

I have today managed to obtain a copy of the actual 80-page "Report of the Inquiry into the London Ambulance Service, February 1993".

The terms of reference of the Inquiry were "To examine the operation of the CAD [Computer-Aided Dispatch] system, including:

a) the circumstances surrounding its failures on Monday and Tuesday 26 and 27 November 1992

b) the process of its procurement

and to identify the lessons to be learned for the operation and management of the London ambulance Service against the imperatives of delivering service at the required standard, demonstrating good working relationships and restoring public confidence."

The Inquiry Team membership is listed as

- Don Page, Chief Executive of South Yorkshire Metropolitan Ambulance and Paramedic Service NHS Trust

- Paul Williams, senior computer audit partner of BDO Binder Hamlyn

- Dennis Boyd, former Chief Conciliation Officer of the Advisory Conciliation and arbitration Service (ACAS)

The principal background facts given about the LAS in the report are that the service "covers a geographical area of about 600 square miles. It is the largest ambulance service in the world. It covers a resident population of some 6.8 million, but its daytime population is larger particularly in Central London. LAS carries over 5,000 patients every day. It receives between 2,000 and 2,500 calls daily; this includes between 1,300 and 1,600 999 calls."

The Inquiry's Report carries no copyright notice, and is freely available (see end of this message). Here are the scanned-in Table of Contents, and the complete text of the Sections entitled "COMPUTER AIDED DESPATCH SUMMARY", "COMPUTER AIDED DISPATCH RECOMMENDATIONS", "KEY SYSTEM PROBLEMS", "CAUSES AND EFFECTS OF BREAKDOWN ON 26 AND 27 OCTOBER 1992", and "FAILURE OF THE COMPUTER SYSTEM. 4 NOVEMBER 1992" (The section "CAUSES AND EFFECTS OF BREAKDOWN ON 26 AND 27 OCTOBER 1992" also contains a very detailed and interesting "Cause-Effects" diagram, with about 35 boxes and many directed links, which is not reproduced here.)

Brian Randell, Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923

= =

REPORT OF THE INQUIRY INTO THE LONDON AMBULANCE SERVICE FEBRUARY 1993

CONTENTS
SECTION and Sub-Section

ANNEX A: List of organisations and individuals who gave evidence

ANNEX B: Glossary of abbreviations

COMPUTER AIDED DESPATCH SUMMARY

1001 What is clear from the Inquiry Team's investigations is that neither the Computer Aided Despatch (CAD) system itself, nor its users, were ready for full implementation on 26 October 1992. The CAD software was not complete, not properly tuned, and not fully tested. The resilience of the hardware under a full load had not been tested. The fall back option to the second file server had certainly not been tested. There were outstanding problems with data transmission to and from the mobile data terminals. There was some scepticism over the accuracy record of the Automatic Vehicle Location System (AVLS). Staff, both within Central Ambulance Control (CAC) and ambulance crews, had no confidence in the system and were not all fully trained. The physical changes to the layout of the control room on 26 October 1992 meant that CAC staff were working in unfamiliar positions, without paper backup, and were less able to work with colleagues with whom they had jointly solved problems before. There had been no attempt to foresee fully the effect of inaccurate or incomplete data available to the system (late status reporting/vehicle locations etc.). These imperfections led to an increase in the number of exception messages that would have to be dealt with and which in turn would lead to more call backs and enquiries. In particular the decision on that day to use only the computer generated resource allocations (which were proven to be less than 100% reliable) was a high risk move.

1002 Whilst understanding fully the pressures that the project team were under to achieve a quick and successful implementation it is difficult to understand why the final decision was made, knowing that there were so many potential imperfections in the system.

1003 The development of a strategy for the future of computer aided despatch within the London Ambulance Service (LAS) must involve a full process of consultation between management, staff, trade union representatives and the Service's information technology advisers. It may also be appropriate to establish a wider consultative panel involving experts in CAD from other ambulance services, the police and fire brigade. Consequently the recommendations from the Inquiry Team should be regarded as suggestions and options for the future rather than as definitive recommendations on the way forward. What is certain is that the next CAD system must be made to fit the Service's current or future organisational structure and agreed operational procedures. This was not the case with the current CAD.

COMPUTER AIDED DESPATCH RECOMMENDATIONS

1009 These are the main recommendations drawn by the Inquiry Team from its investigations into the CAD system, each of which is covered fully in the main text. We recommend:

a) that LAS continues to plan the implementation of a CAD system [3009];

b) that the standing financial instructions should be extended to provide more qualitative guidance for future major IT procurements [3032];

c) that any future CAD system must conform to the following imperatives:

i. it must be fully reliable and resilient with fully tested levels of back-up;

ii. it must have total ownership by management and staff, both within CAC and the ambulance crews;

iii. it must be developed and introduced in a timescale which, whilst recognising the need for earliest introduction, must allow fully for consultation, quality assurance, testing, and training;

iv. management and staff must have total, demonstrable, confidence in the reliability of the system;

v. the new system must contribute to improving the level and quality of the provision of ambulance services in the capital;

vi. any new system should be introduced in a stepwise approach, with, where possible, the steps giving maximum benefit being introduced first;

vii. any investment in the current system should be protected and carried forward to the new system only if it results in no compromises to the above objectives [5004];

d) re-training of CAC staff be carried out on the system to ensure that they are familiar with its features and that they are operating the system in a totally consistent way [5025];

e) a suitably qualified and experienced project manager be appointed immediately to coordinate and control the implementation of the proposed first stage of CAD [50271;

f) that a specialist review be undertaken of communications in the light of the final objectives of CAD and that any recommendations arising are actioned as part of the proposed second phase of CAD [5033]; g) the establishment of a Project Subcommittee of the LAS Board [5040]; h) that LAS recruit an IT Director, who will have direct access to the LAS Board [5041].

KEY SYSTEM PROBLEMS

4007 As detailed earlier there were a number of basic flaws in the CAD system and its supporting infrastructure. In summary, the system and its concept has several major problems:

a) a need for near perfect input information in an imperfect world;

b) poor interface between crews, MDTs [Mobile Data Terminals] and the system;

c) unreliability, slowness and operator interface.

Need for near perfect information

4008 The system relied on near perfect information of vehicle location and crew/vehicle status. Without accurate knowledge of vehicle locations and status the system could not allocate the optimum resource to an incident. Although some poor allocations may be attributable to errors in the allocation routine, it is believed that the majority of allocation errors were due to the system not knowing the correct vehicle location or status of vehicles that may have proved more appropriate.

Poor interface between crews, MDTs and the system

4009 Given that the system required almost perfect information on vehicle location and status, each of the component parts of the chain from crews to despatch system must operate well. This was not the case. From our investigations, possible reasons for the despatch system not knowing the correct vehicle location or status of vehicles that may have proved more appropriate:

a) a failure of the system to catch all of the data;

b) a genuine failure of crews to press the correct status button owing to the nature and pressure of certain incidents;

c) poor coverage of the radio system, i.e. black spots;

d) crews failing to press status buttons as they became frustrated with re-transmission problems;

e) a radio communications bottle neck, e.g. when crews commence duty and try to log on via their vehicle's MDT or during other busy periods;

f) missing or swapped callsigns;

g) faults in the "hand shaking" routines between MDTs and the despatch system, eg MDTs showing Green and OK, but system screens showing them in a different status;

h) crews intentionally not pressing the correct status buttons or pressing them in an incorrect order;

i) crews taking a different vehicle to that which they have logged on to, or a different vehicle/crew responding to that allocated by the system;

j) incorrect or missing vehicle locations;

k) too few call takers.

4010 The above reasons are often interconnected.

Unreliability, Slowness and Operator Interface

4011 It is reported that the system "fell over" a few times before 26 October 1992. More common was the frequent "locking up" of screens. Staff had been instructed to re-boot their screens if they locked up. The system also slowed up when under load and whilst it was doing its "house keeping" at 02:00 hours each morning.

4012 General imperfections include:

a) failure to identify all duplicated calls;

b) lack of prioritisation of exception messages;

c) exception messages and awaiting attention queues scrolling off the top of the allocators'/exception rectifiers' screens;

d) software resource allocation errors;

e) general robustness of the system (workstation and MDT "lockups");

f) slow response times for certain screen based activities.

CAUSES AND EFFECTS OF BREAKDOWN ON 26 AND 27 OCTOBER 1992

4016 On 26 and 27 October 1992 the computer system itself did not fail in a technical sense. Response times did on occasions become unacceptable, but overall the system did what it had been designed to do. However, much of the design had fatal flaws that would, and did, cumulatively lead to all of the symptoms of systems failure.

4017 In order to work effectively the system needed near perfect information all of the time. Without this the system could not be expected to propose the optimum resource to be allocated to an incident. There were many imperfections in this information which individually may not be serious, but which cumulatively were to lead to system "failure".

4018 The changes to CAC operation on 26 and 27 October 1992 made it extremely difficult for staff to intervene and correct the system. Consequently, the system rapidly knew the correct location and status of fewer and fewer vehicles. The knock on effects were:

a) poor, duplicated and delayed allocations;

b) a build up of exception messages and the awaiting attention list;

c) a slow up of the system as the messages and lists built up;

d) an increased number of call backs and hence delays in telephone answering.

4019 Each effect quickly reinforced the others leading to severe lengthening of response times. A more detailed explanation follows.

4020 A cause and effect diagram is shown opposite, Diagram 4.5, for the operation of the system on 26 and 27 October 1992. As the number of incidents increases there are several naturally reinforcing loops which escalate the problems. A description of the course of events and interactions follows.

4021 When the system was fully implemented at 07:00 hours 26 October 1992 the system was lightly loaded. Staff and system could cope with the various problems (left hand side of the diagram) which caused the despatch system to have imperfect information on the fleet and its status. As the number of incidents increased, incorrect vehicle location or status information received by the system increased. With the new room configuration and method of operation, allocators were less able to spot and correct errors.

4022 The amount of incorrect location and status information in the system increased with four direct effects:

a) the system made incorrect allocations: multiple vehicles sent to same incident, or not the closest vehicle sent;

b) the system had fewer resources to allocate, increasing the problems of effect a);

c) as previously allocated incidents fed through the system and suffered from the problems on the left hand side of the diagram which resulted in the system not having the resource's correct status, the system placed covered calls that had not gone through the amber, red, green status cycle, back on the attention waiting list;

d) failures because of the problems on the left hand side of the diagram caused the system to generate exception messages.

4023 Starting with effect 4022 d), the number of exception messages increased rapidly to such an extent that staff were unable to clear the queue. As the exception message queue grew the system slowed. The situation was made worse as unrectified exception messages generated more exception messages. With the increasing number of "awaiting attention" and exception messages it became increasingly easy to fail to attend to messages that had scrolled off the top of the screen. Failing to attend to these messages arguably would have been less likely in a "paper-based" environment.

4024 Effects 4022 b) and c). With fewer resources to allocate the system would recommend what it saw as the closest vehicle. This was often an incorrect allocation as a closer vehicle was actually available. It took longer to allocate resources for three reasons:

a) the allocator had to spend more time finding and confirming suitable resources;

b) incidents were held until a suitable resource became available;

c) resource proposal software took longer to process as resources became more distant.

4025 There was a re-enforcing effect in that as allocators tried to contact a resource, that resource was unavailable for allocation to another incident. Once an allocator "clicked onto" a resource its status turned to dark green thus preventing it from being allocated elsewhere. It is reported that one allocator was allocating resources, but not mobilising them. Any delay in allocation or mobilisation was a delay to a patient.

4026 It also took longer to allocate resources as more two line summaries fed through the system. Standard two line summaries of incidents awaiting resource allocation included those that had previously been covered, but were not seen by the system as complete. As this queue built up it caused the system to slow.

4027 At one stage two line summaries were scrolling onto the screen so fast that in trying to stop summaries moving off the screen, allocators were further slowed in their tasks.

4028 In summary, effects 4022 b) and c) contributed to incorrect allocations, a slowing of the system and uncovered incidents all leading to delays to patients. The number of uncovered incidents was probably increased when at one stage the exception report queue was cleared in an effort to increase the speed of the system.

4029 Effect 4022 a), incorrect allocations, led directly to patient delays and crew frustration. Crew frustration was further increased by delays in arriving at the scene and the reaction from the public.

4030 Crew frustration may have been responsible for:

a) increasing the instances when crews didn't press the status buttons in the correct sequence;

b) the allocated crew taking a different vehicle, or a different crew and vehicle responding to the incident.

4031 In the month preceding 26 and 27 October 1992 crew frustration also led to an increase in radio traffic which, owing to the potential for radio bottlenecks, increased the number of failed data mobilisations and voice communication delays. In turn, and completing the loop, failed data mobilisations and voice communications delays lead to further increased voice communications and crew frustration. On 26 October instruction was for minimum voice communication. Statistics show that the number of successful data mobilisations increased. However, with no voice communications, wrong or multiple allocations were not corrected thus negating the beneficial effect of increase data mobilisations.

4032 Turning to telephone communications between the public and CAC, delays to patients and uncovered incidents greatly increased the number of call backs, thus increasing the total number of calls handled. An increased call volume, together with a slow system and too few call takers caused significant delays in telephone answering, thereby further increasing delays to patients.

FAILURE OF THE COMPUTER SYSTEM. 4 NOVEMBER 1992

4033 Following the CAD problems of 26 and 27 October 1992, CAC had reverted to a semi manual method of operation, identical to that which had operated with a variable degree of success before 26 October.

4034 This method of working comprised:

a) calls being taken on the CAD system (including use of gazetteer);

b) incident details being printed out in CAC;

c) optimum vehicle resource identified through contact with nearest station to incident;

d) mobilisation of the resource via CAD, direct to the station printer or to the MDT.

4035 In general CAC staff were comfortable with operating this system as they found the computer based call taking and the gazetteer for the most part reliable. There were known inadequacies with the gazetteer and occasional "lock-up" problems with workstations, but overall the benefits outweighed the disadvantages. The vehicle crews were also more comfortable as the stations still had local flexibility in deciding which resource to allocate to an incident. The radio voice channels were available to help clear up any mobilisation misunderstandings. Largely as a result of the problems of the previous week, additional call taking staff had been allocated to each shift thus reducing significantly the average call waiting time.

4036 This system operated with reasonable success from the afternoon of 27 October 1992 up to the early hours of 4 November.

4037 However, shortly after 2am on 4 November the system slowed significantly and, shortly after this, locked up altogether. Attempts were made to re-boot (switch off and restart workstations) in the manner that CAC staff had previously been instructed by Systems Options to do in these circumstances. This re-booting failed to overcome the problem with the result that calls in the system could not be printed out and mobilisations via CAD from incident summaries could not take place. CAC management and staff, having assured themselves that all calls had been accounted for by listening to the voice tapes, and having taken advice from senior management, reverted fully to a manual, paper-based system with voice or telephone mobilisation. As these problems occurred in the early hours when the system was not stretched the operational disruption was minimised.

4038 SO [Systems Options Ltd.] were called in immediately to investigate
the reasons for the failure. In particular LAS required an explanation as
to why the specified fallback to the standby system had not worked.

4039 The Inquiry Team has concluded that the system crash was caused by a
minor programming error. In carrying out some work on the system some three
weeks previously the SO programmer had inadvertently left in the system a
piece of program code that caused a small amount of memory within the file
server to be used up and not released every time a vehicle mobilisation was
generated by the system. Over a three week period these activities had
gradually used up all available memory thus causing the system to crash.
This programming error should not have occurred and was caused by
carelessness and lack of quality assurance of program code changes. Given
the nature of the fault it is unlikely that it would have been detected
through conventional programmer or user testing.

4040 The failure of the fallback procedures arises as a consequence of what
was believed at the time to be only a temporary addition of printers. The
concept of the system was that it would operate on a totally paperless
basis. Printers were only added, as a short term expedient, in order to
implement at least a partial system at the originally planned
implementation date of 8 January 1992.

4041 The fallback to the second server was never implemented by SO as an
integral part of this level of CAD implementation. It was always specified,
and indeed implemented, as part of the complete paperless system and thus
arguably would have activated had the system actually crashed on 26 and 27
October 1992. However, there is no record of this having been tested and
there can be no doubt that the effects of server failure on the
printer-based system had not been tested. This was a serious oversight on
the part of both LAS IT staff and SO and reflects, at least in part, the
dangers of LAS not having their own network manager.

ISBN 0 905133 70 6

Further copies available from: Communications Directorate, South West Thames
Regional Health Authority, 40 Eastbourne Terrace, London W2 3QR 071-725 2551

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,
NE1 7RU, UK Brian.Randell@newcastle.ac.uk   PHONE = +44 91 222 7923

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 49

Friday 9 April 1993

Contents

Re: Columbia and Discovery shuttle problems (RISKS-14.47)

Dan Sorenson <viking@iastate.edu>
Thu, 8 Apr 1993 03:02:16 GMT

Today, WHO radio in Des Moines, Iowa ran a story on STS-56 in their newscast. The "fix" is to bypass the sensor, fooling the computer into thinking the valve is properly closed. What's the risk? I somehow doubt totally bypassing a sensor can be any safer than fixing the problem, and the cost of delays might be contrasted with the cost of Challenger.

Beware that of quick kludge, particularly when there are lives literally riding on its working correctly.

Dan Sorenson, DoD #1066 z1dan@exnet.iastate.edu viking@iastate.edu

"Massive Tax Fraud found in Toronto" and EFILE security

Peter Yamamoto <pjyamamo@watdragon.uwaterloo.ca>
Thu, 8 Apr 1993 14:21:43 -0400

I just found a bounced risk in an old mailbox. When it bounced expired locally on some machine, I decided not to pursue it; but in light of the recent "Massive Tax Fraud" claims by the Canadian government, I resubmit it with an update.

Update:

In an earlier unposted risk I mentioned:

> I recently went to one of these services and was appalled at the (relative)
> incompetence of the prepaper and the fact that he sends the data to
> Vancouver over an insecure line (I only found out after it was not
> done in the promised time frame and he explained the delays).

Although the risk I cited was security, the incompetence of the preparer made him over-calculate my refund by $1600. I wonder if the recent "Massive Tax Fraud" (headline of the Kitchener-Waterloo Record, Thursday, April 8) reported by the government is partly due to such incompetent preparers.

On the CTV news last night (Wed. April 7, 11pm), they reported that a financial analyst said that the "Massive Tax Fraud" (in the headlines of the Kitchener-Waterloo Record, Thursday, April 8) was more likely a scare tactic by the Canadian Government since the numbers quoted by the government don't add up and the filing deadline April 31 is approaching.

They said most of the blame is on "fraudulent tax preparers" who are trying to taking advantage of the electronic filing system since the return is not accompanied by receipts.

I suppose the specific "risk" is the one the government took by allowing anybody to become an EFILE tax preparer.

Peter

Previous risk submission (bounced):

Subject: Canadian EFILE tax return confidentiality measures (NOT!)
To: comp.risks
Date: Mon, 1 Mar 93 10:57:28 EST

Canada now has a nationwide program to facilitate the electronic submission of tax forms, called the EFILE Electronic Filing program.

>From the Applicant's kit:

What is EFILE -- understanding the service

The service or combination of services that you choose to provide to your clients determines what type of electronic filer you are. There are two basic services, and therefore two types of electronic filers: preparers and transmitters. ...

Communications system ...

Contact, using a modem, with our EFILE receiving system will have to come through a "packet switch" network. You can buy access to this network directly, from either Telecom Canada (DataPac) or Unitel (FasPac). In order to protect the confidentiality of income tax information, minimum security requirements for data sent over one of these packet switch networks are that the data must be transmitted over secure lines (ie a dedicated line together with membership in RCT's closed user group).

In the near future, an alternative will be available whereby encrypted data is transferred without the need for a dedicated line by "dialing-in" to the network. ...

The risk is that the government's "minimum security" policy only covers transmission to the government computer. Before that, there is the freedom for the preparer to transmit the form anywhere by any means.

This in fact happens since a dedicated line represents a significant cost (approx. $300 installation, $250/month) which means that there are "transmitter centers" to which preparers send their data via modem or diskette. Since tax preparers in Ontario are connecting via modem to centers as far away as Vancouver illustrates that such centers facilitate the task of mass interception if one is really intent on doing so. In any case, it should be clear that the current policy does not adequately protect the confidentiality of the information.

I recently went to one of these services and was appalled at the (relative) incompetence of the prepaper and the fact that he sends the data to Vancouver over an insecure line (I only found out after it was not done in the promised time frame and he explained the delays).

The head office is:

Revenue Canada Taxation, EFILE Project Office, 400 Cumberland Street
Ottawa, Ontario, K1A 0L8
613-957-8113 [Canadians may call collect for serious inquiries]

Video Surveillance Tapes and TV Programs

Sanford Sherizen <0003965782@mcimail.com>
Thu, 8 Apr 93 17:53 GMT

I was recently contacted by someone from Dick Clark Productions, asking me to help them develop an NBC TV special called CAUGHT IN THE ACT. This will be a one-hour special in May featuring real-life videotapes of criminals from surveillance (security) cameras, covert camera installations, and in-car cameras.

The producers contacted me to see if I had any tapes or could help them to locate some. They said that they are looking for solid, dramatic footage--and are especially interested in "dramatic incidents, unsolved crimes, and bungling crooks".

Here is the RISK issue. "We are looking for interesting footage, especially that which will help educate the public about the necessity for video surveillance, and to illustrate how effective cameras can be in preventing and solving crimes."

Recently, there has been a flood of cheap-to-produce programs, where viewers contribute their (sometimes staged only for tv) videos. Many of these programs contain shocking sequences, guaranteed to attract a wide consumer audience. Some social scientists and other killjoys have suggested that these programs add to a sense of doom and danger that is found today, especially among those who gain their newscoverage or sense of the world mainly from tv. While at least one of these programs has led to the capture of wanted criminals, the heightened view of continual violence and the ineffectiveness of law enforcement adds to social tension without resolution, except for more use of surveillance.

Thank you, Dick Clark, but I would rather not have you educate the public about the necessity for video surveillance. That necessity is filled with danger for us all. And it is not even so certain how effective cameras have really been in preventing and solving crimes, with certain well known exceptions.

I'll not be watching the program when it airs. In the meanwhile, I hope readers of RISKS and others interested in contributing to more quality tv and curbing this attempt to glorify surveillance will contact Dick Clark Productions and NBC to let them know that we are being entertained to death.

Sanford Sherizen, Data Security Systems, Natick, Mass.

Re: Using your company's E-mail for private ... (Zak, RISKS-14.47)

Pat Place <prp@sei.cmu.edu>
Wed Apr 07 13:45:14 1993

<XLACHA1@WEIZMANN.weizmann.ac.il> states that companies have the right to control the use of their computers and can therefore limit private use for, say, E-mail. The solution is to consider E-mail access as a fringe benefit. But aren't benefits taxable, so how much should I declare to the IRS for the

437 bytes of this message? I have only counted the text and none of the header information. Pat Place prp@sei.cmu.edu

Re: Sound of the Fury: Sub-liminal highway monitoring...

rob horn <horn%temerity@leia.polaroid.com>
07 Apr 1993 15:20:54 -0400 (EDT)

I have worked with traffic flow equations. The ones I dealt with were subject to shock waves and had some very stiff regions. In fact they are very similar to adiabatic supersonic fluid flow. I suppose one could argue that this is chaotic in the sense that I read into this comment. But they did not have strange attractors.

Rob Horn   horn@temerity.polaroid.com

Lessons from the London Ambulance Service

<WHMurray@DOCKMASTER.NCSC.MIL>
Thu, 8 Apr 93 19:53 EDT

The following line from the report on the London Ambulance Service reminded me of some early experience.

>The resilience of the hardware under a full load had not been tested.

In the late sixties I worked on IBM's "Advanced Administrative System." This was a very large system for its day. It was expected to have 5000 users and, at its peak, 300 developers. The system was very successful and we learned a great deal.

The success of the system was due in large part to the experience of its management. Some of the management team had worked on the American Airlines Sabre System. Their experience was reflected in part by a collection of system lore, stories that were told and retold.

One of the stories was about the behavior of systems under load. It recounted the conversion of the New York Reservation Center of AA to Sabre. The conversion had gone very well. The NY center was the last of many to be converted and no problems were expected.

However, the NY center was also the biggest and represented the largest load. After it was converted, response time, which had been relatively short, flat, and stable, suddenly went up dramatically until the system essentially stopped. There was no plan to back off the load, i.e., de-convert from Sabre back to the manual system. It took three weeks to get the system back on line.

While response time had not appeared to be sensitive to load, at some critical point the system began to spend so much time managing its queues that it did not have time to take anything off of them. The queues grew until the system fell over.

The story may well be apocryphal but the lesson was valid and important and our management was very sensitive to it.

William Hugh Murray, Information System Security, 49 Locust Avenue, Suite 104
New Canaan, CT 06840 1-0-ATT-0-700-WMURRAY   WHMurray at DOCKMASTER.NCSC.MIL

Re: Another Mystery for the San Francisco Muni Metro

Joe Brennan <brennan@cunixf.cc.columbia.edu>
Thu, 8 Apr 93 12:24:47 EDT

> * An `automatic' speed-control system has three speeds, 10, 27, and 50 mph.
>   [Apparently ZERO is not considered a speed.]

These three speeds are recognizable to railfans as the typical of a DC-motor system. The speeds are approximate. The speed is determined simply by the current running through the motors, which is controlled by passing the current through resistors and by feeding the current through pairs of motors in series or parallel. 50 would be full parallel, 27 (about half speed) full series. Those are the only two running speeds, and intermediate speeds are accomplished mainly by coasting, as powered running at intermediate speeds would heat up the resistors, which are meant to be used just to reach a running speed.

The 10 mph speed calls for further explanation. Apparently the system uses "permissive" signalling, meaning the driver does not have to stop at red. Bear in mind that the Muni cars run in streets "by sight" where the drivers have to be trusted to run at a speed appropriate to conditions and not other hit Muni cars or automobiles on the tracks. Because of the limited sight distance in the subway, they're not given free rein as they are in the street, but are held to 10 mph or less. Running at 10 would of course require using the resistors, so what is really done is to apply power briefly and then coast. This should work if the drivers can be trusted. If the drivers cannot be trusted, they shouldn't be allowed in the street either.

> The controls were thought to be `foolproof', because the car
> automatically slows or stops if the operator exceeds the maximum
> indicated speed. There are also impedance bonds in the tracks that
> are supposed to determine whether the track ahead is clear.

The signal system must include timers to detect speed, and some kind of feedback device that controls the car. The simplest, old-fashioned device is a trip, a little arm that rises from track level and hits a "trip cock" hanging from the train, and applies the emergency brake. Since this says "slows or stops" I take it something a little more electronic must be used.

Likewise the signal system detects presence of a car in a section of track, that is, what's known as block signals. I believe this is also

is a permissive system, where cars are allowed to approach right up to
each other as long as they run dead slow, the 10 mph limit. ("Heavy"
subways and mainline railroads would typically have absolute block,
where a second train is not allowed at all in the same block.)

> ``... was the result of the operator deliberately disabling the
> safety system so that he could speed up his train, sources close to the
> investigation said''.

This is extremely bad, not only that the operator did it, but that he
-could- do it. I doubt he has the same car every day, so he had to be
able to prepare this fairly quickly. I wonder whether disabling it
is meant to be done en route under some conditions? --probably not.
If even one signal failed, for example, it would be safer to make
everyone pass it at 10 than at any higher speed.

Joe Brennan Columbia University in the City of New York
brennan@columbia.edu ("affiliation shown for identification only")

Review of "Syslaw" by Rose/Wallace

"Rob Slade, DECrypt Editor, 604-984-4067" <roberts@decus.arc.ab.ca>
7 Apr 93 17:35 -0600

BKSYSLAW.RVW 930402

PC Information Group, Inc.,. 1126 East Broadway, Winona, MN 55987
Syslaw, 2nd ed., Lance Rose and Jonathan Wallace, 1992

The introduction to "Syslaw" states that although the title implies the existence of a new kind of law relating to electronic bulletin board systems, in reality it is simply and extension of existing laws, mores and practices. In the same way, although the book states itself to be aimed at the BBS community, and particularly sysops, there is much here of interest and moment to anyone involved with sharing information through computer systems.

The book also starts with a "disclaimer": the authors suggest that any significant concerns with legal affairs be taken to a lawyer. Parts of the book may give concern to experts in the specific fields: I was disappointed by the coverage of viral programs (and rather intrigued by a somewhat idiosyncratic definition of "worm"). That aside, the book is an excellent overview of the legal situation and considerations with regard to computer communications systems.

Chapter one is entitled "Your rights as a sysop", although "First Amendment" (the first amendment to the American constitution deals with "free speech") arguments seem to comprise the bulk of it. Chapter two discusses contracts, and the advisability to have a formal contract so that there is an express understanding between caller and sysop. Chapter three deals with copyright and other "intellectual property" issues. Chapter four deals with "injurious materials": it is somewhat surprising that it is not more closely related with chapters eight ("Viruses and other dangerous code") and nine ("Sexually explicit material). chapters five, six and seven deal with privacy, crime directly related to BBS operation and search and seizure, respectively. All of them rely quite heavily on examination of the existing American statutes.

A number of appendices are included. B through H are copies of various related American legislation: I is a list of various state computer crime laws (although the table of contents makes reference to "Sexual Exploitation of Children"). Appendix J is an annotated bibliography of sources for further study. Interestingly, for a book supposedly targeted at BBS sysops, none of the materials are cited in "online" form.

Appendix A, however, is probably of greatest interest: it is a sample "caller contract"; an agreement between the "users" and "owners" of computer systems. Written in a "folksy" style, and intended as a understanding between sysops and their "members", it is still a valuable template for any organization with online information systems and general "communications" functions such as email (and, these days, voice mail).

A recommendation that I would make to the authors for the third edition is to make the book less "American". On the face of it, this might seem like a strange request. Laws vary from country to country, and it is impossible to write a book covering all possible laws. However, there are many legal precepts which are common to almost all legal systems. Chapter two of "Syslaw", for example, deals with contracts. It does so in a very general way, applicable to almost all situations. Chapter one, on the other hand, deals with the "First Amendment" to the American Constitution, and is therefore of little use to anyone in any other country. Chapter three falls into the range between: it deals with copyright and other related concepts, but from an American perspective and with specific and extensive reference to American laws. Most of the book falls somewhere into the middle ranges.

Most systems managers and computer operators tend to see "systems law" primarily in relation to "pirate software". Syslaw is a valuable guide in opening discussions of many related topics which are all too often either neglected, or pass over as being of little importance.

copyright Robert M. Slade, 1993 BKSYSLAW.RVW 930402

Availability of Berne Convention (was Re: Personal letters)

"Selden E. Ball, Jr." <SEB@LNS62.TN.CORNELL.EDU>
Wed, 7 Apr 1993 13:54 EST

I don't know why they don't have a copy of the U.S. treaty agreeing to abide by the Berne Convention. The Convention itself is a bit more than 4 years old, though :-). Perhaps you've been looking in the wrong place?

At any rate, as a member of the information elite, the text of the Berne Convention is readily available to you.

The following was clipped from a file available from the gopher server run by Cornell's Law School (fatty.law.cornell.edu). It is one of the historical documents provided to them by the Fletcher School of Law and Diplomacy, Tufts University.

I assume that the first line refers to a UN publication series. You might want to check to see if the Copyright Office carries that. Presumably the Library of Congress does.

For further information, contact:

Peter H. Stott, Fletcher School of Law and Diplomacy/
Urban and Environmental Policy, Tufts University
97 Talbot Avenue Medford MA 02155

pstott@pearl.tufts.edu pstott@igc.apc.org

I hope this helps.

Selden Ball
seb@lns61.tn.cornell.edu

- -

U.N.T.S. No. 11850, vol. 828, pp. 221-293

BERNE CONVENTION
FOR THE PROTECTION OF LITERARY AND ARTISTIC WORKS
OF SEPTEMBER 9, 1886,

COMPLETED AT PARIS ON MAY 4, 1896, REVISED AT BERLIN ON NOVEMBER 13, 1908,
COMPLETED AT BERNE ON MARCH 20, 1914, REVISED AT ROME ON JUNE 2, 1928,
REVISED AT BRUSSELS ON JUNE 26, 1948,
AND REVISED AT STOCKHOLM ON JULY 14, 1967; and

PROTOCOL REGARDING DEVELOPING COUNTRIES

[remainder of document omitted ;-)]

Re: Berne Convention (Robinson, RISKS-14.47)

Mike Godwin <mnemonic@eff.org>
Wed, 7 Apr 1993 19:41:35 GMT

Paul Robinson writes:

>On < Mon, 29 Mar 1993 13:24:37 (PST) > In Comp Privacy 2-11,
>Steven Hodas <hhll@u.washington.edu>
>
<> If I send a personal letter to someone do they have the right to
<> disclose it to others without my consent?
>
>No. The Copyright act of 1978 and later amendments gave statutory

>protection at the federal level for the first time to unpublished works.

To a lawyer like me, this doesn't sound right. True, copyright protection extends to unpublished works, and, since the U.S. became signatory to the Berne Convention, to unregistered unpublished works.

But this has not yet been interpreted to mean that the recipient of a letter cannot *disclose* it without the author's permission--only that the recipient cannot *publish* it. Now, in this medium the distinction between between disclosure and publication is a lot muddier than it is elsewhere, but it seems likely to me that the mere disclosure of e-mail by a recipient is not going to lead to copyright-infringement case unless the recipient takes money for disclosing it. The normal measure of damages in a copyright action is based on the amount of lost profits to the author and/or the amount of profits earned by the publisher. Statutory damages require that the author register the letter with the Copyright Office.

If someone sent me flaming e-mail, and I felt like reposting it to the Net, I certainly wouldn't hesitate for fear of an infringement lawsuit.

(I'd hesitate because I think it's bad manners, but that's about it.)

<> If it is permitted doesn't that suggest that we have greater privacy
<> protection for electronic communication because the ECPA would prohibit
<> that kind of disclosure?
>
>I think you are confusing things. The ECPA gives to Electronic mail the
>same protections which are available for telephone conversations - the
>protection against interception by third parties or the use of intercepted
>E-Mail by law enforcement personnel without a warrant, i.e. what the laws
>against wiretapping and recording of telephone calls, the ECPA provides to
>the same extent to E-Mail.

ECPA explicitly does not prohibit recipients from disclosing the contents of their communications.

Sadly, ECPA also does not provide any protection against "the use of intercepted E-Mail by law enforcement personnel without a warrant." An attempt to exclude illegally seized e-mail would have to be based solely on the Fourth Amendment (a slim reed, IMHO).

>... there are no formalities or requirements of notification in order for
>a work to obtain copyright protection.

Not quite true. As I understand the current Copyright Act, statutory damages, for example, still require registration of copyright.

Mike Godwin, EFF, Cambridge mnemonic@eff.org (617) 576-4510

Berne convention (Robinson, RISKS-14.47)

Jerry Leichter <leichter@lrw.com>

Wed, 7 Apr 93 16:26:08 EDT

[Paul's message] is a mix of truth and irrelevancies. I checked with a friend who is an intellectual properly lawyer, and he looked in one of the standard books on copyright protection (Zimmer). However, the following is MY GLOSS on rather complex (and not completely settled) area of law.

It is true that under the Berne convention copyright notices are optional. This is not a big a change as you might think: Under common-law copyright, they were always optional *until publication*. If someone stole an unpublished work - say, a program sitting in someone's account - and posted it on a bulletin board, copyright protection would still apply, and the original author could come after, not just the person who stole the work, but any party who made a copy from the bulletin board.

There would be a difference in what the copyright owner could come after the various parties *for*, however. He could go for major damages against the thief, but someone who copied the program off the bulletin board could claim that they were an innocent infringer who had no way of knowing the material was protected by copyright. If successful in that claim, about all that could happen would be that the innocent infringer would be required to return or destroy all copies of the material.

Berne changed nothing in this scenario, EXCEPT that the same rights now apply even if the ORIGINAL AUTHOR published the material without a copyright notice. The "innocent infringer" defense is still available. Under Berne, the main effect of INCLUDING a copyright notice - and the authorities on the subject strong recommend that you do - is that it absolutely blocks any attempt at an "innocent infringer" defense. (Of course, if a thief removed the copyright notice and passed the material on to someone who had no reason to suspect that the copyright was claimed on the material, that's another story - just as someone who buys a car from a used car dealer cannot be charged with theft (or even, generally, made to return the car) if it turns out to have been stolen. Buy the same car from some guy in the street who claims to have "lost" the paperwork and you will be treated very differently.)

Mr. Robinson's mention of "licensing" is irrelevant. There is no such thing as licensing in copyright law, which has to do with copying. It is pretty well established that RUNNING a program does not constitute copying it, any more than reading a book constitutes copying it into your brain cells. (There were attempts early on to claim that running a program was like performing a piece of music, but that theory didn't make much sense and went nowhere. If it had, you would have had to receive a "right to copy" of some bizarre limited sort every time you bought a program. The closest analogy now made is that running a program is like playing a recording - permission of the copyright owner is needed to MAKE the recording, but anyone can PLAY the recording as many times as they like, at least for themselves.)

As for the damages, if you are an innocent infringer, you are not liable for any. Of course, you'd better be damn sure of your "innocent infringer" status. If you got the program off a pirate bulletin board that specializes in stolen software, you could be in trouble, copyright notice or no.

Stepping back a bit to look at the ethical issues, I find Mr. Robinson's whole approach most disturbing. I was brought up under the injunction that one should not use someone else's property without permission. If I don't have good reason to believe something is in the public domain, I won't use it without permission. It doesn't matter if the author has gone to the trouble of attaching a legal copyright notice: *The stuff isn't mine.*

The law generally takes as its basis this same moral stand. I don't need to put a sign a my car to tell others that I claim it as mine. Even if I leave it running, with the keys in it, you have no right to use it. If you want to use it, ask me.

For whatever historical reasons in the United States, copyright law has required notice. Trespassing requires notice, too, but that's because in unmarked countryside it's difficult for anyone to know where the boundaries are: If you want to keep people off your land, you have to make it clear where your land starts. You don't need to put a "No trespassing" sign on your front door to tell people to stay out of your house. The Berne convention simply recognizes that it's simple to tell when you are using someone else's words, music - or computer program. There's no ambiguity about it. So why should advance notice be required?

If you want to use the fruit of someone else's work, simple morality says you should get permission - whether blanket permission in the form of a release to the public domain on the work itself, or specific, personal permission. If that inconveniences you, well, just what makes YOUR time and effort so damned important when SOMEONE ELSE did the work?

-- Jerry

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 50

Wednesday 14 April 1993

Contents

Head-on train collision in Berlin

Debora Weber-Wulff <dww@math.fu-berlin.de>
Sat, 10 Apr 1993 08:06:08 GMT

At 14:23 on Good Friday an Intercity train leaving Berlin collided head on with a train approaching Berlin just outside the city limits near Wannsee. This is a portion of track that is being electrified "under pressure", as the German Bundesbahn wants to run its ICE trains on the line from May 23. During the week only one track is used so that workers can work on the other track.

On weekends and holidays both tracks are available. The approaching train was a "special train" that is added to the timetable for holidays to cope with the traffic.

The trains were only going at 30 kmh because of the construction, and at least one of the engineers saw the collision coming: he pulled the brake and jumped the train, his co-engineer ran towards the back of the train and was severely injured. Both engineers in the other train and a passenger were killed, over 20 were wounded, 7 remain in the hospital this morning.

There was much finger-pointing at first: both trains appeared to have proper signals, as they were assumed to be on different tracks; the "Stellwerk" (is that the switch controller?) was said to have been misoperated; each train company (Wannsee is on the border between the DR and the DB train authority: after 3 1/2 years of reunification they still haven't got the trains sorted out) accused the other; workers were said to have inadvertently capped an important cable. A blanket of silence has been imposed, the officials will neither confirm nor deny anything at the moment.

Debora Weber-Wulff, Professorin fuer Softwaretechnik, Technische
Fachhochschule Berlin, FB Informatik, Luxemburgerstr. 10, 1000 Berlin 65

Follow-up on Berlin Train Crash

Debora Weber-Wulff <dww@math.fu-berlin.de>
Wed, 14 Apr 1993 07:38:37 GMT

The preliminary results of the train crash in Berlin on Good Friday were published in the "Tagespiegel" this morning.

It seems that the computerized signals worked perfectly: the "Fahrdienstleiter", the person in charge of setting the switches and the overseeing the signals set the switch wrong - to one-way traffic (workday) instead of two-way traffic (holiday). The computer reacted by setting the outbound signal correctly to "halt". The overseer believed that this was a defect in the system, and overrode the signal by setting the temporary extra signal (which is just for when the track is under construction) to "proceed" without telephoning anyone to investigate the supposed signal error. The overseer overlooked [PGN would say: oversaw] the fact that a non-regularly scheduled train was approaching the switch, he believed that the track was free.

The risks question: How easy should it be for a person to override such a system? Or is this just a question of human error, to be accepted as "Schicksal", fate?

Debora Weber-Wulff, Professorin fuer Softwaretechnik, Technische
Fachhochschule Berlin, FB Informatik, Luxemburgerstr. 10, 1000 Berlin 65

Discovery discovery of ozone data

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 10 Apr 93 11:05:35 PDT

The current Discovery mission is monitoring ozone and several dozen other atmospheric gases. However, the on-board recorder does not have enough storage for the full mission's data, and the data is supposed to be transmitted back to earth. Unfortunately, there is a high-rate data channel problem on the shuttle antenna that is blocking transmission; NASA has been unable to overcome that problem thus far. [Source: San Francisco Chronicle, 10 Apr 1993, A5]

``Navy Calls Satellite a Total Loss''

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 10 Apr 93 11:10:40 PDT

A Navy communications satellite launched via an Atlas rocket on 25 Mar 1993 was placed in an unusable orbit that was at one end thousands of miles too low. The Navy declared the mission a total failure on 9 Apr 1993. [Source: San Francisco Chronicle, 10 Apr 1993, A5]

Police data misused to find home address

Arthur R. McGee <amcgee@netcom.com>
Sun, 11 Apr 93 06:01:29 -0700

[Abstracted by PGN from a UPI item forwarded by ARM from clarinews@clarinet.com, datelined Anaheim, California]

An unidentified employee of the Anaheim Police Department apparently misused his access to the DMV computer system to obtain the home address of a man who had been targeted by anti-abortionists. This led to Chris Criner's house in Tustin CA being picketed in February 1993.

> ``It taught me I can't trust anyone,'' Criner said. ``When you find out the perpetrators of harassment were helped by the Anaheim Police Department, you wonder where does it stop.''

Under state law, unauthorized disclosure of DMV records is a misdemeanor with penalties up to one year in jail plus a fine of $5,000.

36,000 dollar bug!

John Pettitt <jpettitt@well.sf.ca.us>
Tue, 13 Apr 93 20:53:19 PDT

It's that time of year, and I have just got my tax return back from the accountant. During 1992 I had to pay estimated tax on a capital gain from selling stock. The program my accountant used to calculate the amount had TWO major bugs.

Firstly, it did not deduct the amount of state tax I was estimating I should pay before estimating the federal. Secondly, it ignored a foreign tax credit when calculating alternative minimum tax. The net result of this was a $36.8K overpayment! This was a well known PC-based commercial package used by many accountants across the country.

Luckily for me, they changed the program before running the 1992 return and found the mistake -- so I am out some $700 in interest for the period.

However it brings home that the tax code is now so complex that in many cases advisors treat the output of their programs as beyond question. Had the error been the other way and not been found, the consequences in penalties, etc., could have been very worrying.

[For the non-US reader, the US tax code is a gothic monstrosity that nobody would believe if they had not seen it. Being English, I thought the Inland Revenue was bad, but the US system is mind boggling in it's complexity and stupidity.]

[For the tax-minded, I had a very complex foreign source and foreign capital gain transaction with UK tax credits, the total returns (Fed and California) are over half an inch thick.]

John Pettitt

[See a previous item by Edgar Knapp in RISKS-13.42, discussing a nasty bug in MacInTax. John's could have been the SAME PROBLEM! PGN]

hardware GOOD, software BAD?

Caveh Jalali <caveh@csl.sri.com>
Sat, 10 Apr 93 11:25:51 -0700

There has been a considerable amount of traffic on the net concerning Seagate's new 3.5Gb drives that came out a few months ago. As it turns out, SunOS (presumably the Berkeley file system) can't handle partitions over 2 Gb (2^31 - 1), so one is forced to install the drive in two partitions. Didn't MS-DOS have a similar problem only yesterday...

What went wrong? I can't imagine it is more difficult to design, build, and market a 3.5Gb drive than it is to write/fix a file-system implementation to support current hardware.

I just hope this happens before we hit the secondary limit of 8 partitions per drive, or the tertiary limit of 8 LUNs (logical units) per SCSI device!

As a "software dude" i'm somewhat embarrassed to once again have been outdone by the "hardware dudes"!

Re: ... San Francisco Muni Metro (Brennan, RISKS-14.49)

Robert J Woodhead <trebor@foretune.co.jp>
Sat, 10 Apr 1993 13:56:38 GMT

<> ``... was the result of the operator deliberately disabling the
<> safety system so that he could speed up his train, sources close to the
<> investigation said''.

>This is extremely bad, not only that the operator did it, but that he
>-could- do it.

Yes and No. A safety system that cannot be disabled is, in itself, a risk, if the system were to malfunction.

Far better is a safety system that, when disabled, leaves unmistakable evidence that it has been meddled with, thus allowing responsibility to be assigned, and providing a powerful incentive NOT to disable it without justification.

A classic example would be to put the disabling mechanism behind a pane of glass, with a hammer nearby, and a policy that "if the glass gets broken, you'd better be able to explain why."

Robert J. Woodhead, Biar Games / AnimEigo, Incs. trebor@forEtune.co.jp |
AnimEigo US Office Email (for general questions): 72447.37@compuserve.com |

Re: Discovery shuttle problem (Sorenson, RISKS-14.49)

<king@reasoning.com>
Fri, 09 Apr 93 13:55:04 BST

<> ... The "fix" is to bypass the sensor, fooling the computer into
<> thinking the valve is properly closed.

In all fairness, they had alternate sources of information.

As was mentioned in sci.space and in RISKS a couple of days ago, they had telemetry to monitor the temperature of the vent pipe that was downstream of the valve and would have remained cold had the valve not in fact closed.

I don't know whether the software was told to worry about the vent pipe temperature before the rewrite that got them off the ground, but i sincerely hope that when they decided not to check for a valve closure indication they also decided to check for this vent pipe temperature. By now they should know how this pipe temperature normally behaves.

And if the temperature doesn't rise fast enough, either the valve didn't close or it's too cold for the %$#%&$#&^$*^ O-rings, anyway ;-) .
-dk

Re: Turn of the century date problems (Peterson, RISKS-14.45)

Mark Brader <msb@sq.com>
Fri, 9 Apr 1993 18:50:00 -0400

> In a humorous vein, I've regularly proposed a `programmer's cruise' that
> would depart on December 30, 1999. The cruise would be 30 days long
> and would come with the following guarantees ...

There is a bug here. Considering the number of people who seem to think that 2000 will NOT be a leap year, the cruise should extend at least into March!

Mark Brader, SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

[Well, maybe it is more of an `opportunity' than a "bug". PGN]

Re: The FORTRAN-hating gateway (Karn, RISKS-14.45)

<Bob_Frankston@frankston.com>
Sat 10 Apr 1993 15:42 -0400

The problem with "nnnn" in a gateway reminds me of the use of such sequences as Telex end of message and as delimiters. I remember MMMM and LLLL so I wouldn't be surprised at NNNN having a special significance. Perhaps they only worked at the beginning of a line to reduce the likelihood of seeing them during normal transmissions.

IFIP Call for Papers

"Dr. Harold Joseph Highland, FICS" <Highland@DOCKMASTER.NCSC.MIL>
Mon, 12 Apr 93 14:24 EDT

CALL FOR PAPERS
TENTH INTERNATIONAL INFORMATION SECURITY CONFERENCE
IFIP SEC '94 - ARUBA

ORGANIZED BY IFIP TECHNICAL COMMITTEE 11 * Security and Protection in Information Processing Systems * IN COOPERATION WITH THE SPECIAL INTEREST GROUP ON INFORMATION SECURITY OF THE DUTCH COMPUTER SOCIETY AND CO-HOSTED BY THE ARUBA COMPUTER SOCIETY.

MAY 23 - MAY 27, 1994
PALM BEACH, ARUBA, DUTCH CARIBBEAN

The purpose of the Tenth International Information Security Conference IFIP SEC '94 -- "Dynamic Views on Information Security in Progress" -- is to provide an international forum and platform sharing experiences and interchanging ideas, research results, development activities and applications amongst academics, practitioners, manufacturers and other professionals, directly or indirectly involved with information security and protection. It will be held at Palm Beach, Aruba, Dutch Caribbean on May 23rd-27th, 1994.

Those interested in presenting papers are invited to do so by September 30, 1993. The papers may be practical, conceptual, theoretical, tutorial or descriptive in nature, addressing any issue, aspect or topic of information security. Submitted papers will be refereed, and those presented at the conference will be included in the conference proceedings. Submissions must not have been previously published and must be the original work of the author(s).

The International Program Chair is particularly interested in papers on:

Information security aspects in developing nations
Security of health care systems
Aspects of transborder data flow
Fraudulent aspects and networks
Security in banking and financial industry
Evaluation criteria in information security
Cryptology
Risk management and analysis
Contingency planning and recovery

Instructions to Authors

Five (5) copies of the complete paper, which should not exceed 25 double-spaced, typewritten pages, including diagrams, of approximately 5,000 words, must be received by NO LATER THAN September 30, 1993.

Diskettes and electronically transmitted papers will not be accepted. Papers must be sent to the International Program Chairman [address noted below].

Each paper must have a title page which includes the title of the paper, full name(s) of all author(s) and their title(s), complete address(es) including affiliation(s), employer(s), telephone number(s), telefax number(s) and e-mail address(es).

To facilitate the blind refereeing process the author(s)' particulars should only appear on the separate title page. Furthermore, the first actual page of the manuscript should include the title and a 100 word abstract of the paper, explaining its contents.

Note: The language of the conference is English. All submissions and presentations must be written and delivered in the English language. However, at the conference Spanish translation will be available for the audience.

Notification of acceptance of submitted papers will be mailed on or before December 31, 1993. At that time author(s) will be instructed to prepare final camera-ready manuscripts and the final deadline for submission of the camera-ready manuscript is February 28, 1994.

Papers should be submitted to the International program Chair at the Secretariat [address noted later]. All authors of submitted papers will enjoy special benefits at the Conference.

The Referee Process

All papers and panel proposals received by the submission deadline will be considered for presentation at the conference. To ensure acceptance of high quality papers, each paper submitted will be double and blind refereed. All papers presented at IFIP SEC '94 will be included in the conference proceedings, copies of which will be provided to the attendees. All papers will also be included in the formal proceedings of IFIP TC11 to be published by Elsevier Science Publishers (North Holland).

About the Conference

IFIP SEC '94 will consist of a five day/five stream program with advance seminars, tutorials, open forums, special interest workshops and technical sessions. The conference will offer world-renowned and most distinguished speakers as its keynoters, and the highest quality of refereed papers. There will be far over 100 different presentations. This special conference will be held at the convention space situated at Palm Beach on the Dutch Protectorate island of Aruba in the Caribbean.

During the worlds' most comprehensive information security conference, the second Kristian Beckmann Award, honoring the first chairman of IFIP TC 11, will be presented.

IFIP SEC '94 is intended for computer security researchers, security managers, advisors, consultants, accountants, lawyers, edp auditors, IT and system managers from government, industry and the academia, as well as individuals interested and/or involved in information security and protection.

The Tenth International Information Security Conference is organized by Technical Committee 11 of the International Federation for Information Processing, in cooperation with the Special Interest Group on Information Security of the Dutch Computer Society, and will be hosted by the Aruba Computer Society.

Conference Information

Aside from the submission of papers, which should be to the International Program Chair, information about all other matters, including participation registration, travel, hotel and program information, is available from the General Organizing Chair at the Secretariat.

SECRETARIAT IFIP SEC '94 ARUBA
Postoffice Box 1555
6201 BN   MAASTRICHT   THE NETHERLANDS
or
SECRETARIAT IFIP SEC '94 ARUBA
Wayaca 31a
Suite 101/104
ARUBA - DUTCH WEST INDIES

Telephone: +31 (0)43 618989
Telefax: +31 (0)43 619449
Internet E-mail: TC11@CIPHER.NL

Local Limited Contact

If you want you may communicate with Highland@dockmaster.ncsc.mil
and I'll help if I can. HJH

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 51

Wednesday 21 April 1993

Contents

text of White House announcement and Q&As on clipper chip encryption

Clipper Chip Announcement <clipper@csrc.ncsl.nist.gov>
Fri, 16 Apr 93 11:07:20 EDT [RISKS-14.51]

Note: This file will also be available via anonymous file
transfer from csrc.ncsl.nist.gov in directory /pub/nistnews and
via the NIST Computer Security BBS at 301-948-5717.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release   April 16, 1993

STATEMENT BY THE PRESS SECRETARY

The President today announced a new initiative that will bring the Federal
Government together with industry in a voluntary program to improve the
security and privacy of telephone communications while meeting the legitimate

needs of law enforcement.

The initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links.

For too long there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement.

Sophisticated encryption technology has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit called the "Clipper Chip" has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today.

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

A "key-escrow" system will be established to ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique "keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

The "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

To demonstrate the effectiveness of this new technology, the Attorney General will soon purchase several thousand of the new devices. In addition, respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings.

The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities. In order to assess technology trends and explore new approaches (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption that accommodates:

- -- the privacy of our citizens, including the need to employ voice or data encryption for business purposes;

- -- the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;

- -- the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and

- -- the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

The Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice.

Since encryption technology will play an increasingly important role in that infrastructure, the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law.

Further information is provided in an accompanying fact sheet. The provisions of the President's directive to acquire the new encryption technology are also available.

For additional details, call Mat Heyman, National Institute of Standards and Technology, (301) 975-2758.

QUESTIONS AND ANSWERS ABOUT THE CLINTON ADMINISTRATION'S TELECOMMUNICATIONS INITIATIVE

Q: Does this approach expand the authority of government agencies to listen in on phone conversations?

A: No. "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?

A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.

Q: Who will run the key-escrow data banks?

A: The two key-escrow data banks will be run by two independent entities. At this point, the Department of Justice and the Administration have yet to determine which agencies will oversee the key-escrow data banks.

Q: How strong is the security in the device? How can I be sure how strong the security is?

A: This system is more secure than many other voice encryption systems readily available today. While the algorithm will remain classified to protect the security of the key escrow system, we are willing to invite an independent panel of cryptography experts to evaluate the algorithm to assure all potential users that there are no unrecognized vulnerabilities.

Q: Whose decision was it to propose this product?

A: The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision. This approach has been endorsed by the President, the Vice President, and appropriate Cabinet officials.

Q: Who was consulted? The Congress? Industry?

A: We have on-going discussions with Congress and industry on encryption issues, and expect those discussions to intensify as we carry out our review of encryption policy. We have briefed members of Congress and industry leaders on the decisions related to this initiative.

Q: Will the government provide the hardware to manufacturers?

A: The government designed and developed the key access encryption microcircuits, but it is not providing the microcircuits to product manufacturers. Product manufacturers can acquire the microcircuits from the chip manufacturer that produces them.

Q: Who provides the "Clipper Chip"?

A: Mykotronx programs it at their facility in Torrance, California, and will sell the chip to encryption device manufacturers. The programming function could be licensed to other vendors in the future.

Q: How do I buy one of these encryption devices?

A: We expect several manufacturers to consider incorporating the "Clipper Chip" into their devices.

Q: If the Administration were unable to find a technological solution like the one proposed, would the Administration be willing to use legal remedies to restrict access to more powerful encryption devices?

A: This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" (as some countries have effectively done); nor is the U.S. saying that "every American, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an "either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques.

Q: What does this decision indicate about how the Clinton Administration's policy toward encryption will differ from that of the Bush Administration?

A: It indicates that we understand the importance of encryption technology in telecommunications and computing and are committed to working with industry and public-interest groups to find innovative ways to protect Americans' privacy, help businesses to compete, and ensure that law enforcement agencies have the tools they need to fight crime and terrorism.

Q: Will the devices be exportable? Will other devices that use the government hardware?

A: Voice encryption devices are subject to export control requirements. Case-by-case review for each export is required to ensure appropriate use of these devices. The same is true for other encryption devices. One of the attractions of this technology is the protection it can give to U.S. companies operating at home and abroad. With this in mind, we expect export licenses will be granted on a case-by-case basis for U.S. companies seeking to use these devices to secure their own communications abroad. We plan to review the possibility of permitting wider exportability of these products.

White House Public Encryption Management Fact Sheet

Clipper Chip Announcement <clipper@first.org>
Fri, 16 Apr 93 16:41:05 EDT [RISKS-14.51]

Note: The following was released by the White House today in conjunction with the announcement of the Clipper Chip encryption technology.

FACT SHEET
PUBLIC ENCRYPTION MANAGEMENT

The President has approved a directive on "Public Encryption Management." The directive provides for the following:

Advanced telecommunications and commercially available encryption are part of a wave of new computer and communications technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure economic competitiveness in the information age.

Despite its benefits, new communications technology can also frustrate lawful government electronic surveillance. Sophisticated encryption can have this effect in the United States. When exported abroad, it can be used to thwart foreign intelligence activities critical to our national interests. In the past, it has been possible to preserve a government capability to conduct electronic surveillance in furtherance of legitimate law enforcement and national security interests, while at the same time protecting the privacy and civil liberties of all citizens. As encryption technology improves, doing so will require new, innovative approaches.

In the area of communications encryption, the U. S. Government has developed a microcircuit that not only provides privacy through encryption that is substantially more robust than the current government standard, but also permits escrowing of the keys needed to unlock the encryption. The system for the escrowing of keys will allow the government to gain access to encrypted information only with appropriate legal authorization.

To assist law enforcement and other government agencies to collect and decrypt, under legal authority, electronically transmitted information, I hereby direct the following action to be taken:

INSTALLATION OF GOVERNMENT-DEVELOPED MICROCIRCUITS

The Attorney General of the United States, or her representative, shall request manufacturers of communications hardware which incorporates encryption to install the U.S. government-developed key-escrow microcircuits in their products. The fact of law enforcement access to the escrowed keys will not be concealed from the American public. All appropriate steps shall be taken to ensure that any existing or future versions of the key-escrow microcircuit are made widely available to U.S. communications hardware manufacturers, consistent with the need to ensure the security of the key-escrow system. In making this decision, I do not intend to prevent the private sector from developing, or the government from approving, other microcircuits or algorithms that are equally effective in assuring both privacy and a secure key-escrow system.

KEY-ESCROW

The Attorney General shall make all arrangements with appropriate entities to hold the keys for the key-escrow microcircuits installed in communications equipment. In each case, the key holder must agree to strict security procedures to prevent unauthorized release of the keys. The keys shall be released only to government agencies that have established their authority to acquire the content of those communications that have been encrypted by devices containing the microcircuits. The Attorney General shall review for legal sufficiency the procedures by which an agency establishes its authority to acquire the content of such communications.

PROCUREMENT AND USE OF ENCRYPTION DEVICES

The Secretary of Commerce, in consultation with other appropriate U.S. agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal communications systems that process sensitive but unclassified information. I expect this process to proceed on a schedule that will permit promulgation of a final standard within six months of this directive.

The Attorney General will procure and utilize encryption devices to the extent needed to preserve the government's ability to conduct lawful electronic surveillance and to fulfill the need for secure

law enforcement communications. Further, the Attorney General
shall utilize funds from the Department of Justice Asset Forfeiture
Super Surplus Fund to effect this purchase.

Slide presented at White House briefing on Clipper Chip

Clipper Chip Announcement <clipper@first.org>
Mon, 19 Apr 93 9:21:53 EDT [RISKS-14.51]

Note: The following material was handed out a press briefing on the
Clipper Chip on 4/16.

```
                         Chip Operation

                      Microchip
User's Message      +----------------------+
------------------> |                      |     1.  Message encrypted
                    | Encryption Algorithm |         with user's key
                    |                      |
                    | Serial #             |     2.  User's key encrypted
                    |                      |-->      with chip unique key
                    | Chip Unique Key      |
User's Encryption   |                      |     3.  Serial # encrypted
Key                 | Chip Family Key      |         with chip family key
------------------> |                      |
                    |                      |
                    +----------------------+
```

For Law Enforcement to Read a Suspect's Message

1. Need to obtain court authorized warrant to tap the suspect's telephone.

2. Record encrypted message

3. Use chip family key to decrypt chip serial number

4. Take this serial number *and* court order to custodians
of disks A and B

5. Add the A and B components for that serial number = the chip
unique key for the suspect user

6. Use this key to decrypt the user's message key for
this recorded message

7. Finally, use this message key to decrypt the recorded message.

"Clipper Chip"

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Sat, 17 Apr 93 09:12:57 -0400 [RISKS-14.51]

I suppose we should have expected something after all of the sound and
fury of the last few years. The announcement does not really give
enough information though.

My first thought involves conventional compromise: what happens if the
keys are captured through theft *and you know about it* - how difficult
is it to change the keys ? What do you do between the time the loss is
detected and the time a new key set is approved. How difficult is it
to program the chip or do you need a new one ? (and if the chip can
be reprogrammed, how do you prevent covert changes that will not be
discovered until authorization to tap is received and the agency finds
out that it cannot ?). Potentially this must occur every time a trusted
employee leaves.

For some time, I have been playing with dynamic access cards ("tokens")
as seeds for full session encryption rather than just for password devices.
Since the encryption requires three parts (PIN, challenge, and token)
which are only physically together at the secure system, and since only
the challenge passes on the net, and since once encryption starts you
have not only provided protection to the session, you have also authenticated
both ends simultaneously (by the fact that you can communicate), it seems
ideal. *And everything necessary already exists*. From several US companies.
It just has not been put together as a commercial product (FUD at work 8*(.

Since key generation is on-the-fly at the onset of the session, obviously
what the gov needs is not the key but the "key to the key" (of course
computers, even a PC, are really good at this.

The real question is "Why a new chip ?" The technology to do this has been
around for years and several DES chips are available commercially today.
The BCC laptop (I like Beaver better 8*) 007 provides this internally
today with (I believe) the LSI-Logic chip and Enigma-Logic's PC-SAFE (plugs)
does the same with software alone. As indicated in the announcement,
financial institutions have been using encrypted transmissions for years
without any great outcry.

IMHO the real hold-up has been $$$ - cheap error-correcting modem
technology to prevent synch losses rather than a lack of good crypto
algorithms. Today this is a done deal (actually we have known how to keep
in synch since the sixties but you couldn't buy 56kb for under $300.00 at
BizMart - now part of K-Mart ! - then).

True, there are a lot of questions yet to be answered, but again IMHO
most center on the exception cases and not the encryption technology itself.

Padgett

The Clipper Chip

paj <paj@gec-mrc.co.uk>
20 Apr 1993 09:41:21-BST [RISKS-14.51]

I have just read with considerable interest the "White House Crypto Statement" posted to comp.society.

Briefly, it announces a "Clipper Chip" that will provide voice and data encryption. Every chip will have two keys kept in two separate "key escrow" banks. Law enforcement officers needing to conduct a wire tap will get a court order, go to the key escrow banks, and then decrypt the messages.

The encryption algorithm is secret, but a panel of cryptologists could be invited to inspect it.

For more details, call Mat Heyman, NIST, (301) 975-2758

In the "Questions and Answers" section of the statement, the following text appears:

```
> Q:   If the Administration were unable to find a technological
>      solution like the one proposed, would the Administration be
>      willing to use legal remedies to restrict access to more
>      powerful encryption devices?
>
> A:   This is a fundamental policy question which will be
>      considered during the broad policy review.   [...]
>      ... Rather, both concerns can be,
>      and in fact are, harmoniously balanced through a reasoned,
>      balanced approach such as is proposed with the "Clipper
>      Chip" and similar encryption techniques.
```

This is not entirely clear. Does it mean that the Administration might ban all encryption except for the Clipper Chip? If not, how would they stop criminals and terrorists from using something else?

The Administration might sell these chips abroad. How will the Key Escrow system work then?

How will the Administration handle free-trade issues? How can a non-US manufacturer export Clipper devices to the US without getting a look at the algorithm (which is secret). How would key escrow work with a non-US manufacturer?

How will the algorithm be kept secret? What is to stop someone prying the device apart and examining the chip circuitry?

Why is the algorithm secret? RSA is public and seems unbreakable. Ditto DES apart from a few known weaknesses. This smells of a hidden agenda. Could it be trade? Could it be part of a strategy to ban "bootleg" Clipper technology where foreign chips conform to the standard but do not have the keys in escrow.

How will law enforcers match keys to chips? They won't have access to the chip serial number. Maybe the chip transmits its serial number every few seconds of transmission. If so then we have a nice way of doing traffic analysis and tracking on suspects (or anyone else) without needing the keys.

Paul Johnson (paj@gec-mrc.co.uk). | Tel: +44 245 73331 ext 3245

Clinton's Clipper Chip Chaos

<rmoonen@ihlpl.att.com>
Tue, 20 Apr 93 10:45 GMT [RISKS-14.51]

As soon as the official press release on the Clipper chip was posted a barrage of posts concerned with the safety and RISKS of said chip smothered the net. Nearly all of them were negative. For those of you who missed it, the Clipper Chip is purported to be the 'Officially Sanctioned' cryptographic cypher chip. The feature that everyone is getting upset about is that the FBI will have the only general de-cypher box. Furthermore, the algorithm for encryption is secret.

My concern about this whole scheme is greater than I can express here. I'm sure the next couple of RISKS forums will be filled with messages concerning the Clipper Chip, but for what it's worth, here's my $0.02:

I am concerned that this is the first step towards banning any other encryption device that does not use the CC. I am concerned that if there *exists* a general de-cypher box, it can be stolen/hacked/duplicated/captured by aliens. I am concerned about the fact that the encryption algorithm is secret. There is no way we can be sure the algorithm is sufficiently secure. Key length is not the only factor in telling how secure an algorithm is. An encryption scheme should be secure even if the algorithm is known. I am concerned that if this thing takes off in the States, other countries will not follow, making international communications no more secure. And is other countries do follow, there will be more than one decrypt-box, which in turn will multiply the risks of one of these boxes being stolen hacked/corrupted in any other way. This box will be become a *hot* item for organised crime. (Why do I keep seeing scenes from 'Sneakers'?)

In short: I think this whole CC thing is an ungood idea, and I hope for everyone who values his privacy that it will never lift-off.

--Ralph Moonen

Clipper and Who Holds Crypto Keys

"Lance J. Hoffman" <hoffman@seas.gwu.edu>
Wed, 21 Apr 93 16:54:14 EDT [RISKS-14.51]

In the light of the recent Clipper announcement, forum readers may wish to revisit the discussions of "Who Holds the Keys?". A good place to start, in addition to some of the material in CACM of March 1993 (which relates mainly to the FBI's digital telephony initiative), is Proceedings of the 2nd Conference on Computers, Freedom, and Privacy (order no. 533921 from ACM Press, 1515 Broadway, New York NY 10036. The same discussion is available on audiotape from Audio Archives International, 800 747-8069 and on videotape from Sweet Pea Productions, 800 235-4922 (cfpvideo@well.sf.ca.us).

Professor Lance J. Hoffman, Electrical Engineering and Computer Science,
The George Washington University, Washington, D. C. 20052

(202) 994-4955   fax: (202) 994-0227   hoffman@seas.gwu.edu

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 52

Wednesday 21 April 1993

Contents

THE CLIPPER CHIP: A TECHNICAL SUMMARY

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Wed, 21 Apr 93 19:21:48 EDT

THE CLIPPER CHIP: A TECHNICAL SUMMARY
Dorothy Denning
Revised, April 21, 1993

INTRODUCTION

On April 16, the President announced a new initiative that will bring together the Federal Government and industry in a voluntary program to provide secure communications while meeting the legitimate needs of law enforcement. At the heart of the plan is a new tamper-proof encryption chip called the "Clipper Chip" together with a split-key approach to escrowing keys. Two escrow agencies are used, and the key parts from both are needed to reconstruct a key.

CHIP CONTENTS

The Clipper Chip contains a classified single-key 64-bit block encryption algorithm called "Skipjack." The algorithm uses 80 bit keys (compared with 56 for the DES) and has 32 rounds of scrambling (compared with 16 for the DES). It supports all 4 DES modes of operation. The algorithm takes 32 clock ticks, and in Electronic Codebook (ECB) mode runs at 12 Mbits per second.

Each chip includes the following components:

  the Skipjack encryption algorithm
  F, an 80-bit family key that is common to all chips
  N, a 30-bit serial number (this length is subject to change)
  U, an 80-bit secret key that unlocks all messages encrypted with the chip

The chips are programmed by Mykotronx, Inc., which calls them the "MYK-78." The silicon is supplied by VLSI Technology Inc. They are implemented in 1 micron technology and will initially sell for about $30 each in quantities of 10,000 or more. The price should drop as the technology is shrunk to .8 micron.

ENCRYPTING WITH THE CHIP

To see how the chip is used, imagine that it is embedded in the AT&T telephone security device (as it will be). Suppose I call someone and we both have such a device. After pushing a button to start a secure conversation, my security device will negotiate an 80-bit session key K with the device at the other end. This key negotiation takes place without the Clipper Chip. In general, any method of key exchange can be used such as the Diffie-Hellman public-key distribution method.

Once the session key K is established, the Clipper Chip is used to encrypt the conversation or message stream M (digitized voice). The telephone security device feeds K and M into the chip to produce two values:

  E[M; K], the encrypted message stream, and
  E[E[K; U] + N; F], a law enforcement field ,

which are transmitted over the telephone line. The law enforcement field thus contains the session key K encrypted under the unit key U concatenated with the serial number N, all encrypted under the family key F. The law enforcement field is decrypted by law enforcement after an authorized wiretap has been installed.

The ciphertext E[M; K] is decrypted by the receiver's device using the session key:

$$D[E[M; K]; K] = M .$$

CHIP PROGRAMMING AND ESCROW

All Clipper Chips are programmed inside a SCIF (Secure Compartmented Information Facility), which is essentially a vault. The SCIF contains a laptop computer and equipment to program the chips. About 300 chips are programmed during a single session. The SCIF is located at Mykotronx.

At the beginning of a session, a trusted agent from each of the two key escrow agencies enters the vault. Agent 1 enters a secret, random 80-bit value S1 into the laptop and agent 2 enters a secret, random 80-bit value S2. These random values serve as seeds to generate unit keys for a sequence of serial numbers. Thus, the unit keys are a function of 160 secret, random bits, where each agent knows only 80.

To generate the unit key for a serial number N, the 30-bit value N is first padded with a fixed 34-bit block to produce a 64-bit block N1. S1 and S2 are then used as keys to triple-encrypt N1, producing a 64-bit block R1:

$$R1 = E[D[E[N1; S1]; S2]; S1] .$$

Similarly, N is padded with two other 34-bit blocks to produce N2 and N3, and two additional 64-bit blocks R2 and R3 are computed:

$$R2 = E[D[E[N2; S1]; S2]; S1]$$
$$R3 = E[D[E[N3; S1]; S2]; S1] .$$

R1, R2, and R3 are then concatenated together, giving 192 bits. The first 80 bits are assigned to U1 and the second 80 bits to U2. The rest are discarded. The unit key U is the XOR of U1 and U2. U1 and U2 are the key parts that are separately escrowed with the two escrow agencies.

As a sequence of values for U1, U2, and U are generated, they are written onto three separate floppy disks. The first disk contains a file for each serial number that contains the corresponding key part U1. The second disk is similar but contains the U2 values. The third disk contains the unit keys U. Agent 1 takes the first disk and agent 2 takes the second disk. Thus each agent walks away knowing an 80-bit seed and the 80-bit key parts. However, the agent does not know the other 80 bits used to generate the keys or the other 80-bit key parts.

The third disk is used to program the chips. After the chips are programmed, all information is discarded from the vault and the agents leave. The laptop may be destroyed for additional assurance that no information is left behind.

The protocol may be changed slightly so that four people are in the room instead of two. The first two would provide the seeds S1 and S2, and the second two (the escrow agents) would take the disks back to the escrow agencies.

The escrow agencies have as yet to be determined, but they will not be the NSA, CIA, FBI, or any other law enforcement agency. One or both may be independent from the government.

LAW ENFORCEMENT USE

When law enforcement has been authorized to tap an encrypted line, they will first take the warrant to the service provider in order to get access to the communications line. Let us assume that the tap is in place and that they have determined that the line is encrypted with the Clipper Chip. The law enforcement field is first decrypted with the family key F, giving E[K; U] + N. Documentation certifying that a tap has been authorized for the party associated with serial number N is then sent (e.g., via secure FAX) to each of the key escrow agents, who return (e.g., also via secure FAX) U1 and U2. U1 and U2 are XORed together to produce the unit key U, and E[K; U] is decrypted to get the session key K. Finally the message stream is decrypted. All this will be accomplished through a special black box decoder.

CAPSTONE: THE NEXT GENERATION

A successor to the Clipper Chip, called "Capstone" by the government and "MYK-80" by Mykotronx, has already been developed. It will include the Skipjack algorithm, the Digital Signature Standard (DSS), the Secure Hash Algorithm (SHA), a method of key exchange, a fast exponentiator, and a randomizer. A prototoype will be available for testing on April 22, and the chips are expected to be ready for delivery in June or July.

ACKNOWLEDGMENT AND DISTRIBUTION NOTICE. This article is based on information provided by NSA, NIST, FBI, and Mykotronx. Permission to distribute this document is granted.

CPSR calls for public debate on encryption initiative

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 16 Apr 1993 16:43:02 EST

April 16, 1993 Washington, DC

COMPUTER PROFESSIONALS CALL FOR PUBLIC
DEBATE ON NEW GOVERNMENT ENCRYPTION INITIATIVE

Computer Professionals for Social Responsibility (CPSR) today called for the public disclosure of technical data underlying the government's newly-announced "Public Encryption Management" initiative. The new cryptography scheme was announced today by the White House and the National Institute for Standards and Technology (NIST), which will implement the technical specifications of the plan. A NIST spokesman acknowledged that the National Security Agency (NSA), the super-secret military intelligence agency, had actually developed the encryption technology around which the new initiative is built.

According to NIST, the technical specifications and the Presidential directive establishing the plan are classified. To open the initiative to public review and debate, CPSR today filed a series of Freedom of Information Act (FOIA) requests with key agencies, including NSA, NIST, the National Security Council and the FBI for information relating to the encryption plan. The CPSR requests are in keeping with the spirit of the Computer Security Act, which Congress passed in 1987 in order to open the development of non-military computer security standards to public scrutiny and to limit NSA's role in the creation of such standards.

CPSR previously has questioned the role of NSA in developing the so-called "digital signature standard" (DSS), a communications authentication technology that NIST proposed for government-wide use in 1991. After CPSR sued NIST in a FOIA lawsuit last year, the civilian agency disclosed for the first time that NSA had, in fact, developed that security standard. NSA is due to file papers in federal court next week justifying the classification of records concerning its creation of the DSS.

David Sobel, CPSR Legal Counsel, called the administration's apparent commitment to the privacy of electronic communications, as reflected in today's official statement, "a step in the right direction." But he questioned the propriety of NSA's role in the process and the apparent secrecy that has thus far shielded the development process from public scrutiny. "At a time when we are moving towards the development of a new information infrastructure, it is vital that standards designed to protect personal privacy be established openly and with full public participation. It is not appropriate for NSA -- an agency with a long tradition of secrecy and opposition to effective civilian cryptography -- to play a leading role in the development process."

CPSR is a national public-interest alliance of computer industry professionals dedicated to examining the impact of technology on society. CPSR has 21 chapters in the U.S. and maintains offices in Palo Alto, California, Cambridge, Massachusetts and Washington, DC. For additional information on CPSR, call (415) 322-3778 or e-mail <cpsr@csli.stanford.edu>.

Clipped Wings-- The Economic Impediment to the Clipper Chip...

Peter Wayner <pcw@access.digex.com>
Tue, 20 Apr 1993 14:23:39 -0400

If all of the privacy concerns about the Clipper chip magically disappeared, the chip will still encounter widespread economic resistance. Why? Because almost everything can be done cheaper in software and the secrecy surrounding the algorithm effectively prohibits software implementations.

Why would a computer designer add a high-speed encryption chip to the machine? Even if the chips cost about $25 in large quantities, they could still add about $100 to the final cost after everyone takes their markups. The computer designer must ask whether people are willing to spend extra to buy a box when the clone manufacturer in the garage down the street isn't going to be putting one in.

Adding encryption in software is a different proposition. There is a one-time cost of engineering and a small extra cost for increased support. Once the code is written, the manufacturing costs do not increase. Also, software can retrofit machines for no extra cost and add widespread compatibility after the update is finished. This is why Novell, Apple and Microsoft choose to add encryption software in their latest rev of the system software.

It is not even clear that the standard has much of a chance in the phone system. DSP chips and digital designs are becoming more and more part of cellular standards. Why pay extra for another chip if it can be done in the DSP? Weight and power consumption are important considerations for these applications.

I'm sure that the algorithm designers and NSA committee considered the RISKS of exposing the algorithm. Scrutiny weakens the code because it makes it easier for people to attack the system. It is obvious that the committee tried to consider some of the economic RISKS involved in promulgating a "Big Brother" standard. That is why they arranged for the chips to be presented as a fait accompli as part of AT&T's latest phones. But they face an uphill battle against the forces of economics.

--Peter Wayner

Letter to Clinton, re: the encryption proposal

Carl Ellison <cme@ellisun.sw.stratus.com>
17 Apr 1993 19:27:47 GMT

I mailed the following letter to the President today:

To: 0005895485@MCIMAIL.COM (White House)
Subject: Second thoughts about your encryption proposal

17 April 1993

Dear Mr. President --

Since writing my initial reaction I have given considerable second thought to your encryption proposal, announced yesterday. I must withdraw my initial partial support for your plan, pending the release of further details.

My initial assumption was that you were mandating the replacement of every telephone handset in the USA with one which would digitize the person's voice and encrypt it. I assumed that this replacement would start with cellular handsets and proceed through wireless and wired -- in order of severity of vulnerability. Given that the government would mandate such a change and that that change would interfere with the FBI's current ability to tap voice telephone calls on the public networks, it made sense to propose an encryption method which would allow the FBI to continue in court-ordered wiretaps -- specifically via key escrow.

While it would be beneficial from the point of view of improving the privacy and security of citizens from illegal eavesdropping, I now believe that this proposal is far too costly to undertake at this time. The federal government is facing a huge debt and deficit and the private sector is far from thriving. The proposal to pay for some of this equipment with funds from civil forfeiture adds insult to injury, since abuses of civil forfeiture have led me to conclude that law enforcement's right to such funds should be severely restricted if not removed.

If this proposal is only for limited use of such encryption, then it does little to advance the cause of citizen's privacy and it is in direct competition with existing products which already service the small market of citizens who are aware of their vulnerability and who are willing to pay for assurance of their privacy. It is especially disturbing that the press release suggests that this proposal is not merely a call for action but an already designed implementation which some agency of the administration is attempting to impose upon the American people. The talent exists in the private sector to address these security concerns.

Meanwhile, there is a danger that the key escrow provision is intended to imply that all cryptosystems used by citizens in the lawful course of their daily personal and business lives must include key registration. This would be an unacceptable erosion of our current rights, especially of the fundamental right of privacy which you supported so strongly during your campaign. Legislation to this effect would be unenforceable. It would be easily and frequently broken -- leading to the danger that some law enforcement officer with a private grudge would have an easy method of filing a criminal complaint against the innocent victim of his grudge. A requirement for key registration would also come directly into conflict with certain uses of cryptography in advanced computer system design. In those cases, both key registration and use of some government-designed chip are unacceptable.

Meanwhile, there is the additional danger that this proposal would serve as a vehicle for advancing the FBI's wiretap proposal which was rejected by Congress last year and which I oppose on several grounds.

I look forward to full technical details of your proposal and to a public debate on its merits.

Sincerely,

Carl M. Ellison

```
     Senior Technical Consultant - Advanced Development Group
     Stratus Computer Inc.
     55 Fairbanks Boulevard
     Marlborough MA  01752-1298

     TEL: (508) 460-2783
     FAX: (508) 624-7488
     E-mail: cme@sw.stratus.com
             cme@vos.stratus.com
--
 - <<Disclaimer: All opinions expressed are my own, of course.<>
 - Carl Ellison                              cme@sw.stratus.com
 - Stratus Computer Inc.       M3-2-BKW              TEL: (508)460-2783
 - 55 Fairbanks Boulevard ; Marlborough MA 01752-1298  FAX: (508)624-7488
```

Hacking turnpike signs

Paul Schmidt <prs@titan.hq.ileaf.com>
Fri, 16 Apr 93 10:59:38 EDT

Sometime last week, electronic sign boards along Interstate 95 in Connecticut were hacked to say "You all suck." These boards are normally used to announce construction, fog, and whatnot. Apparently it was several hours before State Police and the Highway Department were able to clear the messages. Well, it happened again a day or two ago, with a different message attacking the Governer. A teenager has been caught; he said that there was no password on the Highway Department's computer system.

I originally heard this on a short news blurb on WHJY, a rock station in Providence RI, so I'm sure the accuracy is all you would expect it to be. Confirming reports welcomed!

I'm just waiting for the day that the speed limit signs go electronic.
They'll probably only allow two digits, though...

Re: Head-on train collision in Berlin (RISKS 14:50)

Joseph T Chew <jtchew@Csa3.LBL.Gov>
Wed, 14 Apr 93 13:16:36 PDT

In RISKS 14:50, dww@math.fu-berlin.de (Debora Weber-Wulff) writes:

DWW> ...The computer reacted by setting the outbound signal
DWW> correctly to "halt". The overseer believed that this
DWW> was a defect in the system, and overrode the signal...
DWW> without telephoning anyone to investigate the supposed error.

The last line, of course, explain the proximate cause and points a flashing red arrow toward the root cause. I read RISKS 14:50 just a couple of days after a lessons-learned article on "lockout/ tagout" in Occupational Safety OBSERVER, a newsletter from the Department of Energy's Office of Safety and

Quality Assurance. (Lockout/tagout is a set of rules and procedures meant to keep electricians and others who work with stored energy from releasing it through themselves.)

The article pointed out, strenuously, that the cardinal rule of lockout/tagout is, "*never* remove a tag affixed by someone else." When you have virtual "tags" affixed by a computer, and operators who perhaps were not exposed to the subset of technical endeavors where the lockout/tagout discipline is used, you have a risk added to another risk!

The irony, of course, is that the computer system took the right action but was subverted by its user. I doubt that there will ever be a system so sophisticated that some dumb bunny can't cause a disaster. The lesson: designers of man-in-the-loop systems have to understand operator psychology, and owners of such systems have to provide appropriate training that accounts for such risks and then maintain a culture that places importance on avoiding them.

--Joe

Pliers Found Attached To Shuttle SRBs

<SchwartzM@DOCKMASTER.NCSC.MIL>
Thu, 15 Apr 93 17:15 EDT

In this morning's (4/15) Minneapolis Star-Tribune was a small blurb on a new problem discovered on the recent Discovery shuttle mission. Apparently, the crew that goes out to pickup the Solid Rocket Boosters (SRBs) after they come back down to the ocean via parachute, noted a pair of pliers still "attached" to one of the SRBs. They did not say if they were "jammed" in to some spot or if they were in fact holding on to something. If the latter, one would have to assume that they are probably "Vise-Grips" or a generic version of them. I can see the commercial advertisements now.... "The pliers that grip so tight, they will keep holding on even through the G-Forces of a space shuttle launch".

Apparently NASA is scrambling to figure out what went wrong. One would think so given the sensitivity to another possible failure of the SRBs.

Marc Schwartz Director of Clinical Services Summit Medical Systems, Inc.
Minneapolis, MN.

Re: Columbia and Discovery Shuttle Problems

"Stephen E. Bacher" <seb@draper.com>
14 Apr 1993 14:34:30 -0400 (EDT)

>From: viking@iastate.edu (Dan Sorenson)
>Subject: Re: Columbia and Discovery shuttle problems (RISKS-14.47)
>
>   The "fix" is to bypass the sensor, fooling the computer into

>thinking the valve is properly closed.

Love it - a high-tech implementation of the venerable
"black tape" remedy well known to Car Talk listeners.

You know:
Q: "My Check Engine / alternator / oil pressure light just came on."
A: "Get some black tape..."

Steve Bacher (Batchman)   Draper Laboratory
Internet: seb@draper.com   Cambridge, MA, USA

Badge entry and forgotten badges

<[Anonymous]>
Thu, 15 Apr 93 12:17:31 XXT

I work for a large company with badge entry systems for all buildings and all internal labs. This is normally great, because I can get into my building any time I want, day or night, and I can get into the labs that I need to use, but it keeps me out of places I don't belong. It also does the same for others.

About once a year, however, I forget my badge. This is not a problem for the normal person who comes in after 8:00 in the morning when the building is open and there is a receptionist, but I carpool from quite a distance away, before traffic gets heavy, and I get in about 6:45.

This morning was one of those rare occasions when I forgot my badge. No problem, each building has a phone at the front door that rings through directly to security. I picked it up and told them that I needed to get into the building. They asked me a few questions, like what is my name, my badge number, my phone extension and two or three other such pieces of information, then they opened the door remotely and I was let into the building.

As I was walking to my office, I realized that all of the information I was required to give them is contained on-line in our computer network and anyone with access to a workstation could get this information about anyone in the company in just a few seconds. I'm not recommending that the database be changed, because it is a great aid to employee intercommunication. However, I expect that I could easily get into some building where I don't belong by gathering this information about someone who works in that building. I don't even need to know a name to get this information, the database allows searches by building.

Not too long ago, when I needed to be let in a building, someone from security would come by, check a photo ID, such as a drivers license, then let me in with a key. Even though my company has become much more security conscious during the 5 years I've worked here, I believe it is a security risk to allow building entry based solely on information given over the phone that is contained in a computer database readily

accessible to anyone who can access the network. I'm going to
recommend a change to this procedure.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 53

Thursday 22 April 1993

Contents

Re: RISKS DIGEST 14.52

Don Alvarez <dla@athena.princeton.edu>
Thu, 22 Apr 1993 15:03:41 GMT

Dorothy Denning's summary on the clipper chip was very helpful, but it leaves a good deal up in the air. Fortunately, if you are willing to work on the assumption that the NSA is good at what they do, you can fill in a fair number of details by reading between the lines.

To begin with, based on what she has written, it is trivial to prevent law enforcement from decrypting your messages. I'll explain what I mean by that, and then I'll make a guess at what prevents you from doing so.

Once a session key K is agreed upon by the users, the chip computes two values which are transmitted over the telephone line:

(1) Message stream: E[M ; K]   (Where M is the message)

```
(2) Escrow field:     E[{E[K ; U],N}; F]    (Where F is the Family Key,
                                              N is the Serial Number,
                                            and U is the Unit Key)
```

Law enforcement uses F to obtain N, which points to U in a two-part database. Knowing U allows Law enforcement to obtain K, and then to decrypt M.

Users simply compute M = D[E[M; K]; K] to decrypt the message.

The summary isn't very specific, but it sounds like the message stream is transmitted first, followed by the escrow field. Surely this can't be the case, because all one needs to do is hang up at the appropriate point in the call and prevent the transmission of the escrow field. The other user doesn't need the escrow field to do the decryption, but law enforcement has no other way of obtaining K, even if they already know N,U, and F.

Now, I have enough faith in the NSA's skills to trust that you can't pass the message to the user without also passing the escrow field, but I'd like to see that in writing. My guess is that the protocol requires the escrow field to be transmitted first, and then the chaining mechanisms in the algorithm prevent the receiver from decoding the message without first having fed the escrow field into their chip. On the other hand, if the protocol is up to the end user, then I'll just send the escrow last, and ..oops.. ran out of quarters, have to hang up now. As is so often the case in cryptography, the protocol is as important as the algorithm, and so far we know even less about the protocol than we do about the algorithm.

Following on this line of thinking (ie that NSA is good at what they do), we can deduce a few more things about how wiretaps are handled.

First, who knows F? If the cop on the street knows F then it quickly becomes so widely known that everyone knows it and you might as well send the serial number in the clear. Ergo only the escrow agents know F.

Second, what information does law enforcement get from the escrow agents? Ideally, law enforcement only gets K, the session key governing the conversation for which they have a court order. Unfortunately, in order for law enforcement to get *only* K (and not U), the escrow agents must get together and secretly combine U1 and U2 so that they can unwrap K and give it to law enforcement. But then the escrow agents would also know K, and they would be able to decrypt messages themselves. That's just a very short step away from the omniscient big-brother which the multiple-escrower scheme was designed to prevent. The escrow agents must not allowed to exchange keys with each other. Ergo, law enforcement must assemble U itself in order to find out K. This means that law enforcement now knows the key to unlock every session key ever used on this phone.

Things are starting to look bad, but what about F? We never really figured out what F was for, we just said that only the escrow agents know F. Well, now we know what F is for. Even if law enforcement knows U, they still can't read messages without court orders, because they can't obtain E[K;U] without knowing F, and only escrow knows F.

Something (probably the chaining) keeps users honest. F keeps law enforcement

honest. What keeps the escrow agents honest? That's still a good question,
and hopefully the answer is something other than "Their strong moral
character." I suspect, however, that their strong moral character is all
we'll have to work with.

-Don Alvarez Dept. of Physics, Princeton Univ. dla@athena.princeton.edu

---

RE: (Denning) THE CLIPPER CHIP: A TECHNICAL SUMMARY

<Carl_Ellison@vos.stratus.com>
Thu, 22 Apr 93 12:40 EDT

>Once the session key K is established, the Clipper Chip is used to
>encrypt the conversation or message stream M (digitized voice). The
>telephone security device feeds K and M into the chip to produce two
>values:

> E[M; K], the encrypted message stream, and
> E[E[K; U] + N; F], a law enforcement field ,

Note that if the chip or the user were to choose random numbers K1..Kn
and compute

K = K1 xor K2 xor ... xor Kn

the chip could transmit

E[E[K1; U1] + N; F], a law enforcement field for escrow agency 1 ,
E[E[K2; U2] + N; F], a law enforcement field for escrow agency 2 ,
. . .
E[E[Kn; Un] + N; F], a law enforcement field for escrow agency n ,

(where U1 .. Un are the individual escrow keys)

then the wiretapper would have to show the court order for each message key,
not just once. As designed, however, once the LE agent has acquired U, she
has access to all messages, past and future, using that chip. She can even
sell U to any outfit willing to pay for it, if she is so inclined. The NSA
can't be less bright in cryptographic protocol design than I am. I must
assume that this security bug was intended as a feature.

There could also be more than 2 escrow agencies -- so that, for example, the
New York Times, the Washington Post, the Democratic National Committee and the
Republican National Committee could all be escrow agencies -- could all see
the choice of wiretap targets (both through warrant and through so-called
"national security" grounds) -- could notice any patterns (like Nixon's enemy
list) and could blow the whistle if the government were abusing its wiretap
ability. In this case, global use of encryption and key escrow would give us
a marginal amount of increased citizen rights (while taking away a large
right).

Of course, this is a moot point, intended for those of us who like to think about cryptographic protocols. The real point is that cryptography has always been created and used by private individuals, whether or not governments also use it. It is not used primarily by lawbreakers -- and those criminals who do use it will continue to and will ignore key registration. It has legitimate users, predominantly, and they have legitimate reasons to keep a key as secret as they know how, even if the government doesn't like it. Since the government has no right to read all our files and communications (eg., e-mail love letters I might write), this shouldn't matter to it.

Key registration is a totally new idea in cryptography, is a major erosion of our rights and must not be tolerated, even on a voluntary basis. The RISK here is that after enough years of partial voluntary registration, the FBI would go to Congress with an example (perhaps even made up) of some drug selling, snuff movie making operator of a BBS who lets minors view pornography -- who uses cryptography without key registration -- and will call for key registration to be made law, citing examples of voluntary cooperation in order to claim that "law abiding citizens don't believe that secrecy of keys is a fundamental right".

With the coming rise both of distributed systems and of wireless computer components, cryptography is about to move from a cute toy which some of us play with to an absolute necessity. If we give away the right to privacy in crypto keys, now while there are only a few of us affected, we will soon discover that everyone is affected and Orwell's society is that much closer.

Re: THE CLIPPER CHIP: A TECHNICAL SUMMARY

Steve Holzworth <sch@unx.sas.com>
Thu, 22 Apr 1993 16:40:13 GMT

I don't claim to be up on crypto, but it seems to me that once the "authorized tap" has been performed once, the agency in question now has a copy of the desired keys. They can use these keys at ANY time in the future to decrypt communications between these two parties (without having to go through the discomfort of obtaining a new court order). So a new, parallel database of key pairs will gradually evolve.

Steve Holzworth sch@unx.sas.com SAS Institute - Open Systems R&D Cary, N.C.

Re: THE CLIPPER CHIP: A TECHNICAL SUMMARY

"Keith (K.P.) Hanlan" <keithh@bnr.ca>
Thu, 22 Apr 1993 14:16:00 +0000

Dorothy Denning writes a good coherent summary of the clipper chip. Thanks.

Dorothy writes:
> The law enforcement field is decrypted by law enforcement after
> an authorized wiretap has been installed.

I have one outstanding question that I haven't seen asked yet. Is there a time component in the encryption key? Since wiretaps are presumably authorized for certain time periods with both start and end dates, it should not be possible to decrypt an illegally monitored message.

This also suggests a way to subvert the law enforcement decryption: Would it not be possible fake the encryption device's sense of time? If this were the case, and time is in fact a part of the encryption key, then the message would still be impossible for the law to decrypt. On the other hand, if time is not part of the key, perhaps a defendant could argue that the tapped and decrypted message was tapped before the wiretap was authorized. How could the police prove otherwise? This problem exists without encryption so I suppose it has been addressed. But my understanding of U.S. law is that even if evidence is incriminating, if it is illegally obtained, it will be considered inadmissible. (I don't think that this is the case in Canada for example.)

A second, unrelated question is this: How difficult is it monitor a high-capacity trunk, (say a fibre cable), for encrypted messages. I can just see, using my special Sneakers-influenced "Eyes of Paranoia", some nameless agency looking for work monitoring 10,000 lines just to see who was encrypting stuff. Heck, if it is encrypted, it must be interesting right?

Keith Hanlan KeithH@bnr.ca Bell-Northern Research, Ottawa, Canada 613-765-4645

Clipper Chip: algorithm vs. implementation

Derek Beatty <beatty@cs.cmu.edu>
Thu, 22 Apr 1993 09:42:45 -0400 (EDT)

Some of the debate here on the Clipper Chip has focused on the secrecy surrounding the encryption algorithm. I'd like to point out that not only must the algorithm be secure, but so must its implementation. I suspect that most contributors to RISKS are less than familiar with the various ways that VLSI chips are validated---that probably goes for many (non-NSA) cryptography experts as well. It seems entirely possible to me that an intentional or unintentional back door could be left in the silicon. For example, if the chip is scan-testable, then it might be possible to scan the keys out through the test path---potentially yielding U, "an 80-bit secret key that unlocks all messages encrypted with the chip"! (Or maybe the chip's not testable---why doesn't that make me feel any better?) The point is not the particular details of a possible attack; rather it is the distinction between an algorithm and a circuit. I conduct research on the formal verification of digital circuits, and I am sure that algorithms and circuits are separated by a large gap---who knows what lurks therein?

(And personally, was the name chosen to try to catch our moderator off guard?)

Derek_Beatty@cmu.edu ABD Comp Sci, CMU, 5000 Forbes, Pgh, PA 15213 USA

THE CLIPPER CHIP: A TECHNICAL SUMMARY

<lhe@sics.se>
Thu, 22 Apr 93 08:51:38 +0200

denning@cs.cosc.georgetown.edu (Dorothy Denning) writes:
  The Clipper Chip contains a classified single-key 64-bit block
  encryption algorithm called "Skipjack."

I don't know if I would feel comfortable entrusting sensitive data to
a *classified* encryption algorithm. What is the rationale for that?

If the algorithm was made public, any weaknesses would be discovered
in time. If it is classified, weaknesses may never be known, or known
only to the parties who have access to the classified information.
Also, if you are the paranoid kind: How do you know that the algorithm
isn't made deliberately weak in some way?

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263
S-164 28 KISTA, SWEDEN lhe@sics.se   +46 8 752 15 09   Fax: +46 8 751 72 30

Re: The Clipper Chip [RISKS 14.52]

Kristoffer Eriksson; Peridot AB <ske@pkmab.se>
22 Apr 93 09:25:43 MES (Thu)

I just wonder one thing: why would _anyone_ prefer to use Clipper Chip
encryption over other alternatives, when all it buys you, compared to the
alternatives, is that it allows the authorities to tap your conversations
(whether they need appropriate court order to do so or not) ??

I fear the only solution to that may be the outlawing of all other
encryption alternatives that do not include the same "feature".

Kristoffer Eriksson, Peridot Konsult AB, Stallgatan 2, S-702 26 Oerebro, Sweden
 +46 19-33 13 00 Fax: +46 19-33 13 30 e-mail: ske@pkmab.se

Clipper Chips: After the tap

Jay Schmidgall <shmdgljd+@rchland.ibm.com>
Thu, 22 Apr 1993 07:24:50 -0500 (CDT)

So, at this point the law enforcement agency (LEA) has U1 and U2?
Presumably, then, at any point subsequent to this and without benefit of
contact with the key escrow agents, the LEA can tap and decode the phone
line, providing the tappee doesn't get a new clipper chip.

I would think one of the first things the LEA would do would be to build
up a database of known U1 and U2 values; also, the U1 and U2 values
received from the key escrow agents are likely to be stored [recorded]
somewhere other than the original secure FAX paper -- given the
pervasiveness of our friend the computer, it is as likely to be on a
computer as not, and then a short hop to a computer attached to a

network, mix and match a few crackers and presto! a pirate BBS with U1
and U2 values for anyone from Joe Blow to your neighbor down the block.

Or is this an overreaction?

Perhaps a mandatory "You've been tapped, change your keys" scheme could
be implemented along with this; after the authorization for the tap is
canceled, the tappee would automatically receive new keys? chips? to
ensure secure communication once again.

: jay   jay@vnet.ibm.com   My opinions and ideas, not my employer's.
: shmdgljd@rchland.vnet.ibm.com

Risks in encryption session startup?

<phydeaux@cumc.cornell.edu>
Thu, 22 Apr 1993 09:34:40 -0500

I'll preface this by saying that encryption has never been a big problem in my particular line of software, so I'm slightly hazy on this. However, scanning through the discussions on the Clipper Chip, I came across a general description of how a session works. It appears (and someone please correct me if I'm off the wall here) that two encryption devices, when they initiate a session, must exchange keys in order to decrypt each others messages. Great, but here's my question...what's to stop someone at machine B (who's talking to machine A) from "recording" the key from machine A when the session is started? Since it appears that the key is constant for each chip, machine B can now _always_ decrypt machine A's messages.

If this is the case, does encryption over a cellular link become worthless? Already, the phone ID is transmitted, with an enormous black market in the stolen ID's. Why not capture that encryption key as it goes out?

Or is there something I'm missing?

73 de Dave Weingart   KB2CWF phydeaux@cumc.cornell.edu
phydeaux@src4src.linet.org

RISKS DIGEST 14.52

Jim Sims <sims@pdesds1.atg.trc.scra.org>
Thu, 22 Apr 93 11:05:45 EDT

Being someone outside this (which may be a good feature):

Seems a whole lot easier to just catch the key K during the
negotiation between the boxes....

Then use the black box to reconstruct....

jim

clipper chip is no good

"PGE" <CMARTIN@unode2.nswc.navy.mil>
22 Apr 93 12:30:00 EST

Like everyone else, I feel I must add my 2 cents on the data encryption chip. first, how will this be implemented. Will everyone get a knock on the door next tuesday from the telephone company installing our chip? If not, then the slow increase in user base will make the technology as useful as video-phones. Sure some will get in on the ground floor, but who will they talk too? Reminds me of the scene in Repo Man. The security does no good if you can't use it. Second, math. How many phones in the U.S.A.? Hundreds of millions? Billions? If 300 chips are made in a run, and a run is say, eight hours, that is hmmm 500,000,000 phones/300 chips = (about) 1,300,000. Now for an average work week, (1,300,000chipruns*2persons)/(40hrs*52weeks) = 1250 person/years of work. So, we cannot expect this to occur overnight. So, who gets to have first dibbs on the technology? The rich, the powerful, the government? If so, not very democratic to me.

Next, where in the line will the chip be? I assume the handset which again kicks up the number of chips needed. Also the complexity. I assume that more bandwidth will be needed to get the data to the handset. Fiber-optics? Yeah, in another ten years. Data compression? That can only get you so far. If you place the chip elsewhere, the risk exists that someone can tap illegally in the home. No messy decryption needed there.

To me, knowing that the encryption sceme can be broken at will (by the "right people") does not make me feel secure in using it. The general public would most likely use the logic--if this person can decypher this message, why can't anyone else? Then wrongly or rightly conclude anyone else can.

Next, NSA. Why should I trust them to make the thing secure? They want to listen in, that is part of their job.

Finally, as a chip, it can break. Burn out. Well where are you then. And where is the government? Do they need a warrant for every phone you could use, and have to get new warrants for any new phone you get. Imagine a criminal that continually buys phones so that the warrants can't get through in time to listen in on the conversations. Do they record all the unintelligible conversations prior to getting the key? How much data would this be? What if another encryption is found embedded in the first? How do you prove it is not a compressed abstract picture for the computer? I could see a big new news group forming for abstract art that could be used as a wonderful cover for secret messages. Try decyphering that Jackson Pollack.

The questions just keep coming, and I personally don't like the answers.

Re: The Clipper Chip (Johnson, RISKS-14.51)

Neil W Rickert <rickert@cs.niu.edu>
Thu, 22 Apr 1993 13:10:01 -0500

In Risks Digest 15.51 paj <paj@gec-mrc.co.uk> writes:

>
\>The encryption algorithm is secret, but a panel of cryptologists could be

>invited to inspect it.

This secrecy is perhaps the most troubling aspect.

Here are three requirement that would seem essential for general purpose encryption.

(1) The encryption must be so strong that even if the algorithm were published, it should be impossible to break the code. Otherwise there would always be fear that someone had reverse-engineered the chip to discover the algorithm.

(2) The algorithm must actually have been published. For who could believe assurances of (1) if the designer were unwilling to publish?

(3) The encryption/decryption must be readily doable in software. For in multiprogramming environments, a hardware implementation is inherently dangerous. A hardware implementation would require that user software must transmit the key to the operating system for insertion in the device. This allows too big a window of opportunity for operating system modifications to record user keys.

By virtue of its secrecy, the Clipper fails these tests.

"key escrow" (Clipper Chip; RISKS 14.51)

Mark Seecof <marks@wimsey.latimes.com>
Thu, 22 Apr 93 12:12:44 -0700

(At the risk of redundancy (with other contributors)):

1. Although gov't press releases and gov't surrogates like Dorothy Denning keep talking about warrants (actually, they say "proper authorization") for Clipper keys, the government has never abandoned (and does not even deny) the practice of conducting warrantless wiretaps for "national security" reasons. How will keys be obtained to decrypt such intercepts? My guess--the security of the "escrow" agencies will be secretly compromised. And then, the time will come when the NSA turns over political or criminal information with little or no "national security/foreign/military intelligence" content to the FBI, etc. My fallback guess is that the Skipjack algorithm will have a back door.

2. The key escrow scheme is a pottery container of fecal matter. Right now in California we are enjoying two scandals involving the release, to unauthorized persons, of "secret" data, by employees of government and private organizations, in violation of: their employers' policies, their own terms of employment, state criminal law, and common (civil) law. These (Anaheim PD employee release of DMV address info to anti-abortion terrorists; various people including police employees giving info to an ADL investigator) are representative, not exhaustive of the problem. Does anybody remember the

Walker (U.S. Navy) spy scandal of a few years ago? Walker ring members, despite vetting by the military (perhaps inefficient, but more thorough than likely in civilian agencies), exposure to the most severe legal sanctions, and even the cultural pressures of their military communities, sold out Navy cipher secrets and keys to actual enemies for fairly small amounts of money. N.B.: the Walker ring had no ideological motivations. Anyone who says that the key escrow scheme will protect the privacy of Clipper users is naive, stupid, or wicked. Of course, as someone will point out: "the Walker ring got caught!"--but catching malefactors will not prevent the harm they do before they are detected.

3. The assertion that the government should, by rights, be able to decrypt private communications for "law enforcement" purposes should be challenged. Privacy advocates should not concede this important debate-framing assumption. Advances in digital computing have made it possible for ordinary people to use powerful machine cipher techniques. But such systems will not prevent police agents from eavesdropping directly or by various bugging methods. It may be (I suspect it is so) that depriving the police of convenient wiretapping might have little effect over, say, ten years, on their (police) ability to detect and interfere with criminals.

Mark Seecof <marks@latimes.com>

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 54

Monday 26 April 1993

Contents

Re: Responses to Clipper Chip Discussion in RISKS-14.53

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Sat, 24 Apr 93 14:39:12 EDT

Don Alvarez wrote

> Now, I have enough faith in the NSA's skills to trust that you can't pass the message to the user without also passing the escrow field, but I'd like to see that in writing.

That is certainly the intent.

> First, who knows F? If the cop on the street knows F then it quickly becomes so widely known that everyone knows it and you might as well send the serial number in the clear. Ergo only the escrow agents know F.

F is embedded in every Clipper Chip, but like other chip keys, unknown to the people who use them. Only law enforcement will have a decoder box that allows the law enforcement field to be decrypted. Initially, there will be just one box, and it will be operated by the FBI.

> Second, what information does law enforcement get from the escrow agents? Ideally, law enforcement only gets K, the session key governing the conversation for which they have a court order. Unfortunately, in order for law enforcement to get *only* K (and not U), the escrow agents must get together and secretly combine U1 and U2 so that they can unwrap K and give it to law enforcement. But then the escrow agents would also know K, and they would be able to decrypt messages themselves. That's just a very short step away from the omniscient big-brother which the multiple-escrower scheme was designed to prevent. The escrow agents must not allowed to exchange keys with each other. Ergo, law enforcement must assemble U itself in order to find out K. This means that law enforcement now knows the key to unlock every session key ever used on this phone.

It is imperative that law enforcement get U. If they are tapping a line, there may be dozens of calls on that line per day. It would be totally impractical to have to go to the escrow agents to get the session key for each call. It would be impossible to do real-time decryption under that constraint.

> Things are starting to look bad, but what about F? We never really figured out what F was for, we just said that only the escrow agents know F. Well, now we know what F is for. Even if law enforcement knows U, they still can't read messages without court orders, because they can't obtain E[K;U] without knowing F, and only escrow knows F.

For the same reason as above, it is imperative that law enforcement be able to decode the law enforcement field in order to obtain E[K; U] and then decrypt this to get K. It is completely impractical to go the escrow agents for each conversation.

Steve Holzworth wrote:

> I don't claim to be up on crypto, but it seems to me that once the "authorized tap" has been performed once, the agency in question now has a copy of the desired keys. They can use these keys at ANY time in the future to decrypt communications between these two parties (without having to go through the

After a tap has been completed, government attorneys are required to notify the subjects of the electronic surveillance. At that point, the subjects are certainly free to purchase a new device with a new chip, or perhaps the vendors could simply replace the chip.

> I have one outstanding question that I haven't seen asked yet. Is there a time component in the encryption key? Since wiretaps are presumably authorized for certain time periods with both start and end dates, it should not be possible to decrypt an illegally monitored message.

I am unaware of any time component. Current wiretap laws protect against this. Evidence collected after the warrant has expired can be thrown out in court. In addition, it is illegal for the service provider to implement an intercept after a warrant has expired. With the new technologies, law enforcers will be incapable of executing a tap without the assistance of the service provider.

Lars-Henrik Eriksson has written

> If the algorithm was made public, any weaknesses would be discovered in time. If it is classified, weaknesses may never be known, or known only to the parties who have access to the classified information.

The NSA has a long record of success with crypto, far better than any individual or organization in the public community. In addition, there are plans to bring in expert cryptographers to assess the algorithm.

Dave Weingart wrote:

> It appears ... that two encryption devices, when they initiate a session, must exchange keys in order to decrypt each others messages. Great, but here's my question...what's to stop someone at machine B (who's talking to machine A) from "recording" the key from machine A when the session is started? Since it appears that the key is constant for each chip, machine B can now _always_ decrypt machine A's messages.

The unit keys that are embedded in the chips are not exchanged. Instead, machines A and B negotiate a session key K that is used only for that particular conversation.

Jim Sims wrote:

> Seems a whole lot easier to just catch the key K during the negotiation between the boxes....

It is possible for both ends to negotiate a session key K without transmitting any secret information at all, including K. One way of doing this is with a public-key distribution method. The Diffie-Hellman method works as follows. Machine A picks a secret value xa, and machine B picks xb. A sends the public value ya = g^xa mod p to B and B sends yb = g^xb mod p to A, where p is a huge prime and g is a global constant. Then A computes the session key K = yb^xa mod p = g^xbxa mod p, and B computes K = ya^xb mod p = g^xaxb mod p. Both K's are the same. An eavesdropper sees ya and yb, but since xa and xb are not known, cannot compute K. For more information about key exchange, see for example my book "Cryptography and Data Security" or some other crypto text.

Dorothy Denning denning@cs.georgetown.edu

[There were enough additional messages for several more issues, some raising points already covered by the above message. I have somewhat arbitrarily selected a representative few for the rest of this issue, trying to avoid duplication where possible. There may

be another issue or two yet to come out of the existing backlog.
PLEASE pardon some of the duplication. It is virtually impossible
for me to selectively choose a few nonoverlapping paragraphs from each
message. For those of you who wonder whether RISKS has been taken over
by this discussion, there has been essentially no other topic of concern
for the past week, although something may be brewing in the recent
near-fatal aircraft autopilot failure attributed to software. PGN]

Thoughts on the U.S. Encryption Proposal

Magnus Kempe <Magnus.Kempe@di.epfl.ch>
Fri, 23 Apr 93 09:47:25 +0200

Mr. President:

I am concerned that your proposal fails to address the following issues, among others:

1. Will American companies have to manufacture different lines of products according to the market (US vs. foreign--assuming that they wouldn't be allowed to export the Clipper Chip) ?

2. Will foreign companies be excluded from the American market since they won't have access to the Clipper Chip ?

3. If the technology is ever sold to other countries (foreign governments), how will the US be sure that no foreign government develops the ability to tap American communications, and how will international communications be secure (remember that the two escrow "agencies" are to be located in the US, a seemingly unacceptable proposition for non-American entities) ?

4. What guarantee is there that other encryption schemes will not be outlawed in the future? In particular, what guarantee is there that the right retained by the people to privacy will not be ever more violated by the US government in the future? Will use of other, private, secret encryption become a crime?

5. What guarantee is there that criminals will use the Clipper Chip, knowing that the US government has the ability to decrypt their communications? Isn't it probable that such criminals will resort to publically available encryption systems that they would know are secure from the US government?

6. Since the secrecy of the algorithm seems to be essential, how does your proposal compare to the strength of currently available non-secret algorithms? It is well known in Computer Science that reliance on the ignorance of an enemy party is the worst protection imaginable, since it is a very weak link in the chain of safety.

7. An American hero once said something to the effect that those who are willing to trade liberty for safety deserve neither. Don't you

think you are asking the American people to trade liberty (their right
to privacy) in exchange for an elusive safety (listening to suspected
criminals, if these criminals buy the government's chip)?

8. How is it justifiable to ask the American people that they spend
money (for the Clipper Chip) in order to let the government listen on
them? Given the current state of the economy, is it even possible?

9. Finally, what constitutional article gives you the power to violate
the privacy of the American people? Didn't you swear to uphold the US
constitution?

Sincerely,

Magnus Kempe

Software Engineering Lab, Swiss Federal Institute of Technology, DI-LGL /
EPFL, CH-1015 Lausanne, Switzerland +41-21 693 2580 Magnus.Kempe@di.epfl.ch

---

Re: Clipper Chip (Alvarez, RISKS-14.52)

Jeffrey I. Schiller <jis@mit.edu>
Fri, 23 Apr 93 21:53:09 -0400

> The summary isn't very specific, but it sounds like the message stream is
> transmitted first, followed by the escrow field. Surely this can't be the
> case, because all one needs to do is hang up at the appropriate point in the
> call and prevent the transmission of the escrow field...

One way of solving this "problem" is to have the escrow block consist of:

E[{E[K ; U],N,SHA[{E[K ; U],N}]} ; F]

Where SHA[] represents the Secure Hash Algorithm (in the Capstone
Chip), though frankly a CRC32 would probably do just as well. The
receiving Clipper can then decrypt each received law enforcement block
and verify that the SHA hash of the contents match the supplied hash.
If they fail, the chip ceases to perform any decryption operations on
behalf of the user. Perhaps other information could be included in
the encryption under "F" to make it difficult to supply a law
enforcement block from another prior conversation. This could well be
a detail that was left out of the explanation given to Dorothy.

Btw. I will go on record as being opposed to this entire proposal. My
interpretation of the Constitution (and the Bill of Rights) on this issue is
that the 4th amendment (no search and seizure without a warrant) was intended
to place limitations on the right of the government to interfere with the
people. It is being twisted around by some to imply that we the people never
had the right to privacy in the first place, when a warrant was issued. As
others have mentioned here, I have a real concern that a VOLUNTARY program
today will turn into a mandatory program tomorrow. In my nightmares I envision
an agent of (pick your favorite large, secretive, government agency) telling

Congress:

"Yes Senator, but we gave the American Public privacy five year's ago with the
Clipper program. They still have that privacy today. However some miscreants
in our society... drug dealers and whatnot are still using non-Clipper
unbreakable encryption and we must put a stop to this..."

-Jeff

Clipper Chip Commentary (not suitable for the cynicism impaired)

Daren Stebner <STEBNERD@wl.aecl.ca>
22 Apr 1993 22:03:55 -0600 (CST)

Short Synopsis:

"We're from the government. We're here to help...."

Long Synopsis:

"No, no, no. Don't use those regular old encryption devices; if everyone uses them, then criminals will use them, too. And if criminals use them, Big Brother won't be able to protect you from all those nasty deals they make over the phone. It just makes the work of protecting you poor lost sheep that much harder.

"Here, Big Brother will make things all better, but in order for it to work, you need to use this handy dandy NEW encryption algorithm that HE designed. He even put it on a chip to make it easy for you to use it in all of your communication devices. He even gave it a cute name -- the 'Clipper Chip'. See?! Now, since Big Brother will know how to decode the messages, He'll be able to listen in on the conversations of all of those yucky bad guys so He can put them in jail and make things all better.

"Could we listen in on your conversations too? Well, yes, but we would never dream of infringing on innocent peoples' rights to privacy. That would be a crime and Big Brother doesn't commit crimes. He loves you all and would never do anything to hurt you. Most of all, he just wants to protect you from those terrible, terrible, drug dealers. That's all he would ever use the Clipper Chip for. Isn't that swell of Him?"

Daren Stebner stebnerd@wl.aecl.ca

Clipper chip & databases

"Paul R. Coen" <PCOEN@DRUNIVAC.DREW.EDU>
23 Apr 1993 00:46:41 -0400 (EDT)

A few things have occurred to me as I've read the announcements and the initial reactions.

Each chip contains and broadcasts the serial number. To be frank, if they don't use a lot of different family keys, then that number is going to be rather public, rather quickly.

Legally, what is this going to do to wiretaps? If I have recorded a conversation, have I tapped it? Or have I only tapped it when I decrypt it? This could lead to recording lots of conversations, and then only getting the keys and actually "tapping" once I get someone for something criminal. A change to the law or court ruling could establish this. For now, they need permission up front (with exceptions, noted below), but I could see that changing.

Doesn't the manufacturer need to give the keys to the escrow agencies? With the serial number? Am I missing something, or is there a RISK of the manufacturer becoming compromised?

The other thing is that companies are going to be using this for international calls. And, calls in other countries. I'm sure most of you have noticed that agencies of the US Government tend not to follow the procedural niceties that they at least have to give lip service to here when dealing with communications elsewhere. If the CIA or NSA decides they want a tap, can they get the keys for a unit in another country without a court order, by saying "it's for national security" three times and throwing a rock in the air? Besides, the NSA gets really itchy if they can't just monitor international calls whenever they want. So, what are they going to do -- record the call data and decrypt it later if they need to? They don't need specific authorization now to tap and record international calls. I can't see that changing.

What I read in one of the gov't documents implied that the A.G. was responsible for defining some sort of reasonable authorization. Why do I have a feeling that "national security" is going to come up a lot? Especially since there has been an increase in cold-war style rhetoric in reference to *economic* competition? Regarding profitable technologies as national security concerns for the sake of economic competition is a scary thing. And this chip plays right into that desire for control. As other people have pointed out, once they've got your key, they've got your key. If someone gets it for national security reasons, then you might just be out of luck.

Paul Coen, Drew University Academic Computing pcoen@drunivac.drew.edu

---

Clipper Chip

Tony Harminc <TONY@VM1.MCGILL.CA>
Fri, 23 Apr 93 00:29:38 EDT

Thoughts on the Clipper Chip:

1) One of the selling points of the Clipper chip is that US companies will be able to use it to effect secure communication between their home offices and branches in foreign countries. In particular, it is implied that it is the governments of those foreign countries that will be thwarted in their attempts to listen in to the corporate secrets of America.

Now why would any "friendly" foreign government (e.g. Canada, France,

New Zealand) imaginably permit Clipper to be used on its territory
unless it too has access to the keys for "law enforcement purposes" ?

So if XYZ Corp. wants to talk in private with its French subsidiary XYZ France, SA., the French government will want access to the escrow agents so that it too can present a court order (according to French law, of course) and be given XYZ's key, if it suspects wrongdoing on the part of XYZ France. But this clearly won't do. The US escrow agents will presumably be subject to US law and might be able to refuse a French court order on some US constitutional grounds. So the French will have to have their own pair of agents, and - since there is no advance control of which chips will end up in France - these French agents will have to have the complete list of all keys. Now multiply this by a dozen or so friendly countries, with an equal number of different legal systems and constitutions...

2) Presumably the reason for keeping the algorithms secret is to prevent competitive manufacture of chips (or software) that can communicate with Clippers from being produced. (Such competitors might somehow forget to send their key lists to the escrow agents.)

I know almost nothing of the technology, but it seems far fetched to me that a chip can be manufactured that *absolutely, positively* cannot be reverse engineered, or at least satisfies something analogous to being computationally infeasible to reverse engineer.

There was no mention of quantum effects, but I know of no other way to even begin to make something that can't be examined with appropriate probes. I hope some hardware experts will say something on this topic. Or is it that the hardware design can be reverse engineered, but the algorithms themselves are one-way encrypted ?

3) It is not clear to me how tapping of bidirectional communications works. If the police have a court order to tap the phone of suspected criminal X, and they find that he is holding a Clipper-encrypted conversation with previously unknown person Y, will they be able to decrypt only what X says if they have only X's key from escrow ? Or will they automatically apply for Y's key too, on the grounds that he is an associate of X ?

Ordinary analogue phones (and networks) echo a small amount of the received signal to the sender, but an encrypting phone will have digitized and encrypted the signal before it gets echoed (even if there is a modem and analogue circuit in the loop).

Tony Harminc, Apios Systems Toronto, tony@vm1.mcgill.ca

Baltimore Clipper

407)826-1101
Fri, 23 Apr 93 08:46:34 -0400

With all of the sound and fury surrounding the announcement, I think a few things have been missed. First, no-one has said that Clipper is going to replace the STU-III or the Lockheed Encrypting Modem (just passed up an opportunity to buy a couple for $25 - only 1200 baud) or all of the other devices that exist. Elements of the Norton Utilities and PKZIP would also have to be outlawed. The "user selected table" in UUENCODE would be right out.

Second, prohibition of double encryption using Clipper as one stage would be impossible to enforce through sheer mass. Comes under the same category as strict enforcement of the speed limit.

So what is Clipper ? IMHO it will be a low-cost way to provide *reasonable* protection for routine traffic that up until now has been unprotected. Cellular telephony is the obvious first use to reduce the billion-dollar fraud situation. Transmittal of medical records, legal records, credit reports is another. Privacy laws state that these must be protected. Clipper provides a legal remedy that has been lacking.

Telecommuting is another major problem for most companies who have been back through fear of unautorized interception. Clipper will provide a "warm and fuzzy" feeling with low-cost encrypting modems.

IMHO, Clipper must meet the "good enough" test. Clipper *will* meet the "good enough" test because the designers are not stupid and it would be a major *political* embarrassment should it prove to be easily broken, we just do not know all of the facts yet.

Technically, I can make a guess and say that little of what we have seen as yet is correct. For instance if the Message Key (K) is only 30 bits long and the message is encrypted E(M;K) as mentioned several times, a massive attack with existing technology that is not particularly expen$ive would yield a solution in under a minute. (Hint: check out DSPs). Therefore the message is not encrypted E(M;K).

Further, there is a Family Key (F) and a Unit Key (U) in each chip. The only link to these is the serial number therefore I *suspect* that the serial number will be sent en clair as part of the header. It would be possible to use only selected Family Keys and create E(s/n;F) such that it would easily yield the s/n but why (more later).

So most likely we will have a message key that will be a predetermined function of K,U,&F (FN1). The header might consist of the serial number, followed by an encrypted function of K,U,& F (FN2) that is different from (MK), then the message encrypted with MK.

Before engaging Clipper, both FN1 and FN2 would have to be exchanged.

On starting communication, the header would consist of the serial number, followed by FN2, followed by E(M;FN1). To the receiving Clipper, the serial number would act as a "wake up". Since the chip would have K,U, & F it would then reverse FN2 and create FN1 and decode the message. A longer header could accommodate conference calling. This removes any incentive to spoof the s/n since the receiving chip will assume it is for someone else. (Exercise is left to the student).

A "promiscuous" chip might be designed but it would have to have all U and F keys (of course the total number issued is probably going to be less than the number of ZIP codes so this *is* a danger point...).

The "key master" would hold one element say the s/n,U function, the "gatekeeper" s/n,F. On proper application each would contribute its part but the requesting authority would receive only FN1, not the means to recreate it. Alternately, the requesting authority might receive a duplicate Clipper chip but not the Keys - this protects the keys from disclosure *and* provides physical traceability of the duplicate Clipper. On completion of the tap authorization, the duplicate must be destroyed.

Certainly, there are still some things to be worked out but these are technical details. IMHO we *need* a cheap means of "good enough" encryption, something that can be built into modems and cell phones at a disposable cost. We *need* a workable Clipper, and the government has more to lose in providing a flawed product than we do.

Padgett

Re: Clipper Chip

a.e.mossberg <aem@symbi1.symbiosis.ahp.com>
23 Apr 1993 10:29:50 -0400

One thing (among several) that disturbs me about the Clipper Chip is the release of the decryption key to law enforcement bodies, who have various legal maneuverings to circumvent ever notifying the tappee, after the wiretap has completed, that their key has been compromised.

The key, originally safeguarded by the key escrow bank, is now additionally held by unknown and unaudited persons within law enforcement.

History has shown that the law enforcement community has not been above using information gained during illegal wiretaps... Once they have the key, they have access forever to your conversations.

And, supposing that one is actually notified that they were being wiretapped, and thus need a new key. Will the agency responsible for the tap pay any costs for obtaining new keys?

Further, the information packet provided by Mat Heyman's office fails to address the question of using non-clipper chip encryption. They call their technology "more secure than many other voice encryption systems readily available" -- admitting that more secure systems are available. Why should anyone believe they do not intend to make illegal competing methods of encryption?

andrew mossberg, systems specialist, symbiosis corporation, miami, florida
33166-6202 (305) 597-4110 fax (305) 597-4002 aem@symbiosis.ahp.com

---

time, recording, and clipper

David P. Reed <reed@interval.com>
Fri, 23 Apr 93 10:52:26 PDT

In some of the recent comments on the RISKS of Clipper, it would seem that the commentators are ignoring the results of including omnivorous recording. It is well known that it is possible to record a substantial amount of traffic for archival storage and later analysis. Such recording is not prevented by any encryption scheme, whether keys are escrowed or not.

The resulting RISK of this assumption is that we may erode away the notion that pure recording is a violation of privacy (today's wiretap law prevents recording conversations without a warrant). What could be wrong with law enforcers or others recording everything, now that it is masked by encryption? Surely this is NOT a violation of privacy because you can't read it. I'd bet that such recordings and archival would be authorized by most governmental lawyers as NOT violating privacy on this basis. But in fact, with key escrow, someone on a fishing expedition could in principle recover all past history from an archival database.

I think that the design of Clipper protocols is actually more suitable for ex-post-facto decryption of recorded conversations, rather than for getting access to not-yet-happening transactions. So the notion that we might be moving to a world where recording is real would make sense.

I also notice that the protocol for selecting conversation keys requires an online conversation -- thus one cannot use Clipper for leaving secure voice mail in a voice mail box, as far as I can tell. Similarly, conference calling, etc. need to be considered in the design of secure phones. If conference calling services (such as AT&T's service) require that the security devices be turned off or compromised, there is a risk that users will be deceived about their level of security.

My point, then, is that issues related to recording seem to have been poorly considered in this proposal. Perhaps I'm wrong, but I'd like to understand this better, in the context of societal impacts that may result.

David P. Reed, Interval Research Corporation, 1801-C Page Mill Road
  Palo Alto, CA 94304

Who will use clipper?

Fri, 23 Apr 1993 11:18:42 PDT

An amazing amount of discussion and speculation has been generated by the clipper chip announcement. Special thanks to Dorothy Denning for her summary, and kudos to Don Alvarez for asking good questions. But I have yet to see anyone ask (or answer) the obvious question:

Will the various government agencies be using the clipper chip?

If so, I heartily endorse the policy. It guarantees that government messages cannot be ultimately secret from the governed. It seems to me that the private sector will continue to use whatever encryption is appropriate for their needs, (even should laws to the contrary be passed,) and that the only agencies obliged live with the consequences are those of the government itself.

--Bob

bebert.osbu_north@xerox.com -or- ebert@xsoft.xerox.com -or- (415) 813-7579
-or- XSoft/Xerox Corp. 3400 Hillview Ave. M/S PAHV203 Palo Alto, CA 94303

---

alt.privacy.clipper

Jonathan Papai <PAPAI@kcgl1.eng.ohio-state.edu>
Thu, 22 Apr 1993 23:34 ???

I guess someone should mention the existence of a new newsgroup alt.privacy.clipper . Might as well be me.

-Jon

---

privacy

Lauren Weinstein <lauren@cv.vortex.com>
Thu, 22 Apr 93 19:17 PDT

There is largely unique discussion of clipper going on over on the PRIVACY Forum Digest. For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@cv.vortex.com"; you will receive a response from an automated listserv system.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 55

Tuesday 27 April 1993

Contents

Computer criminal executed in China

<ITB234PEKKAN@qut.edu.au>
Tue, 27 Apr 93 19:51 +1000

RISKS readers might be interested to note a short snippet that appeared in the Courier Mail, the daily newspaper here in Queensland.

> Tuesday, 27 April 1993. BEIJING: The first person in China to be convicted of embezzling bank funds by computer has been executed.

Mr Jani PEKKANEN, Queensland University of Technology, Brisbane, AUSTRALIA
AARnet: itb234pekkan@qut.edu.au

New Disclosures in 2600 Case

Dave Banisar <banisar@washofc.cpsr.org>
Sun, 25 Apr 1993 9:43:32 EST

As you may recall, last November at a shopping mall outside of Washington, DC, a group of people affiliated with the computer magazine "2600" was confronted by mall security personnel, local police officers and several unidentified individuals. The group members were ordered to identify themselves and to submit to searches of their personal property. Their names were recorded by mall security personnel and some of their property was confiscated. However, no charges were ever brought against any of the individuals at the meeting.

Computer Professionals for Social Responsibility ("CPSR") filed suit under the Freedom of Information Act and today received the Secret Service's response to the FOIA lawsuit, in which we are seeking agency records concerning the break-up of the meeting. I think it's safe to say that our suspicions have now been confirmed -- the Secret Service *did* obtain a list of names from mall security identifying the people in attendance at the meeting.

There are three main points contained in the Secret Service's court papers that are significant:

1) The agency states that the information it possesses concerning the incident was obtained "in the course of a criminal investigation that is being conducted pursuant to the Secret Service's authority to investigate access device and computer fraud."

2) The agency possesses two relevant documents and the information in those documents "consists solely of information identifying individuals."

3) The information was obtained from a "confidential source," and the agency emphasizes that the FOIA's definition of such a source includes "any private institution which provided information on a confidential basis."

Taken together, these facts seem to prove that the Secret Service wanted names, they had the mall security people collect them, and they came away from the incident with the list they wanted.

The agency asserts that "[t]he premature release of the identities of the individual(s) at issue could easily result in interference to the Secret Service's investigation by alerting these individual(s) that they are under investigation and thus allowing the individual(s) to alter their behavior and/or evidence."

CPSR, in conjunction with EFF and the ACLU, is planning to challenge the actions of the mall security personnel, the local police and the Secret Service on the ground that the incident amounted to a warrantless search and seizure conducted at the behest of the Secret Service.

David Sobel, CPSR Legal Counel   dsobel@washofc.cpsr.org

Hacker Accused of Rigging Radio Contests

Peter shipley <shipley@merde.dis.org>
Fri, 23 Apr 1993 13:25:21 -0700

Hacker Accused of Rigging Radio Contests
[By Don Clark Chronicle staff writer]
[San Francisco Chronicle 22 Apr 1993]

A notorious hacker was charged yesterday with using computers to rig promotional contest at three Los Angeles radio stations, in a scheme that allegedly netted two Porsches, $20,000 in cash and at least two trips to Hawaii.

Kevin Lee Poulsen, now awaiting trial on earlier federal charges, is accused of conspiring with two other hackers to seize control of incoming phone lines at the radio stations. By making sure that only their calls got through, the conspirators were assured of winning the contests, federal prosecutors said. A new 19-count federal indictment filed in Los Angeles charges that Poulsen also set up his own wire taps and hacked into computers owned by California Department of Motor Vehicles and Pacific Bell. Through the latter, he obtained information about the undercover businesses and wiretaps run by the FBI, the indictment states.

Poulsen, 27, is accused of committing the crimes during 17 months on the lam from earlier charges of telecommunications and computers fraud filed in San Jose. He was arrested in April 1991 and is now in the federal Correctional Institution in Dublin. In December, prosecutors added an espionage charge against him for his alleged theft of a classified military document. The indictment announced yesterday adds additional charges of computer and mail fraud, money laundering, interception of wire communications and obstruction of justice.

Ronald Mark Austin and Justin Tanner Peterson have pleaded guilty to conspiracy and violating computer crime laws and have agreed to help against Poulsen. Both are Los Angeles residents. Poulsen and Austin have made headlines together before. As teenagers in Los Angeles, the two computer prodigies allegedly broke into a Pentagon-organized computer network that links researchers and defense contractors around the country.

Between 1985 and 1988, after taking a job at Menlo Park-based SRI International, Poulsen allegedly burglarized or used phony identification to sneak into several Pacific Bell offices to steal equipment and confidential access codes that helped him change records and monitor calls. After being indicted on these charges in 1989, Poulsen skipped bail and fled to Los Angeles where he was eventually arrested at a suburban grocery store.

One of the unanswered mysteries about the case is how he supported himself as a fugitive. The new indictment suggests that radio stations KIIS-FM, KRTH-FM and KPWR-FM unwittingly helped out.

Poulsen and his conspirators are accused of hacking into Pacific Bell computers to block out other callers seeking to respond to contests at the stations. The conspirators allegedly used the scheme to let Poulsen and

Austin win Porsches from KIIS and let a confederate win $20,000 from KPWR. Poulsen created aliases and phony identification to retrieve and sell one of his Porsches and launder the proceeds of the sale, the indictment states. In February 1989, they arranged for Poulsen's sister to win a trip to Hawaii and $1,000 from KRTH, the indictment states.

[Included in RISKS with permission of the author]

Photocopier operation monitored totally by computer

Ian Staines <Ian_Staines@mindlink.bc.ca>
Fri, 23 Apr 93 18:28 PDT

Our office recently acquired a new photocopier. A sophisticated onboard computer constantly monitors and controls all aspects of the photocopiers operation, and maintenance.

The sorter trays on this machine are driven up and down by servo motors to collate the output. Under normal operation the tray would never be directed by the computer to raise beyond a certain height; however, should there be a problem, two sensors were placed at both limits of the tray's movement to detect a possible over-run. In keeping with the integrated nature of this copier, sensors were of course not wired directly into the servo-motors, but instead were monitored by the main computer.

Today I watched the copier attempt to recover from an interrupted print job: In error, it failed to note the starting position of the sorter tray, and directed the servo-motors to move the tray upwards. unfortunately there did not appear to be a software check in the 'recover' routine to check the over-run sensors. The tray crashed upwards off its rails damaging several components.

Ian_Staines@mindlink.bc.ca

Risk of using too much electricity

J. Philip Miller <phil@wubios.wustl.edu>
Thu, 22 Apr 1993 11:57:46 -0500 (CDT)

In today's St. Louis Post Dispatch there was an article about a local man who had been convicted of growing marijuana for resale. His defense was primarily related to using it to treat his asthma, but what was far more interesting was the way that he was originally arrested. According to the story, he first came to the attention of the authorities because he was using substantially more electricity than his neighbors. They then utilized an airborne infrared detector to infer that he had a substantial number of growlamps in his attic. Based on this they were able to obtain a search warrant and discovered his crop of 150 plants.

It would be interesting to know if the utilities actually have routines that identify "unusual" customers and routinely report this to the authorities or if there was some other reason that this man came to the attention of the

authorities.
-phil

J. Philip Miller, Professor, Division of Biostatistics, Box 8067, Washington
Univ. Medical School, St. Louis MO 63110 (314) 362-3617 phil@wubios.WUstl.edu

Incidents in civil airliners

Martyn Thomas <mct@praxis.co.uk>
Mon, 26 Apr 93 15:16:50 BST

The latest "Feedback" (the newsletter of the confidential human factors incident reporting programme, run by the RAF institute of aviation medicine for the UK civil aviation community) contains two reports relevant to this forum. I copy them without editing - I can't translate the abbreviations. [Comments in square brackets are mine]

[First report]

> A Question: It is now accepted practice to "clear" the many spurious (?) messages which seem to occur for random reasons ("tyre pressure indicators" when the Reversers were locked out AD wise) by pulling and resetting the breaker, often after speaking to Tech. Control. These are "non events" and few are reported, but ought not each one to be MOR/ASR'd with full details so that the software engineers can at least attempt to trace the bugs?

[Feedback replies:]

> The question is really: "When does "just a bug" in the software constitute a broken bit of equipment?" With automatic recording and testing of faults this information should not be lost to the software engineers. There is currently no way of knowing what interrelated combinations of switching have been built up. These could be waiting for one further critical selection to provide a major problem.

[... and the power reset presumably clears these latent problems back to a known state - but it all seems rather arbitrary for important systems. I wonder if the incidents are really logged by the software. If so, someone must know how common they are.

Second report:]

Foreign airline look-alike Boeing twin (glass cockpit) lined up on westerly runway. 2+ aircraft positioning downwind, right hand, for duty runway. Subject aircraft instructed "When airborne, disregard standard instrument departure (which turns right) after noise, turn left, radar heading 190 degrees climbing to flight level 60". Expected readback was verbatim, in fairly un-accented English.

When aircraft observed to turn right the pilot was reminded of previous instruction and responded - "We want to turn left and you want us to turn left but the aeroplane, she wants to turn right, so we are turning right. I sorry (sic)".

At the time, the humour was lost on us. Is the Flight Management System really the boss, or is there the rumoured cut-out/override switch?

[Feedback replied:]

Even if this pilot had taken the autopilot out the flight director was going to take him the same way, which shows how much re-programming skill is needed in the Glass Cockpit.

[... and the accident report would say "pilot error", but surely the system is deficient in design if it is so hard to obey a simple ATC instruction].

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

Clipper questions

Jim Bidzos <jim@RSA.COM>
Mon, 26 Apr 93 23:25:44 PDT

Much has been said about Clipper and Capstone (the term Clipper will be used to describe both) recently. Essentially, Clipper is a government-sponsored tamper-resistant chip that employs a classified algorithm and a key escrow facility that allows law enforcement, with the cooperation of two other parties, to decipher Clipper-encrypted traffic. The stated purpose of the program is to offer telecommunications privacy to individuals, businesses, and government, while protecting the ability of law enforcement to conduct court-authorized wiretapping.

The announcement said, among other things, that there is currently no plan to attempt to legislate Clipper as the only legal means to protect telecommunications. Many have speculated that Clipper, since it is only effective in achieving its stated objectives if everyone uses it, will be followed by legislative attempts to make it the only legal telecommunications protection allowed. This remains to be seen.

The proposal, taken at face value, still raises a number of serious questions.

What is the smallest number of people who are in a position to compromise the security of the system? This would include people employed at a number of places such as Mikotronyx, VSLI, NSA, FBI, and at the trustee facilities. Is there an available study on the cost and security risks of the escrow process?

How were the vendors participating in the program chosen? Was the process open?

A significant percentage of US companies are or have been the subject of an investigation by the FBI, IRS, SEC, EPA, FTC, and other government agencies.

Since records are routinely subpoenaed, shouldn't these companies now assume that all their communications are likely compromised if they find themselves the subject of an investigation by a government agency? If not, why not?

What companies or individuals in industry were consulted (as stated in the announcement) on this program prior to its announcement? (This question seeks to identify those who may have been involved at the policy level; certainly ATT, Mikotronyx and VLSI are part of industry, and surely they were involved in some way.)

Is there a study available that estimates the cost to the US government of the Clipper program?

There are a number of companies that employ non-escrowed cryptography in their products today. These products range from secure voice, data, and fax to secure email, electronic forms, and software distribution, to name but a few. With over a million such products in use today, what does the Clipper program envision for the future of these products and the many corporations and individuals that have invested in and use them? Will the investment made by the vendors in encryption-enhanced products be protected? If so, how?

Since Clipper, as currently defined, cannot be implemented in software, what options are available to those who can benefit from cryptography in software? Was a study of the impact on these vendors or of the potential cost to the software industry conducted? (Much of the use of cryptography by software companies, particularly those in the entertainment industry, is for the protection of their intellectual property. Using hardware is not economically feasible for most of them.)

Banking and finance (as well as general commerce) are truly global today. Most European financial institutions use technology described in standards such as ISO 9796. Many innovative new financial products and services will employ the reversible cryptography described in these standards. Clipper does not comply with these standards. Will US financial institutions be able to export Clipper? If so, will their overseas customers find Clipper acceptable? Was a study of the potential impact of Clipper on US competitiveness conducted? If so, is it available? If not, why not?

I realize they are probably still trying to assess the impact of Clipper, but it would be interesting to hear from some major US financial institutions on this issue.

Did the administration ask these questions (and get acceptable answers) before supporting this program? If so, can they share the answers with us? If not, can we seek answers before the program is launched?

The Real Risk of Clipper

Bill Campbell <billc@glacier.sierra.com>
Mon, 26 Apr 93 15:39:13 PDT

I've been browsing through as much as I could this morning on comp.risks and comp.security.misc about the Cripple Chip. Personally, I will boycott any products that incorporate this insidious device, as well as encouraging any within my own circle of influence to do the same. Unfortunately, these newsgroups are read primarily by individuals who understand well the risks of the chip and its attendant policy. We are "preaching to the choir". After a brief discussion, I offer an idea for how to address a broader audience.

======== The Real Risk of the Clipper Chip ========

Proponents/apologists for the chip make, as I see it, one (and only one) valid point: use of the chip will protect me against the casual eavesdropper better than no encryption at all.

I fear, however, that unless something high-profile is done (and done quickly) the real risk associated with this technology-policy will be borne to fruition. To wit, the American public is by and large profoundly ignorant of technical "stuff", and often very indifferent about protecting their own Constitutional rights. This same gullible public may very easily be convinced by the government that not only is their privacy protected from their nosy neighbor, but also from unlawful invasion by law enforcement and/or other more determined individuals and organizations. This is what I see as the real risk of Clipper.

There are dozens, perhaps hundreds, of commercial, criminal and governmental entities with access to government resources who would not hesitate for a moment to violate my rights if they found it expedient to do so. These individuals and organizations have demonstrated beyond question that they are not constrained by legal or ethical considerations, and as has been suggested in a number of other postings, the technology employed by Clipper (including the dual escrow sham) will probably not even pose so much as an inconvenience to a determined adversary. To suggest otherwise is, at best, profoundly naive.

I believe that as a society we have at least two challenges with respect to addressing this public gullibility/naivete:

1) we need to find some way to dispel the assumption held by many that the government ultimately acts with the best interests of the public in mind. This is unmitigated hogwash. Government by its very nature is a consumer, not a producer. Left to its own, government will progressively consume more and more of a nation's productivity until the nation finally collapses under the weight of its inevitably oppressive and corrupt government, as in the Soviet Union. This can only be prevented by an informed and active citizenry.

2) we need to find a way to effectively educate the public about _specific_ threats to our freedom and prosperity from government action (such as the Cripple Chip) as they arise.

==========

The average person's capacity for self-delusion makes #1 an unlikely candidate for solution, but I have an idea for #2: does anyone out there have a personal acquaintance with, say, Tom "Red October" Clancy, or Michael "Jurassic Park" Crichton? It occurs to me that a best-selling techno-thriller about a government "sponsored" cryptology initiative gone awry might be a very effective method for raising the awareness of the general public. There have already been a number of highly plausible scenarios suggested in both comp.risks and comp.security.misc, that could probably be developed into a story line.

Bill Campbell, Software Engineer, Sierra Geophysics, Inc. billc@sierra.com

---

Worries over the Clipper Chip

<firth@SEI.CMU.EDU>
Tue, 27 Apr 93 08:08:58 -0400

Cui bono?

Who stands to gain from the Clipper Chip encryption system, and what do they stand to gain? From the reports, it seems pretty clear that the users gain very little - the government is providing them with a less secure system at marginally less cost than a more secure one.

So, why would the government go to all this trouble to do badly what the market is already doing quite well? As other have pointed out, one obvious motive is to maintain, and indeed extend, the supposed "right" of the authorities to snoop on private conversations.

However, that won't work. Why should anyone worried about snoopers use an encryption scheme designed to allow snooping? In this, as in much else, Gresham's Law will drive the Clipper from the market.

The answer, of course, is indeed that all other encryption schemes must be outlawed. Given the intense devotion to freedom and individual rights in this country, it is very doubtful whether this could be done directly, by legislative fiat. Hence what I believe to be a deliberate ruse by the government to finesse away this freedom.

You see, friends, if the Clipper becomes the normal, standard, or accepted means of encryption, then *the use of any other encryption scheme can of itself be considered "probable cause" for search and seizure*. And thereby could be lost in the courts what was won at such great cost.

For which reason, I believe the Clipper proposal warrants our united, vocal, and implacable opposition.

Robert Firth

Baltimore Clipper LXVIII

407)826-1101
Tue, 27 Apr 93 08:08:35 -0400

Amazing how diversified the discussion has become with people deciding just what Clipper will do and taking stands against it.

I'm taking the opposite approach. The people who designed it are talented and dedicated. The criteria for design may not be exactly what we might like but it must be *Good Enough* (C). Therefore a few postulates are submitted for consideration. (Haven't been briefed so am free to think out loud 8*).

1) There will be many family keys. There may be only one *right now* but a single key makes no sense. I expect that corporations may be able to buy groups of Clipper chips with a single family key just as I expect corporations to be able to monitor their chips (owner's rights have nothing to do with wiretaps). See the court cases in California concerning monitoring if you doubt this.

2) Once a key is released for a wiretap, there is no way to protect the key and the future use of the chip would be invalidated. Therefore, keys will not be released. When a tap is authorized, the requesting authority will receive a duplicate Clipper chip. A physical device is much easier to account for and a duplicate can process anything the original can. If the plaintext is available, who cares what the key was ?

3) There will be several varieties of Clipper chips, some will allow key programming (Master Clippers ?) but the ones for the general public will be fixed.

4) (Stretching a bit) The algorithm will be kept secret simply because there is no one true algorithm. Reverse engineer two chips and they will not be alike. There are many different ways to say the same thing (and confuse engineers e.g. polymorphic viruses). If so can lay claim to prior art c.a. 1984, 1981 nee IBM 1957 8*).

5) Further suspect there might be some *traps* in the Clipper that will render chip useless if given the wrong inputs ("China Clippers" ?) - see #4.

Like I said, both the government and corporate America *need* Clipper, the designers are some of the best in the world, and the administration has more to lose than we do. Given that, Clipper will work as advertised.

Again, pure conjecture but phun ;*) Padgett [Usual disclaimers apply]

Clipper Chip, et al.

"John A. Pershing Jr." <pershng@watson.ibm.com>
Tue, 27 Apr 93 09:37:01 EDT

I'm wondering how the Clipper Chip (actually, the entire genre of encrypted telephone technology) impacts the rules of evidence presented in a court of law. I believe that current rules of evidence require that, when a phone is being tapped, that a person be listening in on the phone at the time that it is being recorded (tapped). A tape recording by itself is not admissible;

there must be a person who will testify that he (she), indeed, listened in on the phone line and that the tape recording is an accurate representation of what was said.

With encrypted (digital) telephony and POST-HOC decryption, it is not possible to have a human listen in on the live conversation in order to testify to the authenticity of the tape. The only way for this to work is to get the keys in advance and decrypt the conversation in real time.

(Of course, this assumes that federal agents will not purjure themselves regarding evidence. It also does not rule out "fishing expeditions" in which phones are tapped to gather information (never intended to be used as evidence), perhaps as a "pointer" to other hard evidence...

...naww -- it can't happen here!) jp

Re: Responses to Clipper Chip Discussion (Denning, RISKS-14.54)

Magnus Kempe <Magnus.Kempe@di.epfl.ch>
Tue, 27 Apr 93 17:14:51 +0200

The RISKS, weaknesses and anti-constitutional aspects of the Clipper scheme are becoming more and more apparent. For instance, Dorothy Denning writes:

```
: Only law enforcement will have a decoder box that allows the law
: enforcement field to be decrypted. Initially, there will be just one
                                                 ^^^^^^^^^
: box, and it will be operated by the FBI.
```

Who else is going to receive/develop such boxes? I see many possibilities: the IRS/EPA/DEA, criminals, enemy dictatorships, etc.

: After a tap has been completed [...] the subjects are certainly free
: to purchase a new device with a new chip [...]

Wonderful. The feudal "subjects" are _free_ to spend their own money to purchase a new device. It is quite interesting that the protection offered by the Constitution (no taking without compensation) is simply disregarded. A reminder seems in order: We are not subjects--we are freemen.

Even a suspect is under the protection of the Bill of Rights.
In particular, property that is taken away must be compensated (the disclosure of the secret key destroys the value of the chip), especially when _no_evidence_of_crime_ is found. I would have thought it was an essential aspect of the government's proposal: respect and uphold the U.S. Constitution--including the Bill of Rights.

: With the new technologies, law enforcers will be incapable of executing
: a tap without the assistance of the service provider.

This is an irresponsible promise, not a fact. The new technologies increasingly rely on radio transmissions. Listening (i.e. tapping) radio transmissions is the easiest thing in the world, whether the listener is a bureaucrat, a criminal, a spook, or a competitor.

: The NSA has a long record of success with crypto, far better than any
: individual or organization in the public community.

The question is: what _kind_ of success? universal _de_cryption?

Clearly, the prime mover of the Clipper scheme is not to protect the people, but to make it easier for the government (and any government in the future) to monitor the people. The highest RISK is that the government should some day take advantage of the new power it could acquire given the precedent established by this proposal.

I can't wait for government mandated holes in our doors and walls in order to make it possible for the FBI to listen to and watch "criminal activities at home". Where is the difference?

Magnus Kempe, Magnus.Kempe@di.epfl.ch

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 56

Thursday 29 April 1993

Contents

---

747 autopilot faults?

Stephen L Nicoud <stephen@boeing.com>
Tue, 27 Apr 93 11:32:47 PDT

An item from a Boeing News Digest:

Washington, D.C. Office Morning Report - Volume 19 Number 81 April 26, 1993

1. WALL STREET JOURNAL - After an incident in which an Evergreen International Airlines 747 went into a slow roll, lost lift and went into a dive, dropping from 31,000 feet to 19,000 feet, the Federal Aviation Administration began an investigation. It found 30 similar incidents the FAA believes were caused by a broad variety of autopilot faults. The incidents, both fast and slow rolls, showed up on 747s at several airlines over a 22-year period. Many occurred in daylight with a horizon visible, enabling pilots to regain control more quickly -- and postponing the day when the seriousness of the problem would be widely recognized. Among carriers whose 747 autopilots went into rolls are British Airways, TWA, Air Canada and Lufthansa. Boeing, the airlines and aviation regulators are in a quandary. After more than a year of intense investigation following Evergreen's near-disaster, engineers can't agree on whether the fault lies in the autopilot or elsewhere, or on what the remedy should be. Boeing says pilots should pay close attention to their job so they can quickly right the plane should the autopilot throw it into a roll. Autopilots "are designed to assist and supplement the pilot's capabilities and not replace them," a company statement says. "This means our airplanes are designed so pilots are the final control authority and it means that a well trained crew is the first line of safety."

Stephen L Nicoud <stephen@Boeing.Com> bcstec!bcsaic!stephen
Boeing Computer Services Research and Technology, Bellevue, Washington USA

[Also noted by dhartung@chinet.com (Dan Hartung).]

Human vs. computer in space

Pete Mellor <pm@cs.city.ac.uk>
Tue, 27 Apr 93 19:14:13 BST

From The Guardian, Friday April 16th 1993, tabloid supplement, p3, article: ``Down to Earth with a bump'', by Tim Radford:-

------------------Begin extract----------------------

[Astronaut Mike] Collins once compared Apollo's flight to a half a million mile daisy chain, draped round the Moon. A Nasa safety engineer on an earlier voyage put it more graphically. ``Apollo 8 has 5,600,000 moving parts. Even if all functioned with 99.9 per cent reliability, we could expect 5,600 defects.'' On Apollo 11 something did go wrong, but no one now remembers it. When Armstrong and Aldrin climbed back into the module and began the checklist in preparation for blast-off, they discovered that a plastic pin which acted as a circuit breaker for the launch engine had snapped off. They decided it was because a backpack must have bumped it as they left the tiny lunar module. For a few appalling moments it must have seemed as though the nightmare had begun: marooned on the Moon, with only a day's oxygen and no way home. Aldrin poked around, and found a felt-tipped pen, and shoved it in the slot. It worked. A charge of electricity could then start the launch engine. Man had a proper place in the scheme after all. ``Where else,'' said one test pilot in the programme, ``would you get a non-linear computer weighing only 160lbs, having a billion binary decision elements, that can be mass-produced by unskilled labour?''

The classic argument of the what's-the-point lobby, which includes space administrators and big business as well as governments and scientists, and for which Lewis Mumford spoke so eloquently, is that humans in space can't do without computers, but computers can do without humans. This is almost but not quite true, and Aldrin's felt-tipped pen has written one tiny answer to that, and the same point will be made again and again: the history of unmanned space is a history of of technical flaws as well as technical triumphs. Man may not be going to Mars just yet, but he'll get there. He'll be wanted on the voyage.

But that isn't quite the point either. A manned Mars mission would be an awfully big adventure, and not just for the men who set out on it. Does anyone now think the pyramids were really a waste of money?

------------------End extract----------------------

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Spanish Computer Crime Research Association (APEDANICA)

"(Miguel Gallardo)" <gallardo@batman.fi.upm.es>
Tue, 27 Apr 1993 0:14:03 UTC+0200

During 1991 and 1992, many things happened in Spain related with computer risks. Some of them went to the Court, and many others remain in an unhealthy silence. Data stolen from banks, cryptology used by terrorist organizations, hacking, piracy, personal dossiers and blackmailing have been studied by the police, lawyers, journalists and professional technicians.

Moreover, a deep crisis in Spanish economy does not help to recover any investment in data processing. There are too many unpaid bills and half performed projects in computing. At the same time, politicians at the Parliament approved a new Law on Data Protection, and a Data Protection Agency, a Computer Police that is not clear enough who can control and how can it work.

Computer victimization is very high in Spain due to knowledge lack and technical dependency from equipment and service sellers. In an increasingly complex and critical environments, there is almost no local technology industry, and multinationals are very disconcerted because lack of expertise, expensive commercial nets, counter-productive promotional efforts, and political corruption on almost every local big business.

Since December 1992, there is an Association, APEDANICA, that can help to discover sensible troubles related with computers and communications, and its markets. Members of this non-profitable organization acts like expert witness, cryptologist, lawyers, and even as Sherlock Holmes in computer environments.

APEDANICA (ASOCIACION PARA LA PREVENCION Y ESTUDIO DE DELITOS ABUSOS Y NEGLIGENCIAS EN INFORMATICA Y COMUNICACIONES AVANZADAS), Spanish Legal Advanced Communications and Computer Crime Association, is very interested in developing relationships with any other organization with similar goals, all over the World.

Miguel A. Gallardo Ortiz, P.O. Box 17083 - E-28080 Madrid (Spain)
Tel: (341) 474 38 09 - FAX: 473 81 97 E-mail: gallardo@batman.fi.upm.es
President of APEDANICA-Spanish Legal Computer Crime Research Association

Crypto-Schemes and Mobile Digital Services (fwd)

"Lance J. Hoffman" <hoffman@seas.gwu.edu>
Wed, 28 Apr 93 6:30:36 EDT

Forwarded message:
Date: Wed, 28 Apr 93 13:03:57 EST
From: Roger.Clarke@anu.edu.au
Subject: Crypto-Schemes and Mobile Digital Services

At CFP'93, there was considerable debate about whether cryptographic schemes should be designed to be 'crackable' by national security and law enforcement agencies. The Australian situation is that the licences issued for mobile digital telephone services all require the cryptography to be crackable. Now read on ...

New digital phones on line despite objections
By BERNARD LAGAN and ANNE DAVIES
The Sydney Morning Herald, Wednesday 28 April, 1993

CANBERRA: The Federal government has over-ridden the objections of law enforcement agencies and allowed Telecom and Optus to start new digital mobile phone networks which are so secure that conversations can escape officially authorised telephone bugging.

While law enforcement agencies can still intercept calls from mobile phones to an ordinary phone, calls from one digital mobile phone to another cannot be tapped.

The Government agreed to waive the bugging requirement, originally a condition of Telecom and Optus's mobile phone network licences, late last week after strong pressure from both carriers to begin their services without providing technology to allow law enforcement agencies to listen into conversations.

The changes to the system to allow official bugging will take up to two years to complete and will cost more than $25 million, a cost which the Government has agreed to bear.

The Government's waiving of the bugging requirement was made despite strong opposition from law enforcement agencies, who wanted the start of the new digital mobile phone networks delayed until there was technology available to allow conversations conducted on these networks to be intercepted.

The law enforcement agencies argued that once criminals and others who had reason to avoid officially authorised interceptions of their telephone conversations became aware of the loopholes in the new system, they would exploit it.

The exemption was given by the Minister for Communications, Mr Beddall after talks held last week with the acting Attorney-General, Mr Kerr.

It enabled Telecom to launch the country's first digital mobile phone network yesterday.

The Federal Government is reticent about the decision to let the new network go ahead. A spokesman would only say that the Attorney-General was "satisfied" with the operational aspects of the new system.

A spokesman for Minister for Communications, Mr Beddall, said that "the matter had been resolved", and any further queries should be addressed to Telecom and Optus.

General manager of Telecom, MobileNet, Mr John Dearn, refused to confirm or deny that calls made from the new GSM (General System Mobile),mobile phones to other GSM mobile phones could not be intercepted, or that an exemption had been sought from the Government to allow the new GSM service to begin.

"We have an agreement with the Department of Communications that we will not discuss the licence conditions," he said.

Referring to the fact that most mobile phone calls are to fixed phones attached to the ordinary telephone network, Optus chief operating officer, Mr Ian Boatman said that most calls carried on Optus's GSM network would be interceptable by the security agencies.

Optus is understood to have met with the Attorney General last Thursday, and has been given similar exemptions to its licence conditions.

A third licensed operator is Vodaphone. Managing director, Mr Phillip Cornish, said: "These are Government and security matters and Vodaphone had no comment". Vodaphone is not likely to begin its service until late this year.

The three mobile licensees Telecom MobileNet, Optus and Vodaphone Australia - are 'required by their licences to introduce the new digital mobile system, or GSM, as soon as the standard is available.

However it became clear that the formula used to encode the new service, known as the A5 algorithm, was so secure that not even the police or security agencies could listen in.

The dilemma for the Government was that having insisted on the the early introduction of GSM, it faced the prospect of substantial delays if it did not waive the licence condition. Because the standard was so secure, nobody anticipated the difficulty of re-coding and re-encrypting the algorithm to give access to law enforcement agencies.

The Telecom system, costing in excess of $10O million to establish, covers more than 55 per cent of Australian consumers in Sydney, Melbourne, Canberra, Brisbane, Perth, Adelaide, the Gold Coast, Newcastle, Geelong and the Mornington Peninsula, Victoria.

Its high security - compared to the existing 018 mobile telephone network - together with greater clarity is being used by Telecom to attract new customers.

Under the 018 radio phone network, people using sophisticated scanners could pick up private conversations. But the digital technology ensures the telephone transmissions are scrambled and cannot be understood by people with scanners.

Posted by: Roger Clarke, Reader in Information Systems, Dept. of Commerce, Australian National University Roger.Clarke@anu.edu.au +61 6 249 3666/3664

How to rob a bank the cashcard way

Lord Wodehouse <w0400@ggr.co.uk>
28 Apr 93 12:11:00 BST

An article in the UK Sunday Telegrapph on 25 Apr 1993, p. 5, by Barbara Lewis, deals with the current argument that banks in the UK deny that "phantom" withdrawals happen, and all such things from ATMs are because the cashcard owner has let the PIN be revealed. The card used was a free gift from a Total garage (Total - a French petrol company), for use in a money saving offer. The PIN belonged to someone's account. By bringing the two together, and programming the card with a genuine account number taken from a discarded till receipt, Mr Clough was able to fool the machine into paying out.

The requirements included specialised computer knowledge and basic technology. A magnetic card reader and programmer costing as little as 500 pounds (750 dollars) which is capable of turning worthless blanks into cashcards. By using the details of the discard receipt, which contained the full account number, plus the details off a valid card, they were able to "break" the system. They used a machine which could not check the validity of the card with the banks central computer, and so forced validation by the information of the card itself.

From the article, the area of danger is the number of printouts with numbers of cards on them and the ability to find ATMs which are not on-line to the banks computer. They also demonstrated that a careful watcher of users of ATMs can "see" what PIN is used, pick up a receipt discarded by the same person who they watched, and then can make a usable card. The particular ATM still prints all the account number, and not all UK ATMs may work the way this banks one did, but they believe that it is a major loophole.

The banks deny that they are finding lots of "white" cards, and a spokesman for the Association for Payment Clearing Services (APCS) insisted that hat was done was impossible. It seems as usual that the banks are hiding their collective heads in the sand.

Lord John - The Programming Peer   w0400@ggr.co.uk fax - +44 81 423 4070

Re: Too much electricity (Miller, RISKS-14.55)

Mark Shanks <shanks@saifr00.cfsat.honeywell.com>
Tue, 27 Apr 93 14:58:40 MST

I will substantiate the article by J. Phillip Miller. The same circumstances occurred in Holt, Michigan, last year (1992) in the house next to my parents' (address and date available upon request): a search warrant was issued because of higher-than-neighborhood-average electric bills, a sweep by helicopter with infrared camera confirmed thermal hot spots, search of the house turned up marijuana cultivation. Evidently this is a known routine for the electric utilities, but I don't know if there is a chi-square or similar statistic they use to determine what is "substantially" higher usage.

Mark S. Shanks shanks@saifr00.cfsat.honeywel.com

Re: Risk of using too much electricity

Jim Griffith <griffith@fx.com>
Tue, 27 Apr 93 14:09:16 PDT

A similar situation occurred locally a few months back. From memory, the local police (don't remember which city) had reason to believe that an individual was cultivating marijuana in his basement, but they had insufficient grounds for a search warrant. I believe what happened is that they got a PG&E guy to read the suspect's meter, which told them that he was using a *lot* of energy. And that got them a search warrant. The issue that arises, of course, was the legality of the procedure, because the PG&E guy was technically acting as a law enforcement agent, and therefore he violated "unlawful search and seizure" laws.

Again, I'm fuzzy on the details, so take this with a grain of salt. Jim

Jim Griffith griffith@dweeb.fx.com

Risk of using too much electricity [Miller, RISKS-14.55]

Jim Huggins <huggins@eecs.umich.edu>
Wed, 28 Apr 1993 15:42:17 -0400

This is purely speculative, but I would imagine that many utilities now may have routines which flag any unusually high billing amounts and request human confirmation of the accuracy of the figures. We've all heard the stories of Mr. & Mrs. John Q. Public who received an electrical/gas/etc. bill for a couple hundred thousand dollars for their two-bedroom home and had to fight tooth-and-nail with the utility company to get them to realize that they had made a mistake. Such publicity is probably embarrassing enough for is probably embarrassing enough for the company to make a simple double-check routine worth the effort.

Jim Huggins (huggins@eecs.umich.edu)

Re: Risk of using too much electricity (RISKS DIGEST 14.55)

"Dave Bakken" <bakken@cs.arizona.edu>
Wed, 28 Apr 1993 13:24:28 MST

I knew someone who this happened to in the late 70s. He seemed to think that such monitoring of electricity was not uncommon; he was, however, not taken to court, since the police or prosecutor apparently was worried that their search was not legal. They made a verbal agreement with him that he would just stop growing pot in his house and they wouldn't press the matter.

He did mention another interesting variation on this theme. He said that in winter if the police notice that part of your roof (e.g., the attic) has no snow on it then they can (and will) legally search your house, presumably after getting a warrant. I would think that this would hold up in court.

I'm not sure how RISKy this whole subject is, however, unless the electricity monitoring was done by computer...

Dave Bakken

Risk of using too much electricity

Randall Gray <Randall.Gray@ml.csiro.au>
Fri, 30 Apr 93 08:27:08 EST

The *important* risk here is to the "old-timers" ... I suspect one PDP-8 is worth a fair number of grow-lamps ;-) I can't imagine *what* the newspapers would make of it.

Randall Gray, CSIRO Division of Fisheries, Pelagic Fisheries CSIRO Marine
Laboratories, Castray Esplanade, GPO Box 1538, Hobart, Tasmania 7001 AUSTRALIA

Utility monitoring of "Unusual use"

Edwin Culver <culver@cse.bridgeport.edu>
Wed, 28 Apr 93 11:20:53 EDT

In RISKS-14.55, J. Philip Miller (phil@wubios.wustl.edu) wondered if utilities detect "unusual" customers. I know the water company for New Haven, Connecticut asked my mother-in-law why her water usage trebled from one billing period to the next. I think that utility companies are generally expected to monitor "average" or "normal" use for when somebody protests that $1000.00 dollar gas/electric/phone/water bill.

I would be surprised if the St. Louis police could get a warrant just on the basis of high electricity use and an "unusually warm" attic. These may have been used to support statements made by an informant--say a neighbor wondering why this guy had so many visitors at 3:00am. Or the warrant may have been instigated by concerns for violations of local building codes or zoning ordinances. If the fire marshall saw marijuana plants growing in the attic while executing a warrant searching for potential fire code violations would another warrant be needed to arrest the occupant for drug violations?

Edwin M. Culver   culver@cse.bridgeport.com   (203) 468-1803

Re: Risk of using too much electricity (Miller, RISKS-14.55)

Kevin Paul Herbert <kph@cisco.com>
Tue, 27 Apr 1993 11:58:00 -0700

In California, PG&E (the electric utility in many parts of Northern California) issues press releases which indicate that they do this.

Your power company may be quite willing to tell you if they do this, if you call a public affairs office.

Kevin

Can Wiretaps Remain Cost-Effective?

Robin Hanson <hanson@ptolemy.arc.nasa.gov>
Thu, 29 Apr 93 15:32:40 PDT

U.S. Phone companies spend more than 4000 times as much running the phone system ($126b) as police spend on legal domestic phone wiretaps ($31m), to listen to phone conversations without the consent of either party. So if wiretaps are worth at most a few times what police spend on them, we can justify only the slightest modification of our phone system to accommodate wiretaps. Yet the new wiretap chip, and last year's FBI digital telephony bill, both threaten to raise our phone bills by far more than they reduce our taxes for police.

Dorothy Denning claims that wiretaps are worth "billions of dollars per year", based on amounts fined, recovered, etc. But this is just the wrong way to estimate the value of police services, according to standard texts on law enforcement economics. Instead, the value of each wiretap should be not far from how much police would be willing to pay extra for that wiretap. Given alternatives to use hidden microphones, informants, offer immunity, investigate someone else, or to raise the punishment for some crimes, it seems hard to imagine that most wiretaps would still be done if they cost police four times as much as they do now. And even if wiretaps were on average worth four times what police now pay, the option to wiretap the average phone line would be worth only six cents a month.

Yet phone companies must even now perceive substantial costs to supporting wiretaps, even relative to wanting to stay on the good side of police; why else would police be complaining about lack of support? Government policies attempting to preserve wiretaps in the face of technological change would discourage a full global market for phone systems, while government decree would displace marketplace evolution of standards for representing, encrypting, and exchanging voice. Do you think these factors would raise the average $76 monthly phone bill by more than six cents? Even the wiretap chip itself, sold for $30 each while private chips without wiretap support sell for $10, would cost people who buy a new phone every five years an extra 30 cents per month.

The central question is this: would police agencies still be willing to pay for each wiretap, if each wiretapping agency were charged its share of the full cost, to phone users, of forcing phones to support wiretaps? And why not let the market decide the answer? Currently, police must pay phone company "expenses" to support wiretaps. Let us interpret this to mean that phone companies may sell to police the option to perform legal wiretaps on given sets of phone lines, at whatever price the two parties can negotiate. Phone companies could then offer discounts to customers who use phones with wiretap chips, and each person could decide if the extra cost and risk of privacy invasion was worth the price to make life easier for the police.

If it turns out wiretaps aren't worth their cost, so be it; no big deal. Less than one part in a thousand of police budgets is spent on wiretaps, and wiretaps weren't even legal before 1968.

[For references and a more detailed discussion of these issues, ask me for my longer paper with the same title.]

Robin Hanson, MS-269-2, NASA Ames Research Center, Moffett Field, CA 94035
415-604-3361 hanson@ptolemy.arc.nasa.gov

CLIPPING CLIPPER

RISKS Forum <risks@chiron.csl.sri.com>
Thu, 29 Apr 93 19:28:22 PDT

There is an enormous amount of pending mail on the Clipper Chip. However, much of it is now third- or fourth-order incrementalism. Please excuse me if I arbitrarily cut off the discussion rather than try to cull through everything looking for a few gems. I am delighted that this issue raised such a response, and hope that the discussion in RISKS has been helpful. The last words have obviously not yet been said, but it seems silly to continue a discussion that includes considerable misinterpretations of already misleading comments. If you have something really important to add, please make it incremental to the previous discussion, and make it salient. Thanks. PGN

EICAR'93 Call for Papers

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Thu, 29 Apr 1993 18:24:36 +0200

CALL FOR CONFERENCE PAPERS AND PARTICIPATION
eicar CONFERENCE '93

When? December, 1st - 3rd 1993
Where? St. Albans, Hertfordshire, England
The Occasion: 4th Annual Eicar Conference
Submission Deadline: 31st May 1993

Following a successful event in Munich last year, the European Institute for Computer Anti-Virus Research (eicar), is holding its 1993 Conference on 1st - 3rd December.

Eicar is an independent organisation supporting and co-ordinating European activities in the areas of research, control and prevention of computer viruses and related security compromising sabotage software.

The conference will bring together users of computers and the world's leading experts and authorities in the anti-virus field along with the writers of anti-virus products that you are using such as Fridrik Skulason of Frisk - F-Prot, Joe Wells of Symantec - Norton Anti-Virus and Alan Solomon of S&S International - Dr Solomon's Anti-Virus Toolkit.

The conference covers all aspects of computer viruses and other malicious software including the following:-

- virus trends
- infection recovery tools
- network security
- backup measures
- corporate strategies
- case studies
- impact on technology
- forensic procedures
- social implications
- anti-virus technology
- anti-virus product selection
- system security
- risk assessment
- disaster recovery plans
- educational tasks
- epidemiology
- legal aspects
- ethics

Tutorial Day - an optional tutorial on computer viruses and similar SW threats
Day One - will carry two tracks covering state-of-the-art information
Day Two - continues the two tracks and concludes with a panel discussion

Call for Exhibitors

Whether or not you are considering speaking at the conference, you should at least be investigating the sales and marketing opportunities available at the exhibition. For further information on exhibiting at the conference, please contact Rebecca Pitt at the address below.

Submissions of draft papers and panel proposals should be received by Friday, 31st May 1993.

Please send your conference papers in ascii or Word for Windows, to the following address:-

Miss Alison Sweeney, Conference Manager, S&S International Limited
Berkley Court, Mill Street, Berkhamsted, Herts, HP2 4HW, England
Tel: +44 442 877877 Fax: +44 442 877882 Sands@cix.compulink.co.uk

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 57

Monday 3 May 1993

Contents

The risks of non-24-hour days

Debora Weber-Wulff <dww@math.fu-berlin.de>

Sun, 2 May 1993 12:26:02 GMT

A student told this quite believable tale about a German steel-producer last week:

The steel production line is completely automated, with the molten ingots having to cool a certain number of minutes/hours before force is applied to flatten them out. It appears the programmers of the system didn't want to construct their own clock, and so from a security point of view they used the German radio signal put out from Braunschweig (Funkuhr) that gives the exact time. This was used to calculate cooling times. In April, though, there was the day we switched to summer time, and a day with just 23 hours. 3:00 am followed 1:59 am, and the mill controller thought that the cooling time was up, and applied force - splattering still-molten steel around the place and breaking this part of the mill.

Any confirmation of this from sources other than a friend of a friend?

Debora Weber-Wulff, Technische Fachhochschule Berlin, FB Informatik,
Luxemburgerstr. 10, 1000 Berlin 65 dww@informatik.tfh-berlin.dbp.de

Flaws in government computer bond auction

Mark Seecof <marks@wimsey.latimes.com>
Sun, 2 May 93 12:32:35 -0700

On Friday 29 April 93 the Los Angeles Times reported on page D1 in a story by Robert A. Rosenblatt that the U.S. Treasury department will implement a new computerized government securities auction system even though the General Accounting Office (GAO) says it is "deeply flawed." [Paraphrasing and elisions by Mark Seecof.] The purpose of the new system is to prevent fraud and bid-rigging such as Salomon Bros. engaged in during 1990 and 1991.

"The automated network proved highly unreliable during tests of simulated auctions... In one test, five dealers 'were disconnected from the mainframe'... If this happened during an actual auction, the bids would have been lost.

"Another threat comes from the computer clock..., which 'drifts and has to be manually readjusted... This poses a potential problem for those dealers who submit bids seconds before an auction closes... For instance, should the computer clock gain time, dealers could transmit timely bids that are rejected as late.' [NNTP, anyone?]

"Because of these uncertainties, the Treasury is allowing dealers to maintain the old [paper] method of bidding despite the GAO warning that this defeats the purpose of the new network, known as the Treasury Automated Auction Processing System.

"The GAO recommended that the computer effort be delayed while a better system is devised to detect fraud and collusion... The Treasury defended its decision to proceed... 'Our position is that TAAPS has been thoroughly tested

and is ready to be put into production,' a Treasury spokeswoman said.
'Treasury considers this TAAPS program an important first step... We
deliberately chose to introduce automation to the auction process
incrementally and believe this to be a prudent approach.'"

[Mark Seecof says:]
"Prudent incrementalism." Note that this is (a) not a lie, (b) not a response
to the charge that TAAPS is "deeply flawed," and (c) not very satisfying to
the reader. Okay, so bureaucrats will "brazen it out," and implement even
"deeply flawed" systems rather than admit to development failures. Perhaps we
should start rewarding managers for NOT implementing bogus systems? Could we
devise a suitable bureaucratic scheme for doing so? On another note, could an
unethical trader with a copy of the GAO report find a way to gain some
advantage by exploiting TAAPS' flaws?

Mark Seecof <marks@latimes.com>
Los Angeles Times' Publishing Systems Dept.

Evading 1-900 blocking

John Carr <jfc@Athena.MIT.EDU>
Mon, 03 May 1993 08:30:52 EDT

A local TV news program had a story about a new type of phone sex
service. A teenage boy evaded the long distance blocking on his
parents' phone by calling a free 1-800 number and leaving his phone
number. The phone sex service called him back, collect.

The people interviewed on the show acted very shocked that this could happen,
even though the phone company said it wouldn't charge for the calls. In
particular they pointed out that the boy was not required to prove his age.
No suggestions were offered as to how he might do so over the phone.

In my opinion, they were trying to blame technology for a social problem. The
phone company is an easy target. Certainly it's easier to blame them than to
ask controversial questions like "why can't you take responsibility for your
son's actions?" or "what's wrong with talking about sex?".

I was a bit surprised that the report included the free phone number to call.
I wonder how many people will call the service after learning about it from
the news.
--John Carr (jfc@athena.mit.edu)

New Computer Virus Reported in Japan

David Fowler <fowler@oes.ca.gov>
Sat, 1 May 93 19:21:33 PDT

The Kyodo News Agency, in a story datelined Tokyo, warns of a new strain of
computer virus that is to strike computers operating under MS-DOS on the
Japanese Children's Holiday, May 5 (May 4 on this side of the International

Dateline).

Kyoto quotes the Information Technology Promotion Agency, which it describes as "a government-backed computer institute." as identifying the new virus as DApdm-13. This virus, when activated displays the English sentence, "Hey boy, do you know hide-and-seek? Play with me." The virus will then, according to Kyoto, overwrite all data and programs.

Without further elaboration, the news agency says that the virus can be removed by programs already on the market.

David Fowler, San Francisco

stunning vending machines

Edward N Kittlitz <kittlitz@world.std.com>
Fri, 30 Apr 1993 09:14:40 -0400 (EDT)

I just saw a Japanese language report from a network or program called `FNN'. Based upon the abridged subtitles, some people are stealing telephone service. This is accomplished by using a hand-held electric stun gun on a machine which vends telephone debit cards.

E. N. Kittlitz kittlitz@world.std.com

junk mail reduction request can add to your junk mail, too

"Rich Rosenbaum, rosenbaum@lkg.dec.com" <rosenbaum@tuxedo.enet.dec.com>
Sat, 1 May 93 09:29:54 EDT

The Direct Marketing Association maintains a database listing people that prefer to not receive unsolicited marketing material. I've had my name and address added to this list, hoping it would reduce my mail. It seems to have had just the opposite effect recently - I just received a mailing from Sears that begins:

> "Because you have requested through the Direct Marketing Association
> not to receive various solicitations through the mail, ..."

Rich Rosenbaum

Re: SSN for Health Identifier

John R. Levine <johnl@iecc.cambridge.ma.us>
30 Apr 93 12:37:32 EDT (Fri)

[RE a note saying that the Clinton administration seems to be leaning toward making the SSN the national health ID]

There is a thriving business in stolen SSN's so that illegal aliens can get work. The checking is now good enough that the alien needs the name that matches the SSN for the I-9 form to pass, under the bureaucratic rule of thumb that anyone who presents your name and SSN must be you.

This means that people all over the country are now being hassled by the IRS for not reporting income, typically from some place in Southern California or Texas that they've never heard of where the alien was working. There was a sidebar in the Boston Globe yesterday about a local woman who was hounded by the IRS for five years with this problem.

Until now, SSN theft could cause considerable financial pain, but it couldn't kill you. If the national health number is the SSN, this means that when someone steals your SSN and they go to the doctor, their health records will become mixed in with yours. If someone is already fairly sick, it is easy to imagine how a system depending on computerized records could misprescribe drugs or other treatment with fatal effects.

John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

Re: How to rob a bank the cashcard way (Wodehouse, RISKS-14.56)

Anthony Naggs <amn@ubik.demon.co.uk>
Fri, 30 Apr 93 13:19:08 BST

It is interesting Lord Wodehouse's contribution was published here. I had considered sending details myself, but I remembered that my similar submission last autumn was not published, (describing a report on the BBC Newsnight television programme and New Scientist magazine).

> An article in the UK Sunday Telegrapph on 25 Apr 1993, p. 5, by Barbara
> Lewis, ...

Barbara is the journalist, the deceit of the Automated Teller Machines (ATMs) was performed by Bryan Clough, and an unnamed computer expert.

The banks call this "white card fraud" because up to now most attempts have been with the plain white plastic cards supplied by vendors of the card read/write equipment. The banks only find the white cards if they are retained by the ATMs. To my knowledge all ATMs operated in the UK allow three attempts to enter the correct 4 digit PIN. If the third attempt is not validated the ATM retains the card, but after the first or second attempt you can select "cancel" or "error" and have the card returned. If you reinsert the card into the ATM it does not remember your previously failed attempts. Summary: a fraudster has to be very incompetent to let the ATM retain the card.

I spoke to Bryan Clough on Monday about this. He clarified a few of the technical aspects for me, which I hesitate to post here. A brief outline of one of the events described should be enough to worry:

1 The journalist used her cashcard to withdraw money at an ATM.

2 She placed the receipt in the bin provided.

3 Bryan Clough retrieved the receipt.

4 Bryan, and his colleague, took the receipt to a portable computer and card read/write unit, (in their car I think). They programmed 3 cards using information from other cards and the receipt.

5 Presenting each of the 3 cards to an ATM, (not at the bank that issued the card), gave these results:

   1. 10 pounds was withdrawn, debited to the journalist's account.
   2. 10 pounds was withdrawn, the journalist's account was debited with 10 pounds and 3 pence!
   3. The card was rejected as invalid, Mr Clough recovered the card by selecting "cancel".

Note, in this case the PIN was derived from the known card - only the journalist's account number was needed, not her PIN.

In a further conversation with Bryan today he told me that the (UK) Sun newspaper had a short item on this yesterday, and that he was expecting them to do another one on Saturday.

I suspect that the banks insist that this is impossible simply because the managers lack a technical understanding of the technology.

Anthony Naggs (anti-virus consultant)
email: amn@ubik.demon.co.uk   phone: +44 273 589701

Humans NOT needed to save NASA (Mellor, RISKS-14.56)

Norman, Donald <DNORMAN@applelink.apple.com>
03 May 93 01:12 GMT

A contribution to RISKS (14.56) once again repeats the propaganda that it is only through human cleverness and ingenuity that complex space missions are saved. That is sheer propaganda. Oh yes, it is true, but the stories neglect the fact that if it weren't for the requirement to keep the humans healthy and alive, the mission would be dramatically less complex and the reliability would be dramatically greater (and the cost correspondingly less). And if a space launch or two failed, it wouldn't much matter.

Reread that RISKS quote: "For a few appalling moments it must have seemed as though the nightmare had begun: marooned on the Moon, with only a day's oxygen and no way home. Aldrin poked around, and found a felt-tipped pen, and shoved it in the slot. It worked. ... Man had a proper place in the scheme after all."

Notice that the felt-tipped pen prevented the humans from being marooned. But if there were no humans on board, it wouldn't have mattered. What is all this about "Man had a proper place in the scheme after all"?

And then RISKS repeats the old joke: ``Where else,'' said one test pilot in the programme, ``would you get a non-linear computer weighing only 160 lbs, having a billion binary decision elements, that can be mass-produced by unskilled labour?'' (Actually, it is hundreds of billions of elements, and a lot more complex than binary). The problem with this old joke is not the inaccuracy of the numbers (for the correct numbers make the point of the joke even more impressive) but rather the neglect of the twenty to thirty years of training by *very highly skilled* personnel necessary to produce test pilots and the rest of us, to say nothing of the infrastructure and costs required to keep us alive during that period.

Look, folks, the main justification of humans in space is that it is a neat thing to do, that it provides new opportunities for growth, exploration, and colonization. It is probably inevitable, given human curiosity and love of new adventures. I want to do it too. But let us be honest: if you want people in space, then admit it. Justify it on those grounds. Don't lie and say that humans are needed to keep the spacecraft going -- the only reason they are needed for that purpose is because humans are on board in the first place.

There is a NASA report floating about somewhere (the old "Carl Sagan committee" -- of which I was a member -- that performed an expensive several year study of the problem and concluded just that. But the report violated NASA's goals of "man in space" and seems to have been lost in the filing cabinets.

Don Norman   Apple Computer dnorman@apple.com

re: Human vs. computer in space (Mellor, RISKS-14.56)

Craig Partridge <craig@aland.bbn.com>
Fri, 30 Apr 93 08:05:42 -0700

Page 365 of Murray and Cox's, "Apollo: The Race to the Moon", (Simon and Schuster 1989) gives a very different account. According to their version of the story, Armstrong bumped into the circuit breaker with his backpack, and the astronauts reported the damage before going out on their moon walk. During the moon walk, folks on Earth figured how to rewire some of the switches in the LEM to bypass the circuit breaker and arm the ascent engine.

So the astronauts were superfluous... :-)

Craig Partridge

Re: Human vs. computer in space (Mellor, RISKS-14.56)

ESPEN ANDERSEN <EANDERSEN@HBS.HBS.HARVARD.EDU>
30 Apr 1993 07:01:24 -0400 (EDT)

While not disagreeing with Peter Mellor's point about humans having a place in space (that is, on manned space missions), I would like to point out that his example would seem to argue for the opposite. The error that Buzz Aldrin fixed was caused by a misplaced backpack. A computer probably wouldn't do this, not because computers do not misplace things, but because in an unmanned flight there would not be any backpacks--or any switches either. In other words, the error corrected was in the user interface of the lunar module, and the correction was done by the user.

Espen Andersen (eandersen@hbs.harvard.edu)

---

re: Human vs. computer in space (Mellor, RISKS-14.56)

Scott Alexander <salex@jpl-devvax.jpl.nasa.gov>
Fri, 30 Apr 93 13:16:29 PDT

I probably have a bias in this matter working for a laboratory tasked with the robotic exploration of the solar system. Let me reiterate that I cannot speak for JPL (and that they probably disagree with at least some of this.)

It strikes me that the case cited illustrates the advantages of unmanned exploration as well as the advantages of manned exploration. If Armstrong and Aldrin hadn't been on board the module, some mission capabilities would have been lost. However, there would not have been the "nightmare" scenario in which human beings are at risk.

Given that losing humans is considered far worse than any other failure in our space program, the cost of sending humans into space is much higher than the cost of robotic exploration. This limits the number of missions flown. Moreover, the cost to the space program any time an astronaut is lost is tremendous both in terms of money and time lost to the program.

Thus, because of the costs of additional systems and redundancies to support humans and the additional weight (which adds further costs), I believe we need to very carefully choose those situations in which it is worthwhile to send humans versus those situations where sending several robots will produce wider results.

Scott Alexander salex@devvax.jpl.nasa.gov

RE: Human vs. computer in space (Mellor, RISKS-14.56)

<rmehlman%grumpy.decnet@pdsppi.igpp.ucla.edu>
Fri, 30 Apr 1993 18:44:12 PDT

In all fairness, it should be noted that the circuit breaker would not have failed if a human had not been present to brush the plastic pin with his backpack. Further, the increased complexity of *manned* spacecraft greatly increases the number of things which can fail.

The pyramids are a poor example to bring into the argument about manned space exploration. They cost more than just money.

Clipper - A dumb idea

Brian Seborg <seborg@csrc.ncsl.nist.gov>
Fri, 30 Apr 93 12:26:51 EDT

After reading the initial announcement of Clinton's support of the Clipper Chip I thought that the idea was insane! Upon reading more about the chip and following the discussions here I have to express some concern over this technology and the cost of pursuing the implementation of it in government systems. One concern that was raised was the problem that once an entity had been given the escrow key to effect a tap that they could then continue to tap any and all conversations in the future. Dorothy Denning suggested that the purchase of a new unit could be effected, or a simple chip relacement could be done to rectify this situation. I have to suggest that now hardware replacement is "simple" and I have to wonder at the cost and logistics of effecting such a replacement.

Padgett suggests that this is a sound technology whose time has come and which will offer a "good enough" encryption service. Well, I would suggest that "good enough" technology already exists, so why invest in technology which has a built in trap door? It makes no sense!

Also, I am somewhat concerned that we are already ramping up for this effort. NIST is already beginning to allocate resources to this project, as has NSA. How much is this going to cost? It seems to me that we have embarked on a trip but forgotten the map. Why would Clinton set up such a standard before trying to get some consensus from the effected parties? Or is this just a trial balloon?

I think there are many valid questions which have been raised such as who will be the consumers of this technology? What is the point of providing such a chip if criminals are unlikely to use it, or if additional layers of encryption are placed on the communications? Tapping would seem useless if this were the case, unless, as others have pointed out, other forms of encryption were made illegal. But what is the possibility of this? I'd say nil. Such a requirement would be so onerous that it would never be supported. In addition, there is no way that current vendors of encryption software and hardware would lay down while this occurred. Plus, it might not even be constitutional (potentially violating privacy, freedom of press, and expression). So I doubt that doing away with other forms of encryption is being contemplated.

So then what is the use of this chip? It may have some use as a technology, but not in the way currently described. For example, I could think of a use within a corporation. If all computers in a corporation used the encryption provided by such a chip to encrypt sensitive information and an employee left, then the escrow key could be used to get back the information which would otherwise be lost to the company. But this is not the way that is currently being pursued. And since other forms of encryption can be used to thwart tapping attempts, what is the point?

It seems to be an interesting intellectual exercise, and it may indeed have uses in corporations requiring encryption, but the idea that you would provide the "keys to the kingdom" to some currently undefined escrow authority such as the FBI or NSA or the local police will never be supported by security experts or commercial entities.

Let's all agree that we don't want to waste our tax dollars on this project and contact our congresspeople and senators to nip this project in the bud before it becomes the next government sponsored boondoggle.

Brian Seborg, VDS Advanced Research Group

Re: Worries over the Clipper Chip (Firth, RISKS-14.55)

Brinton Cooper <abc@BRL.MIL>
Fri, 30 Apr 93 13:28:21 EDT

Robert Firth, <firth@SEI.CMU.EDU>, asks

>Why should anyone worried about snoopers
>use an encryption scheme designed to allow snooping?

Answering his own question, he says

>The answer, of course, is indeed that all other encryption schemes
>must be outlawed.

When private use of end-to-end encryption is outlawed, how will it be enforced? How will the agents of the Crypto Enforcement Agency (CEA) know that two end-users are sending encrypted traffic and not just random bit streams? Will they mis-interpret binary file transfer as unauthorized use of encrypted data? Will every kermit user be subject to search of his/her premises by CEA agents, bashing in the door under authority of search warrant? Where will it all end?

_Brint

Re: Too much electricity (Miller, RISKS-14.55)

<donb@crash.cts.com>
30 Apr 93 16:33:02 GMT

In a case several years ago in the desert north of Los Angles "excessive" electricity use was the "Probable Cause" for a search warrant. The police did find pot cultivation in an underground garden. The excessive use was determined by a bill found during a raid in Bullhead City Arizona.

The part never mentioned by the press was the bill was while the house and barn were being constructed. Power for the garden was provided by a generator.

DonB

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 58

Monday 10 May 1993

Contents

---

2 Women Accused in Sale of Adoption Information

John C Slimick <slimick+@pitt.edu>
Mon, 3 May 1993 23:53:16 -0400 (EDT)

Abstracted from an AP item in the Buffalo News, May 2, 1993:

Two women accused of selling confidential information about adoptions have pleaded innocent to computer trespass, grand larceny, and other charges. State police and Department of Health officials allege that one of the women, a departmental employee, looked up confidential adoption records in state computers, then passed them onto the other defendant. The other defendant, who ran an adoption group called Birth Parents Network, then allegedly sold the information for $800 a listing to people seeking their birth parents or children.

Comment: It is notoriously difficult to break the sealed records in adoption cases. Many people use private detectives to find out what the court doesn't want them to know. Why not an end run around the records, and, at $800, it's probably cheaper than the detective.

john slimick slimick+@pitt.edu university of pittsburgh at bradford PA

Caller-ID mistakes

John H. Dale <jdale@cos.com>
Tue, 4 May 1993 23:12:22 GMT

The other evening, I received a number from an upset woman. It appears that her caller-id box told her she had just received a call from my number. The only call I had made that evening yielded me a pizza, and the number did not resemble hers. I did not ask her to described the call, because she seemed upset. But I gather I would not have wanted to be accused of making it.

Anybody know whether this happens often? Does the caller-id report include an error check? Are all boxes required to verify the check?

jdale@cos.com

A RISK of Mailing Lists?

Cal Jewell <jewell@Data-IO.COM>
Wed, 5 May 93 11:39:40 PDT

Appended to the end of this message is an announcement I received today. There's a new mailing list in town, the Risk Management and Insurance Mailing list. The new mailing list is named RISK.

Perhaps this is an example of a RISK associated with the growing use of mailing lists.

I wonder how many people, intending to subscribe to a mailing list version of the RISKS digest, will accidentally subscribe to the RISK mailing list.

Cal   jewell@Data-IO.com   ...!pilchuck!jewell

```
# Date:         Wed, 5 May 1993 11:14:55 CDT
# Reply-To: garven@UTXVM.CC.UTEXAS.EDU
# Sender: NEW-LIST - New List Announcements <NEW-LIST@VM1.NoDak.EDU>
# From: "James R. Garven" <garven@UTXVM.CC.UTEXAS.EDU>
# Subject:      NEW: RISK - Risk Management and Insurance Mailing list
#
# RISK on LISTSERV@UTXVM.CC.UTEXAS.EDU    Risk and Insurance Issues
#      or LISTSERV@UTXVM.BITNET
#
#    RISK is an electronic discussion list also known as RISKnet that will
#    allow persons around the world interested in Risk and Insurance
#    Issues to discuss matters of mutual concern.  Although RISK is a
#    moderated list, it is the intention of the moderator to facilitate a
#    "no holds barred" discussion of Risk and Insurance issues.
#    Submissions to RISK are posted and redistributed around the world to
#    all who subscribe, subject to the following constraints:
#
#    1) submitted materials must not be copyrighted;
#
#    2) submissions must be (at least remotely) related to the purposes of
#    the list as outlined below;
#
#    3) basic rules of email etiquette are expected;  i.e., character
#    assassination and/or profanity are not allowed, and neither are
#    anonymous submissions.
#
#    Possible topics for discussion on the list might include any of the
#    following:
#
#    1) Substantive discussion over topics such as corporate risk
#    management, underwriting cycles, insurance solvency and regulation,
#    insurance pricing, insurance economics, economics of legal rules,
#    liability issues, political risk, environmental risk, interactions
#    between insurance and finance, globalization of insurance markets,
#    risk perception and assessment (to name a few).
#
#    2) Comment and contributions on curriculum questions;  suggested
#    texts, new articles of common interest for course-related adoption.
#
#    3) Circulation of draft articles for comment and discussion.
#
#    4) Personal exchanges in the effort to develop a greater sense of
#    community among RISKNet colleagues.
#
#    To join RISK, send electronic mail to LISTSERV@utxvm.cc.utexas.edu
#    (or on BITNET to LISTSERV@UTXVM) and include the following message in
#    the body of your mail:
#
#      Sub RISK John Doe
#
```

```
#   (in the above command, please substitute your own name for John Doe).
#   If you have any questions, please free to contact the owner.
#
#   Owner and Editor:  James R. Garven   garven@utxvm.cc.utexas.edu
#                    Department of Finance
#                    University of Texas at Austin
#                    Austin, TX  78712
#                    USA
#
#   Editor's Note:  Do not confuse the RISK list described above with
#   the RISKS list peered at several sites.  The RISK list is about
#   insurance.  The RISKS list is on issues related to the public use
#   of computer systems.  mgh
```

[ugh. pgn]

Analog vs Digital Speedometers

Martin Minow <minow@apple.com>
Tue, 4 May 93 09:50:41 -0700

I'm not sure if this is worth a Risks posting, but it's an interesting bit of information.

(From alt.folklore.computers, posted by tmoore@bnr.ca)
In article <1993Apr30.214944.25568@dcc.uchile.cl> mlopez@inf.utfsm.cl (Mauricio Antonio Lopez Gutierrez) writes:
>Paul Raveling (raveling@Unify.com) wrote:
<>In article <C5uu7y.2u7y@austin.ibm.com>, guyd@austin.ibm.com (Guy Dawson) writes:
<>>
<>> In our race car we use an analog tach for the driver and record
<>> the telemetry data digitally.
<>>
<>> As for accuracy, the unit is VERY accurate. Internally the system is
<>> digital and drives a stepper motor to which the needle is attached.
<>> This is factory calibrated. The stepper motor mans that the needle
<>> does not bounce around when the driver clips a curb or generally goofs.

<>   Much of this debate is based on opinion only and has little
<> data to back it up.

In the case of a watch it doesn't matter whether it is analogue or digital, for most people most of the time a quarter hour counter will do. In fact the minute hand is really not needed and was omitted from early clocks, the time between the hours was estimated.

In the case of a speedometer the speeds to which one is driving (eg usually the limit) do matter. I was involved in research (yes the evil deed of getting real data) for Ford in Britain and we found that a digital, numeric readout, even in poor seven segment characters was uniformly at least as good and most times better than an analogue display. We found this effect in photographic presentations, a simulator and on the road with a $100,000 prototype. We knew from the "ergonomics" literature that an analogue display was supposed to be better for check reading and estimation but we failed to find what we expected even though the tests were sometimes biased to find out if such an effect occurred. Furthermore, older people preferred this display because the numbers were now so large that it was not necessary to focus on them as much as was necessary to see a needle (especially at night). The time taken to interpret the numeric display was "swamped" by the ease of reading it allowing people to look back at the road during the interpretation time. When we presented the results to a conference the German and Japanese auto researchers rushed back to their labs to do the research which only we had "bothered" to do. Never assume that "common sense" is enough when people's lives may be at stake.

Call the Institute of Consumer Research (ICE) in England (phone
011-44-509-236161 or fax 610725) for further details.

Census imposters invading Cary

George Entenman <ge@mcnc.org>
Fri, 7 May 93 08:32:50 -0400

I found this article in the newspaper last week. It's obvious that the story describes an attempt to "fish for information" on us, but I would like to know what questions you netters think these "census takers" might be asking. The simplest answer is that they are casing the joint to find out how many VCR's and how much jewelry people own, when they are at home, etc. But is there any other data that would have less tangible risks? SSNs, for example?
George Entenman ge@mcnc.org

Census imposters invading Cary, by Beverly Brown, Staff writer
The News and Observer, Saturday, May 1, 1993, Page 7B [Abstracted by PGN]

Cary [NC] - Beware of nosy people at your door claiming to be census workers. They probably aren't. Police Chief David Fortson said several residents have complained about people identifying themselves as census employees and proceeding to ask questions.

Eighty legitimate census workers - carrying red, white and blue identification cards - won't start going door-to-door until May 20, when the town begins conducting a special census. Cary, at odds with the Census Bureau over the town's 1990 census, commissioned a special head-count last year. The latest census says the fast-growing town has a few more than 43,000 residents. But the town estimates that at least 48,000 people call Cary home. At stake are millions of dollars in state funding, allocated on the basis of population.
For a new count, which will involve a week-long canvass, census workers will limit their questions to name, age, race, sex, national origin and relationship to the homeowner.

Fortson said the imposters most likely are opportunists, using public knowledge about the town's forthcoming count as a chance to fish for information. "There are all kinds of things going on in terms of scams," he said. "Perhaps this is another way for folks to pull off a scam. I just don't know."

Computer Problem reveals tax details

John Gray <phyjwdg@vaxb.hw.ac.uk>
Thu, 6 May 93 15:45:40 BST

"The Scotsman", 6th May, reports an incident affecting possibly as many as "a couple of thousand" households in East Kilbride, near Glasgow. Residents have received information on council tax rebates (for low income and invalidity benefit claimants) relating to their neighbours.

Apparently, the computer "broke down" midway through printing the 900,000 bills being issued, and after the computer was restarted, the problem occurred. Apparently, the rebate information on the FRONT of the bill was correct, but that the calculation on the BACK related to the next household (apparently the bills are issued in order of address).

Presumably, when the computer crashed, it ejected one half-printed bill, and proceeded to pair the front and back pages wrongly for the remainder of the run.

A council official said that most families would not be directly identified [though if you know that they live next door....]. The only names in bills would be those of "non-dependents" such as lodgers.

[We had an almost identical case a few years back. PGN]

Videoconferencing Bridge Likes Muscular Lungs

Shyamal Jajodia <SHYAM@mitvmc.mit.edu>
Mon, 03 May 93 14:29:21 EDT

In the April 1993 issue of the MIT Information Systems magazine there is a description of a videoconferencing system. Apparently, in a multi-site conference, each site must call a bridge, or hub, which then acts as the traffic controller for transmission to and from the participating sites. The risk is in the bridge design:

> The bridge relies on voice activation to determine which site to show more or less on the principle that whoever talks the loudest gets seen"

Does this system contravene the Americans with Disabilities Act? I never knew that lung power would some day make me more visible.

Shyamal Jajodia (MIT)

Anonymous <nowhere@bsu-cs.bsu.edu>
Fri, 7 May 93 11:18:17 -0500

This text was forwarded to me by a friend and professional colleague in the UK. I am dismayed that this type of activity is being condoned by an American Governmental Agency. I can only hope that this operation is shut down and the responsible parties are reprimanded. I am extremely disturbed by the thought that my tax money is being used for, what I consider, unethical, immoral and possibly illegal activities.

---- begin forwarded message -------------

AIS BBS Capture log.

To: all interested parties, especially Americans who may wish to ask relevant questions of relevant people.

Capture log from a BBS that claims to be run by the US Treasury Department, Bureau of the Public Debt. Notice - I have not verified that the US government is actually running this BBS, only that the BBS claims that it is.

The capture was made live. I have cut out parts where the same area was visited twice, and the information is identical. Also cut out, is any information that could lead to the caller being identified, as the caller wishes to retain privacy. If indeed this is being run by the US Government, the caller would not wish to be harassed by that organisation.

Also omitted are the "More" prompts for paging the display. And, after the first few displays of the main menu, some of those have also been omitted for brevity.

The file 27-ASM.ZIP was downloaded, to check that there really were source codes. In fact, there were mostly recompilable disassemblies, some good, some bad. I've included, at the end of this file, the beginning of 512.ASM, a disassembly of Number of the Beast. But I've only included the header, the first couple of instructions (discover Dos version) and the end (the '666'). All the meat of the code, I've omitted for brevity, and because this capture is likely to become publicly available.

[portions deleted containing high-order ascii]

```
Bureau of Public Debt, OnLine Information System, AIS Files System

Select: A

File Areas: ----------

  4 ... UNDERGROUND-NEWSLTRS         5 ... UNDERGROUND-PHREAKING
  6 ... UNDERGROUND-HACKING          7 ... UNDERGROUND-VIRUS
  8 ... ABOVEGROUND-POLICY           9 ... ABOVEGROUND-TRAINING
 10 ... ABOVEGROUND-UTILITIES       11 ... ABOVEGROUND-VIRUSES
 12 ... ABOVEGROUND-BULLETINS       13 ... ABOVEGROUND-CRYPTO
 14 ... ABOVEGROUND-MISC            15 ... ABOVEGROUND-NEWSLTR
 17 ... BULLETINS (Non-Current)
```

```
Select area: 7

                    U.S. Treasury Department
                Current File Area : UNDERGROUND-VIRUS

        ZDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD?
        3   [A]  Area Change          [R]  Raw Directory      3
        3   [L]  Locate by Keyword      [W]  Wild Card Search   3
        3   [F]  File List            [B]  Browse a Txt File  3
        3   [N]  New Files            [*]  Main Menu          3
        3   [D]  Download (Global)      [G]  Goodbye            3
        3   [U]  Upload                                  3
        @DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDY
         To request an access level upgrade leave a message for
                        Mary Clark

Bureau of Public Debt     OnLine Information System     AIS Files System

Select: F


Press P to Pause, S to Stop

27-ASM.ZIP    137207 18-02-93  27 ASM files, incl. 1260, 4096, etc.
541.ZIP         3321 25-08-92  541 in ASM
AIDS.ZIP        2065 25-08-92  AIDS in PASCAL
AIRCOP.ZIP      2081 25-08-92  Aircop in ASM
ANTHRAX.ZIP     3688 25-08-92  Anthrax in ASM
ASM.ZIP       183429 25-08-92  Source code for 51 viruses
BLOODY.ZIP      3037 25-08-92  Bloody in ASM
BOB.ZIP         3221 25-08-92  Bob virus in ASM
BOBVIRUS.ZIP    5812 25-08-92  Bob virus in ASM
BOOT.ZIP       25975 25-08-92  Source code for 13 viruses
CANCER.ZIP      1270 25-08-92  Cancer in ASM
CONTEST.ZIP     7680 11-02-93  M. Ludwig's Virus Writing Contest Rules
CRAZY.ZIP        514 25-08-92  Crazy in C
CVIR_C.ZIP      2621 25-08-92  Cvirus in C
CVIRUS.ZIP      3656 25-08-92  CVirus in ASM
DETH001.ROT     4661 08-03-93  Megadeth's Guide to Virus Research part I
-
                        Virii
DETH002.ROT     2662 08-03-93  Megadeth's Guide to Virus Research part II
-
                        Trojans
GRITHER.ZIP     2393 25-08-92  Grither in ASM
GUIDES.ZIP     35541 25-08-92  "How-To" for the budding virus writer
ITALIANS.ZIP    4659 25-08-92  Italiano source in ASM
ITTI-A.ZIP      1589 25-08-92  Itti-Bitti A in ASM
ITTI-B.ZIP      1310 25-08-92  Itti-Bitti B in ASM
LEPROSY.ZIP     2983 25-08-92  Leprosy in C
LEPROSYB.ZIP    4024 25-08-92  Leprosy strain B in ASM
MARAUDER.ZIP    3511 25-08-92  Marauder in ASM
MTE-SRC.ZIP    14272 18-04-92  A supposed disassembly of the Mutation
```

```
Engine
MTE91B.ZIP     12719 29-06-92  Dark Avenger's Mutation Engine
MUSICBUG.ZIP    3322 01-01-93  Music Bug in ???
N1.ZIP          1986 25-08-92  Number One in PASCAL
NEWINSTL.ZIP  161536 25-08-92  Nowhere Man's Virus Creation Lab (PKUNZip
                               1.93)
PEBBLE.ZIP      1454 25-08-92  Pebble in ASM
PS-MPC90.ZIP   41802 31-07-92  Phalcon/Skism Mass Produced Code Generator

SAT-BUG.ZIP    18158 25-02-93  Source Code of a poly-virus
SATNLH.ZIP      2137 25-08-92  Satan's Little Helper in ASM
SHHS.ZIP        2922 25-08-92  South Houston High School in ASM
STONEDII.ARJ    2377 26-03-93  The Stoned 2 virus w/ source
VBASEABC.ZIP  242816 05-02-93  New, accurate virus info database
VCL.ZIP       167472 21-07-92  Nowhere Man's GUI based Virus Creation Lab
                               <Chiba City>
VIRULIST.ZIP  168192 25-08-92  40-Odd Viruses in ASM
VIRUS.ZIP       3191 25-08-92  Virus source in ASM
WORM.ZIP        1110 28-10-92  Internet Worm source code in "C"
XMAS.ZIP         892 25-08-92  Christmas in ???
TPE11.ZIP       7747 23-12-92  Trident Polymorphic Engine ver 1.1

Press (Enter) to continue:
```

[remainder deleted]

------ end of forwarded text --------

I submit this text in an anonymous fashion for fear of reprisal.
I respectfully request that Ken van Wyk and Peter G. Nuemann allow
that it be posted to both VIRUS-L and RISKS Digests. I think the
risks of Government sponsored virus exchange are crystal clear.

Quis Custodiet Ipsos Custodes?

Pyramids in space (Mehlman, RISKS-14.57)

Wayne Throop <throop@aurw44.aur.alcatel.com>
Tue, 4 May 93 12:36:43 -0400

: The pyramids are a poor example to bring into the argument about manned
: space exploration. They cost more than just money.

It's not just cost. After all, manned space exploration costs more than just money, too. It's that, with a few thousand years of hindsight, pyramids *were* a remarkably stupid thing to do with those resources. If I thought that manned space flight was "like" building the pyramids, I'd immediately say "flush it". I mean, was it *really* sensible to build those structures, when the only thing that the heirs of all this effort find practical to do with it is to mine the dressing stones from the surface, recover the burial goods, and promote tourism income?

Hmmmmmm. Do you suppose there were those who said "well, just look at the technological spinoffs! We now can pile large stone slabs up with joints you can't fit a knife into! We can build structures of enormous size with incredibly accurate right angles!"?

Bogus then. Bogus now.

Don't get me wrong, I don't suppose that there are no adequate justifications for manned space exploration. It's just that the argument that "it'll turn out to be just as good an investment as the pyramids" is a remarkably poor one, roughly like saying that "He's evewy bit as good a wabbit hunter as Elmer Fudd."

So what's the computer risk here? Perhaps the oldest of them all. The risk of being impressed by spinning tape drives or blinking lights or neat rows of numbers on printout. Which is, after all, a variant of the very human risk of being impressed by appearance rather than substance.

Wayne Throop throopw%sheol@concert.net

Re: Epilepsy and video games

Antonella Dalessandro <daless@di.unipi.it>
Thu, 6 May 93 16:25:42 METDST

There have been a few postings in the past on alleged pathological (esp. neurological) conditions induced by playing video games (e.g., Nintendo). Apparently, there have been reported several cases of "photosensitive epilepsy", due to the flashing of some patterns and the strong attention of the (young) players. One poster to comp.risks reported some action from the British Government.

A quick search in a database reported the following two published references:

1. E.J. Hart, Nintendo epilepsy, in New England J. of Med., 322(20), 1473
2. TK Daneshmend et al., Dark Warrior epilepsy, BMJ 1982; 284:1751-2.

I would appreciate if someone could post (or e-mail) any reference to (preferably published) further work on the subject. Any pointer to other information and/or to possible technical tools (if any) for reducing the risks are appreciated.

Many thanks,

Antonella D'Alessandro, Pisa -- Italy. daless@di.unipi.it

Re: Humans NOT needed to save NASA (Norman, RISKS-14.57)

Flint Pellett <flint@gistdev.gist.com>

4 May 93 14:31:15 GMT

>A contribution to RISKS (14.56) once again repeats the propaganda that it is
>only through human cleverness and ingenuity that complex space missions are
>saved. That is sheer propaganda.

Even though I'm personally in favor of sending men into space, I don't think they are required or desirable for every mission, and this recent example just cited, if anything, is hardly a strong case in favor of manned missions. Think: if you hadn't had the men there to bump the plastic part and break it in the first place, you wouldn't have had any problem that needed a man to fix. You also need to be careful not to read too much into the "cleverness/ingenuity" issues: a man on the ground could have been just as clever and directed a fairly simple robot arm to insert the felt tip pen. There are examples where having a man there saved the mission, but this wasn't one of them, and economically you'd be a lot farther ahead if you had twice as many unmanned missions (costing half as much) even if 25% of them did fail.

If you want some hard facts, consider the amount that we have spent recently trying to get a working toilet, and how much time was spent trying to fix it. Without men there, you don't need toilets.

Flint Pellett, Global Information Systems Technology, Inc., 100 Trade Centre
Drive, Suite 301, Champaign, IL 61820 (217) 352-1165 uunet!gistdev!flint

Re: Junk mail reduction request can add to your junk mail, too

Steve Mick <smick@llnl.gov>
Fri, 7 May 1993 12:22:46 -0800

Direct mail marketers are, of course, interested in "targeting" their mailings to recipients in known categories such as Porsche owners or toad collectors. I have long felt that if you request that the Direct Marketing Association put your name on the "no unsolicited material" database, you would eventually be categorized as a person interested in privacy issues and mailbox pollution.

Steve Mick, smick@llnl.gov

Re: China executes hacker (RISKS-14.57)

Jonathan Bowen, Oxford University <Jonathan.Bowen@prg.ox.ac.uk>
Fri, 7 May 93 12:14:34 BST

From the front page of "Computing", a weekly UK newspaper, 6 May 1993:

> China executes hacker over #122,000 [UK pounds] theft
>
> The Chinese government said this week it had executed convicted hacker
> Shi Biao as a warning to others that computer crime does not pay.
> Biao, who worked as an accountant at the Agricultural Bank of China,

embezzled more that #122,000 [UK pounds] over three months in 1991 by forging bank-deposit slips. He was caught when he and an accomplice tried to transfer some of the money to the province of Shenzhen in southern China.

Re: Evading 1-900 blocking (Carr, RISKS-14.57)

David A Willcox <willcox@urbana.mcd.mot.com>
Tue, 4 May 1993 16:25:29 GMT

I think that if the owner of a phone line wanted to communicate with sexually explicit services (whether 900 numbers or anything else), he or she should be required to request, in writing, that those services be enabled. (Hey, the phone company could charge for the service!) If you've got kids and don't want to talk dirty on the phone yourself, you do nothing. If you don't have kids, then you can sign up. If you have kids and sign up, then it is up to you to deal with keeping your kids out of it. But the bottom line would be that services would be obligated to reject calls from any line that had not explicitly requested access to such services.

>In my opinion, they were trying to blame technology for a social problem...

There are technological issues here. My own son got involved with one of these "services" recently, and am glad to hear that others are upset about it. A couple of points:

(1) When you call this supposedly free 800-number, you don't have to "leave your phone number", the company gets it automatically when you call. You get a recorded number telling you to hang up. You then get an automatic, collect callback.

(2) The callback apparently doesn't require any explicit response to enable the collect call. If you stay on the line for more than a few seconds, you are charged. There is no mention of how much the call will cost.

To answer your last question:

(1) There is nothing wrong with "talking about sex." However, I do think that there is something wrong with adults describing explicit sex acts to a preteen child. We do discuss sex with our kids, and assume that they discuss it with their friends (in terms rather different than we do with them :-)), but I certainly wouldn't take any of them to a hardcore porno movie.

(2) There is pretty much a consensus in our society that children should not have free access to sexually explicit materials. I may be overstating this, but consider what would happen to an "adult" bookstore owner who sold materials to minors (or at least young minors). I feel that anyone distributing such materials, whether in a store, by mail, or electronically, has the obligation to take reasonable steps to ensure that the recipient is of "reasonable" age.

(3) We will take responsibility for what our son knew he was doing.
called, that we (and he) will take responsibility for. (He called some
other, regular long distance numbers with recorded messages, and has
repaid us for them.) However, I am not happy about this end run around
900-number blocking that turns a supposedly-free phone call into a
charged call.

(The company in question did eliminate the charge, by the way, when informed that they had made a collect, obscene phone call to a minor child. I kind of wish that they hadn't been so accommodating. I was ready to make a very big stink.)

An interesting side effect to all of this. Since our little incident, I have been getting some very unusual mail, not even in a "pain brown wrapper." I had never realized that calling a 1-800 number could put you onto a mailing list!

David A. Willcox, Motorola MCG - Urbana, 1101 E. University Ave., Urbana, IL
61801 217-384-8534 ...!uiucuxc!udc!willcox willcox@urbana.mcd.mot.com

Re: Utility-derived information

Phil Agre <pagre@weber.ucsd.edu>
Mon, 3 May 1993 17:38:46 -0700

Here is the reference for a detailed San Jose Mercury on the use of utility information by the police to detect marijuana growers etc. The article is more generally about the highly developed practice of informal personal-data sharing among various public and private organizations in the San Jose area.

Gary Webb, Utilities give cops data on their customers, San Jose Mercury News, 27 December 1992, pages A1, A21.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 59

Tuesday 11 May 1993

Contents

Worst Computer Nightmare Contest (fwd)

"Arthur R. McGee" <amcgee@netcom.com>
Sat, 8 May 1993 08:44:37 -0700 (PDT)

---------- Forwarded message ----------
Date: Fri, 7 May 1993 09:48:07 -0400
From: ssteele@eff.org (Shari)
Subject: Worst Computer Nightmare Contest

COMPUTER NIGHTMARES
The San Diego Computer Fair '93 is looking for the most awful, woeful tale of "abuse suffered by a human at the hands of a computer." The suffering human will win a weekend in beautiful San Diego to try and forget that horrible episode in his or her life. Send your 1,000 word submission to Computer Nightmare Contest, ComputerEdge Magazine, P.O. Box 83086, San Diego CA 92138.

IFIP resolution on demeaning games

Richard Wexelblat <rlw@ida.org>
Mon, 3 May 93 13:13:06 EDT

According to the "Newstrack" in CACM (2/93; p.13), IFIP has adopted a resolution condemning the production, distribution, and use of computer games that demean human beings and advocate malicious behavior by the players. The resolution points to the growth of brutal war games, sexist games, and games based on themes of racial, ethnic, or religious hatred. The document states: "IFIP appeals to everybody worldwide to censure harmful games, to raise awareness of the issues involved, and to support only computer games that respect human dignity."

(Does anyone know the origin of the issue within IFIP or whether a more complete description exists.)

[I hope everyone catches de meaning. PGN]

Fake ATM Machine Steals PINs

<eric@cadkey.com>
Tue, 11 May 93 10:52:57 -0400

Everyone knows you're supposed to be VERY careful about not revealing your PIN number for your ATM card. How are you supposed to stop this new trick??? At the Buckland Hills Mall, in Manchester CT, last week, some scam artists installed a fake ATM machine. They had negotiated with the Mall officers, pretending to be Bank officials, and had gotten permission. Apparently, they even got the phone company to come in and lay down some lines. Then, they installed an ATM machine they had stolen.

It was programmed to read off the account numbers, remember the PIN as it was typed, then claim some kind of error and refuse to give out money. They left the machine in the mall for a WEEK, collecting PINs, then they came back, took it machine back to "repair", and have since printed up new cards, and have been using the PINs to siphon off money.....

Why didn't I think of that??

[New trick? This is one of the oldest scams going, but it still recurs. PGN]

Teller Users Beware

<tapper@aero.org>
Mon, 10 May 93 12:52:56 PDT

Any of you that use an automated telephone transaction system to do your banking (or to make balance inquiries, etc.) may be interested in an experience I had today.

I dialed in and was connected to a session in progress that belonged to another user (who probably hung up after receiving whatever information he/she requested). I immediately transferred all their money into my account...no just kidding :) I would hate to think that might happen to me, especially since some of these services allow you to move money around.

I would like to suggest to anyone using these type of services (including voice-mail services) to back all the way out of the system before hanging up. Some systems (like Aerospace voice-mail) allow you to disconnect via a command, before hanging up, but many do not. My banking system does not allow me to disconnect without hanging up, but it does allow me to back out of the menus until I reach the main menu which prompts for user password before proceeding. From now on I'm going to make sure I back out to that level before hanging up.

Signed,

Could-have-been-rich.

[Another old classic. The TENEX undetected-hangup problem years ago had similar properties, leaving a dial-up port still active, waiting for the next dial-up to randomly stumble upon a logged-in user session. PGN]

More on Census imposters invading Cary (RISKS-14.58)

George Entenman <ge@mcnc.org>
Mon, 10 May 93 12:32:57 -0400

Saturday's News and Observer had a little article saying that the Census workers in Cary might really have been working for the US Census Bureau.

[But George's item does suggest that there is a problem anyway! PGN]

NIST Advisory Board Seeks Comments on Crypto

Clipper-Capstone Chip Info <clipper@csrc.ncsl.nist.gov>
Tue, 11 May 93 13:42:18 EDT

Note: This file has been posted to the following groups:
    RISKS Forum, Privacy Forum, Sci.crypt, Alt.privacy.clipper

and will be made available for anonymous ftp from csrc.ncsl.nist.gov, filename pub/nistgen/cryptmtg.txt and for download from the NIST Computer Security BBS, 301-948-5717, filename cryptmtg.txt.

Note: The following notice is scheduled to appear in the Federal Register this week. The notice announces a meeting of the Computer System Security and Privacy Advisory Board (established by the Computer Security Act of 1987) and solicits public and industry comments on a wide range of cryptographic issues. Please note that submissions due by 4:00 p.m. May 27, 1993.

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

Announcing a Meeting of the
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

AGENCY: National Institute of Standards and Technology

ACTION: Notice of Open Meeting

SUMMARY: Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App., notice is hereby given that the Computer System Security and Privacy Advisory Board will meet Wednesday, June 2, 1993, from 9:00 a.m. to 5:00 p.m., Thursday, June 3, 1993, from 9:00 a.m. to 5:00 p.m., and Friday, June 4, 1993 from 9:00 a.m. to 1:00 p.m. The Advisory Board was established by the Computer Security Act of 1987 (P.L. 100-235) to advise the Secretary of Commerce and the Director of NIST on security and privacy issues pertaining to Federal computer systems and report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. All sessions will be open to the public.

DATES: The meeting will be held on June 2-4 1993. On June 2 and 3, 1993 the meeting will take place from 9:00 a.m. to 5:00 p.m. and on June 4, 1993 from 9:00 a.m. to 1:00 p.m.

Public submissions (as described below) are due by 4:00 p.m. (EDT) May 27, 1993 to allow for sufficient time for distribution to and review by Board members.

ADDRESS: The meeting will take place at the National Institute of Standards and Technology, Gaithersburg, MD. On June 2, 1993, the meeting will be held in the Administration Building, "Red Auditorium," on June 3 the meeting will be held in the Administration Building, "Green Auditorium," and on June 4, 1993 in the Administration Building, Lecture Room "B."

Submissions (as described below), including copyright waiver if required, should be addressed to: Cryptographic Issue Statements, Computer System Security and Privacy Advisory Board, Technology Building, Room B-154, National Institute of Standards and Technology, Gaithersburg, MD, 20899 or via FAX to 301/948-1784. Submissions, including copyright waiver if required, may also be sent electronically to "crypto@csrc.ncsl.nist.gov".

AGENDA:

- Welcome and Review of Meeting Agenda
- Government-developed "Key Escrow" Chip Announcement Review
- Discussion of Escrowed Cryptographic Key Technologies
- Review of Submitted Issue Papers
- Position Presentations & Discussion
- Public Participation
- Annual Report and Pending Business

- Close

PUBLIC PARTICIPATION:

This Advisory Board meeting will be devoted to the issue of the Administration's recently announced government-developed "key escrow" chip cryptographic technology and, more broadly, to public use of cryptography and government cryptographic policies and regulations. The Board has been asked by NIST to obtain public comments on this matter for submission to NIST for the national review that the Administration's has announced it will conduct of cryptographic-related issues. Therefore, the Board is interested in: 1) obtaining public views and reactions to the government-developed "key escrow" chip technology announcement, "key escrow" technology generally, and government cryptographic policies and regulations 2) hearing selected summaries of written views that have been submitted, and 3) conducting a general discussion of these issues in public.

The Board solicits all interested parties to submit well-written, concise issue papers, position statements, and background materials on areas such as those listed below. Industry input is particularly encouraged in addressing the questions below.

Because of the volume of responses expected, submittors are asked to identify the issues above to which their submission(s) are responsive. Submittors should be aware that copyrighted documents cannot be accepted unless a written waiver is included concurrently with the submission to allow NIST to reproduce the material. Also, company proprietary information should not be included, since submissions will be made publicly available.

This meeting specifically will not be a tutorial or briefing on technical details of the government-developed "key escrow" chip or escrowed cryptographic key technologies. Those wishing to address the Board and/or submit written position statements are requested to be thoroughly familiar with the topic and to have concise, well-formulated opinions on its societal ramifications.

Issues on which comments are sought include the following:

1. CRYPTOGRAPHIC POLICIES AND SOCIAL/PUBLIC POLICY ISSUES

Public and Social policy aspects of the government-developed "key escrow" chip and, more generally, escrowed key technology and government cryptographic policies.

Issues involved in balancing various interests affected by government cryptographic policies.

2. LEGAL AND CONSTITUTIONAL ISSUES

Consequences of the government-developed "key escrow" chip technology and, more generally, key escrow technology and government cryptographic policies.

3. INDIVIDUAL PRIVACY

Issues and impacts of cryptographic-related statutes, regulations, and standards, both national and international, upon individual privacy.

Issues related to the privacy impacts of the government-developed "key escrow" chip and "key escrow" technology generally.

4. QUESTIONS DIRECTED TO AMERICAN INDUSTRY

4.A Industry Questions: U.S. Export Controls

4.A.1 Exports - General

What has been the impact on industry of past export controls on products with password and data security features for voice or data?

Can such an impact, if any, be quantified in terms of lost export sales or market share? If yes, please provide that impact.

How many exports involving cryptographic products did you attempt over the last five years? How many were denied? What reason was given for denial?

Can you provide documentation of sales of cryptographic equipment which were lost to a foreign competitor, due solely to U.S. Export Regulations.

What are the current market trends for the export sales of information security devices implemented in hardware solutions? For software solutions?

4.A.2 Exports - Software

If the U.S. software producers of mass market or general purpose software (word processing, spreadsheets, operating environments, accounting, graphics, etc.) are prohibited from exporting such packages with file encryption capabilities, what foreign competitors in what countries are able and willing to take foreign market share from U.S. producers by supplying file encryption capabilities?

What is the impact on the export market share and dollar sales of the U.S. software industry if a relatively inexpensive hardware solution for voice or data encryption is available such as the government-developed "key escrow" chip?

What has been the impact of U.S. export controls on COMPUTER UTILITIES software packages such as Norton Utilities and PCTools?

What has been the impact of U.S. export controls on exporters of OTHER SOFTWARE PACKAGES (e.g., word processing) containing file encryption capabilities?

What information does industry have that Data Encryption Standard (DES) based software programs are widely available abroad in software applications programs?

4.A.3 Exports - Hardware

Measured in dollar sales, units, and transactions, what have been
the historic exports for:

Standard telephone sets
Cellular telephone sets
Personal computers and work stations
FAX machines
Modems
Telephone switches

What are the projected export sales of these products if there is no change in export control policy and if the government- developed "key escrow" chip is not made available to industry?

What are the projected export sales of these products if the government-developed "key escrow" chip is installed in the above products, the above products are freely available at an additional price of no more than $25.00, and the above products are exported WITHOUT ADDITIONAL LICENSING REQUIREMENTS?

What are the projected export sales of these products if the government-developed "key escrow" chip is installed in the above products, the above products are freely available at an additional price of no more than $25.00, and the above products are to be exported WITH AN ITAR MUNITIONS LICENSING REQUIREMENT for all destinations?

What are the projected export sales of these products if the government-developed "key escrow" chip is installed in the above products, the above products are freely available at an additional price of no more than $25.00, and the above products are to be exported WITH A DEPARTMENT OF COMMERCE LICENSING REQUIREMENT for all destinations?

4.A.4 Exports - Advanced Telecommunications

What has been the impact on industry of past export controls on other advanced telecommunications products?

Can such an impact on the export of other advanced telecommunications products, if any, be quantified in terms of lost export sales or market share? If yes, provide that impact.

4.B Industry Questions: Foreign Import/Export Regulations

How do regulations of foreign countries affect the import and export of products containing cryptographic functions? Specific examples of countries and regulations will prove useful.

4.C Industry Questions: Customer Requirements for Cryptography

What are current and future customer requirements for information security by function and industry? For example, what are current and future customer requirements for domestic banking, international banking, funds transfer systems, automatic teller systems, payroll records, financial information, business plans, competitive strategy plans, cost analyses, research and development records, technology trade secrets, personal privacy for voice communications, and so forth? What might be good sources of such data?

What impact do U.S. Government mandated information security standards for defense contracts have upon demands by other commercial users for information security systems in the U.S.? In foreign markets?

What threats are your product designed to protect against? What threats do you consider unaddressed?

What demand do you foresee for a) cryptographic only products, and b) products incorporating cryptography in: 1) the domestic market, 2) in the foreign-only market, and 3) in the global market?

4.D Industry Questions: Standards

If the European Community were to announce a non-DES, non-public key European Community Encryption Standard (ECES), how would your company react? Include the new standard in product line? Withdraw from the market? Wait and see?

What are the impacts of government cryptographic standards on U.S. industry (e.g., Federal Information Processing Standard 46-1 [the Data Encryption Standard] and the proposed Digital Signature Standard)?

5. QUESTIONS DIRECTED TO THE AMERICAN BUSINESS COMMUNITY

5.A American Business: Threats and Security Requirements

Describe, in detail, the threat(s), to which you are exposed and which you believe cryptographic solutions can address.

Please provide actual incidents of U.S. business experiences with economic espionage which could have been thwarted by applications of cryptographic technologies.

What are the relevant standards of care that businesses must apply to safeguard information and what are the sources of those standards other than Federal standards for government contractors?

What are U.S. business experiences with the use of cryptography to protect against economic espionage, (including current and projected investment levels in cryptographic products)?

5.B American Business: Use of Cryptography

Describe the types of cryptographic products now in use by your organization. Describe the protection they provide (e.g., data encryption or data integrity through digital signatures). Please indicate how these products are being used.

Describe any problems you have encountered in finding, installing, operating, importing, or exporting cryptographic devices.

Describe current and future uses of cryptographic technology to protect commercial information (including types of information being protected and against what threats).

Which factors in the list below inhibit your use of cryptographic products?

Please rank:

```
--    no need
--    no appropriate product on market
--    fear of interoperability problems
--    regulatory concerns
--       a) U.S. export laws
--       b) foreign country regulations
--       c) other
--    cost of equipment
--    cost of operation
--    other
```

Please comment on any of these factors.

In your opinion, what is the one most important unaddressed need involving cryptographic technology?

Please provide your views on the adequacy of the government-developed "key escrow" chip technological approach for the protection of all your international voice and data communication requirements. Comments on other U.S. Government cryptographic standards?

6. OTHER

Please describe any other impacts arising from Federal government cryptographic policies and regulations.

Please describe any other impacts upon the Federal government in the protection of unclassified computer systems.

Are there any other comments you wish to share?

The Board agenda will include a period of time, not to exceed ten hours, for oral presentations of summaries of selected written statements submitted to the Board by May 27, 1993. As appropriate and to the extent possible, speakers addressing the same topic will be grouped together. Speakers, prescheduled by the Secretariat and notified in advance, will be allotted fifteen to thirty minutes to orally present their written statements. Individuals and organizations submitting written materials are requested to advise the Secretariat if they would be interested in orally summarizing their materials for the Board at the meeting.

Another period of time, not to exceed one hour, will be reserved for oral comments and questions from the public. Each speaker will be allotted up to five minutes; it will be necessary to strictly control the length of

presentations to maximize public participation and the number of
presentations.

Except as provided for above, participation in the Board's discussions during the meeting will be at the discretion of the Designated Federal Official.

Approximately thirty seats will be available for the public, including three seats reserved for the media. Seats will be available on a first-come, first-served basis.

FOR FURTHER INFORMATION CONTACT: Mr. Lynn McNulty, Executive Secretary and
Associate Director for Computer Security, Computer Systems Laboratory,
National Institute of Standards and Technology, Building 225, Room B154,
Gaithersburg, Maryland 20899, telephone: (301) 975-3240.

SUPPLEMENTARY INFORMATION: Background information on the government-developed "key escrow" chip proposal is available from the Board Secretariat; see address in "for further information" section. Also, information on the government-developed "key escrow" chip is available electronically from the NIST computer security bulletin board, phone 301-948-5717.

The Board intends to stress the public and social policy aspects, the legal and Constitutional consequences of this technology, and the impacts upon American business and industry during its meeting.

It is the Board's intention to create, as a product of this meeting, a publicly available digest of the important points of discussion, conclusions (if any) that might be reached, and an inventory of the policy issues that need to be considered by the government. Within the procedures described above, public participation is encouraged and solicited.

/signed/
Raymond G. Kammer, Acting Director

May 10, 1993

New NIST/NSA Revelations

Dave Banisar <banisar@washofc.cpsr.org>
Thu, 6 May 1993 19:24:06 EST

Less than three weeks after the White House announced a controversial initiative to secure the nation's electronic communications with government-approved cryptography, newly released documents raise serious questions about the process that gave rise to the administration's proposal. The documents, released by the National Institute of Standards and Technology (NIST) in response to a Freedom of Information Act lawsuit, suggest that the super-secret National Security Agency (NSA) dominates the process of establishing security standards for civilian computer systems in contravention of the intent of legislation Congress enacted in 1987.

The released material concerns the development of the Digital

Signature Standard (DSS), a cryptographic method for authenticating the identity of the sender of an electronic communication and for authenticating the integrity of the data in that communication. NIST publicly proposed the DSS in August 1991 and initially made no mention of any NSA role in developing the standard, which was intended for use in unclassified, civilian communications systems. NIST finally conceded that NSA had, in fact, developed the technology after Computer Professionals for Social Responsibility (CPSR) filed suit against the agency for withholding relevant documents. The proposed DSS was widely criticized within the computer industry for its perceived weak security and inferiority to an existing authentication technology known as the RSA algorithm. Many observers have speculated that the RSA technique was disfavored by NSA because it was, in fact, more secure than the NSA-proposed algorithm and because the RSA technique could also be used to encrypt data very securely.

The newly-disclosed documents -- released in heavily censored form at the insistence of NSA -- suggest that NSA was not merely involved in the development process, but dominated it. NIST and NSA worked together on the DSS through an intra-agency Technical Working Group (TWG). The documents suggest that the NIST-NSA relationship was contentious, with NSA insisting upon secrecy throughout the deliberations. A NIST report dated January 31, 1990, states that

> The members of the TWG acknowledged that the efforts expended to date in the determination of a public key algorithm which would be publicly known have not been successful. It's increasingly evident that it is difficult, if not impossible, to reconcile the concerns and requirements of NSA, NIST and the general public through using this approach.

The civilian agency's frustration is also apparent in a July 21, 1990, memo from the NIST members of the TWG to NIST director John W. Lyons. The memo suggests that "national security" concerns hampered efforts to develop a standard:

> THE NIST/NSA Technical Working Group (TWG) has held 18 meetings over the past 13 months. A part of every meeting has focused on the NIST intent to develop a Public Key Standard Algorithm Standard. We are convinced that the TWG process has reached a point where continuing discussions of the public key issue will yield only marginal results. Simply stated, we believe that over the past 13 months we have explored the technical and national security equity issues to the point where a decision is required on the future direction of digital signature standards.

An October 19, 1990, NIST memo discussing possible patent issues surrounding DSS noted that those questions would need to be addressed "if we ever get our NSA problem settled."

Although much of the material remains classified and withheld from disclosure, the "NSA problem" was apparently the intelligence agency's demand that perceived "national security" considerations take precedence in the development of the DSS. From the outset, NSA cloaked the deliberations in secrecy. For instance, at the March 22, 1990, meeting of the TWG, NSA representatives presented NIST with NSA's classified proposal for a DSS algorithm. NIST's report of the meeting notes that

> The second document, classified TOP SECRET CODEWORD, was a position paper which discussed reasons for the selection of the algorithms identified in the first document. This document is available at NSA for review by properly cleared senior NIST officials.

In other words, NSA presented highly classified material to NIST justifying NSA's selection of the proposed algorithm -- an algorithm intended to protect and authenticate unclassified information in civilian computer systems. The material was so highly classified that "properly cleared senior NIST officials" were required to view the material at NSA's facilities.

These disclosures are disturbing for two reasons. First, the process as revealed in the documents contravenes the intent of Congress embodied in the Computer Security Act of 1987. Through that legislation, Congress intended to remove NSA from the process of developing civilian computer security standards and to place that responsibility with NIST, a civilian agency. Congress expressed a particular concern that NSA, a military intelligence agency, would improperly limit public access to information in a manner incompatible with civilian standard setting. The House Report on the legislation noted that NSA's

> natural tendency to restrict and even deny access to information that it deems important would disqualify that agency from being put in charge of the protection of non-national security information in the view of many officials in the civilian agencies and the private sector.

While the Computer Security Act contemplated that NSA would provide NIST with "technical assistance" in the development of civilian standards, the newly released documents demonstrate that NSA has crossed that line and dominates the development process.

The second reason why this material is significant is because of what it reveals about the process that gave rise to the so- called "Clipper" chip proposed by the administration earlier this month. Once again, NIST was identified as the agency actually proposing the new encryption technology, with "technical assistance" from NSA. Once again, the underlying information concerning the development process is classified. DSS was the first test of the Computer Security Act's division of labor between NIST and NSA. Clipper comes out of the same "collaborative" process. The newly released documents suggest that NSA continues to dominate the government's work on computer security and to cloak the process in secrecy, contrary to the clear intent of Congress.

On the day the Clipper initiative was announced, CPSR submitted FOIA requests to key agencies -- including NIST and NSA -- for information concerning the proposal. CPSR will pursue those requests, as well as the pending litigation concerning NSA involvement in the development of the Digital Signature Standard. Before any meaningful debate can occur on the direction of cryptography policy, essential government information must be made public -- as Congress intended when it passed the Computer Security Act. CPSR is committed to that goal.

David L. Sobel, CPSR Legal Counsel, (202) 544-9240 dsobel@washofc.cpsr.org

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 60

Wednesday 12 May 1993

Contents

Risks of anonymity and credulity

Michael Friedman <mfriedma@us.oracle.com>
Tue, 11 May 93 11:13:39 PDT

In Risks V14, No 58, an anonymous person submitted a claim from another person, who also wished to remain anonymous, that a bulletin board calling itself AIS BBS and claiming to be an official activity of the US Treasury Department, exists and makes virus code available for downloads. Our anonymous poster apparently believes this -

>I am dismayed that this type of activity is being condoned by an American
>Governmental Agency. I can only hope that this operation is shut down and the
>responsible parties are reprimanded. I am extremely disturbed by the thought
>that my tax money is being used for, what I consider, unethical, immoral and
>possibly illegal activities.

I know that most of the people reading this list are a little paranoid about risks, but this is ridiculous. The anonymous submitter did not provide the phone number of the BBS so there is no way we can check the claims, but, even if it exists, does anyone seriously believe that it is being run by the Treasury Department? I fully believe that our government sometimes does things that are stupid, immoral, and illegal, but this isn't the kind of stupidity that they do.

In short, we need to be critical thinkers. In addition, we need to think about the way in which anonymous posting lets things like this get widely disseminated without exposing the original poster to embarrassment and ridicule. The next hoax, lie, or distortion from an anonymous source may not be this obvious. Is the ability to anonymously make this kind of claim a risk?

IFIP resolution on demeaning games

"Barbara B. Simons" <simons@almaden.ibm.com>
Tue, 11 May 93 15:58:04 PDT

ACM Council issued the following statement on computer games a couple of years ago. I believe that, unfortunately, there has been no follow-up.

Barbara

> The pool of potential female and minority scientists and engineers remains virtually untapped, despite demographic trends pointing to the urgent need to train substantial new talent from these sectors. There are products, such as computer games, which are the first significant introduction to technology for most young people. Many girls and minority children do not identify with most of these products which are currently on the market.
>
> It is in society's best interest that these products attract and be accessible to these children.
>
> Through the appropriate mechanisms, ACM will form a proactive interest group which will address these concerns.

Thoreau on Pyramids and Space (Re: RISKS-14.58)

victor yodaiken <yodaiken@chelm.cs.umass.edu>
Mon, 10 May 1993 20:48:20 -0400

In regard to the questions about the value of space travel and pyramids, nobody has mentioned the definitive words of the great engineer (graphite and pencil manufacturing) and philosopher H. Thoreau. They are:

> As for the Pyramids, there is nothing to wonder at in them so much
> as the fact that so many men could be found degraded enough to spend
> their lives constructing a tomb for some ambitious booby, whom it
> would have been wiser and manlier to have drowned in the Nile, and
> then given his body to the dogs. (from Walden)

In fact, the whole chapter called "Economy" is filled with such gems. One more I just have to quote:

> Many are concerned about the monuments of the West and the East, -
> to know who built them. For my part, I should like to know who in
> those days did not build them, - who were above such trifling. But
> to proceed with my statistics.

yodaiken@chelm.cs.umass.edu

⌁Fake ATM Machine Steals PINs (Eric, RISKS-14.59)

K. M. Peterson <KMP@Logos.Prime.COM>
12 May 1993 11:57:08 EDT

[An ATM Trojan Horse of a Different Feather. More on the fragmentary report of Eric's... PGN]

Excerpted from the Boston _Globe_ 12May93. Yankee 24 is a New England ATM network.

"Fake ATM plays gotcha with users"

[AP] MANCHESTER, Conn. -- Some computer-literate thieves stole thousands of dollars by setting up a bogus automatic teller machine in a mall and using it to make counterfeit bank cards, authorities said. The mobile machine, rolled into the Buckland Hills Mall about two weeks ago dispensed money for a time, but eventually ran out, said Manchester police spokesman Gary Wood.

While customers were using the machine, the ATM recorded their account numbers and personal identification codes, authorities said. The thieves then made counterfeit band cards encoded with account information and used them to withdraw money from ATMs in New York City operated by Citibank and Chemical Bank.

About $3,000 in fraudulent withdrawals from the ATMs were discovered by late Monday, said Richard L. Yanak, president of the Yankee 23 ATM network. The withdrawals were made from accounts based at three Hartford area banks. ...

The bogus machine was once an authentic ATM that the thieves either stole of acquired on the used market, Yanak said. Unsuspecting customers were forced to use the 5-foot machine after at least one of the mall's two legitimate ATMs was sabotaged with glue-covered plastic cards.

The scam was uncovered when a local bank found that someone had tried seven or eight times to use one of its bank cards at a New York ATM -- either because of a problem with the card or because the thief tried to withdraw more than the account's limit, Yanak said.

Officials never gave their direct permission to install the machine, [Margaret] Steeves [Yankee 24's marketing director] said. Police believe the thieves returned to the mall on Sunday night or early Monday morning to retrieve the machine. Steeves said ATM customers are protected under federal banking regulations, which limit their liability to $50 if their loss is reported within 48 hours.

K. M. Peterson Systems/Network Management Group, Computervision Corp.

Re: Fake ATM Machine Steals PINs (Eric, RISKS-14.59)

Al Donaldson <al@escom.com>
Wed, 12 May 93 11:24:53 EDT

The new twist on the scam was that this "ATM machine" dispensed money. According to the radio news report I heard yesterday, it gave out "some cash to forestall suspicion that something was wrong."

Re: Epilepsy and video games

Larry Hunter <hunter@work.nlm.nih.gov>
11 May 93 10:19:26

Antonella Dalessandro asks for recent citations on pathological conditions induced by playing video games. Most of the articles I found in a Medline search were about the use of video games as therapy (e.g. for schizophrenics or the developmentally disabled) or in experimental use (e.g. assessing reaction time or attention). However, I did find two major articles on video game pathology from 1990, and some followups and letters since.

TI - Reflex seizures induced by calculation, card or board games, and
     spatial tasks: a review of 25 patients and delineation of the
     epileptic syndrome.
SO - Neurology 1990 Aug;40(8):1171-6
AB - Nine patients had reflex activation of seizures by calculation,
     card and board games, or spatial tasks. The common denominator
     for these and the 16 others reported in the literature appears to
     be activity related to function of the parietal lobe. The
     clinical and EEG findings in all 25 patients support the
     diagnosis of primary generalized epilepsy. Seizures usually start
     during adolescence and consist of myoclonus, absences, and
     generalized convulsions. Specific inquiry about reflex activation
     should be carried out in patients with generalized epilepsy since
     this is rarely provided spontaneously. Attacks could be
     controlled satisfactorily in 89% of our patients. The genetic
     features are those of a primary generalized epileptic disorder

without evidence for a specific inheritance of reflex sensitivity. Neuropsychological analysis of the stimuli points to parietal cortical dysfunction. These stimuli lead to activation of a generalized epileptic process analogous to the occipital cortical participation in the activation of generalized epileptic abnormality occurring in patients with photosensitive epilepsy.

TI - Electroclinical study of video-game epilepsy.
SO - Dev Med Child Neurol 1990 Jun;32(6):493-500
AB - Seven patients (five boys, two girls) with video-game epilepsy (VGE) are reported, which reflects the fact that these games have increased in popularity recently among Japanese children. Their ages at onset ranged from four to 13 years. The seizure phenomena were of three types: generalised tonic-clonic, partial seizure and headache. Interictal physical and neurological examinations were within normal limits. EEGs taken while they played video-games confirmed the diagnosis of VGE and revealed three triggers of seizures: flashing lights, special figure patterns and scene-changing. They were recommended to avoid playing video-games, but sodium valproate was effective if seizures persisted even after such avoidance.

TI - Video games: benign or malignant?
SO - J Dev Behav Pediatr 1992 Feb;13(1):53-4

TI - Nintendo surgery [letter]
SO - JAMA 1992 May 6;267(17):2329-30

TI - Nintendo elbow [letter]
SO - West J Med 1992 Jun;156(6):667-8

TI - Nintendo neck [letter]
SO - Can Med Assoc J 1991 Nov 15;145(10):1202

TI - Nintendo enuresis [letter]
SO - Am J Dis Child 1991 Oct;145(10):1094

TI - Nintendo power [letter]
SO - Am J Dis Child 1990 Sep;144(9):959

TI - Nintendo epilepsy [letter]
SO - N Engl J Med 1990 May 17;322(20):1473

Lawrence Hunter, PhD., National Library of Medicine, Bldg. 38A, MS-54
Bethesda. MD 20894 USA tel: +1 (301) 496-9300 fax: +1 (301) 496-0673

Re: Epilepsy and video games (Dalessandro, RISKS-14.58)

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
11 May 93 22:56:41 EDT

A quick scan of the Ziff-Davis Computer Database Plus, available on CompuServe, using the text words "epilep* AND seizure*" revealed the following references:

1 Australia - video games cleared in epilepsy scare., Newsbytes, March 4, 1993 pNEW03040007. Reference # A13669571 Text: Yes (1234 chars) Abstract: No

2 Japan: Nintendo to research epilepsy & video games., Newsbytes, Feb 17, 1993 pNEW02170003. Reference # A13668827 Text: Yes (1314 chars) Abstract: No

3 Trivial pursuits. ('Cyberzone' television program) (Technology)(Virtual Reality), Computer Weekly, Jan 28, 1993 p28(1). Reference # A13428978 Text: Yes (5116 chars) Abstract: Yes

4 Military contractor converts to more civilian production. (Israel Aircraft Industries), Industrial Engineering, Jan 1993 v25 n1 p28(2). Reference # A13472137 Text: Yes (5019 chars) Abstract: Yes

5 User interfaces: where the rubber meets the road. (Cover Story), Computers in Healthcare, Feb 1993 v14 n2 p16(5). Reference # A13394186 Text: Yes (12409 chars) Abstract: Yes

6 Is TV game harmful to children? British boy dead. (television-based video games), Newsbytes, Jan 11, 1993 pNEW01110003. Reference # A13355402 Text: Yes (1920 chars) Abstract: No

7 Wandering through the brain: the power of a "magic wand" helps neurosurgeons prepare for complicated procedures. (Applications), Computer Graphics World, Oct 1992 v15 n10 p71(2). Reference # A12816647 Text: Yes (8554 chars) Abstract: Yes

8 The Epilog System: automated long-term EEG monitoring for epilepsy. (electroencephalogram)(includes related articles on valid data keys and the volume of data generated by EEGs), Computer, Sept 1992 v25 n9 p5(10). Reference # A12717601 Text: No Abstract: Yes

9 Picture this: wide-ranging developments in data acquisition methods add a new dimension to computer-based medical imaging. (includes related articles on medical image terminology, digital video fluoroscopy and one-dimensional magnetic resonance imaging), Computer Graphics World, Sept 1992 v15 n9 p43(8). Reference # A12672713 Text: Yes (32524 chars) Abstract: Yes

10 Letters. (Letter to the Editor), PC Magazine, August 1992 v11 n14 p19(4). Reference # A12436301 Text: Yes (10284 chars) Abstract: No

11 No-Squint II. (SkiSoft Publishing Corp.'s No-Squint II 1.0 utility program to enhance cursor size on portable computers) (Software Review), Home Office Computing, Sept 1991 v9 n9 p58(1). Reference # A11203289 Text: Yes (1550 chars) Abstract: No

12 Fascinating rhythm: we can reap more from computers that respond to our rhythmical nature., Computer Graphics World, August 1990 v13 n8 p117(4). Reference # A8733680 Text: Yes (7735 chars) Abstract: Yes

13 Are we having fun yet? (ennui among programmers) (Bit by Bit) (column),

Computer Language, August 1990 v7 n8 p113(4). Reference # A8761856 Text: Yes (8946 chars) Abstract: Yes

14 Word processing. (Real Time), Personal Computing, August 1990 v14 n8 p49(2). Reference # A8719958 Text: Yes (4262 chars) Abstract: Yes

15 This SkiSoft word processor is a welcome sight for sore eyes., PC-Computing, March 1990 v3 n3 p56(1). Reference # A8171802 Text: Yes (1448 chars) Abstract: No

16 IBM's research division at work on diverse projects., InfoWorld, July 3, 1989 v11 n27 p37(1). Reference # A7412002 Text: No Abstract: Yes

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Association Carlisle, PA.

Mobile ComSec in Europe (A5)

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Mon, 3 May 1993 19:27:33 +0200

Stimulated by the "Cripple Clipper" Chip discussions, I invested some time to investigate the European approach in this area. Mobile communication security is practically available, since some time, in Western Europe based on some technology which will now alsp be applied in Australia [see Roger Clarke: Risk Forum 14.56). In contacts with people from producers, carriers and Telecom research, I collected the following facts:

- Dominated by Western European telecommunications enterprises, a CCITT subsidiary (CEPT=Conference Europeenne des Administrations des Postes et des Telecommunications; founded 1959, presently 26 European countries, mainly from Western/Northern Europe) formed a subgroup (ETSI=European Telecommunications Standards Institute) which specified, in a special Memorandum of Understanding (MoU) the GSM standard (=Groupe Special Mobile). Presently, ETSI (planned as EEC's Standardisation Institute in this area) has 250 members from industry (63%), carrier (14%), government (10%), appliers and research (together 10%). Research here means essentially Telecom and related "research" institutes.

- GSM documents specify roughly the functional characteristics including secure encryption of transmitted digital messages (see "European digital cellular telecommunication system (phase 2): Security Related Network Functions"). Apart from protocols, details of algorithms are secret.

- GSM contains 3 secret algorithms (only given to experts with established need-to-know, esp. carriers or manufacturers):
    Algorithm A3: Authentication algorithm,
    Algorithm A8: Cipher Key Generator (essentially a 1-way function),
        and
    Algorithm A5: Ciphering/Deciphering algorithm (presently A5/1,A5/2).
  Used in proper sequence, this set of algorithms shall guarantee that

NOBODY can break the encrypted communication.

- Mobile stations are equipped with a chipcard containing A3 and A8, plus an ASIC containing A5; the (non-mobile) base stations (from where the communication flows into the land-based lines) is equipped with an ASIC realising A5 encryption, and it is connected with an "authentication center" using (ASIC, potentially software based) A3 and A8 algorithms to authenticate the mobile participant and generate a session key.

- When a secure communication is started (with the chipcard inserted in the mobile station), authentication of the mobile participant is performed by encrypting the individual subscriber key Ki (and some random seed exchanged between the mobile and base station) with A3 and sending this to the base station where it is checked against the stored identity. Length of Ki: 128 bit.

- If authenticated, the individual subscriber key Ki (plus some random seed exchanged between mobile and basis station) is used to generate a session key Kc; length of Kc: 64 bit. Different from Clipper, a session key may be used for more than one session, dependent on the setting of a flag at generation time; evidently, this feature allows to minimize communication delays from the authentication process.

- Using session key (Kc), the data stream (e.g. digitized voice) is encrypted using the A5 algorithm and properly decrypted at base station.

- A more complex authentication procedure including exchange of IMSI (International Mobile Subscriber Identity) may be used to authenticate the subscriber and at the same time to generate the session key (using a combined "A38" algorithm) and transmit it back to the mobile station.

Comparing the European A5 approach with US' "Cripple Clipper Chip", I find some surprising basic similarities (apart from minor technical differences, such as key lengths and using ASICs only versus Chipcard in the mobile station):

1) Both approaches apply the "SbO Principle" (Security by Obscurity): "what outsiders don't know, is secure!" Or formulated differently: only insiders can know whether it contains built-in trapdoors or whether it is really secure!

2) Both approaches aim at protecting their hemisphere (in the European case, including some interest spheres such as "down-under", to serve the distinguished British taste:-) from other hemispheres' competition.

The most significant differences are:

A) that US government tries to masquerade the economic arguments with some legalistic phrases ("protect citizen's privacy AND protect them against criminal misuse") whereas Western Europeans must not argue as everybody knows the dominance of EEC's economic arguments (and the sad situation of privacy in most EEC countries :-)

B) that US government must produce the rather complex "escrow agencies" where European law enforcers must only deal with ETSI (manufacturers and carriers!) about reduced safety in "A5/n" algorithms (n=1,2,...).

Presently, different "A5/n" algorithms are discussed. Apart from the "secure" original algorithm A5 (now labeled A5/1), a "less secure, export oriented A5/2" has been specified (according to my source which may not be fully informed, this will go to "down-under" :-). One argument for such "A5/n" multiplicity is that availability of more A5/n algorithms may even allow to select, during authentication, one algorithm from the set thus improving security of communication; at the same time, as these algorithms are secret, the secret automatic selection (e.g. triggered by some obscure function similar to the random exchange in the authentication process) may allow to crack the encrypted message.

My (contemporary) conclusion is that security of both A5 and CC is questionable as long as their security cannot be assessed by independent experts. In both cases, economic interests seem to play a dominant role; there are clear indications of forthcoming economic "competition", and I wonder which side Japan will take (maybe they decide to start their own crippled SecureCom standard?)

Klaus Brunnstein (Univ Hamburg; May 3, 1993)

"Security&Control of IT in Society"

<brunnstein@rz.informatik.uni-hamburg.dbp.de>
Mon, 3 May 1993 18:33:16 +0200

SECURITY AND CONTROL OF INFORMATION TECHNOLOGY IN SOCIETY
An IFIP WG 9.6 Working Conference to explore the issues:
August 12 - 17, 1993

Venue: the conference ship M/S Ilich between Stockholm and St.Petersburg

Dependence on information technology (IT) is widespread. IT is used for the option and control of a range of social, industrial, commercial, governmental and regulatory processes, yet it introduces new potential threats to personal privacy and freedom, and new opportunities for criminal activity. These dangers have to be countered and controlled in a manner that balances the benefits of IT. Therefore careful consideration has to be given to determine what constitutes the most effective control and regulation of IT. Such topics should be high on national agendas.

IFIP's Working Group on Information Technology Misuse and the Law (WG 9.6) is holding a working conference to explore these issues, from 12 to 17 August, aboard the conference ship M/S Ilich between Stockholm and St.Petersburg. On the Saturday of the conference week the conference will convene in St.Petersburg for meetings with Russian representatives, providing a valuable opportunity to discuss some of the problems of IT in an emerging capitalist economy.

The conference, Security and Control of Information Technology, will explore major issues, including particular reference to Eastern European Economies. The organisers are keen to attract people representing a wide range of interests, including central government, regulatory bodies, information system users, relevant public interest groups, the legal profession, and academics. Participants from all parts of Europe and beyond will be welcome. In addition to full conference papers there will be discussion groups and shorter presentations.

Eur. Ing. Richard Sizer (UK), chairman of WG 9.6, is conference chairman, Dr. Louise Yngstrom (Sweden) is in charge of local organisation and Prof. Martin Wasik is chairman of the International Programme Committee. The proceedings will be published by Elsevier North Holland and edited by Ing. Sizer, Prof. M. Wasik and Prof. R. Kaspersen (Netherlands).

Those desiring to attend the conference and requiring further information may contact Prof. Wasik at:

Faculty of Law, Manchester University, Manchester M13 9PL, U.K.,
Tel. +44 61 275 3594, Fax +44 61 275 3579.

or for local arrangements, contact Ann-Marie Bodor at:
Dept of Computer ans Systems Sciences, Stockholm University/KTH,
Electrum 230, Sweden, Tel +46 8 162000, Fax +46 8 7039025.

CONFERENCE PROGRAMME

Thursday Evening, August 12

Opening presentation: "The law cannot help"

A debate led by K.Brunnstein (Germany) and R.Kaspersen (Netherlands)
Chairman: Eur. Ing. Richard Sizer (U.K.)

Friday Morning, August 13

Paper 1: "Privacy and Computing: a Cultural Perspective"
R.Lundheim, G.Sindre (Norway)

Paper 2: "Is International Law on Security of Information Systems Emerging ?"
B.Spruyt, B.de Schutter (Belgium)

Paper 3: "On the cutting edge between Privacy and Security"
J.Holvast, R.Ketelaar (Netherlands),
S.Fischer-Huebner (Germany)

Paper 4: "Protection of the Information of Organisations in the Asia-Pacific region"
M.Jackson (Australia)

Friday Afternoon: Two Discussion Streams

Stream 1: International cultural perspectives on IT, privacy and security
(led by J.Holvast)

Stream 2: Priorities for IT in emerging economies (led by R.Kaspersen)

Saturday August 14

Part I: "IT and Security in Russia. Experts view"

"IT and Security in Russia"
E.V. Evtyushin (Russian Agency for New Information)

"IT vs. Security in Russia"
E.A. Musaev (Russian Academy of Sciences)

"Problems of information protection in the Northwestern region of Russia"
P.A. Kuznetsov (Association for Information Protection)

Part II: "IT and Security in Russia - Commercial sector"

TBD (Sberbank of Russia)
TBD (St Petersburg Chamber of Commerce)

Part III: "It and Security in Russia - Public Sector"

TBD (Public Sector)

Part IV: "Western Developments in IT-Security"

R.Hackworth (U.K.): "The OECD Guidelines on IT Security"
M.Abrams (USA): "From Orange Book to new US Criteria"
P.White (U.K.): "Drafting Security Policies"
TBD "INFOSEC Security Issues in the EC"

Sunday August 15: Tour of St.Petersburg

Monday Morning, August 16

Paper 5: "Recent development in IT security evaluation"
K.Rannenberg (Germany)

Paper 6: "On the formal specification of security requirements"
A.Jones, M.Sergot (Norway)

Paper 7: "Symbiosis of IT security standards"
M.Abrams (USA)

Paper 8: "An Academic Programme for IT Security"
L.Yngstrom (Sweden)

Monday Afternoon: Two workshops based on:

Workshop 1:

Paper 9: "Are US Computer Crime Laws Adequate ?"
L.Young (USA)

Paper 10:"Computer Crime in Slovakia ?"
J.Dragonev, J.Vyskoc (Slovakia)

Paper 11:"Computer Crime Coroners for an IT Society"
S.Kowalski (Sweden)

Workshop 2:

Paper 12:"Computer supported security intelligence"
I.Orci (Sweden)

Paper 13:"Design for security functions of chipcard software"
K.Dippel (Germany)

Paper 14: "Court ordered wiretapping in USA"
G.Turner (USA)

CLOSING DISCUSSION AND CONCLUSIONS, Chairman: R.Sizer (U.K)

(TBD: Speakers to be decided. Details of conference sessions are subject to change)

The costs of attending the conference are now set as follows:

One delegate: 4175 Swedish Krona
Two delegates sharing one cabin: 3275 Swedish Krona (per person)
Accompanying person: 3175 Swedish Krona (no conference proceedings)

These prices include accommodation, all meals on board of the M/S Ilich and while in St.Petersburg, an excursion on Sunday and, for delegates, a copy of all conference papers. Cabins on the ship each have a window and a shower.

Cheques or money orders (in Swedish Krona) should be made payable to the account: "Foriningen for Sakerhetsinformatik: IFIP WG 9.6" and sent as soon as possible and, in any event, not later than June 11, to:

Ann-Marie Bodor, Dept. of Computer and Systems Sciences
Stockholm University/KTH, Electrum 230, S-164 40 Kista, Sweden

All registrations are responsible for making their own arrangements for travel to and from Stockholm, and for their visas and insurance. Registrations most probably cannot be accepted after June 11 due to the booking deadline for the cabins on board.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 61

Saturday 15 May 1993

Contents

Opel Corsa Stops for Mobile Phones

Gulbrandsen <oysteing@taskon.no>
Fri, 14 May 93 09:09:52 +0200

>From Motor, the Norwegian AAA monthly:

While testing the new Opel Corsa, we brought along a mobile phone. One conversation was enough to kill the motor completely. The phone was of the new nordic 450-system, and the antenna was in the front seat. At first we took it for a coincidence, but it proved to be repeatable: when calling out or receiving a call, the car abruptly halted. The signals from the phone apparently confused the electronics in the car.

When we later moved the antennae to the back seat, we only felt a slight "tug" from the engine, and with the antennae on the roof, there was no ill effect. The importer has passed the message to Opel, Germany, and we expect it to be fixed ASAP, he says.

The translation is by me, but I hope the meaning gets through. [TNX. PGN]

\ystein Gulbrandsen   Taskon A/S

Re: Analog vs Digital Speedometers

Roger Crew <crew@CS.Stanford.EDU>
Wed, 12 May 93 00:14:22 PDT

Digital speedometers have other interesting properties.

I am reminded of one night when I was out driving on one of the more desolate portions of [...pick your favorite interstate...], noticed another car going absurdly fast and decided to follow it for a bit to see just how fast (...well okay, I had just recently bought my car and was about to yield to the temptation to "push the envelope" a bit...).

The speed turned out to be 85 mph. Oddly enough, the speed remained quite constant. For the first few minutes, I attributed this to the other car having a very good cruise control. I thought it was rather stupid to be setting a cruise control that high, but then, who was I to talk?

A bit more thought and observation revealed that my speed was quite independent of what I was doing with my accelerator pedal or the general terrain I was driving on. I let up on the gas quite abruptly and this time could actually feel the car slowing down --- and still I was going 85 mph.

At this point I noticed the tachometer descending through 4000 rpm and decided I had definitely had enough fun for one night. And then I remembered...

My car is 1982 model. In 1982 there was a federal (US) law in force forbidding speedometers from showing speeds higher than 85 mph. This is all well and good if you have an analog speedometer and can SEE the needle PEGGED against the upper end.

It had never occurred to me until that moment that someone would actually build a digital speedometer that pegs.

(very) shortly thereafter I had gotten down to a relatively sedate 50mph with 2000 rpm on the tachometer. The rest is left as an exercise for the reader...

Roger Crew crew@CS.Stanford.EDU

Re: New NIST/NSA Revelations

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Wed, 12 May 93 10:20:42 EDT

David Sobel, CPSR Legal Council, wrote in RISKS DIGEST 14.59:

> The proposed DSS was widely criticized within the computer
> industry for its perceived weak security and inferiority to an
> existing authentication technology known as the RSA algorithm.
> Many observers have speculated that the RSA technique was

> disfavored by NSA because it was, in fact, more secure than the NSA-proposed algorithm and because the RSA technique could also be used to encrypt data very securely.

This is terribly misleading. NIST issued the DSS proposal along with a public call for comments as part of their normal practice with proposed standards. The community responded, and NIST promptly addressed the security concerns. Among other things, the DSS now accommodates longer keys (up to 1024 bits). As a result of the revisions, the DSS is now considered to be just as strong as RSA.

Dorothy Denning

Clipper - A Trojan Horse

Bill Nicholls <billn@bix.com>
12 May 1993 13:11:05 -0400 (EDT)

I've been following the discussion in RISKS about the Clipper chip with great interest, and have learned a lot about what is planned as well as what weaknesses may exist, and why. But I have gradually become aware of an uneasy feeling, as though I was missing something important about this chip.

After some thought about the situation, I have come to the conclusion that Clipper is in fact a Trojan Horse, in the classic sense. This morning I was thinking about why anyone would use the Clipper chip when existing software security could be much better than what Clipper offers. I can see why NSA and FBI are unhappy about the reality of not being able to crack a really secure system such as the RSA or DES with a 128 bit key, or a one time pad on a floppy disk or CD-ROM.

In fact it is quite clear that current techniques are more than adequate to secure messages beyond even NSA's ability to break economically. The simple fact is that fast microprocessors can generate complexity faster than even huge parallel processors can break it. In my opinion, the balance of privacy has gone over to the individual who uses one of these techniques, and this is a sea change - one that cannot be reversed.

I think NSA, being expert in this domain, recognized this before anyone else. Clipper is clearly an attempt to turn back the clock to an era when they could crack most any system if there was sufficient incentive. Like all such attempts, this too will fail. Why then would it be proposed?

It was proposed because hidden inside the Clipper chip proposal are a number of Trojan Horses, some we are meant to find, and some we are not.

Many people jumped on the key security issue, and I believe that was intended to attract our attention and tie up our resources.

Several good points have been made about that item, which I will not repeat here. Another Trojan that we were meant to find is the 'weak' crypto issue, the Clipper algorithm being unknown and not available for public review. It may well have a hidden trapdoor that would not be found easily, yet if it were public, it would be found eventually. If it were found, the public outcry could well cause a big shift in political power.

Beyond those Trojans there are others which I believe we were not meant to find. Consider how the proposal surfaced. After lengthy *secret* meetings between NIST and NSA, a Presidential order appears putting Clipper into play. What is notable about this?

Clipper is the first proposal for encryption that *requires* registration of the keys. Why? Because, as I said earlier, our ability to encrypt has vastly outstripped the government's ability to decrypt. Registration puts this even, from the government's point of view. So where's the Trojan? The Trojan is the required registration of keys, mandated by presidential order. Once this precedent is established, the government could say "Sure, use any method you like, but register the algorithm and escrow the keys". This new requirement to register methods and keys now has the force of law without ever having been through the proper process - that is the passing of such a law by our elected representatives in the House and Senate, plus a public signing by the President.

I think it is clear that no such law would pass, since it is a infringement on our liberty (IMHO), for which a vague hand waving and repeat of the 'National Security' mantra does NOT suffice to justify. The first hidden Trojan is the attempted end run around the legislative process.

There is a second Trojan in the Clipper proposal that I have not seen discussed. It is the establishment of a fixed (but unknown) method, with a fixed (but knowable) key as the basis for a 'secure' communication. On the surface, this looks acceptable if the key security issues can be resolved. But it really isn't acceptable if you think about how the real world operates. Entirely aside from the security of the keys is the nature of how people handle security.

Given even the suspicion of a compromised security, most people will change their passwords instantly, just to be safe. But what do you do when the change requires justification to management that funds for a new instrument, or more than one, be expended for replacement on the basis of a suspicion? Even if you *know* that an instrument has been decoded, in many cases management will simply accept the government's word that the keys were destroyed rather than replace the instrument(s).

What I suspect would really happen is that compromised instruments would generally remain in place because of human nature to underestimate the potential threat. It may well be that compromising one instrument can make other instruments compromised through some trapdoor we don't know about. So a single compromised instrument could compromise *unknowingly and beyond the key safeguards* any other instrument that had a conversation with it. It seems possible that one legal wiretap could cascade into a lot of illegal wiretaps.

Given the ease with which secure communications can be done today, both voice and data, for no more than the cost of a mid-range PC and some software, I can understand why the FBI and NSA are concerned. I can easily sympathize with their problem because they are carrying heavy responsibilities for the nation. But I believe the attempt to turn back the clock is the wrong answer.

When the Enigma machine was compromised and better methods invented, no one suggested that everyone be forced to use Enigma machines so the government could still break them if needed. But this is exactly what the Clipper chip proposal is attempting to do, and it has no more chance of succeeding than forcing Enigma on everyone would. Worse, it obscures the fact that a sea change has occurred and ignores the need to deal with the new reality. The new reality, for some years now, is that methods exist that are secure from everyone from a *technical breaking* point of view.

The clear conclusion I draw from this is that the FBI and NSA must give new attention to other methods of access to the data they require for security and law enforcement. This may well mean a return to the days of (heavens) spies, listening devices, photographic/video recon and other methods. While the cold war was still on, this would probably be unacceptable, but now I think we can accept the possible handicap to law enforcement and national security rather than yield our own privacy.

In addition, whatever we do as a nation does not prevent other nations from using unbreakable methods, so in any event, both NSA and the FBI need to address the 'other methods' issue to remain effective.

Clipper Chip:
  It isn't needed, we already have better secure methods.
  It isn't wanted, except by the government.
  It isn't effective, since anyone can use better methods.
  It isn't useful because it doesn't address the real problem.

Let's toss this Trojan horse, this bad idea, on the scrap heap of obscurity.

Testimony to Boucher's House Science Subcommittee, 11 May 1993

<whitfield.diffie@eng.sun.com>
Thu, 13 May 1993 at 14h15

The Impact of a Secret Cryptographic Standard
on Encryption, Privacy, Law Enforcement
and Technology

Whitfield Diffie
Sun Microsystems
11 May 1993

I'd like to begin by expressing my thanks to Congressman Boucher, the other members of the committee, and the committee staff for giving us the opportunity to appear before the committee and express our views.

On Friday, the 16th of April, a sweeping new proposal for both the promotion and control of cryptography was made public on the front page of the New York Times and in press releases from the White House and other organizations.

This proposal was to adopt a new cryptographic system as a federal standard, but at the same time to keep the system's functioning secret. The standard would call for the use of a tamper resistant chip, called Clipper, and embody a `back door' that will allow the government to decrypt the traffic for law enforcement and national security purposes.

So far, available information about the chip is minimal and to some extent contradictory, but the essence appears to be this: When a Clipper chip prepares to encrypt a message, it generates a short preliminary signal rather candidly entitled the Law Enforcement Exploitation Field. Before another Clipper chip will decrypt the message, this signal must be fed into it. The Law Enforcement Exploitation Field or LEEF is tied to the key in use and the two must match for decryption to be successful. The LEEF in turn, when decrypted by a government held key that is unique to the chip, will reveal the key used to encrypt the message.

The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of school children. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

In the month that has elapsed since the announcement, we have studied the Clipper chip proposal as carefully as the available information permits. We conclude that such a proposal is at best premature and at worst will have a damaging effect on both business security and civil rights without making any improvement in law enforcement.

To give you some idea of the importance of the issues this raises, I'd like to suggest that you think about what are the most essential security mechanisms in your daily life and work. I believe you will realize that the most important things any of you ever do by way of security have nothing to do with guards, fences, badges, or safes. Far and away the most important element of your security is that you recognize your family, your friends, and your colleagues. Probably second to that is that you sign your signature, which provides the people to whom you give letters, checks, or documents, with a way of proving to third parties that you have said or promised something. Finally you engage in private conversations, saying things to your loved ones, your friends, or your staff that you do not wish to be overheard by anyone else.

These three mechanisms lean heavily on the physical: face to face contact between people or the exchange of written messages. At this moment in history, however, we are transferring our medium of social interaction from the physical to the electronic at a pace limited only by the development of our technology. Many of us spend half the day on the telephone talking to people we may visit in person at most a few times a year and the other half exchanging electronic mail with people we never meet in person.

Communication security has traditionally been seen as an arcane security technology of real concern only to the military and perhaps the banks and oil companies. Viewed in light of the observations above, however, it is revealed as nothing less than the transplantation of fundamental social mechanisms from the world of face to face meetings and pen and ink communication into a world of electronic mail, video conferences, electronic funds transfers, electronic data interchange, and, in the not too distant future, digital money and electronic voting.

No right of private conversation was enumerated in the constitution. I don't suppose it occurred to anyone at the time that it could be prevented. Now, however, we are on the verge of a world in which electronic communication is both so good and so inexpensive that intimate business and personal relationships will flourish between parties who can at most occasionally afford the luxury of traveling to visit each other. If we do not accept the right of these people to protect the privacy of their communication, we take a long step in the direction of a world in which privacy will belong only to the rich.

The import of this is clear: The decisions we make about communication security today will determine the kind of society we live in tomorrow.

The objective of the administration's proposal can be simply stated:

> They want to provide a high level of security to their
> friends, while being sure that the equipment cannot be
> used to prevent them from spying on their enemies.

Within a command society like the military, a mechanism of this sort that allows soldiers' communications to be protected from the enemy, but not necessarily from the Inspector General, is an entirely natural objective. Its imposition on a free society, however, is quite another matter.

Let us begin by examining the monitoring requirement and ask both whether it is essential to future law enforcement and what measures would be required to make it work as planned.

Eavesdropping, as its name reminds us, is not a new phenomenon. But in spite of the fact that police and spies have been doing it for a long time, it has acquired a whole new dimension since the invention of the telegraph. Prior to electronic communication, it was a hit or miss affair. Postal services as we know them today are a fairly new phenomenon and messages were carried by a variety of couriers, travelers, and merchants. Sensitive messages in particular, did not necessarily go by standardized channels. Paul Revere, who is generally remembered for only one short ride, was the American Revolution's courier, traveling routinely from Boston to Philadelphia with his saddle bags full of political broadsides.

Even when a letter was intercepted, opened, and read, there was no guarantee, despite some people's great skill with flaps and seals, that the victim would not notice the intrusion.

The development of the telephone, telegraph, and radio have given the spies a systematic way of intercepting messages. The telephone provides a means of communication so effective and convenient that even people who are aware of the danger routinely put aside their caution and use it to convey sensitive information. Digital switching has helped eavesdroppers immensely in automating their activities and made it possible for them to do their listening a long way from the target with negligible chance of detection.

Police work was not born with the invention of wiretapping and at present the significance of wiretaps as an investigative tool is quite limited. Even if their phone calls were perfectly secure, criminals would still be vulnerable to bugs in their offices, body wires on agents, betrayal by co-conspirators who saw a brighter future in cooperating with the police, and ordinary forensic inquiry.

Moreover, cryptography, even without intentional back doors, will no more guarantee that a criminal's communications are secure than the Enigma guaranteed that German communications were secure in World War II. Traditionally, the richest source of success in communications intelligence is the ubiquity of busts: failures to use the equipment correctly.

Even if the best cryptographic equipment we know how to build is available to them, criminal communications will only be secure to the degree that the criminals energetically pursue that goal. The question thus becomes, ``If criminals energetically pursue secure communications, will a government standard with a built in inspection port, stop them.

It goes without saying that unless unapproved cryptography is outlawed, and probably even if it is, users bent on not having their communications read by the state will implement their own encryption. If this requires them to forgo a broad variety of approved products, it will be an expensive route taken only by the dedicated, but this sacrifice does not appear to be necessary.

The law enforcement function of the Clipper system, as it has been described, is not difficult to bypass. Users who have faith in the secret Skipjack algorithm and merely want to protect themselves from compromise via the Law Enforcement Exploitation Field, need only encrypt that one item at the start of transmission. In many systems, this would require very small changes to supporting programs already present. This makes it likely that if Clipper chips become as freely available as has been suggested, many products will employ them in ways that defeat a major objective of the plan.

What then is the alternative? In order to guarantee that the government can always read Clipper traffic when it feels the need, the construction of equipment will have to be carefully controlled to prevent non-conforming implementations. A major incentive that has been cited for industry to implement products using the new standard is that these will be required for communication with the government. If this strategy is successful, it is a club that few manufacturers will be able to resist. The program therefore threatens to bring communications manufacturers under an all encompassing regulatory regime.

It is noteworthy that such a regime already exists to govern the manufacture of equipment designed to protect `unclassified but sensitive' government information, the application for which Clipper is to be mandated. The program, called the Type II Commercial COMSEC Endorsement Program, requires facility clearances, memoranda of agreement with NSA, and access to secret `Functional Security Requirements Specifications.' Under this program member companies submit designs to NSA and refine them in an iterative process before they are approved for manufacture.

The rationale for this onerous procedure has always been, and with much justification, that even though these manufacturers build equipment around approved tamper resistant modules analogous to the Clipper chip, the equipment must be carefully vetted to assure that it provides adequate security. One requirement that would likely be imposed on conforming Clipper applications is that they offer no alternative or additional encryption mechanisms.

Beyond the damaging effects that such regulation would have on innovation in the communications and computer industries, we must also consider the fact that the public cryptographic community has been the principal source of innovation in cryptography. Despite NSA's undocumented claim to have discovered public key cryptography, evidence suggests that, although they may have been aware of the mathematics, they entirely failed to understand the significance. The fact that public key is now widely used in government as well as commercial cryptographic equipment is a consequence of the public community being there to show the way.

Farsightedness continues to characterize public research in cryptography, with steady progress toward acceptable schemes for digital money, electronic voting, distributed contract negotiation, and other elements of the computer mediated infrastructure of the future.

Even in the absence of a draconian regulatory framework, the effect of a secret standard, available only in a tamper resistant chip, will be a profound increase in the prices of many computing devices. Cryptography is often embodied in microcode, mingled on chips with other functions, or implemented in dedicated, but standard, microprocessors at a tiny fraction of the tens of dollars per chip that Clipper is predicted to cost.

What will be the effect of giving one or a small number of companies a monopoly on tamper resistant parts? Will there come a time, as occurred with DES, when NSA wants the standard changed even though industry still finds it adequate for many applications? If that occurs will industry have any recourse but to do what it is told? And who will pay for the conversion?

One of the little noticed aspects of this proposal is the arrival of tamper resistant chips in the commercial arena. Is this tamper resistant part merely the precursor to many? Will the open competition to improve semiconductor computing that has characterized the past twenty-years give way to an era of trade secrecy? Is it perhaps tamper resistance technology rather than cryptography that should be regulated?

Recent years have seen a succession of technological developments that diminish the privacy available to the individual. Cameras watch us in the stores, x-ray machines search us at the airport, magnetometers look to see that we are not stealing from the merchants, and databases record our actions and transactions. Among the gems of this invasion is the British Rafter technology that enables observers to determine what station a radio or TV is receiving. Except for the continuing but ineffectual controversy surrounding databases, these technologies flourish without so much as talk of regulation.

Cryptography is perhaps alone in its promise to give us more privacy rather than less, but here we are told that we should forgo this technical benefit and accept a solution in which the government will retain the power to intercept our ever more valuable and intimate communications and will allow that power to be limited only by policy.

In discussion of the FBI's Digital Telephony Proposal --- which would have required communication providers, at great expense to themselves, to build eavesdropping into their switches --- it was continually emphasized that wiretaps were an exceptional investigative measure only authorized when other measures had failed. Absent was any sense that were the country to make the proposed quarter billion dollar inventment in intercept equipment, courts could hardly fail to accept the police argument that a wiretap would save the people thousands of dollars over other options. As Don Cotter, at one time director of Sandia National Laboratories, said in respect to military strategy: ``Hardware makes policy.''

Law, technology, and economics are three central elements of society that must all be kept in harmony if freedom is to be secure. An essential element of that freedom is the right to privacy, a right that cannot be expected to stand against unremitting technological attack. Where technology has the capacity to support individual rights, we must enlist that support rather than rejecting it on the grounds that rights can be abused by criminals. If we put the desires of the police ahead of the rights of the citizens often enough, we will shortly find that we are living in police state. We must instead assure that the rights recognized by law are supported rather than undermined by technology.

At NSA they believe in something they call `security in depth.' Their most valuable secret may lie encrypted on a tamper resistant chip, inside a safe, within a locked office, in a guarded building, surrounded by barbed wire, on a military base. I submit to you that the most valuable secret in the world is the secret of democracy; that technology and policy should go hand in hand in guarding that secret; that it must be protected by security in depth.

Recommendations

There is a crying need for improved security in American communication and computing equipment and the Administration is largely correct when it blames the problem on a lack of standards. One essential standard that is missing is a more secure conventional algorithm to replace DES, an area of cryptography in which NSA's expertise is probably second to none.

I urge the committee to take what is good in the Administration's proposal and reject what is bad. \begdis

o The Skipjack algorithm and every other aspect of this proposal should be made public, not only to expose them to public scrutiny but to guarantee that once made available as standards they will not be prematurely withdrawn. Configuration control techniques pioneered by the public community can be used to verify that some pieces of equipment conform to government standards stricter than the commercial where that is appropriate.

o I likewise urge the committee to recognize that the right to private conversation must not be sacrificed as we move into a telecommunicated world and reject the Law Enforcement Exploitation Function and the draconian regulation that would necessarily come with it.

o I further urge the committee to press the Administration to accept the need for a sound international security technology appropriate to the increasingly international character of the world's economy.

◀ ▲ ▶ ℹ Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 62

Monday 17 May 1993

Contents

Cut and Paste risks

Elizabeth Zwicky <zwicky@erg.sri.com>
Mon, 17 May 93 09:51:07 -0700

A few years ago, one of our main servers went down, and failed to reboot. Investigation showed that it had been halted with the instruction to reboot on a kernel named "imagen.df", which naturally had not worked well. Further investigation showed that only our most junior system administrator had been logged into it at the time. She was adamant, if not frantic, in her denial of having done any such thing. Fortunately, she had been logged into it from another machine in an xterm with a scrollbar, and we were able to scroll it back to the point before the machine went down, where a wide variety of peculiar error messages became visible. Messages like "dumpdates: permission denied", and "dump: bad key 'i'" appeared before a final "fastboot" took effect. In horror, she said "All I did was drop my pencil and when I straightened up it was gone!" It seems that when she leaned over to pick up the pencil, her elbow cut and pasted an ls of /etc at the prompt. Fortunately "clri" is very picky about its syntax, or we might have had a really interesting mess. As it happened, "fastboot" was the first command which was willing to take the remainder of its line as valid arguments.

We wrote this off as a once-in-a-lifetime event until Friday, when another server went down suddenly. This one came back OK, and we didn't have to search for the culprit, a relatively senior administrator who turned himself in shamefacedly: "I hit the wrong mouse button. It pasted a fastboot. It's all my fault."

I've never liked the X method of cutting and pasting much, but I'm beginning to feel actively hostile towards it.

Elizabeth D. Zwicky zwicky@erg.sri.com

CHI & the Color-blind?

Vannevar Yu <vannevar@Panix.Com>
Sat, 15 May 93 18:17:57 EDT

In the May 1993 issue of Credit Card Management (vol.6, no.2, New York, NY) a special report on "Collections Technology" utilizing color graphic displays was described in p.66:

> "A black icon facing left to right means a call was placed, but no contact was made. A red icon facing left to right means a call was placed and contact was made, but a promise to pay was not received. A green icon facing left to right means a promise to pay was arranged. An icon facing right to left means the debtor called the collector."

Given that the use of computers with fancy color displays will become more common with time, how do we ensure that color-blind people can use these displays without any confusion? Although one of my color-blind friends can tell that there is a difference between, say red and green, a simple change in monitor contrast/brightness levels (or being assigned to a different terminal or a particular day) would probably be enough to throw him off. With disabilities-related legislation in the United States in place, such issues regarding computer-human interaction will definitely get more attention.

Update on risks in semiconductor manufacturing

rob horn <horn%temerity@leia.polaroid.com>
14 May 1993 21:27:51 -0400 (EDT)

The miscarriage risk information on semiconductor manufacturing is based on multiple epidemiological studies. The largest of these was by UC Davis and tracked 15,000 employees at 14 plants. The studies were examining effects from microwave exposure, low frequency magnetic fields, solvents, paints, CRT usage and electrostatic field exposure. In one portion of the manufacturing process a solvent related problem was found. No other statistically significant effects were found.

The solvent risk is from the family of solvents known as glycol ethers, with particular risk from the ethylene glycol ethers. These solvents are used in the photolithography process. This is the stage where the semiconductor is coated with a photoresist layer, this layer exposed through a mask, and then partially removed. Most photolithography processes involve solvents of various sorts. The study isolated the effect to sites using glycol ethers. The other solvents may be dangerous, but the safety precautions appear to be adequate.

The risk magnitude is an increase of between 40 and 100% in the miscarriage rate for workers in photolithography where ethylene glycol ethers are used.

Industry reaction is mixed. There is relief that the other safety measures are effective. The ethers are not the most dangerous chemical used. There are far more toxic chemicals involved elsewhere. There is disappointment that the safety measures in place in photolithography are inadequate. There was also relief that suspected hazards from CRT usage, EMF, and ESF did not cause an increase in the miscarriage rate.

The semiconductor industry is already several years into major overhauls and redesigns to reduce health, safety, and environmental hazards. All of the glycol ethers were already targets for gradual elimination as health and significant environmental hazards. The disposal for one gallon of such waste now exceeds $50. This study will accelerate their elimination. This will have a significant economic impact because the alternative processes with low health and environmental impacts are very different. Often it is easier to close the old factory and build a new one. When making a change this big, there is often an associated site relocation, job losses, etc.

Health hazards in the electronics manufacturing industry are not new. The toxic chemicals hazards from printed circuit board manufacturing and soldering stations are some earlier significant dangers.

Rob Horn   horn@temerity.polaroid.com

Re: Epilepsy and video games

Edwin Culver <culver@cse.bridgeport.edu>
Fri, 14 May 93 11:07:15 EDT

Larry Hunter and others were asking about seizures induced by video games. Not being a neurologist, I wonder if these are similar to those caused by "photic stimulation", which has been implicated in some aircraft accidents.

Some people, when exposed to flickering or flashing lights will have seizures
which are quite similar to epileptic seizures. In aircraft, this can be a
problem for general aviation pilots, who look through the propeller disk.
During most of the flight, the frequency is too high to cause problems, but
during a landing, especially into the setting sun, the propeller may cause
flickering sufficient to induce a seizure. There are, apparently, degrees of
severity: some people will seize from a single flash of the right duration.

Edwin M. Culver culver@cse.bridgeport.com (203) 741-8736

Don't Depend on makedepend

Dave Wortman <dw@pdp1.sys.toronto.edu>
Mon, 17 May 1993 14:09:28 -0400

Context: makedepend is a program that processes a set of C program files
and determines interdependencies among those files. It is frequently used
in large software systems to (attempt to) guarantee that a Makefile correctly
describes the dependencies in a piece of software. There is often a software
building step called "make depend" that invokes the makedepend program.
Many users of makedepend run it automatically as a part of system building
without much appreciation for what it is doing.

Makedepend has a documented undependability!!

In the man page for makedepend under the heading "Bugs", we find the
remarkable statement:

"If you do not have the source for cpp, the Berkeley Unix C preprocessor then
makedepend will be compiled in such a way that all #if directives will
evaluate to "true" regardless of their actual value. This may cause the
wrong #include directives to be evaluated." ...

This appears to open a large hole for incorrectly building software.
If the Makefile dependencies generated by makedepend are wrong then there
is a chance that the software built using the Makefile will also be wrong.

I think the authors of makedepend made a bad decision in allowing the program
to become functional in a situation where they knew it could get the
wrong answer. To their credit, at least they documented the problem.
If the source for Berkeley cpp is unavailable then it shouldn't be possible
to compile makedepend.

Risks:
- wrong answers from makedepend could lead to wrong software.
- the ordinary user of makedepend has no way of knowing whether the
  makedepend they are using will get the right answer or not.
- many users of makedepend are unaware that makedepend can get the
  wrong answer.

makedepend problem - a real world example

Dave Wortman <dw@pdp1.sys.toronto.edu>
Mon, 17 May 1993 20:02:09 -0400

Shortly after posting my message concerning problems with makedepend
I came across an unsolicited example of the problem in a posting by
Michael Turok (mlt@blues.infores.com) to the comp.windows.x newsgroup.

...
makedepend chokes on one of X11 include files (as distributed
by Sun) - namely Xos.h:

```
#if     !defined(SUNOS41) || defined(__STDC__)
#       include <string.h>
#       define  index   strchr
#       define  rindex  strrchr
#else   /* BSD && !__STDC__ */
#       include <strings.h>
#endif  /* !SUNOS41 || __STDC__ */
```

Here 'makedepend' evaluates both #if and corresponding #else statements
to 'true' and tries to open the file <strings.h> which doesn't exist
under Solaris2. ...

Business Week: ADP Flubs

<Bob_Frankston@frankston.com>
Sun 16 May 1993 14:21 -0400

There is an article in the May 24, 1993 issue of Business Week covering errors in Automatic Data Processing's handling of key tabulations and statistics including undercounting the shareholder votes for a company (the 72.4 million counted were not enough) and misreporting key government labor statistics in the late 1980's that resulted in exaggerating job losses until 1991 by 540,000 jobs.

In my mind the issue is not so much the ADP errors, as the dependence we have on such calculations without effective fallback and reasonableness checks. Errors, while not forgivable, will occur whether it is a programming error, a management oversight or a systemic flaw.

As we build these statistics into policy, the best we can hope for is that there is some effective feedback to reduce volatility. My fear is that bad statistics can lead to policies that only amplify the problem. Can hyperinflation be caused by misreporting CPI figures? Perhaps the job figures influenced the recent election.

Mobile Phones and airbags (was: Opel Corsa Stops...)

Olivier MJ Crepin-Leblond <o.crepin-leblond@ic.ac.uk>

Sat, 15 May 1993 19:22:15 +0100

In Risks-Digest 14.61, O\ystein Gulbrandsen relays a description of the
effect of a mobile phone on the electronics of an Opel (or Vauxhall
here in UK :-)) Corsa engine.

By coincidence a similar subject came-up in a conversation I had with
a colleague last week. This is second-hand information, but it
appears that the electronics for some AIRBAG impact safety systems
were also affected by mobile telephones, and that in a few cases,
the airbags were inflated spontaneously while the car was being
driven, and of course, without any impact.
It would be interesting if anyone could confirm this. Before hearing
the Opel corsa story, I was most skeptical about it, but now...

Olivier M.J. Crepin-Leblond, Digital Comms. Section, Elec. Eng. Department
Imperial College of Science, Technology and Medicine, London SW7 2BT, UK

Re: Denning on NIST/NSA Revelations (Sobel, RISKS-14.59)

Marc Rotenberg <Marc_Rotenberg@washofc.cpsr.org>
Sun, 16 May 1993 11:30:25 EST

David Sobel, CPSR Legal Council, wrote in RISKS DIGEST 14.59:
<>   The proposed DSS was widely criticized within the computer
<>   industry for its perceived weak security and inferiority to an
<>   existing authentication technology known as the RSA algorithm.
<>   Many observers have speculated that the RSA technique was
<>   disfavored by NSA because it was, in fact, more secure than the
<>   NSA-proposed algorithm and because the RSA technique could also
<>   be used to encrypt data very securely.

Dorothy Denning responded in RISKS Digest 4.60
> This is terribly misleading. NIST issued the DSS proposal along with a
> public call for comments as part of their normal practice with proposed
> standards. The community responded, and NIST promptly addressed the
> security concerns. Among other things, the DSS now accommodates longer
> keys (up to 1024 bits). As a result of the revisions, the DSS is now
> considered to be just as strong as RSA.

Denning has to be kidding. The comments on the proposed DSS were uniformly
critical. Both Marty Hellman and Ron Rivest questioned the desirability of
the proposed standard.

One of the reasons for the concern was the secrecy surrounding the development
of the standard. The documents disclosed by NIST and NSA to CPSR make clear
that NSA used its classification authority to frustrate the attempt of even
NIST's scientists to assess the candidate algorithm.

This is not part of "normal practice." In fact, NSA's efforts to blindfold
NIST and the secrecy surrounding the process violated the central intent of
the Computer Security Act, the very law that governs the relationship between

NIST and NSA.

Marc Rotenberg, CPSR Washington office

Dr. D. Denning on DSS v. RSA (Sobel, RISKS-14.59)

<WHMurray@DOCKMASTER.NCSC.MIL>
Sat, 15 May 93 22:56 EDT

The point is that NSA dislikes RSA "because (it) could also be used to encrypt data very securely." While it may be true that DSS with a 1024 bit modulus is as secure for digital signatures as RSA, it does not meet either the congressional mandate or the requirement.

The congressional mandate was for a public-key standard, not for a digital signature standard. The requirement is for a mechanism for key exchange. The DSS is a ruse; it is an attempt to appear to meet the congressional mandate without meeting the requirement.

I think that the CPSR statement is both accurate and to the point.

William Hugh Murray, Executive Consultant, Information System Security
49 Locust Avenue, Suite 104; New Canaan, CT 06840 1-0-ATT-0-700-WMURRAY

NIST Answers to Jim Bidzos' Questions

Jim Bidzos <jim@RSA.COM>
Mon, 17 May 93 14:05:18 PDT

Date: Mon, 17 May 1993 16:44:28 -0400 (EDT)
From: ROBACK@ECF.NCSL.NIST.GOV
Subject: Answers to Your Questions
To: jim@RSA.COM

To: Mr. Jim Bidzos, RSA Data Security, Inc.

From: Ed Roback, NIST

Mr. Ray Kammer asked me to forward to you our answers to the questions you raised in your e-mail of 4/27.

We've inserted our answers in your original message.

From: SMTP%"jim@RSA.COM" 27-APR-1993 03:13:12.75
To: clipper@csrc.ncsl.nist.gov
CC:
Subj: Clipper questions
...
Date: Tue, 27 Apr 93 00:11:50 PDT

From: jim@RSA.COM (Jim Bidzos)

Here are some questions about the Clipper program I would like to submit.

Much has been said about Clipper and Capstone (the term Clipper will be used to describe both) recently. Essentially, Clipper is a government-sponsored tamper-resistant chip that employs a classified algorithm and a key escrow facility that allows law enforcement, with the cooperation of two other parties, to decipher Clipper-encrypted traffic. The stated purpose of the program is to offer telecommunications privacy to individuals, businesses, and government, while protecting the ability of law enforcement to conduct court-authorized wiretapping.

The announcement said, among other things, that there is currently no plan to attempt to legislate Clipper as the only legal means to protect telecommunications. Many have speculated that Clipper, since it is only effective in achieving its stated objectives if everyone uses it, will be followed by legislative attempts to make it the only legal telecommunications protection allowed. This remains to be seen.

>>>> NIST: There are no current plans to legislate the use of Clipper. Clipper will be a government standard, which can be - and likely will be - used voluntarily by the private sector. The option for legislation may be examined during the policy review ordered by the President.

The proposal, taken at face value, still raises a number of serious questions.

What is the smallest number of people who are in a position to compromise the security of the system? This would include people employed at a number of places such as Mikotronyx, VSLI, NSA, FBI, and at the trustee facilities. Is there an available study on the cost and security risks of the escrow process?

>>>> NIST: It will not be possible for anyone from Mykotronx, VLSI, NIST, NSA, FBI (or any other non-escrow holder) to compromise the system. Under current plans, it would be necessary for three persons, one from each of the escrow trustees and one who knows the serial number of the Clipper Chip which is the subject of the court authorized electronic intercept by the outside law enforcement agency, to conspire in order to compromise escrowed keys. To prevent this, it is envisioned that every time a law enforcement agency is provided access to the escrowed keys there will be a record of same referencing the specific lawful intercept authorization (court order). Audits will be performed to assure strict compliance. This duplicates the protection afforded nuclear release codes. If additional escrow agents are added, one additional person from each would be required to compromise the system. NSA's analysis on the security risks of the escrow system is not available for public dissemination.

How were the vendors participating in the program chosen? Was the process open?

>>>> NIST: The services of the current chip vendors were obtained in accordance with U.S. Government rules for sole source procurement, based on unique capabilities they presented. Criteria for selecting additional sources will be forthcoming over the next few months.

AT&T worked with the government on a voluntary basis to use the "Clipper Chip" in their Telephone Security Device. Any vendors of equipment who would like to use the chips in their equipment may do so, provided they meet proper government security requirements.

A significant percentage of US companies are or have been the subject of an investigation by the FBI, IRS, SEC, EPA, FTC, and other government agencies. Since records are routinely subpoenaed, shouldn't these companies now assume that all their communications are likely compromised if they find themselves the subject of an investigation by a government agency? If not, why not?

>>>> NIST: No. First of all, there is strict and limited use of subpoenaed material under the Federal Rules of Criminal Procedure and sanctions for violation. There has been no evidence to date of Governmental abuse of subpoenaed material, be it encrypted or not. Beyond this, other Federal criminal and civil statutes protect and restrict the disclosure of proprietary business information, trade secrets, etc. Finally, of all the Federal agencies cited, only the FBI has statutory authority to conduct authorized electronic surveillance. Electronic surveillance is conducted by the FBI only after a Federal judge agrees that there is probable cause indicating that a specific individual or individuals are using communications in furtherance of serious criminal activity and issues a court order to the FBI authorizing the interception of the communications.

What companies or individuals in industry were consulted (as stated in the announcement) on this program prior to its announcement? (This question seeks to identify those who may have been involved at the policy level; certainly ATT, Mikotronyx and VLSI are part of industry, and surely they were involved in some way.)

>>>> NIST: To the best of our knowledge: AT&T, Mykotronx, VLSI, and Motorola. Other firms were briefed on the project, but not "consulted," per se.

Is there a study available that estimates the cost to the US government of the Clipper program?

>>>> NIST: No studies have been conducted on a government-wide basis to estimate the costs of telecommunications security technologies. The needs for such protection are changing all the time.

There are a number of companies that employ non-escrowed cryptography in their products today. These products range from secure voice, data, and fax to secure email, electronic forms, and software distribution, to name but a few. With over a million such products in use today, what does the Clipper program envision for the future of these products and the many corporations and individuals that have invested in and use them? Will the investment made by the vendors in encryption-enhanced products be protected? If so, how? Is it envisioned that they will add escrow features to their products or be asked to employ Clipper?

>>>> NIST: Again, the Clipper Chip is a government standard which can be used voluntarily by those in the private sector. We also point out that the President's directive on "Public Encryption Management" stated: "In making this decision, I do not intend to prevent the private sector from developing, or the government from approving, other microcircuits or algorithms that are equally effective in assuring both privacy and a secure key-escrow system." You will have to consult directly with private firms as to whether they will add escrow features to their products.

Since Clipper, as currently defined, cannot be implemented in software, what options are available to those who can benefit from cryptography in software? Was a study of the impact on these vendors or of the potential cost to the software industry conducted? (Much of the use of cryptography by software companies, particularly those in the entertainment industry, is for the protection of their intellectual property.)

>>>> NIST: You are correct that, currently, Clipper Chip functionality can only be implemented in hardware. We are not aware of a solution to allow lawfully authorized government access when the key escrow features and encryption algorithm are implemented in software. We would welcome the participation of the software industry in a cooperative effort to meet this technical challenge. Existing software encryption use can, of course, continue.

Banking and finance (as well as general commerce) are truly global today. Most European financial institutions use technology described in standards such as ISO 9796. Many innovative new financial products and services will employ the reversible cryptography described in these standards. Clipper does not comply with these standards. Will US financial institutions be able to export Clipper? If so, will their overseas customers find Clipper acceptable? Was a study of the potential impact of Clipper on US competitiveness conducted? If so, is it available? If not, why not?

>>>> NIST: Consistent with current export regulations applied to the export of the DES, we expect U.S. financial institutions will be able to export the Clipper Chip on a case by case basis for their use. It is probably too early to ascertain how desirable their overseas customers will find the Clipper Chip. No formal study of the impact of the Clipper Chip has

been conducted since it was, until recently, a classified technology; however, we are well aware of the threats from economic espionage from foreign firms and governments and we are making the Clipper Chip available to provide excellent protection against these threats. As noted below, we would be interested in such input from potential users and others affected by the announcement. Use of other encryption techniques and standards, including ISO 9796 and the ISO 8730 series, by non-U.S. Government entities (such as European financial institutions) is expected to continue.

I realize they are probably still trying to assess the impact of Clipper, but it would be interesting to hear from some major US financial institutions on this issue.

>>>> NIST: We too would be interested in hearing any reaction from these institutions, particularly if such input can be received by the end of May, to be used in the Presidentially-directed review of government cryptographic policy.

Did the administration ask these questions (and get acceptable answers) before supporting this program? If so, can they share the answers with us? If not, can we seek answers before the program is launched?

>>>> NIST: These and many, many others were discussed during the development of the Clipper Chip key escrow technology and the decisions-making process. The decisions reflect those discussions and offer a balance among the various needs of corporations and citizens for improved security and privacy and of the law enforcement community for continued legal access to the communications of criminals.

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 63

Tuesday 18 May 1993

Contents

Read any good magazines lately? [with permission, for RISKS]

<rslade@sfu.ca>
Tue, 18 May 93 12:42:47 PDT

Memoirs of a (media star) virus researcher [MEMOIR7.CVP   930515]

I have been known, from time to time, to make rather unkind statements about the accuracy of virus reports in the mainstream media. Some of my antipathy arises simply from the fact that there is an awful lot of "mythology" surrounding viral programs, and most of the pieces that appear in the media simply perpetuate this. Some of my experience, however, is first hand.

I like live radio best, and TV news the worst. "Live" anything gives you a bit of control, whereas TV is, in my view, arrogant, sensational and overpaid. However, the electronic media still doesn't have an "all-computer" channel, so most of the media reports about viral programs happen in print media. I've had a few forays there as well, but would like to outline one recent experience.

A reasonably prominent periodical devoted to security topics has been advertising for writers in, among other areas, the virus field, so I sent some sample materials off. I did not hear anything for about eight months, and then got a call asking me to do an article. On groupware. Well, OK, regardless of the topic I can use the money. Only there isn't very much money slated for this, slightly under $400 for roughly three pages of material. (Please have it ready in 20 days.) It doesn't take long, at that price, for the "rate per hour" to drop into the basement.

However, it is not enough to write the article. No, one has to contact the vendors, and hear what they have to say on the topic. This, actually, consumes the most time. Some research, and roughing out an outline, took up two hours. A rough draft took three. Polishing the final draft took about an hour. Lots of room for profit there. (Of course, when you consider the years it takes to build the background to be able to do that, it tends to reduce the margin a bit ... :-) But contacting three consultants, two user group representatives, and eleven representatives from seven major vendors took more than fourteen hours spread over a ten day period. In the end it got me one very helpful vendor contact (Carol Smykowski from Fischer International, very nice lady), one returned message, one faxed spec sheet from a loosely related product and a heavy parcel that arrived postage due after the deadline. Needless to say, this was less than helpful to the project.

In the end, the article was rejected. Not enough "vendor quotes".

However, is my whining and complaining of any importance to you? Well, yes, it is. What is really important here is the fact that most of the articles being generated in the "trade press" are, by and large, "infomercials" on the printed page. Articles are being written, by people who, if they have a technical background at all, are writing out of their field, and are being judged on the acceptability of the content to vendors and advertisers. The vendors, quite happy with the situation, are in no hurry to be helpfully involved in the process (or, indeed, even to return phone calls).

(As two examples, I cite the recent (as this is written) releases of PKZip 2.04 and MS-DOS 6.0. For the first month after the release of the new PKZip, while the nets were stretched by the reports of the various bugs, and the latest release by PKWare to try to correct them, PC Week blithely rhapsodized over "version 2" and advertised that it had version 2.04c (the real buggy one) on its own board. Meanwhile, in spite of the protests of the virus research community *before* MS-DOS 6 was released, and the almost immediate storm of reports of bugs and problems with various of the new features, the trade press is only now, after six weeks of ecstatically positives reviews of MS-DOS 6, starting to report some of the potential problems.)

The primary distribution of this article will, of course, be the Internet, as it is also my primary source of information. Unfortunately, the population of "the net" is likely around two to five million. A large number, perhaps, but very small in comparison to the estimated hundred million PC users alone. And in that "larger" world, the inaccurate "non-net" media tends to hold much more importance.

copyright Robert M. Slade, 1993   MEMOIR7.CVP   930515

Vancouver Institute for Research into User Security   Canada V7K 2G6
ROBERTS@decus.ca Robert_Slade@sfu.ca rslade@cue.bc.ca   p1@CyberStore.ca

Re: Cut and Paste risks (Zwicky, RISKS-14.62)

Pete Mellor <pm@cs.city.ac.uk>
Tue, 18 May 93 10:12:06 BST

Elizabeth Zwicky's report (RISKS-14.62) about cut and paste with the elbow reminded me of the "Case of the Overhanging Data Entry Operator", an anecdote which caused some amusement many years ago in the customer support department of one of the British manufacturers of mainframe computers, for whom I then worked.

In those days, keying data directly onto disk, instead of punching onto cards first, was relatively new, and "Direct Data Entry" was a selling point. The DDE station was an intelligent terminal with disk, screen and keyboard. The operator used to log in giving a password.

There was a fault in the password handling whereby a leading space would be accepted as part of the password when this was set, but leading spaces were ignored when the password was keyed at login. The temporary work-around was, obviously, not to use spaces in passwords.

On one site, the support engineers were puzzled to find that, despite this advice, the fault was being repeatedly triggered on one DDE station, although the operator concerned emphatically denied having pressed the space bar when entering a new password.

The proximal cause turned out to be that the operator was a well-built woman ...

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@city.ac.uk

Subject: Re: Cut and Paste risks (Zwicky, RISKS-14.62)

Byron Rakitzis <netapp!byron@netcom.com>
Mon, 17 May 93 21:54:46 PDT

While the X method for cut and paste may be poorly designed, I think there is another RISK associated with system admin using window systems: namely, the tendency to leave a window open with the root account logged in. I don't mean to sound holier-than-thou, but it was always my practice to limit my actions as root to as few as possible, by always explicitly su-ing to root, performing a task, and logging out again. While this does not eliminate the aforementioned risk, it does tend to minimize it.

Byron Rakitzis. <byron@netapp.com>

Re: Cut and Paste risks (Zwicky, RISKS-14.62)

Tim Cook <tim@deakin.edu.au>
18 May 1993 15:49:59 +1000

I think the advantages of cut-and-paste with X clients far outweigh such a potential problem.

We should identify the main source of the risk, which in my opinion is general access to super-user privileged shells. This can be greatly reduced by employing one of those utilities that provide individual super-user privileged commands to specific users from their own accounts. It would be much harder to paste something that did damage in this scenario.

Tim Cook, Systems Engineer, Deakin University.

Re: Cut and Paste risks (Zwicky, RISKS-14.61)

Christopher Lishka <lishka@dxcern.cern.ch>
Tue, 18 May 1993 11:22:57 GMT

>I've never liked the X method of cutting and pasting much,
>but I'm beginning to feel actively hostile towards it.
>   Elizabeth D. Zwicky zwicky@erg.sri.com

Not to mention mixed platform, mixed GUI cut-and-paste problems. I am a system manager for both VMS and Ultrix systems. I use an Ultrix machine running Motif for my GUI, while most of the VMS users have DECwindows.

The main problem is the differing cut-and-paste buttons: Motif uses the middle button, while DECwindows uses the right button (assuming a right-handed mouse set-up). This becomes a problem when I run a standard DECwindows applications with the display on Motif. Only the left mouse button (select text) remains constant.

Plus, some DECwindows applications (notably DECwindows Mail) like to reset the cut-and-paste buffer if you switch input focus to a certain window. (E.g., DECwindows Mail seems to put the text of the current message in the cut-and-paste buffer automatically.) My autofocus mouse (ala Sun) wreaks havoc with this. Many times I have selected text in one window, moved the mouse to a terminal window, pasted, and had the entire contents of a mail message run as Unix commands because I had accidentally had my mouse cross over the DECwindows Mail window (focusing input briefly on it).

My solution? Live with it. It has not gotten to a point yet where I feel the need to hunt down the various settings files (*if* this is possible) to fix the problems by creating "Lishka's own standard GUI set-up". Being a system manager, I use a good variety of computers and their various GUIs frequently. Furthermore, I have to help users a lot, and I have found that if I customize my own GUI and shell settings too much, then I can't function with the standard GUI and shell commands. (It is very embarrassing to type all of these arcane short-cut aliases in front of a user at her/his terminal, and have them not work! You look incompetent....)

How to practice safe cut-and-paste practices? *NEVER* paste into a terminal window with a superuser session (be it "SYSTEM" or "root"). This means one has to type it all, possibly leading to transcription errors, but one should always double-check important commands anyway.

Of course, as Ms. Zwicky's message shows, a lot of times pasting into a superuser session window is unintentional. More than once I have gone to scroll my xterm window (using the middle button in the scroll-bar area), only to hit the middle button a microsecond too early. BLAM! I've just pasted a mail message into my VMS SYSTEM session, and all of its contents are being interpreted as commands. Luckily nothing major has happened because of this!

Sometimes I think going back to a good old VT100 terminal would be safer all around....

Christopher Lishka   PPE Division, CERN   lishka@dxcern.cern.ch

---

Re: Cut and Paste risks (Zwicky, RISKS-14.62)

Joseph Hall <Joseph_Hall@motsat.sat.mot.com>
Tue, 18 May 1993 14:37:36 -0700

The Macintosh Programmer's Workshop (MPW) shell provides an interesting solution to this problem ... you execute a line of text as a command by pressing the ENTER key (on the numeric keypad). RETURN simply inserts a carriage return in the text. Similarly, pasted text isn't interpreted as commands to be executed.

I wouldn't mind it at all if xterms, cmdtools etc. worked this way. I've yet to experience disaster as a result of X pasting, but I've come close.

Joseph Nathan Hall, Software Systems Engr, GORCA Systems Inc.
jnhall@sat.mot.com joseph@joebloe.maple-shade.nj.us (609) 732-3194

---

re: CHI & the Color-blind? (Yu, RISKS-14.62)

Eric Haines <erich@eye.com>
Tue, 18 May 93 10:22:58 -0400

An article which color interface designers would benefit from reading:

Gary W. Meyer and Donald P. Greenberg, "Color-defective vision and computer graphics displays", IEEE Computer Graphics and Applications, v. 8, n. 5, Sept 1988, p. 28-40.

It discusses how to select colors which are appropriate for the various types of color blindness, along with reasonable general solutions.

Eric Haines

Re: CHI & the Color-blind?

"Tom Ohlendorf - TSU Admin. DP, (410) 830-3642" <D7AP002@TOA.TOWSON.EDU>
Tue, 18 May 1993 08:08 EDT

> "A black icon facing left to right means a call was placed, but no
> contact was made. A red icon facing left to right means a call was
> placed and contact was made, but a promise to pay was not received.
> A green icon facing left to right means a promise to pay was arranged.
> An icon facing right to left means the debtor called the collector."

Not only are the color blind affected by the new monitors, so are the dyslexic. I can very easily see a dyslexic person interpreting a right to left icon as left to right. Suppose the person is color blind and dyslexic....

Tom Ohlendorf, Programmer/Analyst, Towson State University,
Towson, MD 21204 OHLENDORF-T@TOA.TOWSON.EDU (410) 830-3642

RE: CHI & the Color-blind?

David Tarabar <dtarabar@hstbme.mit.edu>
Tue, 18 May 93 15:26:14 -0400

The CHI community is aware of the potential problems that Vannevar Yu has pointed out. For example, the Macintosh User Interface Guidelines has 8 pages devoted to the use of color in applications. They urge developers to "Always develop for black and white first and then colorize that design". They point out that to accommodate "people with color-deficient vision", "you shouldn't use color as the only means of communicating important information. Color should be used redundantly."

I'm sure that other user interface guidelines and texts make similar points. Perhaps the risks here are that applications developers are not aware of (or ignore) the literature about human interface design.

Dave Tarabar dtarabar@hstbme.mit.edu

Re: Denning on NIST/NSA Revelations (Sobel, Denning, Rotenberg)

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Tue, 18 May 93 16:54:22 EDT

In response to David Sobel's statement about NIST and the DSS, I wrote in RISKS-14.60:

> ... NIST issued the DSS proposal along with a public call for comments as part of their normal practice with proposed standards. The community responded, and NIST promptly addressed the security concerns. Among other things, the DSS now accommodates longer keys (up to 1024 bits). As a result of the revisions, the DSS is now considered to be just as strong as RSA.

In RISKS 4.62, Marc Rotenberg responded:

> Denning has to be kidding. The comments on the proposed DSS were uniformly critical. Both Marty Hellman and Ron Rivest questioned the desirability of the proposed standard.
>
> One of the reasons for the concern was the secrecy surrounding the development of the standard. The documents disclosed by NIST and NSA to CPSR make clear that NSA used its classification authority to frustrate the attempt of even NIST's scientists to assess the candidate algorithm.

The DSS is similar to a scheme by El Gamal, which was presented at CRYPTO 84 and subsequently published in the IEEE Trans. of Information Theory (July 85). It is even closer to a scheme by Schnorr, which was presented at CRYPTO 89. The DSS is not classified and the basic approach has been under scrutiny by the crypto community since 84. All of the cryptographers that I have spoken with at NIST have made the assessment that the DSS (as revised in response to the comments by Hellman, Rivest, and others) is at least as strong as RSA for comparable key lengths.
I am unaware of any evidence to the contrary.

Also in RISKS-14.62, Bill Murray wrote

> While it may be true that DSS with a 1024 bit modulus is as secure for digital signatures as RSA, it does not meet either the congressional mandate or the requirement. The congressional mandate was for a public-key standard, not for a digital signature standard. The requirement is for a mechanism for key exchange.

According to NIST, there was no Congressional mandate for a public-key standard. Congress did give NIST the charge to develop standards for sensitive, unclassified information, but it left open to NIST exactly what those standards should be. On its own initiative, NIST issued a solicitation for a public-key standard in the Federal Register, June 30, 1982. My understanding is that the solicitation was very broad and did not identify exactly what functions such a standard would need to provide. Several years later NIST, at their discretion, proposed the DSS.

In retrospect, we can now look back and see how the DSS fits in with Clipper

and Capstone. The result will be a complete package that has encryption,
signatures, and key management/exchange. Thus, the advantage of RSA over the
DSS in its ability to do key exchange disappears.

It is very easy to be critical of a process when you are looking at it from
the "stands" instead of the "court" and from hindsight rather than from
current action and concerns.

Dorothy Denning

Re: NIST's reply to Bidzos (RISKS-14.62)

<horning@src.dec.com>
Tue, 18 May 93 11:22:55 -0700

Ed Roback's last sentence is the zinger, in terms of revealing
the state of mind of those involved in this effort:

> ...and of the law enforcement community for continued legal
> access to the communications of criminals.

What ever happened to "innocent until proved guilty"?

Also, Clipper is only mandated for government use (he says).
I'm all in favor of exposing criminals in government, but is
this really the most cost-effective way?

Jim H.

Re: NIST's reply to Bidzos (RISKS-14.62)

Frederick Roeber <roeber@vxcrna.cern.ch>
Tue, 18 May 1993 10:56:42 GMT

They mean "suspects", not "criminals", don't they?

Re: NIST's reply to Bidzos (RISKS-14.62)

Jim Sims <sims@pdesds1.atg.trc.scra.org>
Tue, 18 May 93 08:49:06 EDT

```
<>        NSA's analysis on the security
<>        risks of the escrow system is not available for public
<>        dissemination.
<>
>>> >>>>  NIST:    It will not be possible for anyone from Mykotronx, VLSI,
<>        NIST, NSA, FBI (or any other non-escrow holder) to
<>        compromise the system.
```

Really? Then why is the NSA/NIST/etc *so* reluctant to release
details of the system? Details that are certainly known
(piecemeal) to the *anyone*s mentioned above.

<> To prevent this, it
<> is envisioned that every time a law enforcement agency is
<> provided access to the escrowed keys there will be a record
<> of same referencing the specific lawful intercept
<> authorization (court order). Audits will be performed to
<> assure strict compliance. This duplicates the protection
<> afforded nuclear release codes. If additional escrow
<> agents are added, one additional person from each would be
<> required to compromise the system.
<>
>>> >>>> NIST: No. First of all, there is strict and limited use of
<> subpoenaed material under the Federal Rules of Criminal
<> Procedure and sanctions for violation. There has been no
<> evidence to date of Governmental abuse of subpoenaed
<> material, be it encrypted or not. Beyond this, other
<> Federal criminal and civil statutes protect and restrict the
<> disclosure of proprietary business information, trade
<> secrets, etc. Finally, of all the Federal agencies cited,
<> only the FBI has statutory authority to conduct authorized
<> electronic surveillance. Electronic surveillance is
<> conducted by the FBI only after a Federal judge agrees that
<> there is probable cause indicating that a specific
<> individual or individuals are using communications in
<> furtherance of serious criminal activity and issues a court
<> order to the FBI authorizing the interception of the
<> communications.

You just *don't* get it, do you? You can make all the laws you want.
You *CANNOT* force anyone to comply with them.

And all the assurances you can give about due process and Federal
judges agreeing, etc doesn't hold water. What Federal judge agreed to
the ATF/FBI sponsored stupidity in Waco Texas recently?

As we have already seen severe erosion of the 'unwarranted search
and seizure' protection for the sake of the phony War on Drugs, how
can you expect anyone to believe the same thing wont happen on a much
larger scale. It's *so* much easier to search electronic
communications than someone's car.... Just ask the NSA.

And speaking of "only after a Federal judge agrees" it seems like you
just introduced a SINGLE failure point into the marvelous triple-lock
system so cleverly crafted....

skeptical, jim

Re: NIST's reply to Bidzos (RISKS-14.62)

Chris Phoenix <efi!chrisp@uunet.UU.NET>
Tue, 18 May 1993 22:28:16 GMT

I have put together a few sentences from NIST. Together they paint a rather scary picture. I don't think I've changed any meanings by taking anything out of context.

```
>>>>>  NIST:      There are no current plans to legislate the use of Clipper.
>         .... The
>             option for legislation may be examined during the policy
>             review ordered by the President.
>>>>> NIST:          ....  We also
>             point out that the President's directive on "Public
>             Encryption Management" stated: "In making this decision, I
>             do not intend to prevent the private sector from developing,
>             or the government from approving, other microcircuits or
                        ^^
>             algorithms that are equally effective in assuring both
       ^^^^^^^^^^         ^^^^^^^^^^^^^^^^
>             privacy and a secure key-escrow system."
           ^^^^^^^^^^^^^^^^^^^^^^^^
>
>>>>> NIST:      You are correct that, currently, Clipper Chip functionality
>             can only be implemented in hardware.  We are not aware of a
>             solution to allow lawfully authorized government access when
>             the key escrow features and encryption algorithm are
>             implemented in software.  .....  Existing software
>        encryption use can, of course, continue.

>>>>> NIST:      No studies have been conducted on a government-wide basis to
>             estimate the costs of telecommunications security
>             technologies.  The needs for such protection are changing
>             all the time.
```

To me it looks like the line quoted from the President's directive only protects private encryption if done in hardware. As they themselves say, there is no known way to enforce the escrow of software encryption keys. Can anyone speculate on the likely results of this "option for legislation" that the President is going to "examine"?

So my feeling from reading all this is that the government may try to legislate the use of encryption that can be implemented only in hardware. I can see it now. "Responding to privacy concerns about the Clipper chip, AT&T has privately developed a new encryption chip using a proprietary algorithm. .... 'In order to ensure that this chip will assure privacy as well as complying with new escrow laws, the algorithm has been submitted to NIST's approval process, and we have made a few changes,' says AT&T spokeswoman ...."

It would not surprise me at all if Clipper ended up in all Newtons, cordless phones, and faxes by the year 2000. This will cause someone to make incredible amounts of money. Has anyone wondered where all this money will go? I am not trying to form a conspiracy theory here--it is possible that the Clipper really was motivated by wiretaps and no one realized how many Clippers could end up being sold. But given the upcoming proliferation of wireless computers, I think this question needs to be asked now. Whatever the origins of Clipper, there is now a serious risk of corruption associated with it just from the money involved. Does anyone have hard estimates on how much additional money flow would be generated by using Clipper in all wireless computers and communication products for the next 10 years?

Chris Phoenix, chrisp@efi.com, 415-286-8581

Re: NIST's reply to Bidzos (RISKS-14.62)

Carl Ellison <cme@ellisun.sw.stratus.com>
18 May 1993 22:40:00 GMT

>What is the smallest number of people who are in a position to compromise the
>security of the system?

```
>>>>>  NIST:      It will not be possible for anyone from Mykotronx, VLSI,
>               NIST, NSA, FBI (or any other non-escrow holder) to
>               compromise the system.  Under current plans, it would be
>               necessary for three persons, one from each of the escrow
>               trustees and one who knows the serial number of the Clipper
>               Chip [...]
```

Clearly, NIST doesn't consider release of a chip's key to outside criminals by one FBI agent to be a compromise of security, if that agent got the key from the escrow agencies in a normal way. Does this mean that once a person has been subjected to a wiretap, he doesn't deserve any security -- no matter what the reason for the tap?

What of the ability of a single gov't employee illegally to declare a national security tap and by weight of authority get escrow holders to release keys? This, too, sounds like a single-source of failure.

What of the possibility of buying two people, one in each agency, to get copies of the whole database? That sounds like 2 rather than 3 to me.

>Did the administration ask these questions (and get acceptable answers) before
>supporting this program? If so, can they share the answers with us? If not,
>can we seek answers before the program is launched?
>

```
>>>>> NIST:       These and many, many others were discussed during the
>               development of the Clipper Chip key escrow technology and
>               the decisions-making process.  The decisions reflect those
>               discussions and offer a balance among the various needs of
>               corporations and citizens for improved security and privacy
>               and of the law enforcement community for continued legal
>               access to the communications of criminals.
```

Clearly, NIST believes that a set of meetings behind closed doors is an
adequate discussion and that we the public should thank them for their
effort and applaud their claimed "balance among the various needs of
corporations and citizens for improved security and privacy and of the law
enforcement community for continued legal access to the communications of
criminals".

Whatever happened to scientists at NIST? Why does it sound like we're
hearing from PR men?

Carl Ellison, Stratus Computer Inc., 55 Fairbanks Boulevard ; Marlborough MA
01752-1298 cme@sw.stratus.com TEL: (508)460-2783

Compromising the escrow agencies

"McInnis, M.R. (Mickey)" <mcinnis@vnet.IBM.COM>
Mon, 17 May 93 23:44:48 CDT

I'm surprised that no one has commented on what I see as an obvious way
to compromise the escrow agencies for Clipper.

Suppose for instance that clipper phones were already available for several
years. Suppose that during the recent Waco standoff, the BATF went to some
gullible federal judge and said:

> "We have found that these people have got a large number of Clipper
> equipped phones. They keep using different phones, and it takes us
> hours or days to process the paperwork, contact the escrow agencies,
> etc. for each new phone they use.
>
> These delays are making a dangerous situation worse and give the
> cultists enough time to plan actions and execute them
> before we can decipher the recorded conversations. It endangers
> the children in the compound and the law enforcement people around
> the compound.
>
> We need you to sign this order that requires the two escrow agencies
> to release the entire set of keys to us. (Since we don't know the
> serial numbers of all the phones he might have.) Of course, we
> don't want the media and the cultists to find out about it, so there
> is a gag order included.
>
> Of course, we will destroy our records once the standoff is over."

The frightening thing about this is that they only have to convince one
federal judge.

Mickey McInnis mcinnis@vnet.ibm.com

◀ ▲ ▶ ℹ

Search RISKS using swish-e □

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 64

Wednesday 19 May 1993

Contents

A Risk of Risks Elided (or no news not always best)

Mike Coleman <coleman@twinsun.com>
Tue, 18 May 93 21:07:18 PDT

The default behavior of the popular newsreader 'nn' is to split (undigestify) digests such as RISKS. Unfortunately, nn seems to omit included articles, such as the Jim Bidzos inclusion in Ed Roback's submission in RISKS 14.62.

Until this is fixed, nn users can include this line in their ~/.nn/init:

```
set split false
```

This should put an end to many unhappy non sequiturs.

Rewards offered for finding bugs in Japanese encryption methods

<forman@cs.washington.edu>
Thu, 13 May 93 10:22:19 -0700

In RISKS-14.60 Klaus Brunnstein implies that "Security by Obscurity" (not making an encryption method public) is a poor way to get a secure encryption method. Both the USA's Clipper Chip and Europe's A5 standards use Security by Obscurity.

Japan doesn't seem to rely on this arcane method:

Professor Shigeo Tsujii of the Tokyo Institute of Technology is offering $3000 to anyone who can find a bug in his new encryption method called "NIKS-TA". (Described in his 15-page thesis.)

Similarly, in 1989 NTT offered $9100 (1M yen) for finding a bug in their encryption method.

> [This could be RISKy if the reward is not big enough,
> and someone on the "other side" is offering more? PGN]

Re: Clipper (Denning, RISKS-14.63)

Jim Bidzos <jim@RSA.COM>
Wed, 19 May 93 10:17:16 PDT

Dorothy Denning wrote in RISKS-14.63, with respect to the key management advantage of RSA over DSS, that the Capstone chip makes the key management advantage "disappear."

I believe that trust is a very significant part of the advantage RSA enjoys over DSS/Capstone, whether for signatures or key management. The scrutiny RSA has withstood in the 17 years since its discovery contributes to that trust. The only way to make that advantage "disappear" is to publish everything about Capstone, including the algorithm that the keys you manage are used with, and wait a few years and a few hundred papers before proposing it as a standard. (Since DES has withstood similar scrutiny, RSA and triple-DES have an advantage to users both in and out of the US that is likely never to disappear as it appears the government will never publish Clipper/Capstone details.)

Re: Clipper (Denning, RISKS-14.60; Rotenberg, RISKS-14.62)

Eric S. Raymond <esr@snark.thyrsus.com>
Wed, 19 May 1993 16:32:46 -0400 (EDT)

In <CMM.0.90.1.737688970.risks@chiron.csl.sri.com> Marc Rotenberg wrote:
> Denning has to be kidding. The comments on the proposed DSS were uniformly
> critical. Both Marty Hellman and Ron Rivest questioned the desirability of
> the proposed standard.

Mr. Rotenberg, as a public figure operating in the political arena, has to exercise a certain diplomatic restraint in responding to Ms. Denning's claims. I am, thankfully, under no such requirement.

As a long-time RISKS reader and contributor, I observe that that this is not the first time that Ms. Denning has apparently operated as a mouthpiece for the NSA's anti-privacy party line on DES and related issues.

I believe Ms. Denning's remarks must be understood as part of a continuing propaganda campaign to marginalize and demonize advocates of electronic privacy rights. Other facets of this campaign have attempted to link privacy advocates to terrorists and drug dealers by suggesting that only criminals need fear wiretapping.

These are serious charges. I make them because, in the wake of the Clipper proposal, I do not believe civil libertarians can afford any longer to assume that their opponents are persons of good will with whom they can simply debate minor differences of institutional means in a collegial way.

It's time for someone to say, in public and on this list, what I know many of us have been thinking. The future is *now*. Electronic privacy issues are no longer a parlor game for futurologists; they are the focus of a critical political struggle, *and the opponents of privacy are fighting their war with all the tools of force, deception, and propaganda they can command*.

The histories of the DES, the FBI wiretap proposal, and now the Clipper proposal must be considered against a wider background of abuses including the Steve Jackson case, "Operation Longarm", and the routine tapping of U.S. domestic telecommunications by NSA interception stations located outside the geographic borders of the United States.

These form a continuing pattern of attempts by agencies of the U.S. government to pre-empt efforts to extend First and Fourth Amendment privacy protections to the new electronic media. In each case, the attempt was made to present civil libertarians with a fait accompli, invoking "national security" (or the nastiness of "kiddie porn") to justify legislative, judicial and practical precedents prejudicial against electronic privacy rights.

While I would not go so far as to claim that these efforts are masterminded by a unitary conspiracy, I believe that the interlocking groups of spies, bureaucrats and lawmen who have originated them recognize each other as cooperating fellow-travelers in much the same way as opposing groups like the EFF, CPSR and the Cypherpunks do. Their implicit agenda is to make the new electronic communications media transparent to government surveillance and (eventually) pliant to government control.

One of the traits of this culture of control is the belief that manipulative lying and dissemblage can be justified for a `higher good'.

I believe that Ms. Denning's disingenuous claim that the DSS "is now considered to be just as strong as RSA" is no mere technical misapprehension. I believe it is propaganda aimed at making objectors non-persons in the debate. I cannot know whether Ms. Denning actually believes this claim, but it reminds me all too strongly of the classic "Big Lie" technique.

It is important for us to recognize that the propaganda lie is not an aberration, but a routine tool of the authoritarian mindset. And the authoritarian mindset is, ultimately, what we are confronting here --- the mindset that regards the fighting of elastically-defined `crime' as more important than privacy, that presumes guilt until innocence is proven, that demands for government a license to override any individual's natural rights at political whim.

We cannot trust representatives of an institutional culture that was *constructed* to deal in information control, lies, secrecy, paranoia and deception to tell us the truth.

We cannot accept the authoritarians' unverified assurances that the sealed interior of the Clipper chip contains no `trapdoor' enabling the NSA to eavesdrop at will.

We cannot trust the authoritarians' assertions that they have no intention of outlawing cryptographic technologies potentially more secure than the Clipper chip.

We cannot believe the authoritarians' claims that `independent' key registries will prevent abuse of decryption keys by government and/or corrupt individuals.

We cannot --- we *must not* --- cede control of encryption technology to the authoritarians. To do so would betray our children and their descendants, who will work and *live* in cyberspace to an extent we can barely imagine.

We cannot any longer afford the luxury of treating the authoritarians as honest dealers with whom compromise is morally advisable, or even possible. Whatever their own valuation of themselves, the thinly-veiled power grab represented by the Clipper proposal reveals a desire to institutionalize means which a free society, wishing to remain free, *cannot tolerate*.

Big Brother must be stopped *here*. *Now.* While it is still possible.

Eric S. Raymond <esr@snark.thyrsus.com>

Re: Clipper (Raymond, RISKS-14.64)

Dorothy Denning <denning@cs.cosc.georgetown.edu>
Wed, 19 May 93 18:37:24 EDT

Eric Raymond has accused me of being part of a propaganda campaign and a "Big Lie." Among his wild speculations, he wrote:

> I believe that Ms. Denning's disingenuous claim that the DSS "is now
> considered to be just as strong as RSA" is no mere technical misapprehension.
> I believe it is propaganda aimed at making objectors non-persons in the
> debate. I cannot know whether Ms. Denning actually believes this claim, but
> it reminds me all too strongly of the classic "Big Lie" technique.

Frankly, I don't know how to respond his allegations other than by saying that I am not and have never been on the payroll of NIST, NSA, or the FBI and that every word I have published has been completely on my own initiative. While I frequently speak with people in these agencies (mainly to ask them questions so that I can be informed) and have considerable respect for them, I am operating on my own initiative and making my own independent evaluations based on all the evidence I can find. I try to avoid pure speculation as much as possible.

My objective in responding to Sobel in the first place was to point out that, in my best judgement, the DSS as revised is as secure as RSA. I did that so that readers would not be led to believe the contrary. Let me elaborate more.

The security of the DSS is based on the difficulty of computing the discret log. (The Diffie-Hellman key exchange, invented in 1976, is likewise so based.) The security of the RSA is based on factoring. My understanding is that the computational difficulty of these two problems is about the same for comparable key lengths, and indeed, the fastest solutions with both come using the same basic technique, namely the number field sieve. If I'm wrong here, I am happy to be corrected by someone who knows more than I do about this.

There are other factors, of course, that must be taken into account. With both schemes, you have to make sure you get good primes. In the case of the DSS, you want really random ones so that you don't get ones with "trapdoors." This is readily done and the chances of getting a trapdoor one are minuscule. For a reference, see Daniel Gordon's paper from Crypto '92.

I still remember the day when George Davida called me up to say that he had cracked RSA. It turned out that he had found a way of exploiting the digital signatures to get access to plaintext (but not keys). I generalized his mathematics and published a paper in CACM (April 84). The solution is to hash messages before they are signed, which has other advantages anyway. I also remember various articles by people pointing other potential vulnerabilities with RSA if the primes weren't picked right.

There are potential weaknesses in all of these public-key methods, but they can be resolved. As near as I can tell, NIST has resolved the potential problems with the DSS, and I am confident that if new ones are found, they will resolve them too.

Dorothy Denning

Clipper chip

<drand@osf.org>
Mon, 17 May 93 17:55:43 EDT

I've just read one of the longer tirades in risks about the clipper chip and feel like putting my foot into the whirling blades :)

Have the naysayers totally forgotten the point of making crypto gear available to individuals? Right now I cannot lift my portable phone without assuming I'm talking to several people aside from the person I call. I treat it as I would a contact on ham radio.

The crooks can listen to us, the government has always been able to. Now, for the first time, there would be some control. Perhaps it isn't perfect. This is irrelevant. It is so many orders of magnitude more secure than any phone system today.

Without the chip being ubiquitous, we cannot have this capability in every one of perhaps a billion phones (guesstimate) in the country. It would be too expensive and totally useless. Both parties must have the same gear.

That the crooks could always create more effective crypto gear is also a red herring. Maybe they could. But the law is being structured so that this itself would be considered probable cause of a crime. We'll have to see if (how much) this is abused. One hopes that just the unlicensed crypto gear would not be sufficient to indict honest people.

Doug Rand drand@osf.org

Re: Clipper - "destroyed" keys

Roger Crew <rfc@research.microsoft.com>
Tue, 18 May 1993 13:05:14 -0700

> Even if you *know* that an instrument has been decoded, in many
> cases management will simply accept the government's word that the
> keys were destroyed rather than replace the instrument(s).

The following excerpt from Peter Wright's _Spycatcher_ comes to mind:

> Jagger was the MI5 odd-job technical man... [He] had an extraordinary array of skills, of which the most impressive was his lockpicking. Early on in training I attended one of the regular classes he ran for MI5 and MI6 in his lockpicking workshop. The cellar room was dominated by a vast array of keys, literally thousands of them, numbered and hung in rows on each wall. Jagger explained that as MI5 acquired or made secret imprints of keys of offices, hotels, or private houses, each one was carefully indexed and numbered. Over the years they had developed access in this way to premises all over Britain.
>
> ``You'll never know when you might need a key again,'' explained Jagger as I stared in astonishment at his collection.

> ``The first rule if you are entering premises is only pick the
> lock as the last resort,'' said Jagger, beginning his lecture.
> ``It's virtually impossible to pick a lock without scratching
> it---and that'll almost certainly give the game away to the
> trained intelligence officer... What you have to do is get hold
> of the key---either by measuring the lock or taking an imprint of
> the key.''

Though this incident dates from the mid 50's, Peter Wright held his post in MI5 (British domestic intelligence) until 1976, and there's no reason to believe that their procedures (w.r.t. keys and locks) changed significantly during that period. And evidently people changed their locks sufficiently infrequently that MI5 felt it worth the expense of maintaining a key farm...

Roger Crew rfc@research.microsoft.com

Re: Clipper/Capstone: No reasonable expectation of privacy?

<Henry_Burdett_Messenger@cup.portal.com>
Wed, 19 May 93 09:42:12 PDT

Nobody has mentioned a risk of the Clipper/Capstone proposal that I thought of last weekend.

You see, we aren't supposed to use Clipper; it will cost too much for ordinary telecommunications usage. Furthermore, there will be no great demand from the citizenry to encrypt their telephones: after all, the ones they already have work perfectly well.

The Supreme Court has already ruled that conversations held over cordless telephones can be intercepted and used as evidence against you without any wiretap warrants*. You have "no reasonable expectation of privacy" on a cordless telephone. How long until the Supremes rule that telephone conversations on wire phones in the clear are also fair game? After all, the Government has given you Clipper; it's your fault if you're not using it...

Therefore, I fear that this will become a class issue: those who can afford Clipper can afford (limited) privacy, but it's open season on those who can't. How *convenient* for our friends in law enforcement!

* Contrast this with early rulings on party lines, where you were not allowed to disclose the content of conversations overheard on a party line.

Henry B. Messenger henry_burdett_messenger@cup.portal.com

Re: Clipper and the "Man in the Middle"

Stephen G. Smith <sgs@grebyn.com>
Sat, 1 May 93 01:36:27 -0400

One thing that I have not seen in the discussion of the Clipper is that
it seems to be totally vulnerable to a "man in the middle" attack.

Take two Clipper chips. Connect them back-to-back. Add some "glue" to pass dialing/routing signals. Insert in the line, either by actually cutting the wire, or by diverting the call in the switch. Now when the victim makes a call, the data is in clear between the two chips. The result is that the tapper now has a clear conversation, the victim has no way of telling if he has been tapped, and there is no need for the song and dance with "escrow agencies".

Note that this attack will work with any protocol that uses "zero knowledge" key exchange. The actual encryption method is completely irrelevant. The only defense is to be able to recognize your caller's key. Something tells me this may be very difficult ....

The only place where the Clipper can provide even minimal security is in mobile communications, where the communications line cannot be cut.

The giveaway that something is fishy, of course, is that the Government will not use the Clipper chip for classified communication. If it's so good, why won't they use it?

Steve Smith   Agincourt Computing
sgs@grebyn.com   (301) 681 7395

Re: Epilepsy and video games (Culver, RISKS-14.63)

David Honig <honig@ruffles.ICS.UCI.EDU>
Tue, 18 May 1993 20:01:01 -0700

"Larry Hunter and others were asking about seizures induced by video games. Not being a neurologist, I wonder if these are similar to those caused by "photic stimulation", which has been implicated in some aircraft accidents.

Some people, when exposed to flickering or flashing lights will have seizures which are quite similar to epileptic seizures. In aircraft, this can be a problem for general aviation pilots, who look through the propeller disk. During most of the flight, the frequency is too high to cause problems, but during a landing, especially into the setting sun, the propeller may cause flickering sufficient to induce a seizure. There are, apparently, degrees of severity: some people will seize from a single flash of the right duration."

Yes, the seizure-risk from video games is exactly that from any flashing light ---whether from propeller, CRT, or LCD.

Re: makedepend problem - a real world example (Worthman, RISKS-14.62)

Conrad Hughes <chughes@maths.tcd.ie>
Wed, 19 May 93 14:31:12 BST

>... makedepend chokes on one of X11 include files (as distributed by Sun)...

On the machine I use (running MIPS RISC/os) makedepend chokes under such circumstances, but doesn't die. The problem arises when you proceed to compile it, and compilation fails because this file doesn't exist and can't be built, yet there is a dependency on it. This consequently doesn't result in a risk, as rather than being built incorrectly, the software cannot be built - typically software should be installed by someone with enough experience to fix such include problems (and what with the nightmarish mess that is the MIPS header file directory tree I've garnered more than my fair share of _that_ experience recently). So - I can't see this bug producing risks other than compilation failure: all it can do is produce too extensive a dependency list, in which case unnecessary parts of the program may be built during compilation, _but_ since the real make process will correctly evaluate all conditional expressions which makedepend assumes are true, the unnecessary parts will not be linked in or installed if you use the supplied "make install"..

[Thinks a bit more] On second thoughts - if someone is guilty of what I'd term bad practice and has an explicit make line for an included file which also modifies some other already-built part of the source beyond just building the required file then a risk does arise. A makefile which does this kind of thing is guilty of fairly poor practice anyway I think..

conrad hughes (chughes@maths.tcd.ie)

Re: Cut and Paste risks (Cook, RISKS-14.63)

Robert L Krawitz <rlk@Think.COM>
Wed, 19 May 93 10:14:35 EDT

> We should identify the main source of the risk, which in my opinion is general access to super-user privileged shells. ...

Yes, but that still doesn't eliminate problems, since most of these accidents are caused by accidentally hitting the mouse buttons rather than carelessness as to what window the mouse is in. The design of most mice makes it very easy to inadvertently hit buttons (this seems to be true on Suns, it was true with both the 1985-style and the current DEC mice, and even with Lisp Machine mice).

The problem is that it's very easy to brush a mouse button while reaching for the mouse, or while moving it. Looking at the way I hold the mouse, my index finger is practically on top of the middle button and my middle finger nearly touches the right button, making an accident of this nature practically inevitable.

Cut and paste is most definitely very useful, and getting rid of it is an overreaction. However, by requiring two independent actions to perform it (e.g. the shift key on the keyboard along with a mouse button), the risk of such an accident is reduced.

I've changed the mouse actions in my xterm windows to use shift bindings for the mouse keys. It's very rare that my left hand is camped on the shift key while my right hand is reaching for the mouse.

Robert Krawitz, Thinking Machines Corp, 245 First St., Cambridge, MA 02142
<rlk@think.com> (617)234-2116 Member of the League for Programming Freedom

Re: CHI & the Color-blind? (Yu, RISKS-14.62)

Flint Pellett <flint@gistdev.gist.com>
19 May 93 14:42:53 GMT

> ...

It seems to me that the answer to that is simple, and it isn't merely color/no color that it relates to: Don't place an over-reliance on icons to convey meaning because they don't always do so (whether colored or not), and the old saying that a picture is worth a thousand words isn't always true. Consider in the example above, if the words "No contact", "Contacted", "Promised", and "Called Us" were displayed instead of the icons, (or under each icon) how much clearer it all would be. (If I had to use the system above, I see myself having to refer constantly to an explanation sheet that says what each icon means, and I would expect to often make mistakes.) Too often people have been creating icon symbols to replace words when the word they replace is one that everyone would understand (at least if they speak that language), and the icon they come up with is one nobody recognizes. You'll find that even people who don't speak the language can learn a word just as easily as they can learn an icon. Icons tend to fail to convey meaning most often when they are trying to replace verbs.

You can make it an option in your interface to let the user choose between use icons/use words/use both, but don't force "only icons" on people. Then you won't have to worry about color-blindness issues.

Flint Pellett, Global Information Systems Technology, Inc., 100 Trade Centre
Drive, Suite 301, Champaign, IL 61820 (217) 352-1165 uunet!gistdev!flint

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 65

Sunday 30 May 1993

Contents

Flight control computers `to bypass pilots'

<Brian.Randell@newcastle.ac.uk>
Thu, 20 May 1993 11:38:26 +0100

[In the following item, the statement: "The system also ensures that no mistakes are made" especially caught my eye! And I imagine that RISKS readers such as Don Norman will have something to say about: "[Pilots] will control by exception, in other words leaving all routine tasks to be done automatically by the computers." Brian Randell, Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne, NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 91 222 7923]

Flight control computers 'to bypass pilots'

The Independent (a national UK paper), 19 May 93

Christian Wolmar reports on a new electronic system for air communications

While aircraft flown with the aid of computers have transformed the role of pilots, communications between aircraft and ground control have changed little since the early days of aviation. "Roger" and his pal "out" still feature prominently, and misunderstood instructions have led to several of crashes.

All that is set to change. Yesterday the first test demonstration of equipment which will allow pilots and air traffic controllers to communicate through computers was held. An experimental BAC 1-11 "flying laboratory", belonging to the Defence Research Agency at Bedford, flew above East Anglia sending and receiving messages on its on-board computer.

This project, called the Experimental Flight Management System, is part of a Europe-wide programme that is expected to enable commercial aircraft to begin communicating in this way by 1998, saving time and reducing the risk of accidents.

Trevor Gilpin, programme manager for the National Air Traffic Services, the organisation responsible for air traffic control, says the new system has many advantages: "The airwaves are getting very cluttered and would not be able to cope with the expected doubling of air traffic over the next 15 years. The system also ensures that no mistakes are made."

Pilots will be able to get weather information on their screens, whereas at the moment they can only do so by tuning to a special radio frequency.

The messages from ground control can also go direct to the plane's auto pilot, which raises the possibility, already mooted by the European aircraft manufacturing consortium Airbus, that pilots may become redundant. Aircraft could be controlled from the ground with a person in the cockpit as a failsafe. A ground-based computer could ensure pilots have carried out its instructions and send a warning if they have failed to do so.

Mr Gilpin feels that there will always be a pilot but accepts that the role of both pilot and air traffic controller will be different: "They will control by exception, in other words leaving all routine tasks to be done automatically by the computers."

At the core of the system is a new form of radar communication, called Mode S, which allows information to be transmitted electronically. For it to be used widely, new transmission centres will have to be built throughout Europe. Mode S allows aircraft to be tracked in four dimensions - including time - which enables tighter control of airspace, reducing delays. Partial introduction of the system is expected in 1996.

Electronic information also needs to be sent between air traffic control centres and already nine, mainly in northern Europe, are able to send messages to each other's computers. This is reducing delays since previously air traffic control centres had to telephone each other with flight plan information.

The urgency of introducing the new system was highlighted last month in a letter to Flight International in which a pilot said that air communications between the Far East and Eastern Europe were so bad because of high demand and old equipment that an accident appeared inevitable. He said: "If and when an accident does occur, I can imagine the amount of words which will be spoken and published in the press and official inquiries wondering how a state of affairs like this has been allowed to exist for so long."

A long-haul pilot also told the Independent that at times he was unable to contact ground control when there were bad radio conditions over the Atlantic "while the guy in the back can phone his wife on a mobile telephone using satellite links".

UK Hacker trial

Brian Randell <Brian.Randell@ncl.ac.uk>
Wed, 26 May 1993 15:50:41 +0100

Hackers given six months for 'intellectual joyriding'
The Independent, 22 May 1993, STEPHEN WARD

TWO COMPUTER hackers given six-month prison sentences yesterday were the first to be jailed under legislation, passed in 1990, to outlaw the practice.

Neil Woods, 24, and Karl Strickland, 22, had pleaded guilty to the offences.
In March, Paul Bedworth, a Yorkshire schoolboy who regularly communicated with Woods and Strickland, and was arrested at the same time, was cleared of similar charges by a jury after a 15-day trial. He had pleaded not guilty and claimed that he had become addicted to hacking.

All three were trapped by sophisticated police and British Telecom telephone tracking in several countries. Before the 1990 Computer Misuse Act, those who gained access to other people's computer networks had to be prosecuted for causing damage or stealing information, but in the case which ended yesterday the judge accepted that the accused had not been intending to cause damage, and had not profited in any way.

Sentencing the two graduates at Southwark Crown Court, Judge Michael Harris said: "I have to mark your conduct with prison sentences, both to penalise you for what you have done and for the losses caused, and to deter others who might be similarly tempted."

The offences were committed over three years before and after the 1990 Act was passed. Strickland, a research assistant at Liverpool University, and Woods, of Chadderton, Oldham, Greater Manchester, a computer salesman and computer science graduate from Manchester University, pleaded guilty to conspiring to obtain telegraphic services dishonestly, and engaging in the unauthorised publication of computer information.

Woods also admitted causing #15,000 of damage to a computer owned by the then Polytechnic of Central London.

The two did not meet until after their arrests in June 1991, although they "spoke" on screen under their codenames. Among hackers, Woods was known as "Pad", and Strickland as "Gandalf" (the wizard in Tolkien's Lord of the Rings). Using personal computers at home, they were frequent illegal users of a BT network called PSS, and a system known as "Janet", which linked academic institutions throughout Britain.

Strickland's hi-tech conquests included the United States space agency Nasa and ITN's Oracle network- since replaced by Teletext. Woods keyed into systems run by the Ministry of Defence, the European Community and the Financial Times.
Counsel for both men agreed that their clients, who received their first computers when they were 11 years old, became "obsessed" with them.

"If your passion had been cars rather than computers we would have called your conduct delinquent, and I don't shrink from the analogy of describing what you were doing as intellectual joyriding," the judge said.

He went on: "There may be people out there who consider hacking to be harmless, but hacking is not harmless. Computers now form a central role in our lives, containing personal details, financial details, confidential matters of companies and government departments and many business organisations.

"Some, providing emergency services, depend on their computers to deliver those services. It is essential that the integrity of those systems should be protected and hacking puts that integrity into jeopardy."

He said that hackers needed to be given a "clear signal" by the courts that their activities " will not and cannot be tolerated".

The judge added that he had hesitated long and hard before sending two young men to jail. Although there were powerful factors in their favour, prison for them was inevitable, he said.

Detective Sergeant Barry Donovan, formerly attached to Scotland Yard's computer crimes squad, said that since the publicity surrounding the arrest of Woods and Strickland, the amount of hacking in Britain had decreased dramatically, although it was still an international problem.

Computerised Intensive Care Unit

H}kan Karlsson <ch92hka@csd.uu.se>
Fri, 28 May 1993 14:36:56 +0200

The Swedish issue of "Apple News" (2/93) includes an article about a computerised Intensive Care Unit at the Hospital for Sick Children in Toronto, Canada. Each bed has a Macintosh Quadra at the bedside monitoring blood pressure, temperature, etc., and controlling various life-critical functions. Unfortunately(naturally?), the article has no information about the reliability of the system. The hospital is a part of the University of

Toronto and responsible for development of the system is Gordon Tait and clinic manager is Dr. Geoffrey Barker.

I would like to get more information about this system, especially reliability questions and risk assessment.

H.Karlsson   Department of Computer Science, University of Uppsala, Sweden
(ch92hka@cs.uu.se)

Computerized telephone solicitations

Jane Beckman <jane@stratus.swdc.stratus.com>
Fri, 28 May 93 15:34:56 PDT

I heard on the radio about two weeks ago that a judge had ruled that computerized (non-live-human) phone calls were indeed legal, as a form of free speech, and thus struck down a law banning them.

In the time since the ruling, I have received *two* computerized advertisements on my phone at work. This is a much higher proportion than in times past, when it was more like two a year. Obviously, the computerized phone advertisers are making up for lost time!

Jane Beckman   [jane@swdc.stratus.com]

Credit-card retention by phone number

<ark@research.att.com>
Tue, 25 May 93 18:06:21 EDT

Today I received electronic mail from a friend of mine in Sweden saying that he had gotten a substantial credit card bill from a camera store in New York and didn't remember having ordered anything. It didn't take me long to figure out what had happened.

Sweden has substantial import duties on photographic equipment, but exempts equipment acquired and used abroad and then brought home. My friend has occasion to visit the US several times a year and often takes the opportunity to add to his equipment collection when here.

If his trip includes a visit to my house, it is particularly convenient for him to order stuff, charge it to his credit card, and ask it to be shipped to me.

Several weeks ago, I had occasion to order from the same store. As with every order of mine except the first, they asked me `Would you like us to charge that to the same credit card you used for the last order?' and I said `yes.' Since it had always worked before, I didn't bother to verify the number.

Evidently they file credit card numbers by shipping address rather than by cardholder address, because my friend's credit card number became the one in

my file.
--Andrew Koenig ark@europa.att.com

Cash machine keypad risk?

Paul Potts <potts@oit.itd.umich.edu>
Thu, 20 May 93 15:14:30 EDT

I've been using ATMs very frequently for at least 7 years,
but this is the first time I've ever had this problem...

A few days ago on my way in to work I stopped at a cash machine to get some money for cappucino. When punching in my password, I noticed there was a significant delay between pushing the key and the corresponding "beep." The keypad seemed to be behaving erratically. I tried to punch in $20.00 to withdraw. This proceeded something like <2> <pause> <beep>, <0>

Stop The Madness!

"Arthur R. McGee" <amcgee@netcom.com>
Thu, 27 May 1993 12:56:45 -0700 (PDT)

So did anyone else watch or tape yesterday's Donahue which talked about(yes, it was just a matter of time) Virtual Reality and Sex?<sigh>

I just heard a new term the other day, "Cybergasm."<sigh> I now really know how Stanton feels, I'm sick of all the weirdness and sensationalism too.

Oh yeah, here's something from the latest EDUPAGE newsletter:

---------- Forwarded message ----------

[stuff deleted]

YOU CAN'T SAY THAT ON THE INTERNET. Censorship has hit the Internet, where battles over free speech are being waged on several fronts. Colleges in Canada have banned all electronic discussions of sex, and controversy is raging stateside over a program that automatically wipes out anonymous messages and the suspension of a California professor who ran a BBS that carried messages harassing a female student. Congress has even gone so far as to order a study of whether bulletin boards, on-line services and cable TV are being used to encourage "crimes of hate." (Wall Street Journal 5/24/93 B1)

[stuff deleted]

Art "Rambo" McGee [amcgee@netcom.com] [72377.1351@compuserve.com]
Voice: [1-310-320-BYTE]

The risks of teaching about computers and the law

Peter D. Junger <junger@samsara.law.cwru.edu>
Fri, 21 May 93 16:13:46 EDT

A fortnight ago, in order to postpone the necessity of grading final exams, I started writing a simple-minded encryption program, which uses a "one-time pad" as a key, for use this Fall in my class on Computers and the Law. The program is intended to demonstrate certain things that lawyers who are going to deal with the problems generated by computers should know: things like the nature of an algorithm and the fact that any text (that is encoded in binary digits) of length n contains (if one just has the key) all other texts of length n.

Although in that course we shall mainly be concerned with copyright and patent issues relating to computer programs, we should also spend some time on security issues and on government regulation of computer programs. And that, of course, includes the regulation of the export of computer programs, including cryptographic programs and technical information relating to such programs. I shall also have to discuss cryptographic programs when dealing with issues of computer security, since it would profit lawyers to be aware of the fact that cryptography can do far more than the law can to keep one's confidences confidential. The latter point is, of course, of particular importance to members of a profession who have a legal and moral duty to keep their clients' confidences confidential from everyone, but especially from the agents of the state.

As I was writing this program I realized that it itself, and any `technical data' relating to it, might be subject to federal export licensing regulations, since I intended to give copies of it to, and discuss it with, my students and make it available to anyone who wants it, even foreigners. Even if I do not put it on an anonymous FTP server, as I originally planned, there is no way that I can guarantee that all the students who enroll in my class will be citizens or permanent residents of the United States.

After a little quick research I have determined that my program may be--and, in fact, probably is--subject to such licensing, though whether by the Department of Commerce or that of State is a matter that it will take some sixty days for the bureaucrats to determine. The trouble is that the program, which should run on any PC clone running MSDOS 3 or higher, and which now consists in its entirety of 174 bytes of 8086 machine code, which I am pretty sure I can get down to 170 bytes or less, is squarely covered by the definitions of Category XIII of the U.S. Munitions List (as is my old Captain Midnight Decoder, which I got during the War for a boxtop--or was it an Ovaltine label?--and change).

The relevant subdivision of Category XIII of the Munitions List is (b), which provides in relevant part:

> (b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including:

> (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:
>
> .... [none of the exceptions appear to be applicable to my program]

There is no exception for encryption software that is so simple minded that a law teacher, whose only degrees are in English and law, can hack it out in about six hours, most of which time was spent chasing bugs that were the result of typos. I estimate that the average computer literate 12-year old could have written the program in about 20 minutes.

In the course of my researches, which so far have consisted of speaking to a very pleasant person at the Department of Commerce's Bureau of Export Administration, to a not very nice major and a slightly nicer person at the Department of State's Bureau of Politico-Military Affairs, Office of Defense Trade Controls, and to a not un-nice person, whose name I was not allowed to know, who supposedly was at NSA, and wading an inch or so into a seven inch stack of Commerce Department regulations and a few more inches of statutes, I have concluded that if I `export' my little program without first getting a license I may be subject to a fine of not more than $1,000,000, or imprisonment for not more than ten years, or both.

This isn't so bad, since in the case of the actual program it is pretty clear that `exporting' means exporting, so, since I don't intend to export the program, the only problem is that posting it on an FTP server on the internet gets into a `grey' area (according to the unknowable at NSA). Of course, if the program is considered to be my expression--which it must be if it is protected by the copyright laws--it is probably a violation of the First Amendment to require me to get a license before I can export it. But since I don't intend to export it--and the unknowable, on whom I dare not rely, did keep saying that it was a matter of my intention--I can treat that issue as an academic problem. (By the way, it is my position that the actual program--the machine code--not being in any sense expression--cannot Constitutionally be protected by copyright law; this is a position that the lower courts have--at least _sub silentio_--uniformly rejected, but it is a good bet that the Supreme Court will agree with me when it finally gets around to considering this issue!)

The real trouble is that Category XIII contains as its final subdivision paragraph (k), which covers

> (k) Technical data . . . related to the defense articles listed in this category.

And that, of course, means that I cannot lawfully export technical data about my program without first obtaining a license.

But the regulations relating to technical data that is included on the Munitions List say, in effect, that the `export' of technical data includes talking about the defense article to which the data relates--which in my case is my piddling little program--in the presence of someone who is neither a citizen of the United States nor admitted to permanent residence in the United States. So, if any foreign students sign up for my course I will be required to get a license--which I am not sure I can get at all, and certainly will not be able to get in time to teach my course--before describing the program to my class, explaining how to use it, and giving them the source code--which, by the way, I contend _does_ contain expression--to load in with the debug program.

I admit that I am not greatly concerned about the potential criminal penalties that might be imposed if I do discuss the program with my students without a license, and not only because I don't have a million dollars and--far all I know--may not have ten years. I cannot imagine anyone--except perhaps that major--who would be stupid enough to try to punish me for discussing my trivial program with my students.

But how can I teach this particular bit of computer law if the very act of teaching amounts--at least in theory--to a criminal violation of the very law that I am teaching? That this is not a logical paradox is an illustration of the fact that the law is not logic; but I still feel that I am trapped in an impossible situation.

It is hard for me as a law teacher to believe that this regulatory scheme that requires me to get a prior license each time that I speak about, or publish the details of, my trivial program (or, in the alternative, to make sure that no foreigners get to hear or read what I have to say about it) can withstand a constitutional challenge on First Amendment grounds.

The "secret" of how to keep a secret in 170 bytes or less is not something that imposes any conceivable threat to the security of the United States, especially not when the underlying algorithm is well known to most who are, and many who aren't, knowledgeable about computers--or, for that matter, about logic. And thus the government can't constitutionally punish me for revealing this "secret" of mine or talking and writing about how it works. And even if the government could constitutionally punish me after the fact, that does not mean that they can impose a prior restraint on my speaking or writing about the "secret". Prior restraints on speech or publication--and especially licensing schemes--are especially vulnerable to constitutional attack, since the First Amendment provisions relating to the freedom of speech and of the press were adopted in large part to prevent the federal government from adopting the type of censorship and licensing that had prevailed in England under the Tudor and Stuart monarchies.

And yet I am so intimidated and disheartened by this unconstitutional scheme that I dare not explain in a submission to Risks, which undoubtedly has foreign subscribers, how my silly little program works. And even if I were willing to take that risk, I could not in good conscience impose it on our moderator.

And if I have problems now, just think how ridiculous the

situation will be if the government tries to outlaw all encryption
programs and devices other than the Clipper Chip.

[For those of you who understand how my program works and who take the effort to write your own encryption program based on that understanding, I have a special offer. If you will just send me an E-mail message certifying that you are a United States Citizen, I will send you (at any address on the internet that is within the United States), a UUENCODEd key that when applied by your program to this particular submission to Risks--after all headers have been stripped off--will produce a working copy of my program, which is a COM file that runs under MSDOS. (Be sure that your copy of this submission uses the Carriage Return / Line Feed combination as the End of Line indicator.)]

Peter D. Junger

Case Western Reserve University Law School, Cleveland, OH
Internet: JUNGER@SAMSARA.LAW.CWRU.Edu -- Bitnet: JUNGER@CWRU

[Incidentally, at last week's IEEE Symposium on Research in Security and Privacy, a rump group decided that because crypto falls under munitions controls, the right to bear arms must sanction private uses of cryptography! PGN]

Disaster Avoidance & Recovery Conference & Exhibition May 26-28

Nigel Allen <ae446@freenet.carleton.ca>
Wed, 19 May 93 22:16:03 EDT

Here is a press release from the Disaster Avoidance & Recovery '93 Conference.

Disaster Avoidance & Recovery Conference & Exhibition May 26-28;
To: Assignment Desk, Daybook Editor
Contact: John Mungenast of Insystex Inc., Ventura, Calif.,
805-650-7052, or
George J. Whalen of G.J. Whalen & Co. Inc., New Rochelle,
N.Y., 914-576-6750

News Advisory:

Disaster Avoidance & Recovery '93, sponsored in part by AT&T, NCR and Power Quality magazine, will take place May 26-28, at the Sheraton Premiere at Tyson's Corner, in Vienna, Va.

CEOs, participants from government, technology, financial manufacturing and utility companies, other major industry and key government groups are expected.

They will hear from a blue-ribbon faculty of experts whose presentations will deal with all sides of disaster preparedness and recovery, sharing latest planning methods and technology to ward off, deal with and rapidly recover from natural or man-made disasters.

The intensive three day conference points up the reality that U.S. businesses, buildings and people are more at-risk than ever before and that our technology-dependent society now relies on a "house of cards" of interdependent computers, telephone and power utilities.

Keynote speaker will be Rep. Dick Swett (D-N.H.), who sees preparedness as a "new war" against natural and man-made threats. Assessments of recent wide-area disasters (Hurricanes Andrew and Iniki, floods, Nor'easters, tornados, earthquakes, fires and blizzards) and a comprehensive review of the terrorist attack on the World Trade Center will introduce topics such as evacuation, medical care and shelter, building vulnerability, standby power, elevator design flaws, plus how to plan against high-rise disasters.

Participants will also discover that only a handful of utilities now have tested, workable disaster and recovery plans in place... that few power companies have "mutual aid plans" with telephone companies, even though they share the same poles and conduits and despite the fact that telephone companies rely in part on electric utility power.

Counter-terrorism authorities will advise on protective measures, while telecommunications, computer, power and business recovery xperts will deal with how disasters can strike through our near-total dependency on computer technology and its vulnerability to the minute-by-minute quality of electrical power.

There is a side benefit of all this: the wave of new methods, technology and products now emerging to improve preparedness of U.S. businesses is stimulating the economy with new jobs, new contracts and new opportunities. Additional information and details about Disaster Avoidance & Recovery '93 can be obtained from John Mungenast at Insystex Inc., the conference organizer, 805-650-7052 during business hours (Pacific time).

Nigel Allen, Toronto, Ontario, Canada ae446@freenet.carleton.ca

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 66

Tuesday 1 June 1993

Contents

Possible RISK in data retrieval?

Dale Drew <d44758@druid.Tymnet.COM>
Thu, 20 May 93 12:26:27 PDT

Has anybody seen this? I can forsee many potential risks in an on-line data retrieval system involving Probationers. How do the Probation Officers call in to check or (:gasp:) update their data? I've asked BI Inc., but have not heard a reply:

BOULDER, Colo., May 12 /PRNewswire/ -- BI Inc. (NASDAQ-NMS: BIAC), the nation's leading provider of electronically monitored systems for corrections, today announced receipt of notification from the United States Patent Office of issuance of a patent to BI on April 20, 1993. BI's newly granted patent includes the application presented in the BI PROFILE(TM) automated administrative caseload management system.

At no cost to corrections agencies, BI PROFILE provides automated administrative caseload management via a computer located at BI Monitoring Corp.'s central station. Probationers are assigned individual PIN numbers and security passwords, and required to call a 900 number once a month to report any administrative changes. BI's computer asks the callers a series of questions (i.e., change in home telephone number, address, employment, etc.). Each call placed averages 2 or 3 minutes in duration and is charged to the probationer's home telephone bill. Considered exception reporting, BI PROFILE only provides reports to corrections agencies if probationers fail to call in on their pre-assigned monthly date or if any status changes are reported during the calls. Prior to BI PROFILE, administrative caseload management of probationers has been via a manual system which has put a significant burden on corrections agencies as the number of probationers continues to rise at the federal, state and local levels.

Additional options available on BI PROFILE are features to insure that probationers are calling from the designated telephone number, that probationers have not previously called in for the month, collection of monthly probation supervision fees and 800 telephone service for the indigent population. BI has additional patents pending on these and other BI PROFILE options as well.

BI PROFILE services are offered to the corrections market by BI through its wholly owned subsidiary, BI Monitoring Corp. (BIMCORP). "BI PROFILE is another service offering from BI Monitoring Corporation that is the direct result of BI's strategy to expand its recurring revenue base," said John K. Fulda, Jr., BI's corporate vice president in charge of BI Monitoring. "We believe that the BI PROFILE family of services offers tremendous growth potential for BI Monitoring Corporation in the years ahead," he concluded.

CONTACT: Joanna Manley of BI, 303-530-2911; or Tom Dean of
Innovative Research, 212-421-2543, for BI

[Dale Drew, Sr. Information Security Specialist, BT North America, Inc.
(408) 922-6004 d44758@druid.Tymnet.COM]

X application to finger

<nandu@cs.clemson.edu>
Fri, 21 May 93 13:54:00 EDT

Here is an interesting episode.

I run an X application (public domain) that, given a list of remote sites and a list of userids, periodically "finger"s the sites, searching to see if the named users are logged on. If yes, they are updated on a small screen window.

Following is a mail I received from the security officer at one of the sites...It was interesting to note that sys admins *are* on the lookout for even those minor chances of hacking

-------- The mail --------

I assume since you're logged into the console, you have some responsibility for machine.cs.univ.edu:

It appears that somebody may have cracked your system, and is using it as a base to attempt to break into other systems: every six minutes, some process on your machine contacts the finger daemon on cs.anotheruniv.edu and attempts to see who is logged on. This is generally taken as an attempt to extract usernames, preparatory to hacking the system.

Strangely, this seems to be correlated to your being logged in. It appears
to have started on May 12th. I've ignored it before now since until this
point it has been only a minor annoyance. We would appreciate your looking
into this matter, and seeing that it ceases.

Nandakumar Sankaran, Graduate Student, Computer Science Department

G34, Jordan Hall, Clemson University, Clemson, SC 29634 (803) 656 6979
nandu@cs.clemson.edu

Re: Fake ATM Machine Steals PINs

Brinton Cooper <abc@BRL.MIL>
Wed, 19 May 93 17:13:49 EDT

<eric@cadkey.com> describes the now-well-known fake ATM scam for capturing account and PIN numbers for subsequent forging in order to relieve consumers of the burden of large account balances. Recall that the ATM "scam artists" obtained permission from officials of the shopping Mall where the scam took place.

He asks, "How are you supposed to stop this new trick???" Like many RISKS, you don't "stop" the trick but you minimize the RISK:

1. You needn't be the first in your block to use the new ATM.

2. Watch for announcements from your bank or credit union of new locations. Our credit union announces in its newsletter *every* new ATM which it owns/installs (i.e., were members pay no fee for access). One could have been suspicious of the (around here) then-uncommon installation in local groceries, but they were announced as mentioned.

3. You could always phone the bank whose name appears on the ATM. If there's no name, who's running the machine?

_Brint

COMPASS '93 ANNOUNCEMENT

Dolores Wallace <wallace@swe.ncsl.nist.gov>
Tue, 1 Jun 93 11:37:52 EDT

[FOR SOME REASON THE CONFERENCE MANAGEMENT DID NOT SEND THIS ANNOUNCEMENT
TO RISKS UNTIL 1 JUNE, WHICH IS AFTER THE ANNOUNCED DEADLINE FOR DISCOUNTED
REGISTRATION. Karen Ferraiolo (see below) has agreed to give a special
deal to RISKS SUBSCRIBERS, SO THAT YOU MAY REGISTER UNTIL THE END OF THIS
WEEK AT THE REDUCED RATE. However, she asks that you let her know ASAP.
We do not generally run conference announcements in full, but in light of
the closeness of the date and the special consideration for RISKS readers,
it seemed appropriate. This conference has always been closely related to

the RISKS subject matter. PGN]

COMPASS '93
Eighth Annual Conference On Computer Assurance:
Systems Integrity, Software Safety, and Process Security

June 14-17, 1993
Gaithersburg, MD

U.S. Department of Commerce
Technology Administration
National Institute of Standards and Technology

COMPASS	IEEE Aerospace and Electronics Systems Society
Sponsors	IEEE National Capital Area Council

In Cooperation with British Computer Society

Conference	Arca Systems, Inc.
Sponsors	ARINC Research Corporation
	Control Systems Analysis, Inc.
	CTA, Inc.
	IBM
	Logicon, Inc.
	National Institute of Standards and Technology
	Naval Research Laboratory
	Naval Surface Warfare Center
	Systems Safety Society
	TRW Systems Division
	U.S. General Accounting Office

The goal of COMPASS, an acronym formed from COMPuter ASSurance, is to advance the theory and practice of the creation and use of critical systems through the medium of scientific and engineering meeting and publications. COMPASS expresses the idea of "Pointing the Way" and of "enCOMPASSing" many technologies and technical disciplines. The logo, a variation of yin-yang overlaying a compass rose, symbolizes both of these ideas. We invite you to participate in COMPASS activities and increase the benefits of COMPASS.

Monday, 14 June 1993

8:00 am	Registration Opens
9:00 am - 4:00 pm	Tutorials (Parallel Sessions)

1. "Formal Methods with Automated Support Using PVS", John Rushby, SRI International

   This tutorial provides an introduction to formal methods with special focus on the use of automated support tools such as PVS, a Prototype "next generation" Verification System that attempts to provide the benefits of powerful and effective automation for an expressive specification language. Worked examples will be demonstrated "live" and include examples from hardware design, fault tolerance, and real-time.

2. "Federal Criteria (New Orange Book)", Janet Cugini, NIST

This tutorial, on the preliminary draft of the Federal Criteria for Information Technology Security, will cover background, future work, protection profiles, TCB functional components, development assurance requirements, and evaluation assurance requirements. It includes constructing a protection profile and the seven defined protection profiles.

Tuesday, 15 June 1993

8:00 am Registration Opens

9:00 am Welcome
James H. Burrows
Director, Computer Systems Laboratory, NIST

Opening Remarks
Judith Bramlage, COMPASS '93 General Chair

9:15 am Program Information
John J Marciniak, COMPASS '93 Program Chair

9:30 am Keynote
Peter Neumann, SRI International
"Myths of Dependable Computing: Shooting the Straw Herrings in Midstream"

10:30 Break

11:00 am Technical Session 1 "Verification Technology"
Moderator: Connie Heitmeyer, Naval Research Laboratory

"A Tool for Reasoning about Software Models", Sidney Bailin, CTA, Inc.

"An Incremental Protocol Verification Method for ECFSM-based Protocols", C. Huang, National Cheng Kung University

"A Verifier for Distributed Real-Time Systems with Bounded Integer Variables", Farn Wang and Al Mok, University of Texas

1:00 pm Lunch

2:00 pm Special Topics (Invited talks)
Moderator: Peter Neumann

"Global Protection against Limited Strikes (Trusted Software Methodology)", Carol Taylor, National Security Agency

"Application of the High Trust Process Model to

Complexity Management and System Architecture in the
SDI", John McHugh, University of North Carolina, and Greg
Chisholm, Argonne National Laboratory

3:00 pm Break

3:30 pm Special Topics continued

"Using Ada in Secure Systems", Roberta Gotfried,
Hughes Aircraft Company

"A Risk-Based Approach to Cost-Benefit Analysis of
Software Safety Activities", Stephen C. Fortier, Intermetrics,
and James Bret Michael, Argonne National Laboratory

4:30 Adjourn from NIST

7:00 pm Birds of a Feather (Parallel Sessions; held at Marriott)
"Processes (Capability Maturity Model)", John Baumert, CSC
"Standards for Formal Methods", Roger Fujii, Logicon, Inc.

(Dessert will be provided)

Wednesday, 16 June 1993

8:00 am Registration Opens

9:00 am Keynote Address
Rona Stillman, Chief Scientist, U.S. GAO

10:00 am Break

10:30 am Technical Session 2 "Reliability Measurement"
Moderator: Reginald Meeson, Institute for Defense Analyses

"Rare Conditions - An Important Cause of Failures", Herb
Hecht, SoHaR, Inc.

"Experimental Evidence of Sensitivity Analysis Predicting
Minimum Failure Probabilities", Jeffrey Voas, Jeffrey
Payne, and Chris Michael, Reliable Software Technologies,
Corp. and Keith Miller, College of William and Mary

"Assigning Probabilities for Assurance in MLS Data Base
Design", Lucien Russell, Argonne National Laboratory

1:00 pm Lunch

2:00 pm Technical Session 3 "System Safety"
Moderator: Michael L. Brown, Naval Surface Warfare Center

"Risk and System Integrity Concepts for Safety-Related
Control Systems", Ron Bell, Health and Safety Executive (UK)

"Identifying Generic Safety Requirements", Jarrellann
Filsinger, Booz-Allen & Hamilton and J.E. Heaney,
The Mitre Corporation

"Software Safety and Program Slicing", Keith B.
Gallagher, Loyola College and NIST, and James R. Lyle, NIST

3:30 pm   Break

4:00 pm   Debate
Moderator: Emilie J. Siarkiewicz, Rome Laboratory
Resolved: "Productivity & Techniques of Assurance Can Co-exist"

Debaters: Peter Neumann (SRI), Charles Bonneau (Mitre),
Phil Parker (CTA, Inc.), John McHugh (UNC), and Jon Dehn (IBM)

5:00 pm   Adjourn

6:30 pm   Banquet (at Marriott Hotel)
Speaker: Dorothy Denning, Georgetown University

Thursday, 17 June 1993

8:00 am   Registration Opens

9:00 am   Technical Session 4 "Management and Developmental Issues"
Moderator: Charles Payne, NRL

"Developing Secure Systems in a Modular Way", Qi Shi and
John McDermid, University of York

"On Security Policy Modeling", James Freeman, CTA, Inc.

"Management Aspect of Software Safety", Stephen Cha,
Aerospace Corporation

10:30 am   Break

11:00 am   Panel 1 "Developing Standards and Issues"
Moderator: Dolores Wallace, NIST

"MIL-STD-SDD (Software Development and Documentation)",
Raghu Singh, SPAWAR, U.S. Navy

"Software Safety Standards - A European Perspective",
Robin Bloomfield, Adelard

"ISO 9000 Standards", Taz Daughtrey, Babcock & Wilcox

"MIL-STD-882C", Michael L. Brown, Naval Surface Warfare Center

1:00 pm   Lunch

2:00 pm Panel 2 "Results of Workshops/Studies"
Moderator: H.O. Lubbes, Naval Research Laboratory

"Mitre Critical Assurance Workshop", Chuck Howell,
Mitre Corporation

"An International Survey of the Industrial Applications
of Formal Methods", Susan Gerhart, National Science Foundation

"Federal Criteria (Report on Comments Workshop)", Eugene
Troy, NIST

3:30 pm Awards and Closing Ceremony

Location NIST, located in Gaithersburg, MD, is approximately 25
miles northwest of Washington, D.C. The meeting will be
held in the Green Auditorium of the Administration Building.

Social Functions

Birds of a Feather (Dessert) will be held at the Gaithersburg Marriott on Tuesday, June 15th at 7:00 pm. A banquet with a cash bar and banquet speaker will be held at the Gaithersburg Marriott on Wednesday, June 16th at 6:30 pm.

Transportation

BWI Limo, 301/441-2345, offers commercial van service from Baltimore-Washington Airport to Gaithersburg area. Call for reservations. Airport Transfer Van Service, 301/948-4515, is available from Dulles International and Washington National Airports to Gaithersburg. The Washington Metro has subway service to Gaithersburg. Metro can be boarded at Washington National Airport. Take a Yellow Line train marked "Mount Vernon Square" to Gallery Place and transfer to a Red Line train marked "Shady Grove" to Shady Grove. Service is every 6 to 15 minutes depending on the time of day. The Shady Grove station is approximately four miles from the Marriott Hotel. Contact Marriott for shuttle information.

Accommodations

Conference registration does not include your hotel reservation. A block of rooms has been reserved at the Gaithersburg Marriott Hotel, 620 Perry Parkway, Gaithersburg, MD 20877. The hotel phone number is 301/977-8900. The special room rate is $70.00 single or double. To register for a room, please use the enclosed hotel reservation form and send it directly to the hotel no later than May 31, 1993. After that date the rooms will be released for general sale at the prevailing rates of the hotel. [PERHAPS KAREN CAN HELP NEGOTIATE A LATER DATE HERE... PGN]

Registration Karen Ferraiolo
Information COMPASS '93 Registration
Contact Arca Systems, Inc
8229 Boone Blvd, Suite 610
Vienna, VA 22172

Phone: 703/734-5611
Fax: 703/790-0385

Technical   Judith Bramlage
Information   U.S. General Accounting Office
Contact   441 G Street NW
Washington, DC 20548
Phone: 202/512-6210
Fax: 202/512-6451

Driving Instructions

>From northbound I-270 take Exit 10, Rt. 117 West, Clopper Road. At
the first light on Clopper Road, turn left on to the NIST grounds.
>From Southbound I-270 take Exit 11B, Route 124 West, Quince Orchard
Road. At the second light turn left on to Clopper Road. At the
first light on Clopper Road, turn right on to the NIST grounds. To
reach the Administration Building, turn left after passing the
guard office. Signs will direct you to visitor parking.

Transportation will be provided to and from the Gaithersburg
Marriott and NIST Monday through Thursday.

==============================

Conference Registration Card

Advance Registration (Before 30 May 1993) [4 JUNE FOR RISKS READERS]

Conference Registration (includes 1 copy of proceedings)_____
Proceedings Only _____
Extra Proceedings _____ copies _____
Tutorial #1 - Formal Methods _____
Tutorial #2 - Federal Criteria _____

Name____
Company____
Street Address____
Rm. No./Mail Code____
City, State, ZIP____
Country____
Business Telephone____
IEEE Membership Nbr____
Co-Sponsor Name____
Total Amount US $____

_____ Check here is you will be using the shuttle to and from
the Marriott and NIST (free!).

Form of Payment

_____   Check enclosed made payable to COMPASS '93. (Checks
from outside the USA must be written on a USA

bank.)

_____ MasterCard No.________________________Exp._____
_____ VISA Card No.__________________________Exp._____
_____ Diners Club No.________________________Exp._____
_____ American Express No.__________________Exp._____
Authorized Signature____

Request for refunds after 30 May 1993 will be subject to a $15 administrative fee.

See below for registration fees and mailing instructions.

"In reviewing the Institute for Electrical and Electronics Engineers' plans for COMPASS Conferences, The Assistant Secretary of Defense (Public Affairs) finds this event meets the standards for participation by DoD personnel under instruction 5410.20 and DoD Standards of Conduct Directive 5500.7. This finding does not constitute DoD endorsement of attendance which must be determined by each DoD component."

Registration Fees

NOTE: Members belong to sponsoring or cosponsoring organizations.

Advanced (before 30 May 1993) [4 JUNE FOR RISKS READERS]

			Speakers,
		Non-	One-Day &
	Members	Members	Students
Conference	250	315	100
Tutorial	50	70	50
Proceedings Only	20	30	20

On-Site (after 30 May 1993) [4 JUNE FOR RISKS READERS]

			Speakers,
		Non-	One-Day &
	Members	Members	Students
Conference	300	375	100
Tutorial	70	90	50
Proceedings Only	20	30	20

Fee includes coffee breaks, lunches, and social functions

Place Conference Registration Card in envelope and mail to :

Karen Ferraiolo
COMPASS '93 Registration
Arca Systems, Inc
8229 Boone Blvd, Suite 610
Vienna, VA 22172
Phone: 703/734-5611
Fax: 703/790-0385

==============================

Hotel Registration Card
Marriott Hotel, 301/977-8900

Name____
Company____
Street Address____
Rm. No./Mail Code_____________________________________
City, State, ZIP______________________________________
Country____
Business Telephone____________________________________
Arrival Date____
Departure Date____
Number of Persons_____________________________________

Rate $70 single or double (apply 12% tax to rate). All reservations must be received by 30 May 1993. All room reservations must be guaranteed by a one-night deposit. Deposit will guarantee first night availability, and will be credited to last night of reservation. Deposit refunded if request received 48 hours prior to reserved arrival.

Form of Payment

_____ Check enclosed made payable to The Gaithersburg Marriott
_____ One night deposit enclosed $___________________
Guaranteed by_______________________________________Exp._____
Card No.____
Authorized Signature__________________________________

Please place in envelope and mail to:

The Gaithersburg Marriott
620 Perry Parkway
Gaithersburg, MD 20877

==============================

Board of Directors

Chair: Dolores R. Wallace, NIST
Vice-Chair: Anthony Shumskas, Logicon, Inc.
Treasurer: Dario DeAngelis, Logicon, Inc.
Secretary: Michael L. Brown, Naval Surface Warfare Center
IEEE AESS: Robert Ayers, ARINC, Inc.
IEEE NCAC: Arthur Cotts
Members: Judy Bramlage, U.S. General Accounting Office
John Cherniavsky, National Science Foundation
Frank Houston, Weinberg Associates
H.O. Lubbes, Naval Research Laboratory
Juan Zumbado, IBM

Conference Committee

General Chair:	Judith L. Bramlage, U.S. General Accounting Office
Program Chair:	John J. Marciniak, CTA, Inc.
Arrangements:	Laura M. Ippolito, NIST
Publications:	Ann Boyer, Control Systems Analysis
Publicity:	Paul Anderson, Space and Naval Warfare Systems Command
Registration:	Karen Ferraiolo, Arca Systems, Inc.
Treasurer:	Bonnie P. Danner, TRW Systems Division
Tutorials:	Michael L. Brown, Naval Surface Warfare Center

Program Committee

Paul Ammann, George Mason University
Michael L. Brown, Naval Surface Warfare Center
Albert Mo Kim Cheng, University of Houston
Jarrellann Filsinger, Booz-Allen & Hamilton
John J. Marciniak, CTA, Inc.
Reginald N. Meeson, Jr, Institute for Defense Analyses
Matthew Morgenstern, Xerox Design Research Institute
Adam Porter, University of Maryland
James Purtilo, University of Maryland
Marvin Schaefer, CTA, Inc.
Cynthia Wright, Defense Information Systems Agency
Tony Zawilski, The Mitre Corporation

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 67

Tuesday 1 June 1993

Contents

Crypto as "Right to Bear Arms" issue

Larry Hunter <hunter@ncbi.nlm.nih.gov>
Tue, 1 Jun 93 11:46:47 -0400

Following Peter Junger's depressingly Kafkaesque description of why US export restrictions on cryptographic technology (or even technical data related cryptography) makes it probably illegal to discuss his 174-byte MSDOS program implementing a one-time pad in the law class he teaches, our esteemed moderator said:

> Incidentally, at last week's IEEE Symposium on Research in Security and Privacy, a rump group decided that because crypto falls under munitions controls, the right to bear arms must sanction private uses of cryptography!

This is a point I have been making in private for some time. I am completely convinced that framers of the Constitution would have wholeheartedly endorsed citizen access to effective encryption as a fundamental right. It's a natural part of the outlook that posits that the citizenry should be able to publish subversive literature in their basements, own enough weaponry so that a local militia should be able to hold off the government, and that there is a positive obligation to rise up in revolution against an unjust government.

However, there are several practical problems with the idea. First of all, constitutional rights must be balanced against each other. Your right to bear arms is balanced against the rights of your neighbors to pursue their happiness in an orderly society. One consequence of that balance is that you cannot legally possess nuclear weapons or even, say, a .50 caliber machine gun privately. PGN's statement not withstanding, just because a munition is export regulated does not mean that private US uses of these weapons are allowed. It is not hard to imagine the Supreme Court finding a compelling state interest in regulating cryptologic technology in the same manner it does machine guns. So the "right to bear arms" strategy for defending encryption doesn't seem likely to succeed practically. Second, the approach seems to stipulate that secure encryption is a "dangerous" technology, which I suspect is a mistake. After all, "arms" are weapons, instruments of combat, something to fight with. That is not how to envision encryption. To my mind, it is much more like a private place, or a refuge; quite the opposite of an instrument of combat. Encryption and related technologies empower individuals and private associations, without threatening anyone else. Arms empower people precisely through direct threats to others. This distinction is not a small one. We should be fighting the claim that cryptography is useful primarily to criminals (and is therefore threatening) for precisely the same reason.

On the other hand, perhaps we could enlist the NRA in defending effective encryption. Powerful allies are crucial in this fight, and I for one would be willing to find common ground with all kinds of folks to ensure that effective encryption technology becomes widely available.

[Please note explicitly that I do not speak for the the National Library of Medicine or the US Government on this issue. Thanks.]

Larry Hunter, National Library of Medicine, Bethesda MD. hunter@nlm.nih.gov

Re: Peter D. Junger's risks of teaching... (RISKS-14.65)

Paul Robinson <TDARCOS@MCIMAIL.COM>
Sun, 30 May 1993 19:48:23 -0400 (EDT)

> A fortnight ago, in order to postpone the necessity of
> grading final exams, I started writing a simple-minded encryption
> program, which uses a "one-time pad" as a key, for use this Fall in
> my class on Computers and the Law.

It's always nice to try things. I'm working on writing an SMTP gateway to run on PCs to make E-Mail much more accessible to them. The stuff out there is complicated and troublesome to use. You mentioned that your program is only 174 bytes: that's good; we need people to write things small and tight.

> As I was writing this program I realized that it itself,

> and any `technical data' relating to it, might be subject to
> federal export licensing regulations,

I suspect if this is what the law means, then the law is on its face unconstitutional.

You might want to write to the EFF or the ACLU.

Try asking someone at the office the following question: If a reporter for the New York Times were to publish your algorithm in the paper, would the reporter or the Times be required to get a license before it could print the article?

If he says yes, then he is declaring the law is a law mandating prior restraint.

Judges frown heavily on laws mandating prior restraint, and especially since we are talking about the work of a private individual, not someone working on a contract for a government agency. If you know the law, you know that while the courts usually uphold laws unless the other party can show that the statute is unconstitutional, if a law is shown to constitute prior restraint, the courts tend to strike down the law unless there is an extreme burden proven by the government, i.e. that there is no other way to fix the problem the law supposedly solves.

If the law would even be able to withstand challenge, it would have to do so using the method going back to the censorship laws on motion pictures, it may be that if the law in question is an attempt to license a particular type of expression, the agency may be held to the same standard as that used in the censorship laws, i.e. that the agency must promptly issue a license or file suit to prevent distribution. A law that permits an agency to restrict publication of a work and use delay to hold it out of distribution is clearly unconstitutional.

The Copyright office has already taken a look at this issue: a work expressed on a computer does not become something different from a work printed on paper.

Question: do you think the law would require you to get a license before publishing this in a technical journal? Or require the journal in question to do so?

>   After a little quick research I have determined that my
> program may be--and, in fact, probably is--subject to such
> licensing,

I've never had to handle stuff I wrote but I sometimes have questions regarding stuff which I've sent as E-Mail or mailed overseas to people.

I generally ignore such laws; I believe there is a general "public" exemption for publicly published material or anything not subject to specialized licensing, i.e. if something is put on a BBS or is sold over the counter in a store, it can be shipped anywhere in the world (except Vietnam, Libya and Cuba, and any of the countries with banns, such as Iraq, etc.) PKWare has encryption in it and the people there discovered that the restrictions don't apply to it as long as they don't ship to Vietnam or Cuba.

> ... I have concluded that if I `export' my little program
> without first getting a license I may be subject to a fine
> of not more than $1,000,000, or imprisonment for not more
> than ten years, or both.

Do you really expect people who are involved in trying to keep anyone from learning anything about encryption to admit that it's okay to export something or to give out information?

There was a case a while back in which a man who left the CIA published something without getting approval. In a case that was decided by the Supreme Court, the rules permitted them to require - since he had signed a contract - him to get approval to write anything for publication, for life, it still did not require him to get approval to give speeches extemporaneously.

Call (or better, write) the Office of the General Counsel for one of these organizations and ask two simple question and ask a yes or no answer, "If there was an encryption program written from scratch by a non-government employee, published by a reporter in the New York Times, would the Times or the reporter be required under the ITAR regulations or other federal laws, to obtain a license before it could publish the article?" "And would they be subject to fines or imprisonment for doing so without a license?" (There are lots of people who are not American Citizens and not legal residents who read the Times, as well as copies sent overseas.)

If they say no, you have a legal ruling from them.

If they say "yes" then you should put out a press release saying so:

"X department claims it has right to require
newspapers to obtain government licenses to print
stories and can impose fines and imprisonment on
reporters or newspapers who do not obtain
government licenses in advance."

Quote from the letter, and name the source. Send it to your local newspaper and the Times and others. To get reporters to notice, you have to hit them where they live.

> Of course, if the program is considered to be my expression--which
> it must be if it is protected by the copyright laws--it is probably
> a violation of the First Amendment to require me to get a license
> before I can export it.

It also depends on the size. A program that is only 174 bytes in length may be so short that the application and expression merge, especially if it's the only means available to perform the application at hand. Also, something that is minor and inconsequential in nature may not be subject to copyright protection.

What that long item means is that a two-line poem is too short to be copyrightable; a 5 note song is also too short. With applications now approaching 20 meg and more, 174 bytes might be considered so short it's not copyrightable.

> It is hard for me as a law teacher to believe that this
> regulatory scheme that requires me to get a prior license each time
> that I speak about, or publish the details of, my trivial program
> (or, in the alternative, to make sure that no foreigners get to
> hear or read what I have to say about it) can withstand a
> constitutional challenge on First Amendment grounds.

It wouldn't. My guess is the law has never been enforced or challenged. The law is probably void as (1) prior restraint (2) vague (3) overly broad (4) excessive fines (4th Amendment).

> [...]

That doesn't necessarily apply that the recipient is in the U.S. Any site that's on the Internet can be accessed by telephone which can be anywhere. MCIMAIL is in the U.S. but anyone on a telex network or Datanet address worldwide can call into it.

But I am, for the sake of argument, willing to declare that I am an American Citizen and would like a copy.

Paul Robinson -- TDARCOS@MCIMAIL.COM

Export Controls on Cryptography

<WHMurray@DOCKMASTER.NCSC.MIL>
Mon, 31 May 93 09:13 EDT

Professor Peter Junger describes a program thus:

>The program is intended to demonstrate certain
>things that lawyers who are going to deal with the problems generated by
>computers should know: things like the nature of an algorithm and the
>fact that any text (that is encoded in binary digits) of length n
>contains (if one just has the key) all other texts of length n.

Of course, if what he says above is true, and he asserts that he can so demonstrate, then I can produce an algorithm and a key to demonstrate that the program that he has described is encoded under the description. Indeed, I can produce an infinite number of such keys and algorithms, all of which decode to the the same algorithm. Surely, that should be sufficient to convince a jury of twelve that it was his intent to do so.

He has already published this description on RISKS. I think that his very text offers evidence that he "knows" that RISKS is exported. Surely, I can offer "proof" that he had "reason to know."

Do I not now have a prima facia case? Out of his own mouth, pen, keyboard!? Have I not now succeeded in shifting the burden of proof to him? What defense might he offer? (That someone else can produce an equal number of algorithms and keys that do not decode to such a program?) Will it convince? Am I not now in a position to convict, at least in many cases, on mere accusation?

Junger, you still have time to deny that you wrote that post. If you fail to recant on a timely basis, I plan to denounce you to the thought police.

And for those of you who think that I have failed to make my case, I suggest that you read the history dealing with the thought police. History is clearly on my side.

William Hugh Murray, Executive Consultant, Information System Security
49 Locust Avenue, Suite 104; New Canaan, Connecticut 06840
1-0-ATT-0-700-WMURRAY; WHMurray at DOCKMASTER.NCSC.MIL

Crypto Export Controls

<WHMurray@DOCKMASTER.NCSC.MIL>
Mon, 31 May 93 09:31 EDT

> [...]

Is there anyone out there who can find grounds to exclude my notebook, or any other modern computer, from this definition, whether or not it contains encryption software? Is it the intent of the law to include my computer? It is possible to arrive at a definition that includes what the law intends and excludes my computer? Can we safely leave the the discretion to distinguish to the signals intelligence elite?

William Hugh Murray, Executive Consultant, Information System Security
49 Locust Avenue, Suite 104; New Canaan, Connecticut 06840
1-0-ATT-0-700-WMURRAY; WHMurray at DOCKMASTER.NCSC.MIL

Re: Peter D. Junger's risks of teaching... (RISKS-14.65)

Carl Ellison <cme@ellisun.sw.stratus.com>
Mon, 31 May 93 12:27:37 EDT

It sounds to me like you're trying to publish, not export.

Back in the bad old days, the NSA tried to prevent publication of information about cryptology including lectures to foreign students, conferences with foreign nationals present, ... This attempt was soundly defeated (and that may be why we've had these less obvious struggles in the years since then).

Publication is legal -- happens all the time -- no license. International meetings are legal -- happen all the time -- no license. You can buy a full technical description of the DES algorithm from the US Govt

(FIPS-PUB-46), with no export controls and then write code from that. RS&A
published their algorithm as equations in the Feb 1978 CACM and to a user
of Mathematica, what they published was perfectly good code.

You tell me: is an anonymous FTP node a publication or an export medium?
What about a magazine which includes a floppy disk?

> [Incidentally, at last week's IEEE Symposium on Research in Security
> and Privacy, a rump group decided that because crypto falls under
> munitions controls, the right to bear arms must sanction private uses of
> cryptography! PGN]

That's one approach.

I prefer distinguishing between cryptographic munitions (eg., crypto devices which are specially hardened for battlefield use or crypto devices containing secret NSA algorithms or algorithms created by companies and sold to the government as alternatives for secret NSA algorithms), standard commercial cryptography (crypto algorithms (devices or software) invented in the private sector and intended for private sector customers) and free cryptography (algorithms invented by individuals, often in academia, fully published, available anywhere in the world that there are programmers (eg., DES and RSA, (for non-commercial use))).

Clearly, the first should be considered arms and controlled by the State Department, the second a product of commerce and controlled by the Commerce Department, and the third a product of free speech and totally uncontrolled.

Meanwhile, a good reading of David Kahn's "The Codebreakers" shows that cryptosystems in the latter two categories have traditionally been at least as strong as those in the first category, so it makes no sense to try to categorize these systems based on someone's (eg., NSA's) opinion of their cryptographic strength.

[My comments to NIST for this week's conference made essentially these points, although in those I referred to two classes instead of the three there clearly are.]

Carl Ellison, Stratus Computer Inc., 55 Fairbanks Boulevard ; Marlborough MA
01752-1298 (508)460-2783 cme@sw.stratus.com [RIPEM PUBLIC KEY DELETED]

Re: Peter D. Junger's risks of teaching... (RISKS-14.65)

Tim Poston <tim@iss.nus.sg>
Tue, 1 Jun 1993 13:06:34 GMT

risks@CSL.SRI.COM (RISKS Forum) writes:
Peter D. Junger's posting had
: There is no exception for encryption software that is so simple minded
: that a law teacher, whose only degrees are in English and law, can hack
: it out in about six hours, most of which time was spent chasing bugs

: that were the result of typos. I estimate that the average computer
: literate 12-year old could have written the program in about 20 minutes.

Surely this is covered by the sensible supralegal principle "De minimis non curat lex"? (The law does not concern itself with trifles.) Without this principle, almost any law stated in natural language can be run into the ground. With it, a sane court would throw out any case that a deranged prosecutor might bring.

Granted that law and sanity can be far apart, that often "The law is an ass", and so on, but surely one must assume it is not _completely_ psychotic to make (as P. D. Junger has) the decision to spend one's working life teaching and/or practising it?

Tim Poston

Re: Peter D. Junger's risks of teaching... (RISKS-14.6)5

Jonathan Haruni <jharuni@micrognosis.co.uk>
Tue, 1 Jun 93 14:17:52 BST

Peter D. Junger (junger@samsara.law.cwru.edu) wrote:
> [about his amusing and sad conundrum of being unable to teach law students
>   about a law without breaking it.]

I think that if you give your students copies of your comp.risks article, they should all be sufficiently disheartened with American law that they will quit the program and you can then present your lectures to a class devoid of foreign (or any) students.

Alternatively, you could check passports at the door, and boot out foreign students during the parts of your class which are essential to American Sickurity. By doing so you will raise eyebrows well outside of the computer-and-law sphere of interest and you may bring this ludicrous situation into the limelight. But then, you may get sacked.

Probably a much more effective solution to your problem, and one which has recently been proven perfectly legal and acceptable in an American court, would be for you to merely shoot dead all the foreigners in your class, after which you can speak freely.

Your posting raised some questions in my mind, and perhaps after your recent research into the topic you would be able answer:

What exactly do you have to do to "export" a crypto system ? You raise the ambiguous possibility of putting it on a public FTP site. What happens if you go abroad and do so ? Go abroad with the sytem in your mind only - no magnetic or paper copies of any kind - type the code in from scratch at a keyboard outside the U.S., and post it to an FTP site outside the U.S. Have you "exported" the code ?

What if you come up with a general idea for a simple crypto system and then
avoid thinking about it until you have left the country. You leave,
then create the system, type it in and post it. Have you exported it ?
Are you ever allowed to bring it back to the USA again ?

Jonathan.

Re: Peter D. Junger's risks of teaching... (RISKS-14.65)

Martin Minow <minow@apple.com>
Tue, 1 Jun 93 09:27:34 -0700

I was surprised that Peter Junger did not conclude his discussion of the problems caused by his 174-byte encryption program with the all-purpose academic response:

-- a grant proposal to study the issue.
-- an article published in an appropriate academic journal.

At the very least, there should be ample material here for a graduate seminar.

Thanks for a wonderful submission.

Martin Minow minow@apple.com

Re: Peter D. Junger's risks of teaching... (RISKS-14.65)

Jerry Leichter <leichter@lrw.com>
Tue, 1 Jun 93 15:40:49 EDT

In a recent Risks, Peter D. Junger talks about his attempts to deal with the US export regulations that define cryptographic equipment as weaponry, and place strict controls on the export either of the "weaponry" or "technical data" about them.

While more sophisticated in his writing, what Mr. Junger is really doing is simply repeating an argument we've seen many, many times on the net:

1. Anyone can write cryptographic software, so where is the secrecy?

2. The regulations as written forbid export of such things as - a favorite example that Mr. Junger surely did not re-invent independently - Captain Midnight Decoder rings.

Let me turn the question around. Sure, it's easy to find examples at the extreme where the regulations look silly; how would YOU phrase a regulation to control the export of cryptographic devices? Yes, I know some people believe the world is a benign place - the Cold War is over and all that (funny, before the end of the Cold War the same people had no trouble finding other arguments supporting their position); they need go no further. For the rest of us: Even today, you might want to control export of, say, very high-speed encryption chips, especially suitable for use in military command and control systems. How about conjectural software, 500 man-years in the making after a large research investment, for breaking cryptosystems used by the US for communicating with its embassies abroad? (Not all software is trivial to develop!)

Mr. Junger teaches law. Perhaps he'll take up the challenge of suggesting regulatory wording that covers "significant" cryptographic "equipment" - along the way, perhaps, coming up with a distinction that can be made in some useful way among "equipment", "software", and "specifications".

The only distinction *I* can see how to make is between cryptosystems in actual (past, present, or planned future) operational use, and everything else. The first class could presumably be covered under existing espionage laws; but is that really enough? Such laws would probably NOT cover the 500-man-year product mentioned above.

Mr. Junger is also surprised at his inability to get a straight answer on the regulations, as they apply to his trivial program, from a number of government officials he spoke to. I think he's being naive.

A number of years ago, while I was traveling out of state, my car's license plate was stolen. I called the police to report the stolen plate, and asked what I should do. I was told that I could not move the car until I went to the main registry office (60-70 miles from where I was, with no convenient transportation) to get a temporary plate. Not thinking, I pointed out how impractical this was. The cop's response was the same: I'd have to get a temporary plate. Not being TOO dense, I thanked him for the information and hung up.

Now, you know, and I know, and the *cop* knows, that it's absurd to expect someone to spend a full day, at considerable inconvenience and expense, traveling across state to get a temporary plate so they can drive home. Anyone rational would tell me to do what I actually did: I made a cardboard replacement plate (with a suitable note) and went about my business.

But the *cop* couldn't tell me that. He couldn't even hint at it. In his particular position, it is not his place to suggest to someone that they violate the law, even if the violation is a trivial one of a plainly silly law. I'm sure Mr. Junger will confirm that no lawyer would have suggested that I do it either - though a decent lawyer, not being a direct representative of the law enforcement community, would no doubt have seen his way clear to mention that LEGALLY I had to get the replacement plate, but in practice nothing was likely to happen if I didn't.

What would Mr. Junger have expected government officials charged with enforcing the export laws to say? "Hey, just ignore it? It's silly?" No bureaucrat will EVER say that; and, in fact, no bureaucrat in such a position SHOULD say it. It's not the bureaucrat's place to judge the regulations; it's his position to enforce them. He certainly has latitude in deciding which violations that come across his desk are worth pursuing - and certainly the chances of anyone being prosecuted for exporting a Captain Midnight decoder ring are a hell of a lot less than the chance that I would have gotten into

trouble for driving home with my cardboard plate - but he's just plain not in
a position to tell you that.
-- Jerry

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 68

Tuesday 1 June 1993

Contents

Error on California Unemployment Checks

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 1 Jun 93 17:26:46 PDT

The California Employment Development Department sent out 75,000 duplicate unemployment checks --- which it attributed to a "computer error" [you guessed it, right?]. "Those who cash their checks will be asked to reimburse the state or will have future benefits docked," said a spokesperson.
[Source: San Francisco Chronicle, article by Jonathan Marshall, p. A15.]

[I wonder what the increased workload will be in trying to recover from this accident, and whether they will actually catch all of those who cashed the extra check or will do so at some point in the next six months! PGN]

Re: Fake ATM Machine Steals PINs

"Dan Franklin" <dan@diamond.bbn.com>
Tue, 1 Jun 93 14:59:45 EDT

Brinton Cooper <abc@brl.mil> suggests several good ways to reduce the RISK that you're dealing with a fake ATM machine.

Another way to "authenticate" an ATM machine is to use it to ask for your bank balance--a piece of information only a genuine ATM would (presumably) have. Since you can't do this without giving the machine your PIN, a failure means you have to check your bank balance every few days thereafter to see if someone made a withdrawal--or just change your PIN. But if you believe the risk of the machine being fake is low, and a way to phone the bank whose name appears on the machine is not apparent, this is another possibility.

Dan Franklin

Re: CHI & the Color-blind?

John R. Levine <johnl@iecc.cambridge.ma.us>
20 May 93 21:12:50 EDT (Thu)

The question of whether color-blind people can see signs and controls isn't particularly a computer related one, but is certainly made more of an issue by the complex interfaces common in computerized systems.

The number of people affected is surprisingly large. I'm not very color blind and have no trouble telling red from green, so long as they are fairly bright, but a have a real problem with black-on-red or red-on black signs and displays. They look like, say, maroon on crimson, with practically no contrast. (For some reason, green doesn't seem to have this problem.) I believe this is a common problem for the large number of slightly color blind people. For the more severely color blind there is also the better-known problem is of not being able to distinguish between reds and greens of similar brightness.

For designers of computer displays, I'd think it would be straightforward to test them for color-blind robustness by replacing the color pallette used in the program with a monochrome one that maps each color to an suitably bright shade of grey. Or if that's hard, one could always point a video camera at the sign or display and show the image on a black-and-white TV.

Regards,
John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

Defending Crypto with the 2nd Amendment

"Peter K. Boucher" <boucher@csl.sri.com>
Tue, 1 Jun 93 16:13:52 -0700

There's a risk in associating your cause with the 2nd Amendment.
Some constitutional protections are "more equal" than others.

hunter@ncbi.nlm.nih.gov (Larry Hunter) writes:

> ... One consequence of that balance is that you cannot legally possess
> nuclear weapons or even, say, a .50 caliber machine gun privately.

"A well regulated militia, being necessary to the security of a free state,
the right of the people to keep and bear arms, shall not be infringed."

Everyone I know who has studied the history of this statement agrees that it means that "the people" must have unrestricted access to all types of arms, in order to a) obviate the need for a standing army, and b) defend the country in the absence of a standing army. No one I know expects (or desires) that private ownership of nuclear arms be allowed (although private ownership of the most powerful weapons of the day, such as canons, was common in the 18th century, and is exactly what the framers of the constitution sought to protect). Also, a .50 caliber machine gun can be purchased legally in most states, if you pay the appropriate federal tax.

Paul Robinson <TDARCOS@MCIMAIL.COM> writes:

> Judges frown heavily on laws mandating prior restraint, ...

This is good if use you some other amendment (not the 2nd) to back up your case. The Brady Bill (which mandates a 5-day waiting period on the purchase of a handgun) is pure prior restraint. There is no empirical evidence whatsoever that it will have any beneficial impact on the level of violent crime in the U.S. Such laws have been enacted in several states, but none has ever been shown to have reduced any aspect of violent crime. Even though the premise of such laws is "government must restrain the people prior to the purchase of a handgun, on the chance that the purchaser might be planning to commit a crime with it," none of them has ever been struck down for this reason.

Pick another amendment with which to defend crypto, because the 2nd is risky.

Peter K. Boucher

Re: Crypto and the 2nd Amendment (Hunter, RISKS-14.65)

"David A. Honig" <honig@binky.ICS.UCI.EDU>
31 May 93 20:34:21 GMT

PGN writes:

> [Incidentally, at last week's IEEE Symposium on Research in Security
> and Privacy, a rump group decided that because crypto falls under
> munitions controls, the right to bear arms must sanction private uses of
> cryptography! PGN]

While this may amuse some, this actually addresses at a profound and often overlooked intent of the 'Founding Fathers'. The People are guarenteed the right to bear arms, not just for personal defense (which was obvious to them), but also because: politicians prefer unarmed peasants. An unarmed populace is much easier to dominate. And so is a populace without the ability to have privacy.

David Honig

Re: Crypto as "Right to Bear Arms" issue, followup

Jim Purtilo <purtilo@cs.UMD.EDU>
Tue, 1 Jun 93 18:25:51 -0400

Just a point of information concerning Larry Hunter's post on the analogy between encryption as a "fundamental right" and other rights, such as those recognized by the US Bill of Rights. Larry observes:
# ... I am completely convinced that framers of the Constitution would have
# wholeheartedly endorsed citizen access to effective encryption as a
# fundamental right. ...

Unfortunately, Larry then reasons that "the `right to keep and bear arms' strategy for defending encryption doesn't seem like to succeed practically" based upon some erroneous assumptions concerning the second amendment.

# .... there are several practical problems with the idea. First of all,
# constitutional rights must be balanced against each other. Your right to
# bear arms is balanced against the rights of your neighbors to pursue their
# happiness in an orderly society. One consequence of that balance is that
# you cannot legally possess ... , say, a .50 caliber machine gun privately.

Of course, some thoughtful citizens would observe that there is no balancing act in Larry's statement. Your neighbors' ability pursue their happiness in an orderly society is enhanced by both your and their ability to accept responsibility for personal safety in this otherwise unsafe world. And this includes responsibility for protection from potentially corrupt governments.

Regardless, by the analogy to personal weaponry (machine gun), Larry weakens his point unnecessarily, since in fact these *can* be owned and used in this country. They are taxed and regulated, but nevertheless legal to own by any honest citizen, not otherwise having local restrictions. The real balancing act in his analogy is between too-powerful government and the threat posed by an armed citizenry -- and in fact our history has many examples where the government has backed off or altered potentially unfair policies based upon the fear of the consequences when We the People reasserted control via arms.

Information is the ultimate in personal "arms". In today's age, how else than by knowing the citizenry's thoughts and plans can a government preserve and protect its power base? That is to say, encryption technology becomes a powerful protection of citizens from from too-big government, and *control* of encryption is that big-government's counter.

Fortunately, Larry concludes with a message many of us soundly support:
# We should be
# fighting the claim that cryptography is useful primarily to criminals (and
# is therefore threatening) for precisely the same reason [that we fight
# claims that speech, arms, etc. are only useful to criminals.]

Jim Purtilo

Get yer RSA encryption now! (more on CLIPPER)

Jay Schmidgall <shmdgljd+@rchland.ibm.com>
Thu, 20 May 1993 08:16:07 -0500 (CDT)

In RISKS DIGEST 14.64, drand@osf.org writes:
|> That the crooks could always create more effective crypto gear is also a red
|> herring. Maybe they could. But the law is being structured so that this
|> itself would be considered probable cause of a crime. We'll have to see if
|> (how much) this is abused. One hopes that just the unlicensed crypto gear
|> would not be sufficient to indict honest people.

Ok, I guess I must have skimmed over this part. Let me see if I understand this properly:

> If I have got more secure crypto gear, probable
> cause exists that I have committed a crime.

Hmmm. Does this include any crypto gear that may have been purchased before the corresponding CLIPPER-enabled gear became available? Or am I allowed to deduct the cost of the gear I previously bought as well as the cost of the new CLIPPER gear I must buy to fall into line with the law?

Of course, this becomes a powerful tool for anyone interested in secured international information exchange. Since it is probable that most countries that use an existing (more secure?) encryption standard are not likely to switch to CLIPPER, any one exchanging such information must own gear capable of understanding that encryption. Hence, probable cause and you are tapped.

Hmmm again. Does knowledge of the encryption algorithm also count as probably cause? After all, one can always do it in software... Hmmm again. Do they have to be able to find a program which implements it, or merely some text which describes the algorithm?

I expect this will become worse than the witch hunts of old; however, instead of starting a rumour that someone you don't like is a warlock or witch, the rumour will be that "Jay knows RSA!"

Somehow, to me this seems the most horrific part of this whole mess. I do hope I've misunderstood.

jay@vnet.ibm.com (c) Copyright 1993. All rights reserved.

Re: Clipper (Bidzos, RISKS-14.64)

<Carl_Ellison@vos.stratus.com>
Wed, 19 May 93 21:48 EDT

Jim Bidzos writes:

>The only way to make that advantage "disappear" is to publish everything about
>Capstone, including the algorithm that the keys you manage are used with, and
>wait a few years and a few hundred papers before proposing it as a standard.

Whit Diffie also asked for publication of the Skipjack algorithm.

That's good, as far as it goes, but it's possibly more important to publish papers giving design rules and cryptanalysis methods so that the readership can judge the quality of your cipher design methods. This occurs in the private sector (especially in academia) but is not something we're likely to see from the NSA.

Although I would love to learn their methods, I wouldn't want the NSA to publish these details. I want my tax dollars to be of some good and NSA secrecy is part of that package.

So -- I just don't want any NSA involvement in commercial cryptography. We'll limp along on our own. Perhaps, if we do something really stupid (eg., use RSA when the NSA knows that the PRC's cryptanalysts know how to factor 1000 bit numbers in seconds) they'll be nice enough to tell us, but that's the limit of the interaction I would hope to have with the NSA.

In particular, I hope this round of examination of export policy exempts commercial cryptography (especially freely available code) from controls. It's not even good gallows humor that my company is restricted from shipping DES subroutine code to a country where there is DES subroutine code already on BBSs.

Then again, maybe that is how we will have to develop code from now on: write code assuming that the customer will find and install his own public domain subroutine packages of DES, RSA, etc. ....

Re: AIS BBS (RISKS-14.61)

Kim Clancy <clancy@csrc.ncsl.nist.gov>
Mon, 17 May 93 10:02:00 EDT

I am the sysop for the AIS BBS mentioned earlier. I would like to submit 2 pieces of information for your readers. One, the bbs number is 304-420-6083, although that will be changing soon, details are on the bbs. The second is that the screen captures displayed in the message to RISKS were done at at time when Mary Clark was taking care of the administrative function of upgrading user's access. She is a trainee and has no decisions on the management of the bbs; that is my job. I don't want to see her name tied to this as she is only functioning as directed. Her name was only on the bbs for a short period of time and has since been removed. It is unfortunate that this screen capture occurred during the very short period of time her name was listed, at least I view it as that. Any questions about the bbs should be directed to me. Thanks much. Kim Clancy

---

Re: Questioning AIS purpose and defending anonymous posting

Paul Ferguson <fergp@sytex.com>
Mon, 17 May 93 09:55:57 EDT

(Friedman, RISKS-14.60)

This reference was extracted from Computer Underground Digest, (CuD), #5.36 (May 16 1993), File 2--Building Bridges of Understanding in LE & Comp. Community -

> The problem with many of these formats is that they tend to exclude
> the average computer user or law enforcement agent. There's now an
> alternative. Kim Clancy, a security specialist for the Dept. of
> Treasury's Office of Public Debt, has begun the "round-table forum
> on Mindvox to bring a variety of views into open dialogue. The intent
> is to increase the understanding by the public of the legitimate tasks
> of law enforcement, and to expand an awareness of the civil liberties
> concerns of the computer public for investigators and others. Law
> enforcement personnel are understandably hesitant to engage in such
> discussions. But, from what I've seen, there is no ranting, the
> discussions are generally of high quality (although an occasional
> topic drift does occur), and those participating are sincere in their
> attempts to stimulate discussion.

[...]

> Kim's [Clancy] credentials for moderating this type of a forum are
> impressive. In addition to her security and anti-virus skills, she
> set up the AIS BBS, BBS run by Dept. of Treasury, Bureau of Public
> Debt. Run by Computer Security Branch, AIS BBS is intended as a
> resource for security specialists, scholars, or others seeking
> information about the varieties of computer abuse and how to combat
> them. The files range from CERT advisories, documents on viruses,
> and "underground" files to simple public domain/shareware utilities,
> such as virus checkers. For those lacking ftp access, AIS BBS is
> an excellent source of information and a public service of value
> to a broad range of computer professionals and researchers. The
> AIS number is currently (304) 420-6083, in late may it will
> change to (304) 480-6083.

[remainder deleted]

Since the proverbial cat is out of the bag, I think the original poster was justified to post the alert anonymously. I'd heard about this "service" being run by Clancy a while back, but had actually verified that virus disassemblies were available on AIS. Since that time (and quite possibly since public disclosure or because of a change of direction), the SysOp of that system who was once listed as "Mary Clark" has since been replaced by Clancy as the point of contact on the system. Also, it would appear that they have removed the virus disassembly from public access.

I don't think that its proper to question a posters integrity simply on the basis that the message was posted anonymously. I think that there are instances where anonymity on the network can be a good (and sometimes necessary) thing. The situation of anonymous posting is solely dependent upon the language, content and context of the information contained within the message and in these interesting days of Big Brother, it might even be in some folks best interest to post anonymously any information that may be considered derogatory with regards to Uncle Sugar.

Power to the "little" people.

Paul Ferguson, Network Integrator, Centreville, Virginia USA fergp@sytex.com

---

Risks of anonymity and credulity (Friedman, RISKS-14.60)

Vesselin Bontchev <bontchev@informatik.uni-hamburg.de>
Wed, 12 May 93 22:45:02 +0200

I don't know who the anonymous submitter was, but I do know who is the second person who wished to remain anonymous, for the simple reason that he has sent me the full file non-anonymously. In fact, I know this person personally and he is a very respectful person. BTW, the part that has been published here is less than 1% of the full file. I can send it to you, if you still don't believe. [...]

> I fully believe that our government sometimes does
> things that are stupid, immoral, and illegal, but this isn't the kind of
> stupidity that they do.

Well, maybe you shouldn't be that much confident about the things that your government can do... Anyway, I do not know whether the US Government really supports the BBS in question. All I know is that the BBS claims to be "official".

> In short, we need to be critical thinkers. In addition, we need to think
> about the way in which anonymous posting lets things like this get widely
> disseminated without exposing the original poster to embarrassment and
> ridicule. The next hoax, lie, or distortion from an anonymous source may not
> be this obvious. Is the ability to anonymously make this kind of claim a
> risk?

Actually, the anonymous poster did a service to all of us by bringing such a topic for discussion. What are the RISKS of ignoring valuable information, just because the person who has posted it wished to remain anonymous? Another issue is what are the RISKS of misusing the freedom of speech and officially spreading viruses around...

I am Bulgarian and my country is known as the home of many productive virus writers, but at least our government has never officially distributed viruses...

bontchev@fbihh.informatik.uni-hamburg.de
Vesselin Vladimirov Bontchev   Virus Test Center, University of Hamburg
Vogt-Koelln-Strasse 30, rm. 107 C, D-2000 Hamburg 54, Germany +49-40-54715-224

Re: RISKS DIGEST 14.60

Jim Thomas (tk0jut1@niu.bitnet) <TK0JUT1@NIU.BITNET>
Thu, 13 May 93 02:19 CDT

In Risks (Vol 14 #58) appeared a post that makes us appreciate freedom of speech and information exchange we enjoy in the U.S. The primary risk I've learned after reading the post is that anonymous posters with an axe to grind are potential threats to freedom of expression.

Two anonymous posters falsely depict AIS BBS, a bulletin board run by Dept of Treasury/Office of Public Debt personnel as a public information service, as a board engaged in "unethical, immoral, and possibly illegal activities" [...]

The remainder of the anonymous post presents screen captures of directories and files to which the poster objects. Especially troublesome for the anonymous accusers are virus-oriented files.

AIS is a reputable and professionally run open-access BBS. It has one of most extensive collections of text and other files related to all aspects of security in the country. Some may object to some of the materials, just as some might object to RISKS DIGEST or CuD being "funded" with taxpayers money. It strikes me as reprehensible to take selected material out of context and piece together an image of immorality or worse by presenting a misleading image of the materials on the BBS and the purposes for which those materials are intended. That the accusers make their claims while hiding behind the cloak of anonymity strikes me as the type of cowardice associated with witch hunts.

The anonymous posters seem to be bothered by the existence of virus source code on the board. I wager one would learn far more about virus writing and distribution tactics from VIRUS-L than from the AIS files, but the two anonymous posters seem to be part of a handful of strident pseudo-moral entrepreneurs who feel that only the information they judge as appropriate for public consumption should be made available. I'm surprised that the anonymous critics did not also include a demand that public libraries also be closed.

It is one thing to disagree with the position of another and raise the contentious issues as a matter of public debate. It is quite another to engage in the cowardly act of anonymously distorting the function of a legitimate and widely-used BBS by insinuating "unethical, immoral, and possibly illegal activities."

CuD ran an interview with the AIS BBS personnel (CuD 4.37, 1992), and a few excerpts may put the purposes of AIS BBS in perspective:

*** begin excerpts ***

Q: What is this Board? (name, number, who runs it (dept & sysop). What kind of software are you using? When did the Board go on-line?

A: The Bulletin Board System (BBS) is run by the Bureau of the Public Debt's, Office of Automated Information System's Security Branch. The mission of the Bureau is to administer Treasury's debt finance operations and account for the resulting debt. The OAIS security branch is responsible for managing Public Debt's computer systems security. The AIS BBS is open to the public and the phone number for the Board is (304) 420-6083. There are three sysops, who manage the Remote Access software. The BBS operates on a stand-alone pc and is not connected to any of other Public Debt systems. The Board is not used to disseminate sensitive information, and has been up operating for the past 15 months. <<This interview was as of mid-1992 - jt<>

Q: What are the goals and purposes of the Board?

A: The BBS was established to help manage Public Debt's security program. Security managers are located throughout Public Debt's offices in Parkersburg, WV and Washington DC. The security programmers saw a need to disseminate large amounts of information and provide for communication between program participants in different locations. Because the Board was established for internal purposes, the phone number was not published. However, the number was provided to others in the computer security community who could provide information and make suggestions to help improve the bureau's security program. Gradually, others became aware of the Board's existence.

Q: What kinds of files and/or programs do you have on the Board? Why/how do you choose the files you have on-line?

A: There is a wide variety of files posted. In the beginning, we posted policy documents, newsletter articles from our internal security newsletter, bulletins issued by CERT, such as virus warnings, and others for internal use. I located some "underground" files that described techniques for circumventing security on one of the systems we manage. The information, from Phrack magazine, was posted for our security managers to use to strengthen security. When we were called by others with the same systems, we would direct them to those files as well. Unexpectedly, the "hacker" that had written the file contacted me through our BBS. In his article he mentioned several automated tools that had helped him take advantage of the system. I requested that he pass on copies of the programs for our use. He agreed. This is how our "hacker file areas" came to be. Other hackers have done the same, and have we also received many files that may be useful. It is, indeed, an unusual situation when hackers and security professionals work together to help secure systems. However, this communication has been beneficial in strengthening an already secure system.

Q: How did you get the idea to set it up?

A: The security branch accesses many BBSs on a daily basis for research purposes, information retrieval and to communicate with others. Since our security program is decentralized, the BBS seemed to be an effective way of communicating with program participants in diverse locations.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 69

Friday 4 June 1993

Contents

Interference from mobile telephones

Erling Kristiansen <erling@wm.estec.esa.nl>
Fri, 4 Jun 93 09:04:45 +0100

Communications Week International, 31 May 1993, brings an article under the headline "Radio Storm Hits GSM", which I paraphrase below.

Handsets for the European digital mobile phone system GSM are reported to cause interference with hearing aids as well as car electronics (the latter has been reported in RISKS before). Tests in Australia, Germany, and the Unites States show that the burst transmission mode (TDMA - Time Division Multiple Access) used for GSM and other digital cellular systems causes interference with hearing aids as far away as 30 meters. At a range of 3-5 meters, hearing-aid wearers experience a humming noise. In some cases the noise is painful, according to the report.

Car manufacturers are concerned that GSM handsets may interfere with electronic devices, including those that control air bags and ABS brakes.

Volkswagen has found interference with several systems, but the article is not specific about which ones. So has Mercedes.

BMW say they have done tests but found no interference.

The article goes on to discuss the merits of TDMA, as compared to analog and CDMA systems. The conclusion seems to be that TDMA is more prone to causing interference due to its rather high-powered burst mode of transmission.

The issue is raised of whether it is up to GSM designers/manufacturers to solve the problem, or whether the manufacturers of those systems that GSM (and other digital phone systems) interferes into, have to take measures to protect themselves against interference. There is no conclusion on this issue, but various views are presented.

Finally, commercial issues are addressed. Some manufacturers question the extent of the issue but fear that it may dampen the export of GSM.

Erling Kristiansen, ESTEC Noordwijk, The Netherlands.

Zapped by the phone?

Richard Wexelblat <rlw@ida.org>
Wed, 2 Jun 93 15:27:42 EDT

June's Spectrum has an article, "The Cellular Phone Scare" subheaded:

> Despite the media hype, not one study has shown a link between cellular phones and brain cancer; nonetheless, more research is under way.

In spite of a clear anti-danger bias, the article presents a good survey of work-to-date on the effects of non-ionizing radiation. (IEEE _Spectrum_, June 1993, 43-47)

Re: Flight control computers to bypass pilots (RISKS-14.65)

Erling Kristiansen <erling@wm.estec.esa.nl>
Fri, 4 Jun 93 08:37:31 +0100

The Independent article says
> Yesterday the first test demonstration of equipment which will allow pilots
> and air traffic controllers to communicate through computers was held.

It is not quite true that this was the first demonstration of such capabilities. The European Space Agence (ESA), in cooperation with several organizations and airlines, demonstrated our PRODAT satellite mobile communication system with, among other features, ATC digital communication, starting in 1987.

The trials included installations on several aircraft - including the very same BAC 1-11 quoted in the Independent article. One Airbus 310 was flying the equipment for more than a year, and ATC experimenters were collecting flight data on a regular basis, but the system was not actually part of the ATC operations of this aircraft. One dedicated flight, with a private Jetstream aircraft, between Madrid and London, was carried out with the PRODAT link as primary ATC communication channel (and voice as backup) for the part of the flight taking place in Spanish airspace.

Admittedly, the scope of the PRODAT trials was more limited than that of the Mode-S. The goal was to demonstrate the feasibility of digital satellite communication for ATC (and airline) purposes. All equipment was to prototype standards, and a possible commercialization would have taken place in a second phase.

The trial system incorporated capabilities for the controller to access flight data, but no to down (up?)-load data into the aircraft equipment.
Pilot-to-controller messaging was also provided.

The aeronautical part of PRODAT has been discontinued for a variety of reasons (competing systems, standardization going in other directions). PRODAT still continues, and is on the verge of commercial deployment for land mobiles - but that is another story.

The RISK? When the press proclaims a FIRST, do not always believe it.

Erling Kristiansen, ESTEC, European Space Agency, Noordwijk, The Netherlands

WANTED: Article describing 10 Biggest Failures of Technology

Richard J Frost <rfrost@jrc.flinders.edu.au>
Fri, 04 Jun 93 11:12:18 +0900

There was an article published in a computer journal back in the 70's with a title similar to "The 10 Biggest Failures of Technology". It described technology failures in America and its effects.

It included the famous blackout of America and other major failures that were linked with failing technology.

Has anyone heard of it? Does anyone know where I can get this article?

Please email replies to the address below. Thanks [CC RISKS also. PGN]

Richard Frost, CSIRO, Flinders Joint Research Centre in Information Technology
Adelaide, SOUTH AUSTRALIA rfrost@jrc.flinders.edu.au +61 8 201 3651

Cryptic probable cause

"Gary Preckshot" <gary_preckshot@lccmail.ocf.llnl.gov>
4 Jun 1993 10:01:20 U

Jay Schmidgall writes:
> Ok, I guess I must have skimmed over this part. Let me see if I understand
> this properly:
>   If I have got more secure crypto gear, probable
>   cause exists that I have committed a crime.

> Hmmm. Does this include any crypto gear that may have been purchased
> before the corresponding CLIPPER-enabled gear became available?

There was an interesting article in the June 2 Wall Street Journal to the effect that such a significant proportion of cash in the USA was now contaminated by cocaine that cocaine contamination was becoming non-evidentiary. In Florida, one study found 97% of all bills exhibiting cocaine contamination. In Chicago, another study (by a DEA forensic chemist) found 33% of all bills in circulation had detectable cocaine.

To date, about three Federal courts have ruled that evidence seized because of dog sniffs or contaminant detection was illegally seized. It seems unlikely that any presumption could be attached to using secure crypto gear that the Government couldn't break because there are many innocent activities and reasons that people could advance for not wanting the Government or anyone else reading their mail. Consequently, a law prohibiting the use of non-breakable crypto gear seems the only way the Government could declare that such use was de facto incriminating. Such a law already exists in precedent. Ham radio operators are not allowed to use non-standard codes or unrecognized spoken languages.

A keypad security risk

Sean Matthews <sean@mpi-sb.mpg.de>
Wed, 2 Jun 93 14:48:46 +0200

This weekend I was staying with a friend who works in a secure building, and I went with him one evening so that I could borrow a computer to read my mail, and things. This was in the evening, and there was no-one in the building to let him in, so he had to key in the pass number on the outside door for the first time in months.

This number is four digits long, and contains a duplicate. How do I know this? Because of the ten buttons on the key pad, seven were covered in dust, and had clearly not been touched in a long time, and it was easy to see that he entered four digits (also, four is the number you expect).

Random four-digit passnumbers do not provide exactly high security, but they do provide some. When the set of passnumbers is reduced to 36, there is not even the vestige of security left.

Sean Matthews <sean@mpi-sb.mpg.de> Max-Planck-Institut fuer Informatik
Im Stadtwald, W-6600 Saarbruecken, Germany phone: +49 681 302 5363

Re: Cash machine keypad risk? (Potts, RISKS-14.65)

Michael S. Polymenakos <mpoly@Panix.Com>
31 May 1993 12:33:25 -0400

On a related note, I once approached an ATM that was displaying what was clearly a diagnostic screen of hexadecimal numbers. There were a few numbers shown on top (registers?) and 5-6 rows of long hex strings preceded by what must have been memory addresses. There was no response to the keypad (I tried). Considering what may have happened to the ATM Card and/or the account balance of the person who may have been using the machine when this happened, I decided to look for another bank, rather than risk using the 'sister' machine in the same branch.

Michael Polymenakos

Re: Fake ATM Machine Steals PINs

Phil White <philw@vice.ico.tek.com>
Wed, 02 Jun 93 22:03:46 PDT

Another method that might allow you to "authenticate" an ATM machine:

Enter an incorrect PIN as your first attempt.
Try a balance query if the ATM seems to accept the bad PIN.

At least at my bank's ATMs, you are given a second chance to enter the correct PIN after entering the wrong one. Come to think of it, this might decrease the odds your PIN will be stolen by someone who observes you keying in the number.

Phil White Tektronix, Beaverton, OR USA :: philip.w.white@tek.COM

[First entering an incorrect password was also noted by
mpoly@Panix.Com (Michael S. Polymenakos),
mlf@genrad.com (Matt Fichtenbaum),
Bill.Cordan@dundee.ncr.com (Bill Cordan),
HOLDEN_PHILIP/HP1600_01@hpopd.pwd.hp.com (Philip Holden),
rmehlman%grumpy.decnet@pdsppi.igpp.ucla.edu . THANKS! PGN]

Re: Fake ATM machines

Lars Wirzenius <wirzeniu@cc.helsinki.fi>
Sun, 16 May 1993 21:44:10 +0300

>[New trick? This is one of the oldest scams going, but it still recurs. PGN]

In a Swedish novel from 1982, ``Datadyrkarna'' (roughly, `the data lock-picks', or `the data worshippers') by Jan-J"oran Stenhagen (a pseudonym, according to back cover), one part of the plot is about the same scheme (but without giving money). The crooks set up a fake ATM and had it collect the PINs. They did the money collecting part at the end of the month, when most people had just got their salaries (they are usually paid monthly, not weekly as I understand is more common in the US), and had a lot of money on their accounts.

The rest of the book and its sequel contain a lot of other interesting issues about data safety, and risks of computerization. The two crooks (the main characters in the book) start with making their employer go bankrupt (after she had angered them), continue with the ATM scam, and then attack the social security system and rob most of the money going through it.

The ISBN is 91-46-14287-8, published by Wahlstr"om & Widstrand. I don't have the sequel, although I have read it. Alas, I doubt either has been translated to English.

Lars.Wirzenius@helsinki.fi (finger wirzeniu@klaava.helsinki.fi)

Re: Fake ATM Machine Steals PINs

<Bob_Frankston@frankston.com>
Tue, 1 Jun 1993 18:44 -0400

The reality is that one cannot be overly careful about ATMs one uses. I use BayBank in the Boston area. One reason (aside from proximity to MIT over 25 years ago) is that they've got zillions of their own ATMs as well as being on a number of worldwide ATM networks. It isn't realistic to be paranoid about every one. The risk of proposing interminable vigilance as a "solution" is that it doesn't solve the problem and only shifts the blame to the poor user who has enough to worry about. And by doing so reduces the pressure to actually solve the problem. In any case, it is worth the $50 exposure (if the bank really presses the issue) on stolen ATM cards to apply my Type A inclinations to other sources of worry.

It reminds me that Olmstead (sp?) who created many parks in the 1800's including Central Park in New York was (supposedly) against placing lights in them because it would encourage foolish behavior like walking in the parks at night where one is likely to be mugged.

Re: Fake ATM Machine Steals PINs (Peterson, RISKS-14.60)

Grant Grundler <grant@oas.olivetti.com>
Wed, 26 May 93 12:26:42 PDT

How can a user report fraud within 48 hours if the fraud isn't apparent until an ATM account statement shows up (Normally once a month)? Do I have to report fraud within 48 hours my bank drops my statement in the mail?

I know some of this has been discussed before. This is not a new problem.

Possible Solutions (and my comments):
1) Enable user to verify the ATM is "real".
   (technically feasible? too expensive? How secure? will Banks adopt this?)
2) Use the ATM only at your local bank.
   (Certainly reduces the usefulness of ATM cards)
3) Don't use an ATM - just write personal checks or use credit cards.
   (Risk is transferred to business to verify personal check. Not accepted
    everywhere, not anonymous, or transaction costs store about %2)
4) Carry more cash?

Grant Grundler voice: +1.408.366.3583
grant@oas.olivetti.com fax: +1.408.366.3606

[Similar comments from Rebecca Walpole walpolr@instruction.cs.orst.edu.]

Cryptography and the Bill of Rights

Robert I. Eachus <eachus@spectre.mitre.org>
Wed, 2 Jun 93 12:15:01 EDT

"David A. Honig" <honig@binky.ICS.UCI.EDU> wrote:

> While this may amuse some, this actually addresses at a
> profound and often overlooked intent of the 'Founding Fathers'.
> The People are guaranteed the right to bear arms, not just for
> personal defense (which was obvious to them), but also because:
> politicians prefer unarmed peasants. An unarmed populace is
> much easier to dominate. And so is a populace without the
> ability to have privacy.

...and so is a populace without access to reliable news, and to the opinions of other citizens, and...

Thomas Jefferson would have been the first to argue that the right of free speech, and to peaceably assemble are more fundamental and more important than the right to bear arms. In fact he did so argue, and that is one of the reasons that the first and second amendments are in that order. Modern cryptography is much more important as a component of free speech than as a weapon in and of itself. (But, a free press is a more important weapon than rifles or cannons, see Tom above.)

Peter D. Junger makes it clear that restrictions implicit in ITAR seriously limit the exercise of free speech. (If a law professor restricts his speech, in particular what he feels free to discuss in class, after carefully reading the ITAR regulations, then there can be no question that those regulations have a chilling effect on free speech.) Is this chilling effect unconstitutional? It depends on whether those regulations reflect the intent of the Senate in signing a treaty, or just the catch-all wording of some bureaucrat issuing regulations to implement and international agreement.

IMHO, unless the Senate debate on an international treaty specifically discussed the limitations to freedom of speech involved in limiting the export of crypto gear, the issue does not arise. Everything that I have seen on ITAR specifically recognizes the individual US citizen's right to free non-commercial speech, and severely limits everything else, so I suspect that this reflects congressional intent. (I thought about doing the search after lunch, and realized that the best approach is to ask--in a polite letter--a few of the Senators who were there. I'll post any responses received...)

Robert I. Eachus

More on the risks of teaching ...

Peter D. Junger <junger@samsara.law.cwru.edu>
Fri, 04 Jun 93 11:15:18 EDT

I have received a large number of personal responses to my article on the risks of teaching about computers and the law (RISKS-14.65) as well as the responses that appeared in RISKS-14.67. (I am afraid that I lost some of the personal responses, so if you haven't received a reply, please send me another copy of your message.) These have been most interesting and helpful and, for the most part, supportive.

I would, however, like to correct some misapprehensions that appear in the response by Jerry Leichter entitled "Re: Peter D. Junger's risks of teaching..." (RISKS-14.67).

Mr Leichter writes:

> While more sophisticated in his writing, what Mr. Junger is really doing is simply repeating an argument we've seen many, many times on the net:
>
> 1. Anyone can write cryptographic software, so where is the secrecy?
>
> 2. The regulations as written forbid export of such things as - a favorite example that Mr. Junger surely did not re-invent independently - Captain Midnight Decoder rings.

But my trouble is that _I_ (not anyone, not anyone else, but just dear old _moi-je_) wrote an encryption program that does not contain anything secret or original and yet the ITAR regulations require me to get a license before I _talk_ about this program with my students, if any of them should happen to be foreign, without first obtaining a license from the State Department, a license, which if it is granted, I could not expect to get before the semester is over. So I am not making the very sensible argument that Mr. Leichter pooh-pools as old hat. (I have no recollection of having ever seen any reference to my old--or any other--Captain Midnight Decoder (which I don't recall was a ring--wasn't it sort of a flat disk with a knob in the center?) during the last several decades, but if Mr. Leichter is sure I did not "reinvent" this example, I won't argue that point with him.)

Though I think it is sort of silly to require me to get a license to export my program, since I don't want to export it--I just want to talk about it and publish it and post it on my FTP server, all within the United States--that is not my problem. Once again, what I am concerned with is the requirement that I get a license to talk (or publish) information about my program within the United States, a requirement that is blatantly unconstitutional.

Thus Mr. Leichter's example of requiring a license for the exportation of an encryption _chip_ has nothing to do with my problem. (I must admit, however, that I cannot conceive of a case where the export of an encryption chip, that was not developed by or on behalf of the government, could be a serious threat to our national security.)

His other example does, however, have some bearing on my problem, if only because it illustrates how unclear, how far from being present, how farfetched, is the danger of allowing information about cryptography to get into the hands of the foreigners, for this example is: "conjectural software, 500 man-years in the making after a large research investment, for breaking cryptosystems used by the US for communicating with its embassies abroad". (Who would spend all that time and money to accomplish such a goal, whether those who did it (were it done) would be deterred by export regulations, and whether a program of such complexity could ever work are exercises that are left to the reader.)

Even though we are basically talking about different issues, however, the desire of Mr. Leichter to regulate the export of devices does ultimately collide with the Constitutional right of free speech that is my concern. As he puts the problem:

> Mr. Junger teaches law. Perhaps he'll take up the challenge of suggesting regulatory wording that covers "significant" cryptographic "equipment" - along the way, perhaps, coming up with a distinction that can be made in some useful way among "equipment", "software", and "specifications".

The trouble with this challenge--besides the fact that I have no interest in drafting such regulations--is that the constitution forbids the regulation of speech and that "specifications" fall squarely within the category of speech. What is really interesting is that "software" seems to be both "equipment", which is unprotected, and speech, which is constitutionally protected. (That's why I find computers and the law an interesting subject.)

The problem that I face is not how to draft unconstitutional regulations but how to challenge them. The fact that the regulations are not enforced makes it difficult to get their constitutionality before the courts. And the fact is that the regulatory scheme is not enforced by the bureaucrats, despite Mr. Leichter's claim that that is their job; instead, as one who responded to me privately put it, they rely on "FUD (Fear, Uncertainty and Doubt) to dissuade people from using and distributing effective cryptographic software."

Peter D. Junger

Case Western Reserve University Law School, Cleveland, OH
Internet: JUNGER@SAMSARA.LAW.CWRU.Edu -- Bitnet: JUNGER@CWRU

WHITE HOUSE ELECTRONIC MAIL

Steen Hansen <steen@kiwi.swhs.ohio-state.edu>
Fri, 4 Jun 93 08:33:15 -0400

```
Forwarded message:
>  For Immediate Release                         June 1, 1993
>
>           LETTER FROM THE PRESIDENT AND VICE PRESIDENT
>        IN ANNOUNCEMENT OF WHITE HOUSE ELECTRONIC MAIL ACCESS
>
>      Dear Friends:
>
>      Part of our commitment to change is to keep the White House
>  in step with today's changing technology.  As we move ahead into
>  the twenty-first century, we must have a government that can show
>  the way and lead by example.  Today, we are pleased to announce
>  that for the first time in history, the White House will be
>  connected to you via electronic mail.  Electronic mail will bring
>  the Presidency and this Administration closer and make it more
>  accessible to the people.
>
>      The White House will be connected to the Internet as well as
>  several on-line commercial vendors, thus making us more
>  accessible and more in touch with people across this country.  We
>  will not be alone in this venture.  Congress is also getting
>  involved, and an exciting announcement regarding electronic mail
>  is expected to come from the House of Representatives tomorrow.
>
>      Various government agencies also will be taking part in the
>  near future.  Americans Communicating Electronically is a project
>  developed by several government agencies to coordinate and
>  improve access to the nation's educational and information assets
>  and resources.  This will be done through interactive
>  communications such as electronic mail, and brought to people who
>  do not have ready access to a computer.
>
>      However, we must be realistic about the limitations and
>  expectations of the White House electronic mail system.  This
>  experiment is the first-ever e-mail project done on such a large
>  scale.  As we work to reinvent government and streamline our
>  processes, the e-mail project can help to put us on the leading
>  edge of progress.
>
>      Initially, your e-mail message will be read and receipt
>  immediately acknowledged.  A careful count will be taken on the
>  number received as well as the subject of each message.  However,
>  the White House is not yet capable of sending back a tailored
>  response via electronic mail.  We are hoping this will happen by
>  the end of the year.
>
>      A number of response-based programs which allow technology
>  to help us read your message more effectively, and, eventually
>  respond to you electronically in a timely fashion will be tried
>  out as well.  These programs will change periodically as we
>  experiment with the best way to handle electronic mail from the
>  public.  Since this has never been tried before, it is important
>  to allow for some flexibility in the system in these first
>  stages.  We welcome your suggestions.
>
>      This is an historic moment in the White House and we look
>  forward to your participation and enthusiasm for this milestone
>  event.  We eagerly anticipate the day when electronic mail from
>  the public is an integral and normal part of the White House
>  communications system.
>
>          President Clinton       Vice President Gore
>      PRESIDENT@WHITEHOUSE.GOV      VICE.PRESIDENT@WHITEHOUSE.GOV
```

Did they have an address for Hillary?

Paul Robinson <TDARCOS@MCIMAIL.COM>
Fri, 4 Jun 1993 04:00:00 -0400 (EDT)

Someone wrote me to ask:

```
> Thank you for relaying information concerning the high-tech
> White House.   Did they have an address for Hillary?  I can't
> imagine her suffering first.lady@whitehouse.gov.  Seriously,
> I need to get to her press secretary.
```

I wanted to see if there was anything:

```
% telnet
telnet> open whitehouse.gov 25
Trying 198.137.240.100 ...
Connected to whitehouse.gov.
Escape character is '^]'.
220 SMTP/smap Ready.
helo
250 Charmed, Im sure.
vrfy hillary
250 <hillary>
```

"250" in this case, is an "ok" indicating the mail-server receiving
the request considers the address to be valid. So try that, then:

  hillary@whitehouse.gov

That will probably go to one of the clerks that handles her correspondence.

Paul Robinson -- TDARCOS@MCIMAIL.COM

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 70

Friday 4 June 1993

Contents

Re: Did they have an address for Hillary?

Olivier MJ Crepin-Leblond <o.crepin-leblond@ic.ac.uk>
Fri, 4 Jun 1993 19:43:37 +0100

Paul Robinson (TDARCOS@MCIMAIL.COM) writes:

```
> I wanted to see if there was anything:
>
> % telnet
> telnet> open whitehouse.gov 25
> Trying 198.137.240.100 ...
> Connected to whitehouse.gov.
> Escape character is '^]'.
> 220 SMTP/smap Ready.
> helo
> 250 Charmed, Im sure.
> vrfy hillary
> 250 <hillary>
>
> "250" in this case, is an "ok" indicating the mail-server receiving
> the request considers the address to be valid.  So try that, then:
>
>    hillary@whitehouse.gov
```

Alas, this will most probably not work.
If you type

```
vrfy foobar
250 <foobar>
vrfy tdarcos
250 <tdarcos>        [ Eh Paul ? Didn't know you worked there :-) ]
```

etc.

In fact, anything is accepted by the mailer, so that no new address can be traced before it is officially released. A finger request at that site returns a standard message; a "rup" of that site (to see "if the President is busy reading your beloved messages" :) returns a "port mapper failure".

Still not ready to give up ?

Okay, how about trying "talk president@whitehouse.gov" ?
The reply is: "No talk daemon on requested machine"

I leave it to RISKS readers to find out if president@whitehouse.gov
is on Internet Relay Chat (IRC). :-)

Olivier M.J. Crepin-Leblond, Digital Comms. Section, Elec. Eng. Department
Imperial College of Science, Technology and Medicine, London SW7 2BT, UK
Internet/Bitnet: <foobar@ic.ac.uk> - Janet: <foobar@uk.ac.ic>

[Also noted by
bryk@ida.org (Bill Brykczynski)
Dave Bachmann <bachmann@austin.ibm.com>
tep@SDSC.EDU (Tom E. Perrine)
Frederick W. Wheeler <wheeler@ipl.rpi.edu>
Donald_L._Wegeng.henr801c@xerox.com
"Jonathan I. Kamens" <jik@gza.com>
Pat Place   prp@sei.cmu.edu
Mark.Maimone@A.GP.CS.CMU.EDU
Jerry McCollom <jmc@hal.com>
"Albert Peters" <albert@cs.Stanford.EDU>
Peter J. Scott <pjs@euclid.Jpl.Nasa.Gov>]

Re: Hillary's e-mail address

Sidney Markowitz <sidney@apple.com>
Fri, 4 Jun 93 14:59:19 -0700

Someone in the White House must be paying attention to RISKS Digest.

In RISKS-14.69, Paul Robinson showed

```
<> telnet> open whitehouse.gov 25
[...]
<> vrfy hillary
<> 250 <hillary>
```

I just tried it and got back

```
 vrfy
 500 Command unrecognized
```

It looks like they sealed off this possible security risk.

  [Also noted by "Albert Peters" <albert@cs.Stanford.EDU>.
  Perhaps we need to add the White House to the RISKS LIST! PGN]

health effects of VDTs - an update

Kenneth R Foster <kfoster@eniac.seas.upenn.edu>
Wed, 2 Jun 93 09:30:24 -0400

I am uploading a chapter from our new book Phantom Risk: Scientific Inference and the Las (MIT Press June 1993, Foster, Bernstein, Huber, eds.) Hopefully it adds something to the public concern about health effects of VDTs - and maybe some users will buy the book! K. R. Foster (kfoster@eniac.seas.upenn.edu).

From PHANTOM RISK: SCIENTIFIC INFERENCE AND THE LAW
K. R. FOSTER, D.E. BERNSTEIN, P. W. HUBER, EDS.
MIT PRESS JUNE 1993

Miscarriage and Video Display Terminals: An Update

Kenneth R. Foster
Dept. of Bioengineering
Univ. of PA
Phila. PA 19104
kfoster@eniac.seas.upenn.edu

The link between miscarriages and use of video display terminals (VDTs) became a public issue around 1980 with the reports of clusters of reproductive mishaps in women users of VDTs. In 1986 I traced the development of the VDT debate (Foster 1986). Now, six years later (and a decade after the controversy began), I describe the current state of the issue.

All together, about a dozen clusters were reported. These included 7 adverse outcomes of 8 pregnancies at the offices of the solicitor general in Ottawa; 10 out of 19 at the offices of the attorney general in Toronto; 7 of 13 at the Air Canada offices at Dorval Airport, Montreal; 8 of 12 at Sears, Roebuck in Dallas, Texas; 10 of 15 at the Defense Logistics Agency in Atlanta; 3 of 5 at Pacific Northwest Bell in Renton, Washington; and 5 of 5 at Surrey Memorial Hospital in Vancouver. The problems included birth defects, spontaneous abortions, respiratory problems in the newborns, Down's syndrome, spina bifida, and premature birth.

Despite attempts by health authorities to investigate the matter, the clusters were never adequately explained. I have been able to locate reports of a follow-up investigation by the U.S. Army Environmental Hygiene Agency of the cluster at the Defense Logistics Agency (Tezak 1981), and by the Centers for Disease Control (1981) of the cluster at Sears, Roebuck. Both verified the existence of a cluster; neither established any apparent link to the women's use of VDTs.

The interpretation of a cluster is problematic. Any unexpected grouping of problems (a cluster) may indicate some problem of public health significance. More commonly, investigation by health authorities of a reported cluster fails to identify a problem that can be remedied by public health measures. However tragic the outcomes may be to the people involved, the grouping of cases may have been a statistical event with no epidemiologic significance. Roughly one pregnancy in five ends in spontaneous abortion (the reported rates vary widely, depending on how early pregnancy is diagnosed); roughly one child in a hundred is born with a major birth defect. Simple calculations will show that many clusters will occur every year among the 10 million North American women who use VDTs. The issue, so easily raised, took a decade to resolve.

In the remainder of this chapter, I will summarize two lines of evidence related to the possible reproductive risks from use of VDTs. The first is the many studies on possible teratological effects of electromagnetic fields; the second is the series of progressively more sophisticated epidemiologic studies searching for a possible link between adverse pregnancy outcomes and use of VDTs.

Electromagnetic Fields

Public concern about VDTs has focused on several factors. As judged by contemporary newspaper articles, initial fears concerned possible X-ray emissions from the terminals, no doubt reflecting the scare in the late 1960s about X-ray emission from color television sets (Foster 1986). However, measurements by several government agencies on thousands of terminals showed that X-ray emissions are extremely low and in the overwhelming majority of cases are unmeasurable (Zuk et al. 1983). Emissions of ultraviolet, visible, and infrared radiation are also small, and far below recommended exposure limits. VDTs produce no measurable microwave radiation, notwithstanding one early (incorrect) report by an investigator to the contrary.

In their coverage of the issue, the lay media has frequently mentioned possible effects of low-frequency magnetic fields that are present near the terminals. These fields include components at power-line frequency (50-60 Hz) associated with the power supply, and fields with a more complex time dependence from the coils that move the electron beam around the screen.

The power-frequency fields from VDTs are comparable with those from other appliances; at a distance of 30 cm from the terminal, typical field strengths are a few v/m (electric field) and 4-7 Mg (magnetic flux density) (Jokela et al. 1989).

The fields from the beam deflection coils are more complex. If displayed on an oscilloscope, they would resemble a sawtooth wave with a repetition frequency of approximately 20 Khz (for the coils responsible for horizontal beam movement) and 60 Hz (vertical motion). The field from the vertical deflection coil has a peak amplitude of about 10-15 Mg at a distance of 30 cm from the screen (Jokela et al. 1989); that from the horizontal deflection coil is smaller but at a higher frequency. The corresponding electric field strength is typically a few volts per meter at a distance of 30 cm from the terminals. These field strengths are far below the levels associated with known hazards of electromagnetic fields (excessive heating of tissues or nerve excitation and shock) and far below recommended exposure limits.

In Vitro and In Vivo Studies

Two lines of evidence are related to the question of possible reproductive risk from VDTs: animal studies and epidemiologic observations on human populations. I consider the first and most confusing of these: animal tests for possible teratogenic effects of low-frequency magnetic fields.

In 1982 Delgado and colleagues reported that chicken eggs exposed to pulsed magnetic fields showed a striking number of malformations in the embryos inside (Delgado et al. 1982; Ubeda et al. 1983). The fields were comparable in strength with those from VDTs but weaker than the earth's magnetic field. Further, the investigators claimed, small changes in the waveshape of the field made a large difference in the rate of the malformations that were induced. Four independent attempts to confirm the findings were unsuccessful (Maffeo et al. 1984; Stuchly et al. 1988; Sandstrom et al. 1986; Sisken et al. 1986).

Delgado's findings were widely reported in the lay media, often with speculation about their possible significance to hazards from fields from VDTs and other appliances. The unsuccessful attempts at replication received little media attention.

Project HenHouse

To address the questions that the Delgado studies raised, the US Office of Naval Research commissioned at great expense a multi- laboratory replication of the original study, under the name Project HenHouse. Six laboratories in the United States, Canada, and Europe conducted replicate experiments, using the same techniques, identical exposure apparatus, and precisely measured fields (Berman et al. 1990). Each experiment involved the exposure of fertilized chicken eggs to pulsed magnetic fields, and subsequent examination of the embryos.

The outcome of Project HenHouse was very puzzling. Four of the laboratories--including that of colleagues of Delgado--found no statistically significant differences in the rate of malformations in the exposed versus control eggs. A fifth laboratory reported a borderline-significant increase. The sixth reported a statistically significant increase (but a smaller one than originally reported by Delgado et al.). If the results of all six studies are combined, they indicate a borderline significant increase in rate of malformations in the exposed eggs--in contrast with the very striking effect originally reported by Delgado et al. (Berman et al. 1990).

Thus, the results of Project HenHouse were neither clearly positive nor clearly negative. The simplest interpretation is that five of the six studies were negative, and that the one positive study was different in some important respect from the other five. Whether the sixth was in error or whether there is something important in its results is a question that cannot at present be answered.

The latest development in this episode is the preliminary report by Litovitz et al. (1992) of a teratogenic effect of weak magnetic fields on chicken eggs. Litovitz claimed that the critical variable of exposure is the "coherence" of the field. As of this writing these results have not been published; whether they will be confirmed and accepted by other scientists remains to be seen.

In retrospect, Delgado's study probably did not merit the widespread attention it received. The biological system (fertilized chicken eggs) differs too much from human embryos for the test to have much value for risk assessment; on the other hand it is too complex to be of much use for basic scientific research on mechanisms of interaction of fields with a biological systems. Chickens are not inbred, and are notoriously variable in the frequency of chick malformations and fertility of eggs. Finally, a project officer from the Office of Naval Research who visited Delgado's lab (Thomas C. Rozzell, private communication) told me that the initial experiment was crudely done and the applied fields were poorly characterized.

After ten years of research on the "Delgado effect" with so little to show for it, funding agencies and most scientists have lost interest in the matter. As well they should.

Other Animal Studies

Since the early 1980s, at least 17 animal studies have been searched for effects of pulsed magnetic fields on animal embryos. (Berman 1990 provide a comprehensive review.) The literature is very inconsistent, with some studies reporting effects and others (including attempts to replicate earlier positive findings) finding none. Berman concludes

> ... we cannot clearly relate an increase in the
> incidence of abnormal embryos resulting from exposure
> to pulsed magnetic fields to any patterns of pulse
> frequency, field intensity, pulse shape, or rate of
> change in the intensity.... Until the important
> variables in pulsed magnetic fields are determined and
> the mechanism of effects is identified, it may not be
> possible to extrapolate such effects to humans. (1990, p. 47).

This conflates two issues. The first is the absence of any clearly reproducible phenomena. Until some reproducible phenomenon appears, with some defined relation between dose and response, that can be consistently observed by independent investigators, it will be difficult to draw any conclusions from the data. The second is the relevance of these results to human health, assuming that the effects themselves are real. That depends on the biological similarity between the animal subjects and humans, the exposure conditions, and other factors. Whether these studies will point to a mechanism for human injury is, at present, a matter of speculation.

Epidemiologic Evidence

A much clearer picture has emerged from the epidemiologic studies. By now, a dozen epidemiologic studies have been conducted in the United States, Canada, Finland, Sweden, and elsewhere on reproductive problems associated with use of VDTs. (A good, but dated, review is Blackwell and Chang 1988.) They have been overwhelmingly--but not totally--negative, finding no links between use of VDTs and spontaneous abortion or birth defects.

The studies vary widely in their methods, and I will not review them in detail here. Table 6.1 summarizes their results in terms of the relative risk, which is the risk (probability) of an undesired consequence in a VDT user, divided by the probability of the same consequence for an otherwise similar nonuser (see chapter 1). The table also shows the 95 percent confidence intervals, i.e. margins of sampling error in the studies. Virtually all of the results indicate no increase in risk associated with use of VDTs. But some of these studies did report positive or equivocal findings, which has helped to keep the issue alive. The most widely publicized of these studies was that of Goldhaber et al. (1988), who reported a 1.8-fold increase in risk of miscarriage among women who worked with VDTs for more than 20 hours a week during their first trimester of pregnancy. This increase was at the edge of statistical significance.

Goldhaber's study was generally well done, but it had one major weakness that resulted from its retrospective design. To determine the subjects' use of VDTs during pregnancy, the investigators sent them a questionnaire, as much as three years after their pregnancies. The investigators did not independently verify the subjects' actual use of the terminals. At the time the study was conducted, the possible reproductive hazards of VDTs were well publicized; it is likely, as the investigators themselves suggested, that women with adverse pregnancy outcomes might have been more likely than other women to report using VDTs. Goldhaber's study was widely reported in the lay media, without the careful reservations of the investigators, and usually without mention of the negative findings of the other studies.

The most recent, and undoubtably the best, study on reproductive risk of VDTs was published early in 1991 in the New England Journal of Medicine by Schnorr and colleagues. The investigators, working for the National Institute for Occupational Safety and Health (NIOSH), conducted a retrospective cohort study that compared groups of telephone operators who used VDTs with telephone operators in otherwise similar jobs who did not. The investigators found no link between spontaneous abortion and use of VDTs during the first trimester of pregnancy. Whether this study will end the VDT debate remains to be seen.

The epidemiologic literature on the VDT-miscarriage question frequently mentions the great difficulty of measuring reproductive risk. These problems are not reflected in the 95 percent confidence intervals in the table, which show only the statistical uncertainties due to sampling error.

For example, several of the papers listed in the table discuss at length the problem of reporting bias, which might be introduced if not all of the subjects in a study were equally likely to report use of VDTs during their pregnancies. Two studies (Goldhaber et al. 1988; McDonald et al. 1988) mentioned this as a possible explanation for a small apparent excess of miscarriages among VDT users.

Another problem is the difficulty of reliably detecting miscarriages that occur early in pregnancy. Because of this difficulty, an investigator has a choice of including only miscarriages that occur after a month or more of pregnancy (and thus missing a large fraction of all miscarriages), or of including earlier miscarriages and finding some way to determine precisely when the subjects became pregnant. Most studies choose the former approach.

A final difficulty arises from the many different birth defects that can occur. A study that retrospectively examines medical records for any association between birth defects and use of VDTs can, therefore, make many different comparisons. However, by the statistical tests that most scientists adopt, 1 comparison out of 20 will show a difference that is statistically significant--even if there is no real difference in the groups being compared. (This problem is discussed in chapter 1, and again in chapter 4.)

Because of these and other problems, one can never achieve complete consistency in epidemiologic studies--but the dozen studies summarized in the table come pretty close. They certainly rule out the large increases in risk that some people inferred from the clusters.

Recently, public concern has shifted to the much more difficult question of possible risks from the fields associated with the terminals, which these studies do not directly address. In the NIOSH study, for example, both the VDT and non-VDT operators were exposed to similar levels of 60 Hz electromagnetic fields from the equipment they used. Consequently, the study is inconclusive on the question of hazard from fields. This point was raised in a letter to the editor of Science News from the president of a company that makes radiation shields for VDTs (Doilney 1991).

An adequate epidemiologic study on reproductive risk from 60 Hz fields from VDTs would be very hard to mount. The NIOSH investigators measured the fields from the terminals, and found them to be comparable to those from many other sources in the environment.

The latest development in this issue is a preliminary report of a Finnish epidemiologic study (Hietanen et al. 1992) of a 3.5- fold increase in risk of miscarriage in VDT operators who were exposed to extremely low frequency magnetic fields greater than 9 Mg from the terminals. The study has not been published as of this writing and there is no way to judge its quality; perhaps the issue of reproductive risk from VDTs will remain alive.

Other Problems Associated with Use of VDTs Of greater concern to many scientists and health authorities have been diverse ergonomic and psychosocial problems associated with the use of computers in the workplace (World Health Organization 1989).

Ergonomic problems include workstation design, glare, legibility of display, seating, and keyboard height. A panel assembled by the U.S. National Research Council judged radiation hazards to be highly unlikely, and focused in its report on issues such as glare, legibility of video displays, and background lighting (National Academy of Sciences 1983).

Perhaps more important still are psychosocial problems. To my mind the fundamental problem is that many clerical workers using VDTs simply have lousy jobs. A data entry operator who spends the day keying numbers into a computer, with every keystroke counted, little opportunity for personal interaction, and rigid performance standards to meet might well experience emotional and perhaps physical problems. If only radiation shielding could fix such problems!

Carpal tunnel syndrome (CTS) is a painful condition associated with repetitive motions of the hand, that afflicts workers in many occupations, including VDT operators. CTS arises from compression of the median nerve as it passes through a small opening (the carpal tunnel) in the wrist (Spinner et al. 1989); and can be relieved by a simple operation. The problem has been reported among workers in diverse occupations, including meat cutting and clerical workers, but there are few reliable data on its incidence and the medical literature on CTS is sketchy and anecdotal. The syndrome is clearly a matter of concern to VDT operators and their employers, and might be prevented by better keyboard design or other ergonomic considerations. Clearly, more study on CTS is needed.

Other, less well defined, health problems have been reported from use of VDTs (Bergqvist 1989; Council on Scientific Affairs 1987). Since the mid-1980s, there have been scattered reports of rashes and other skin problems among VDT users; follow-up studies have been unable to find the cause of the problem or associate it with the terminals or other factors in the office environment. This has, however, led to at least one lawsuit (see "The Legal Context" at the end of Part I).

On reviewing the history of the VDT debate, I am struck by the great disparity between the ease with which concerns about reproductive hazards from the terminals were raised, and the great difficulty in adequately addressing them. The clusters, in retrospect, were probably chance events of no epidemiologic significance. But the question of whether use of VDTs increases reproductive risk took ten years and a dozen studies to address, and (from a recent preliminary report) it has still not been settled. It is time to focus instead on the more serious ergonomic and psychosocial problems associated with use of computers in the workplace.

References

Berg, M. 1988. Skin problems in workers using visual display terminals--a study of 201 patients. 19 Contact Dermatitis 335- 341.

Bergqvist, U. 1989. Possible health effects of working with VDUs. 46 Br. J. Indus. Med. 217-221.

Berman, E., L. Chacon, D. House, B. A. Koch, W. E. Koch, J. Leal, S. Lovtrup, E. Mantiply, A. H. Martin, G. I. Martucci, K. H. Mild, J. C. Monahan, M. Sandstrom, K. Shamsaifer, R. Tell, M. A. Trillo, A. Ubeda, and P. Wagner. 1990. Development of chicken embryos in a pulsed magnetic field. 11 Bioelectromagnetics 169- 187.

Berman, E. 1990. The developmental effects of pulsed magnetic fields on animal embryos. 4 Repro. Toxicol. 45-49.

Blackwell, R., and A. Chang. 1988. Video display terminals and pregnancy. A review. 95 Br. J. Obstet. & Gynaecol. 446-453.

Brandt, L. P. A., and C. V. Nielsen. 1990. Congenital malformations among children of women working with video display terminals. 16 Scand. J. Work Environ. & Health 329-33.

Bryant, H. E., E. J. Love. 1989. Video display terminal use and spontaneous abortion risk. 18 Int. J. Epidemiol. 132-8.

Butler, W. J., and K. A. Brix. 1986. Video display terminal work and pregnancy outcome in Michigan clerical workers. In Allegations of reproductive hazards from VDUs. Nottingham UK: Humane Technology 67-91.

Centers for Disease Control, Family Planning Evaluation Division. 981. Cluster of spontaneous abortions. Report EPI-80-113-2.

Council on Scientific Affairs. 1987. Health effects of video display terminals. 257 J. Am. Med. Assn. 1508-1512.

Delgado, J. M. R., J. Leal, J. L. Monteagudo and M. G. Gracia. 1982. Embryological changes induced by weak extremely low frequency electromagnetic fields. 134 J. Anat. 533-551.

Doilney, J. A. 1991. Science News 387. June 22. Letter to the editor.

Ericson, A., and B. Klln. 1986. An epidemiological study of work with video screens and pregnancy outcome: II. A case- control study. 9 Am. J. Indus. Med. 459-475.

Foster, K. R. 1986. The VDT debate. 74 Am. Scientist 163-168.

Goldhaber, M. K., M. R. Polen, and R. A. Hiatt. 1988. The risk of miscarriage and birth defects among women who use visual display units during pregnancy. 13 Am. J. Indus. Med. 695-706.

Hietanen, M., M. L. Lindbohm, P. von Nandelstadh, P. Kyyrnen, and M. Sallmn. 1992. Effects of exposure to magnetic fields of VDTs on miscarriages (abstr), 1st Congress of the European Bioelectromagnetics Association, Brussels, Belgium. January.

Jokela, K., J. Aaltonen, and A. Lukkarinen. 1989. Measurements of electromagnetic emissions from video display terminals at the frequency range from 30 Hz to 1 Mhz. 57 Health Physics 79-88.

Edstrm, R., and B. Klln. 1985. Dataskarmsarbete och graviditet. 82 Lakartidningen 687-688.

Kurppa, K., P. C. Holmberg, K. Rantala, and T. Nurminen. 1984. Birth defects and video display terminals, 2 The Lancet 1339.

Kurppa, K., P. C. Holmberg, K. Rantala, T. Nurminen, and L. Saxen. 1985 Birth defects and exposure to video display terminals during pregnancy. 11 Scand. J. Work Environ. Health 353-356.

Maffeo, S., M. W. Miller and E. L. Carstensen. 1984. Lack of effect of weak low frequency electromagnetic fields on chick embryogenesis. 139 J. Anat. 613-618.

Mackay, C. J. 1989. Work with visual display terminals: psychosocial aspects and health. 31 J. Occup. Med. 957-968.

McDonald, A. D., N. M. Cherry, C. Delorme, and J. C. McDonald. 1986. Visual display units and pregnancy: evidence from the Montreal Study. 28 J. Occup. Med. 1226-1231.

McDonald, A. D., J. C. McDonald, B. Armstrong, N. Cherry, A. D. Nolin, and D. Robert. 1988. Work with visual display units in pregnancy. 45 Br. J. Indus. Med. 509-515.

Miller, D. A. 1974. Electric and magnetic fields produced by commercial power systems. In J. G. Llaurado, A. Sances, and J. H. Battocletti, eds., Biologic and clinical effects of low-frequency magnetic and electric fields 62-70. C. Thomas.

National Academy of Sciences. 1983. Video displays, work, and vision. Washington DC: National Academy Press.

Nurminen, T., and K. Kurppa. 1988. Office employment, work with video display terminals, and course of pregnancy. Reference mothers' experience from a Finnish case-referent study of birth defects. 14 Scand. J. Work Environ. Health 293-298.

Sandstrom, M., K. H. Mild, and S. Lovtrup. 1986. Effects of weak pulsed magnetic fields on chick embryogenesis. In Proceedings of the International Scientific Conference: Work with video display units 60-63. Stockholm: Swedish National Board of Occupational Safety.

Schnorr, T. M., B. A. Grajewski, R. W. Hornung, M. J. Thun, G. M. Egeland, W. E. Murray, D. L. Conover, and W. E. Halperin. 1991. Video display terminals and the risk of spontaneous abortion. 324 N. Eng. J. Med. 727-733.

Sisken, B. F., C. Fowler, J. P. Mayaud, J. P. Ryaby, J. Ryaby, and A. Pilla. 1986. Pulsed electromagnetic fields and normal chick development. 5 J. Bioelec. 25-34 (1986).

Slesin, L., and M. Zybko. 1983. Video display terminals: Health and safety. New York: Microwave News 41-46.

Spinner, R. J., J. W. Bachman, and P. C. Amadio. 1989. The many faces of carpal tunnel syndrome. 64 Mayo Clinic Proc. 829-836.

Stuchly, M. A., et al. 1988. Teratological assessment of exposure to time-varying magnetic field. 38 Teratology 461-466.

Ubeda, A., J. Leal, M. A. Trillo, A. Jimenez, and J. M. R. Delgado. 1983. Pulse shape of magnetic fields influences chick embryogenesis. 137 J. Anat. 513-536.

Tezak, R. W. 1981. Investigations of adverse pregnancy outcomes. Service Report 66-32-1359-81. Aberdeen Proving Ground MD: U.S. Army Environmental Hygiene Agency, Defense Contract Administration.

Wahlberg, J. E., and C. Lidn. 1988. Is the skin affected by work with visual display terminals? 6 Occup. Dermatoses 81-85.

Westerholm, P., and A. Ericson. 1987. Pregnancy outcome and VDU-work in a cohort of insurance clerks. In B. Knave, P. G. Widebck, eds., Work with display units 86, at 87-93. Amsterdam: Elsevier.

Windham, G. C., L. Fenster, S. H. Swan, and R. R. Neutra. 1990. Use of video display terminals during pregnancy and risk of spontaneous abortion, low birth-weight, or intrauterine growth retardation. 18 Am. J. Indus. Med. 675-688.

Zuk, W. M., M. A. Stuchly, P. Dvorak, and Y. Deslauriers. 1983. Investigations of radiation emissions from video display terminals. Public Affairs Directorate, Dept. of Health and Welfare Canada, Report 83-EHD-91.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 71

Tuesday 8 June 1993

Contents

Summer Slowdown Time

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 8 Jun 93 11:16:19 PDT

Our annual RISKS Summer Slowdown Time is about to start. I will be within
fingershot of the Internet only on selected occasions for the next four weeks,

so do not be surprised if there are not many RISKS issues. However, please continue to send in any horror stories (or even wonderful success stories --- we have not had very many of those lately).

The rate of BARFmail resulting from RISKS mailings has increased painfully in recent weeks. Some of that may be due to students leaving for the summer and general job instabilities. Last Friday, when I put out three issues on one day, I cleaned up the mess of newly rejected addresses after each mailing; the second and third mailings each generated still *MORE* newly rejected addresses, all on the same day. (I ignore directory overflows, which have also increased dramatically, assuming some of you are away; I regret if RISKS is exhausting your directories!) The BARFmail situation never converges, probably because the Internet is incredibly dynamic and the number of flaky sites remains large. Even more annoying is the persistence of E-Mail messages whose FROM: addresses are unanswerable.

Phone Company Malfunction

Brinton Cooper <abc@ARL.ARMY.MIL>
Tue, 8 Jun 93 14:10:21 EDT

>From the BALTIMORE SUN, Tuesday, 8 June:

BALTIMORE -- Chesapeake & Potomac Telephone's "intercept" system -- the recordings and artificial voices activated by calls to disconnected or changed numbers -- was knocked out yesterday by a computer glitch in Richmond, Va., the company said. As a result, customers dialing numbers not in service were connected to a recorded message that all circuits were busy, according to C&P spokesman Paul G. Wood.

The problem was caused by "redundant" computer databases at a center in Richmond, which are alternately in service as new information on telephone-number changes is loaded five times a day. The changeover was being made about 11:30 a.m. when a computer processing problem occurred, cutting off access to the system, Mr. Wood said.

The problem was expected to be resolved last night, he said.

NIST Official Says Private Crypto May Be Outlawed

Mark Seecof <marks@wimsey.latimes.com>
Mon, 7 Jun 93 14:57:26 -0700

I read in the new Network World (Network World; vol. 10, no. 23; June 7, 1993) at page 6, in a story headlined "Clipper Chip Foes Denounce Scheme Over Cost Issues" by Ellen Messmer which begins on page 2, that:

--> NIST Deputy Director Ray Kammer said the government is considering
--> banning all other encryption and making Clipper Chip mandatory.

Assuming that this quote is accurately reproduced (a typo such as the inadvertent excision of the word "not" could change the meaning completely) it would appear to me to be a most inflammatory statement, given the discussion of the issue I've been reading in RISKS Digest and elsewhere.

Perhaps someone could check into this?

Mark Seecof <marks@latimes.com>

Re: NIST Official Says Private Crypto May Be Outlawed (Seecof)

Marc Rotenberg <Marc_Rotenberg@washofc.cpsr.org>
Tue, 8 Jun 1993 10:05:54 EST

Kammer spoke yesterday at the CPRS crypto conference. While he did say that government was considering all options (including presumably restrictions on non-government technology), the possibility of making private uses of crypto illegal seems very unlikely. And John Podesta from the White House said later during the day that the White House was not considering such restrictions.

Marc

NIST CSSPAB 6/4/93 Resolutions

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 4 Jun 1993 20:46:59 EST

Computer System Security and Privacy Advisory Board, June 4, 1993

Resolution #1

At Mr. Kammer's request we have conducted two days of hearings. The clear message of the majority of input was that there are serious concerns regarding the Key Escrow Initiative and the Board concurs with these concerns. Many of these issues are still to be fully understood and more time is needed to achieving that understanding.

Accordingly, this Board resolves to have an additional meeting in July 1993 in order to more completely respond to Mr. Kammer's request and to fulfill its statutory obligations under P.L. 100-235. The Board recommends that the inter-agency review take note of our input collected, our preliminary finding, and adjust the timetable to allow for resolution of the significant issues and problems raised.

Attached to this resolution is a preliminary distillation of the serious concerns and problems.

Resolution #2

Key escrowing encryption technology represents a dramatic change in the nation's information infrastructure. The full implications of this encryption technique are not fully understood at this time. Therefore, the Board recommends that key escrowing encryption technology not be deployed beyond current implementations planned within the Executive Branch, until the significant public policy and technical issues inherent with this encryption technique are fully understood.

[Attachment to Resolution #1]]

- A convincing statement of the problem that Clipper attempts to solve has not been provided.

- Export and important controls over cryptographic products must be reviewed. Based upon data compiled from U.S. and international vendors, current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography (DES and RSA)

- The Clipper/Capstone proposal does not address the needs of the software industry, which is a critical and significant component of the National Information Infrastructure and the U.S. economy.

- Additional DES encryption alternatives and key management alternatives should be considered since there is a significant installed base.

- The individuals reviewing the Skipjack algorithm and key management system must be given an appropriate time period and environment in which to perform a thorough review. This review must address the escrow protocol and chip implementation as well as the algorithm itself.

- Sufficient information must be provided on the proposed key escrow scheme to allow it to be fully understood by the general public. It does not appear to be clearly defined at this time and, since it is an integral part of the security of the system, it appears to require further development and consideration of alternatives to the key escrow scheme (e.g., three "escrow" entities, one of which is a non-government agency, and a software based solution).

- The economic implications for the Clipper/Capstone proposal have not been examined. These costs go beyond the vendor cost of the chip and include such factors as customer installation, maintenance, administration, chip replacement, integration and interfacing, government escrow systems costs, etc.

- Legal issues raised by the proposal must be reviewed.

- Congress, as well as the Administration, should play a role in the conduct and approval of the results of the review.

[NIST Resolutions on Key Escow Issues and Clipper provided by
CPSR Washington office, 666 Pennsylvania Ave., SE Suite 303,
Washington, DC 20003   rotenberg@washofc.cpsr.org]

Fuzzy subway control used successfully (so far) in Sendai, Japan

Paul Eggert <eggert@spot.twinsun.com>
Sat, 5 Jun 93 13:49:11 PDT

David Kahaner (US ONR Asia) recently reported on the predictive fuzzy control system used in the Sendai, Japan subway. This system, designed in 1982 by Seiji Yasunobu, has been in commercial operation since 1987, and now operates in a 15-km subway containing 17 stations, serving nearly 1 million persons daily. It was implemented entirely by replacing traditional Proportional-Integral-Derivative (PID) control software in each train's onboard minicomputer. It reportedly outperforms even skilled human operators in both smoothness and accuracy of stopping, and consumes 10% less energy than expected with PID control. No accidents have been reported since it was installed.

The system is being copied in several places, notably Tokyo. Kahaner writes:

> The commitment of Sendai City to this new technology seems not to be only in the trust of Japanese engineers, but also in successful tests prior to the actual production of control systems for commercial use. We were told that when the system was put into operation it ran smoothly, to everyone's satisfaction, and has required neither modification nor improvements.

On the down side, the system was designed in an ad-hoc manner. Even though it is relatively simple, it needed extensive testing before use, and the overall system relies on human backup. To produce desirable properties like robustness, safety, and stability in more ambitious fuzzy systems, much better design and verification methods are needed.

Kahaner's report can be FTPed from cs.arizona.edu in the file japan/kahaner.reports/fuzzy5.93; it also appeared on 1993-06-04 in comp.research.japan <1up4gi$b56@optima.cs.arizona.edu>.

French Fry Robots!

Dwight D. McKay <mckay!dwight@ecn.purdue.edu>
Mon, 7 Jun 1993 20:14:44 -0500

A while back you may recall a message I posted about a local fast food place installing a robotic soft drink machine. The machine filled drink orders as they were entered into the cash register terminals.

Now there's a device for handling french fries!

I saw one at a fast food place my family stopped at on the way to North Carolina last week. The device consisted of the usual side-by-side set of hot oil fryers, with a vertically moving, overhead arm added. The arm moved along an overhead track between the fryers, a feed hopper and the serving area. The cycle consisted of picking a bin from a storage area, filling it at the feed hooper and dropping it into the fryer. When a bin finished frying, the arm picked up the bin, shook the bin, then dumped the frys into the serving area. There was no obvious sign that this system was hooked into the rest of the store's ordering system. I was pleased to see that there was some sort of big red shutoff button near the serving end of the system, however the machine is not enclosed in any way.

The risks? When the drink robot fails to work some soft drink gets spilt, but what happens if there's a problem with a machine that is working around hot oil?

Dwight D. McKay -- mckay!dwight@ecn.purdue.edu

My grocery store is not dumb

Martin Minow <minow@apple.com>
Fri, 4 Jun 93 17:48:17 -0700

At my local supermarket (which has wonderful food and excellent service, by the way), I usually pay with a Visa card. Like most San Francisco supermarkets, they have a customer "terminal" with a magnetic card reader: you run your card through it and sign the receipt that the cash register prints out. Couldn't be simpler.

Yesterday, the clerk asked me for the card so she could run it through the "old-style" card imprinter. Apparently, enough people have been re-writing the magnetic stripes on their cards (so the billing goes somewhere else) that the clerks now sight-verify the receipt, making sure that the number embossed on the plastic card matches the number read from the magnetic stripe.

Sigh, isn't progress wonderful?

Martin Minow minow@apple.com

radio smartcards

Gary McClelland <mcclella@yertle.Colorado.EDU>
Tue, 8 Jun 1993 11:02:31 -0600

The Business Focus section of the Boulder Daily Camera (6/8/93) describes the product of a local start-up company. I _think_ this is a new variation on smartcards. Each card contains an antenna that allows communication with a "paperback book sized" transceiver. The card contains a 256-bit FRAM (stable memory requiring no power supply) to take the place of the usual magnetic strip. One would buy the card for preset amounts like other smartcards. Using the card would only require flashing the card in the vicinity of the reader; the reader then sends a signal back to the card altering the information stored in the FRAM.

Intended uses are high volume transactions where physical contact between the card and scanner is too time consuming. Suggested uses include road tolls (more privacy than the fixed transmitter on the car), mass transit, student cafeteria payments, dorm security, etc. Another suggestion was "per-use" charges for things like ski lifts (will be tested at a Japanese ski area next year) and amusement park rides which are now usually charged on a "per-day" pass basis.

No mention in the article of how many bits are reserved for encryption keys or whether each card will have its own Clipper chip :-). Although the same section of the newspaper had a decent discussion of ATM risk issues, the article on this smartcard didn't mention any risks. The cost of an annual ski pass would surely motivate someone to build one's own radio device for resetting the FRAM. And would using a portable computer with a mouse cord on an airplane reset my FRAM? :-)

gary mcclelland, univ of colorado, mcclella@yertle.colorado.edu

Formal Methods in Safety-Critical Standards

<Jonathan.Bowen@prg.ox.ac.uk>
Mon, 7 Jun 93 22:06:31 BST

You may be interested in a recent paper on the recommendations concerning the use of formal methods for safety-critical systems in current and emerging standards:

"Formal Methods in Safety-Critical Standards" by J.P. Bowen.
To appear in Proc. Software Engineering Standards Symposium
(SESS'93), Brighton, UK, 1-3 September 1993.
IEEE Computer Society Press, 1993.

A copy in PostScript format is available via anonymous FTP under
ftp.comlab.ox.ac.uk:/pub/Documents/techpapers/Jonathan.Bowen/sess93.ps
(192.76.25.2) if you wish to retrieve a copy.

Jonathan Bowen, Oxford University

2nd Call for Papers - ISOC Symp. on Net. and Dist. Sys. Security

Dan Nessett <nessett@ocfmail.ocf.llnl.gov>
Mon, 7 Jun 1993 12:37:14 -0800

CALL FOR PAPERS
The Internet Society Symposium on
Network and Distributed System Security

3-4 February 1994, Catamaran Hotel, San Diego, California

The symposium will bring together people who are building software and hardware to provide network or distributed system security services. The symposium is intended for those interested in practical aspects of network and distributed system security, rather than in theory. Symposium proceedings will be published by the Internet Society. Topics for the symposium include, but are not limited to, the following:

* Design and implementation of services--access control, authentication,
   availability, confidentiality, integrity, and non-repudiation
   --including criteria for placing services at particular protocol layers.

* Design and implementation of security mechanisms and support
   services--encipherment and key management systems, authorization
   and audit systems, and intrusion detection systems.

* Requirements and architectures for distributed applications and
   network functions--message handling, file transport, remote
   file access, directories, time synchronization, interactive
   sessions, remote data base management and access, routing, voice and
   video multicast and conferencing, news groups, network management,
   boot services, mobile computing, and remote I/O.

* Special issues and problems in security architecture, such as
   -- very large systems like the international Internet, and
   -- high-speed systems like the gigabit testbeds now being built.

* Interplay between security goals and other goals--efficiency,
   reliability, interoperability, resource sharing, and low cost.

GENERAL CHAIR:
   Dan Nessett, Lawrence Livermore National Laboratory

PROGRAM CHAIRS:
   Russ Housley, Xerox Special Information Systems
   Rob Shirey, The MITRE Corporation

PROGRAM COMMITTEE:
   Dave Balenson, Trusted Information Systems
   Tom Berson, Anagram Laboratories
   Matt Bishop, Dartmouth College
   Ed Cain, U.S. Defense Information Systems Agency
   Jim Ellis, CERT Coordination Center
   Steve Kent, Bolt, Beranek and Newman
   John Linn, Geer Zolot Associates
   Clifford Neuman, Information Sciences Institute
   Michael Roe, Cambridge University
   Rob Rosenthal, U.S. National Institute of Standards and Technology
   Jeff Schiller, Massachusetts Institute of Technology
   Ravi Sandhu, George Mason University
   Peter Yee, U.S. National Aeronautics and Space Administration

SUBMISSIONS: The committee seeks both original technical papers and proposals
for panel discussions on technical and other topics of general interest.
Technical papers should be 10-20 pages in length. Panels should include three
or four speakers. A panel proposal must name the panel chair, include a
one-page topic introduction authored by the chair, and also include one-page
position summaries authored by each speaker Both the technical papers and the
panel papers will appear in the proceedings.

Submissions must be made by 16 August 1993. Submissions should be made
via electronic mail to

1994symposium@smiley.mitre.org.

Submissions may be in either of two formats: ASCII or PostScript. If the committee is unable to read a PostScript submission, it will be returned and ASCII requested. Therefore, PostScript submissions should arrive well before 16 August. If electronic submission is absolutely impossible, submissions should be sent via postal mail to

Robert W. Shirey, Mail Stop Z202
The MITRE Corporation
McLean, Virginia 22102-3481 USA

All submissions must include both an Internet electronic mail address and a postal address. Each submission will be acknowledged through the medium by which it is received. If acknowledgment is not received within seven days, please contact either Rob Shirey <Shirey@MITRE.org> or Russ Housley <Housley.McLean_CSD@xerox.com>, or telephone Mana Weigand at MITRE in Mclean, 703-883-5397.

Authors and panelists will be notified of acceptance by 15 October 1993. Instructions for preparing camera-ready copy for the proceedings will be postal mailed at that time. The camera-ready copy must be received by 15 November 1993.

Workshop on Digital Systems Reliability and Nuclear Safety

John Camp <jcamp@swe.ncsl.nist.gov>
Thu, 3 Jun 93 16:23:24 EDT

First Announcement, Workshop on Digital Systems Reliability and Nuclear Safety
September 13-14, 1993, Rockville Crowne Plaza Hotel, Rockville, Maryland

U.S. Nuclear Regulatory Commission
U.S. Department of Commerce
Technology Administration
National Institute of Standards and Technology

WORKSHOP CO-CHAIRS
Leo Beltracchi, U.S. Nuclear Regulatory Commission
Dolores Wallace, National Institute of Standards and Technology
SPONSORED BY:
The United States Nuclear Regulatory Commission
IN COOPERATION WITH:
The National Institute of Standards and Technology

As analog hard-wired process control systems and safety systems within nuclear power plants wear out, they are being replaced with systems using digital technology. There are many unique design and safety issues for digital systems. The Nuclear Regulatory Commission is developing regulations and guidelines to address these issues.

This workshop will provide state of the art information to the Nuclear Regulatory Commission staff and to the nuclear industry. The purposes of this workshop are to:

- provide feedback to the NRC from outside experts regarding potential safety issues, proposed regulatory positions, and research associated with the application of digital systems in nuclear power plants, and

- continue the in-depth exposure of the NRC staff to digital systems design issues related to nuclear safety by discussions with experts in the state of the art and practice of digital systems.

September 13, 1993

OPENING SESSION

8:30 Welcome
Commissioner E. Gail de Plenque
U.S. Nuclear Regulatory Commission
8:45 Welcome and Opening Statement
Mr. Eric Beckjord, Director, Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

9:00 Welcome and ACRS Perspective
Dr. J. Ernest Wilkins, Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission

ISSUE PERSPECTIVE FOR NUCLEAR POWER PLANTS

9:15 Presentation on NRC Regulatory Positions and Guidelines
Mr. William Russell
Associate Director for Inspection and Technical Assessment
Office of Nuclear Reactors, U.S. Nuclear Regulatory Commission

9:45 Presentation on NRC Research Activities
Mr. Leo Beltracchi, Senior Project Manager
Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Comm.

10:15 Industry Perspective, Mr. Richard Blauw, Commonwealth Edison Company
10:45 Break

11:00 Experiences from Application of Digital Systems in a NPP
Mr. Paul Joannou, Ontario Hydro

TECHNICAL SESSION: DIGITAL SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

11:30 Hardware Aspects for Safety-Critical Systems
Mr. Al Sudduth, Duke Power Company

11:50 Software Aspects for Safety-Critical Systems
Dr. Susan Gerhart, University of Houston, Clear Lake

12:10 Human Aspects for Safety-Critical Systems
Dr. Lewis Haines, Nuclear Industry Independent Consultant

12:30 Discussion

1:00   Lunch

TECHNICAL SESSION: SOFTWARE ENGINEERING FOR HIGH INTEGRITY SYSTEMS

2:30   System and Software Hazard Analysis for Nuclear Applications
Dr. Nancy Leveson, ICS Department, University of California

2:55   Formal Methods for Requirements, Specifications
Dr. John McHugh, University of North Carolina

3:20   Software Test Cases Derived from Formal Requirements
Mr. Robert Poston, Interactive Development Environments
3:45   Break

4:00   Object Oriented Design for Safety-Critical Systems
Dr. Barbara Cuthill, National Institute of Standards and Technology

4:25   Questions and Discussions on Technical Session

September 14, 1993

TECHNICAL SESSION: METHODS FOR REDUCING RISKS IN SOFTWARE SYSTEMS

8:30   Automated Tools for Safety-Critical Software
Ms. Anne-Marie Lapassant, Commissariate a L'Energie Atomique

8:55   Risks of Safety-Critical Software
Dr. Winston Royce, TRW, Incorporated

9:20   Software Metrics for Safety-Critical Applications
Mr. Kyle Rone, IBM Houston, Texas

9:45   Software Reliability for Safety-Critical Applications
Mr. Jon Musa, AT&T Bell Laboratories
10:10 Break

10:25 Software Configuration Management for Safety-Critical Applications
Mr. Ron Berlack, Configuration Management International

10:50 How Much Software Verification and Validation is Adequate for
Nuclear Safety?   Mr. Roger Fujii, Logicon, Incorporated

11:15 Software Verification and Validation for New Technology in Nuclear
Settings, Dr. Lance Miller, Science Applications International Corp.

11:40 Certification of Software for Reuse into Safety-Critical Applications
Ms. Charlotte Scheper, Research Triangle Institute

12:05 Questions and Discussions on Technical Session
1:00   Lunch

2:30   PANEL: Application of Workshop to NRC activities
Moderators: Mr. John Gallagher - Office of Nuclear Reactor Regulation

Mr. Leo Beltracchi - Office of Nuclear Regulatory Research
Panel Members
Dr. John McHugh, National Academy of Science
Dr. Joseph Naser, Electric Power Research Institute
Dr. Susan Gerhart, University of Houston, Clear Lake
Dr. Winston Rouce, TRW Incorporated
Mr. Frank McGarry, NASA Goddard Space Flight Center

Panel Issues:
- Are the proper issues being addressed?
- What other issues need to be addressed?
- Are proposed NRC regulatory positions complete and correct?
- What are the considerations for further research?

4:30 NRC Closing Remarks

LOCATION

The Workshop will be held at the Holiday Inn Crowne Plaza, Rockville, Md. Three airports are easily accessible to the Rockville area: Washington National Airport, Baltimore-Washington International Airport, and Dulles International Airport.

REGISTRATION

Registration will begin at 8:00 a.m. The Workshop will run from approximately 8:30 a.m. to 5:00 p.m. each day. The registration fee of $75 covers workshop materials and proceedings that will be mailed to participants after the workshop. A registration form is enclosed and may be duplicated; a separate form must be forwarded for each attendee. For pre-registration, the registration form must be mailed to the NIST Office of the Comptroller or faxed to Lori Phillips by September 1, 1993. All requests for cancellations and refunds must be submitted to Lori Phillips (see address and fax number at the end of the General Information section of this brochure) in writing prior to September 1, 1993. For answers to your registration questions contact:

- Lori Phillips, NIST, Telephone: 301/975-4513, Fax: 301/948-2067

ACCOMMODATIONS

Workshop registration does not include your hotel reservation. A block of rooms has been reserved at:

- The Holiday Inn Crowne Plaza
  1750 Rockville Pike
  Rockville, Md. 20852 USA
  Telephone: 301/468-1100

$98 single or $108 double. Please add 12% tax to this rate. To register for a room, please use the enclosed hotel reservation form and send it directly to the hotel no later than August 27, 1993. After that date the rooms will be released for general sale at the prevailing rates of the hotel.

TRANSPORTATION

BWI Limo, 301/441-2345, offers commercial van service from
Baltimore-Washington Airport to the Rockville area. Call for reservations.

Montgomery Airport Shuttle, 301/990-7005, is available from Dulles
International and Washington National Airports to Rockville.

>From Washington National Airport
The Washington Metro has subway service to Rockville from National
Airport. Take a Yellow Line train marked ~Gallery Place~ to Metro
Center and transfer to a Red Line train marked ~Shady Grove~ to
~Twinbrook~. Service is every 6 to 15 minutes depending on the time
of day. The time from National to the Rockville, Twinbrook Metro
stop is about 50 minutes. The hotel is adjacent to the Twinbrook
Metro stop, toward Rockville Pike.

>From Dulles International Airport
Take Dulles Access Road to the Washington Beltway I495. Go toward
Maryland (signs may say Bethesda/Rockville). Take the I270 spur off
of I495. Go about 3-4 miles into Maryland. Take the Montrose Road
Exit off of I270 (2nd exit on cloverleaf). Go about one mile and
turn left on to Rockville Pike (Rt. 355). The Crowne Plaza will be
one-half mile on the right.

COFFEE BREAKS AND LUNCHES

Refreshments will be provided at the morning, mid-morning and afternoon
breaks. Attendees are on their own for lunch.

TECHNICAL CONTACTS

- Leo Beltracchi, NRC
  Telephone: 301/492-3549
  Email: lxb@nrc.gov

- Dolores Wallace, NIST
  Telephone: 301/975-3340
  Email: wallace@swe.ncsl.nist.gov

[FOR WORKSHOP AND HOTEL RESERVATION FORMS, CONTACT Lori Philips or request
on-line forms from John Camp <jcamp@swe.ncsl.nist.gov>. TOO LONG TO INCLUDE
IN RISKS.]

AMAST'93 (Algebraic Methodology and Software Technology)

Pippo Scollo <scollo@cs.utwente.nl>
Tue, 8 Jun 93 23:58:07 +0200

Starting Thursday 10 June, the AMAST'93 Advance Programme and Registration
Information are available by anonymous ftp (with any password) on the machine

ftp.cs.utwente.nl

in plain text form as well as LaTeX sources.

You can get these files from directory pub/doc/amast93, which has the following contents:

```
 AdvaProg.asc : AMAST'93 Advance Programme        (plain text)
 RegInfo.asc  : AMAST'93 Registration Information (plain text)
 AdvaProg.tex : AMAST'93 Advance Programme        (LaTeX source)
 RegInfo.tex  : AMAST'93 Registration Information (LaTeX source)
```

Requests of further information should be sent to the Conference Secretariat:

Mrs. Joke Lammerink, Mrs. Charlotte Bijron, Mrs. Alice Hoogvliet-Haverkate
University of Twente, Fac. Informatica
P.O. Box 217, NL-7500AE Enschede
phone: + 31 53 893680, fax: + 31 53 315283
e-mail: {lammerin | bijron | hoogvlie}@cs.utwente.nl

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 72

Wednesday 9 June 1993

Contents

Phone lottery in Phoenix

"Kriss A. Hougland" <hougland@enuxhb.eas.asu.edu>
Wed, 9 Jun 93 11:08:33 MST

Since the Suns here in Phoenix are in the NBA playoffs, one of the ticket offices discovered that something was amiss. Since the only way to get any of the remaining tickets is by calling up either of the two ticket offices, this happened for one of the games...

On one of our local channels, they reported that employees from the company that installed the phone for the ticket office (I believe it was Dillard's) had been discovered to have "fixed" (I don't know the proper term they used) the phone lines so the callers (employees of the installing phone equipment) would be the first to get through to place orders for the tickets. The news show went on to add that disciplined action(s) had been taken by the company and the company would not comment on the situation.

The "modification" to the phone system was detected by the ticket office.

(I thought rigging/modifying the odds of a dial-in only event was cardinal.
(sorry for the pun) No No.)

Grassroots vs. Astroturf Movements

Shyamal Jajodia <SHYAM@mitvmc.mit.edu>
Wed, 09 Jun 93 17:31:27 EDT

This morning there was a report on National Public Radio on what it called Astroturf letter writing campaigns. Apparently some lobbying firms have started offering this service to clients likely to be affected by legislation about to come up for vote.

For a fee they will generate a large number of letters which will put forward the client's case to several selected mailing lists. These letters also contain an exhortation to sign and mail the included PROTEST letters which are pre-addressed to the area congressional rep. Such campaigns were found by several congressmen who are in favor of the Clinton Administration's proposed BTU tax.

On the face of it it seems like the good old American democratic system. The risk identified by one of the Congressman was that the high levels of noise generated by these computer aided campaigns are making it difficult for them to identify the genuine missive from Mrs Bramley in Peoria.

SHYAM

RISK of undefined abbreviations, RE Health effects of VDTs - an update

Mark A. Hull-Richter <mhr@tdat.elsegundoca.ncr.com>
Wed, 9 Jun 93 14:31:30 PDT

Mr. Rogers' article is most certainly both welcome and informative on an otherwise overreported and underanalyzed area of potential health risk. Unfortunately, he uses an abbreviation in the article whose meaning is undefined, at best, and ambiguous at worst.

In reference to the strength of the magnetic fields measured at 30cm distance from a VDT, he lists the strength of the magnetic fields as "4-7 Mg," and elsewhere repeats the use of this abbreviation.

By the normal standard abbreviation scheme that I am familiar with (and I believe most people are as well), the abbreviation "Mg" should be interpreted as "Megagauss", which is absurd in the context. The average strength of the Earth's magnetic radiation field at ground level ranges between 2-2.5 mg (that's milligauss), and even the dangers supposedly related to magnetic fields have been generally associated with fields in excess of 10mg, coupled with continuous exposure over long periods of time. (A good discussion of this subject can be found in the book "Cross-Currents," the name of whose author escapes me at the moment, and also his sequel on a similar subject, the title of which also escapes me at the moment.)

As a side note, I had our electric company send a representative out to my house a couple of years ago, specifically to measure the EMF radiation from various instruments and equipment in my house. This was largely in response to a scare about power line proximity and the fact that my house overlooks a freeway, on the other side of which are power transmission lines totalling 506 kilovolts of electricity. It turned out that the EMF level outside the house at chest height was 1.5-2.5 mg, whereas the average EMF level _inside_ the house, mid-room at chest height, was around 5mg. Our waterbed heater generated over 10mg at bed surface level, and the most dangerous room in the house was the kitchen, with a reading of 6-9mg mid-room. Surprisingly, the highest radiation levels were from electric alarm clocks, ranging 140-300+mg at the face, down to somewhere between 40-50mg at a distance of 3 feet. The VDTs? My wife's EGA read 15mg at the screen, down to 1.5mg at 3 feet, and my monochrome was slightly higher

(I forgot the exact reading).

Now, Mr. Rogers, what did _you_ mean by "Mg?"

Mark A. Hull-Richter, NCR Teradata, 100 N. Sepulveda Blvd., # 11-257
El Segundo, CA 90245   (310) 524-5782   mhr@ElSegundoCA.NCR.com

Citibank ATM risk

No gas will be sold to anyone in a glass container <SKASS@DREW.DREW.EDU>
Tue, 08 Jun 1993 23:44:13 -0400 (EDT)

Yesterday, I walked up to a Citibank ATM (a relatively new one at 2nd Ave. and 4th St. in Manhattan) and the screen displayed the question "What language would you like to use for your transaction," a question I usually get only after inserting my card and entering my PIN. I was a bit puzzled, but think I have an answer. Two "features" of this particular ATM in combination may present quite a risk.

Feature 1: Citibank ATMs don't swallow cards. You insert, then immediately withdraw them to start a transaction. I appreciate this feature, having left my card in an ATM before.

Feature 2: After selecting your transaction, but before receiving cash

> or a balance or making a deposit, you must answer the question
> "After this transaction, can we help you with anything else?"
> This question is very oddly placed. I don't want to think about
> my next transaction until this one is finished.

What may have happened:

The previous customer (call her Maria), inserted and withdrew her card, entered her PIN, chose a language, selected a transaction, and was then perhaps confused by the question about an additional transaction (Feature 2), or just slipped on the touch screen. Between having to answer questions like "Is this correct?" and "Would you like a receipt?" it would be easy to keep hitting the Yes button. When Maria finished her first transaction, she took her receipt, and having already retrieved her card, turned and walked out, not realizing she had pre-ordered another transaction. Presumably I could have effected a second transaction on her account, withdrawing some large sum of money. I've never made two transactions in a row on a Citibank ATM, so I can't be sure that the language question is routinely presented again, but nothing else seems to make sense, especially since when I pressed the Cancel button right off, I got the message "Your transaction has been cancelled," then the usual "Insert your card, then withdraw it quickly" opening message.

Any Citibank programmers out there who care to comment? Even if I've misread the situation, this scenario is all too plausible. Feature 1 and Dubious Feature 2 (a programming hack, I'd almost have to guess) just don't work together.

Steve Kass (skass@drew.drew.edu), Department of Mathematics and Computer Science Drew University, Madison, NJ 07940

Re: Fake ATM Machine Steals PINs

Debora Weber-Wulff <dww@math.fu-berlin.de>
Sun, 6 Jun 1993 12:42:13 GMT

>Another method that might allow you to "authenticate" an ATM machine:
> Enter an incorrect PIN as your first attempt.
> Try a balance query if the ATM seems to accept the bad PIN.

Won't work in Germany. You don't get 3 tries per card insert, you get 3 tries on the *lifetime of the card*! If you goof up 3 times, the card is marked invalid and has to be sent in to a special office for resetting. Takes about 2-3 weeks. And balance queries are usually not done with ATM machines, but with extra boxes that give a list of transactions since the last query - this has shifted the costs and work of preparing statements to the user. You have to stand there and wait while the silly thing grinds out 3-4 pages, usually with a page of advertising (Grrrrrrrr....). This also saves postage for the banks.

Debora Weber-Wulff, Professorin fuer Softwaretechnik, Technische Fachhochschule Berlin, FB Informatik, Luxemburgerstr. 10, 1000 Berlin 65

[Thanks, Debora. One of the joys of RISKS is that our international contributors keep the U.S. folks on their toes. For example, John Oliver <j.oliver@uow.edu.au> in Wollongong, Australia, chided me for my item in RISKS-14.71 about RISKS "Summer Slowdown Time". He said
"Shame on you. This is WINTER! John Oliver" PGN]

What's in it for the grocer?

Dave Kristol <dmk@allegra.att.com>
Tue, 8 Jun 93 22:02:23 EDT

Margins on sales in supermarkets are reputed to be very low. Credit card companies usually charge a couple of percent on transactions with their cards. So, credit card sales in supermarkets would wipe out the retailers' profits. Yet, payment by credit cards in supermarkets is expanding.

Obviously the credit card companies are offering the grocers lower than usual rates. What do they get in return? Are they accumulating buying profiles on people who use credit? If so, how do they use the information they gather?

Can I expect a letter from Proctor and Gamble: "We see you bought Crest in March and May of 1992, but you haven't bought it since. How come? (And here's a 50 cent coupon to encourage you to buy it again.)"

In a similar vein, supermarkets around here offer various forms of "price clubs", whereby you get an extra discount on selected items if you present your card at check-out. Are THEY accumulating buying profiles? How are THEY using the information?

[Have I become excessively paranoid about invasions of privacy?]

Dave Kristol

Re: French Fry Robots! (McKay, RISKS-14.71)

Dean Kling <dkling@ornews.intel.com>
8 Jun 1993 16:28:40 -0700

>The risks? When the drink robot fails to work some soft drink gets spilt, but
>what happens if there's a problem with a machine that is working around hot
>oil?

Such technology is being used successfully in the semiconductor industry. Similar robots handle automated wet stations, wherein silicon wafers are dunked into a variety of etchants, including hydrofluoric and sulfuric acids. It takes a competent design and reasonable control limits, but is capable of being done successfully.

Dean F. Kling
dkling@ptd.intel.com (503) 642-6829 No, I don't speak for Intel

Re: French Fry Robots! (McKay, RISKS-14.71)

The Polymath <hollombe@polymath.tti.com>
Tue, 8 Jun 93 17:39:43 PDT

Most likely the robot's work cell is protected by light beam barriers,
floor mat switches or both. Tripping either system should cause the robot
to immediately stop moving until the system is reset. This sort of setup
is required by ANSI/OSHA regulations for robot work cells.

}The risks? ...

Some hot oil gets splashed (the robot isn't pouring oil, just dipping things
in it). Not a good thing, to be sure, but not likely a tragedy, either. I
note the (required) manual cutoff button is located away from the hot oil
tanks.

The Polymath (aka: Jerry Hollombe, M.A., CDP, Head Robot Wrangler at Citicorp
3100 Ocean Park Blvd., Santa Monica, CA 90405 (310) 450-9111, x2483

And yet, a Risks report contains more errors! (Camp, RISKS-14.71)

Paul Robinson <TDARCOS@MCIMAIL.COM>
Tue, 8 Jun 1993 22:44:57 -0400 (EDT)

John Camp Writes in Risks 14.71:

Subject: Workshop on Digital Systems Reliability and Nuclear Safety

> >From Washington National Airport
> The Washington Metro has subway service to Rockville from National
> Airport. Take a Yellow Line train marked ~Gallery Place~ to Metro
> Center and transfer to a Red Line train marked ~Shady Grove~ to
> ~Twinbrook~.

This worries me when even minor details can't be gotten right.

In Washington DC, the Yellow Line train at National Airport goes in two
directions. The one going toward Washington is labeled "U Street/Cardoza" and
goes THROUGH Gallery Place! This isn't a new event; the extension to the
Yellow line has been running for more than a year.

Also, one transfers from the Yellow to the Red Line AT GALLERY PLACE. The
Yellow Line does not and never has run to Metro Center!

There is, however, a Blue Line that DOES go to Metro Center from National
Airport, at which point one can also transfer to the Red Line. But THAT train
- the Blue Line - would be labelled "New Carrolton" and doesn't go anywhere
near Gallery Place!

This worries me that if small details like this are wrong, what other things could also be wrong? Maybe they'll run an ad for this symposium in the {Washington Star}! :)

(The :) is because The Star Folded many years ago.)

Paul Robinson - TDARCOS@MCIMAIL.COM

Re: RISKS-14.71 error

Bruce Limber <blimber@cap.gwu.edu>
Wed, 9 Jun 1993 12:35:01 -0400 (EDT)

The conference announcement in RISKS-14.71 contains incorrect directions for taking the Metro from National Airport to the Holiday Inn Crowne Plaza. I'm sending a correction to lammerin@cs.utwente.nl and, should you wish to publish it separately, the correct directions are these:

There is a free shuttle bus between the terminal and the National Airport Metro station. At the station, purchase a farecard to Twinbrook. (Fare varies according to the day of week and the time you enter, and will be either $2.00 or $3.15 one way.)

Take the yellow train marked "Mt. Vernon Sq." to the Gallery Place station; there, transfer to a train marked "Shady Grove" and ride to the Twinbrook station; the hotel is beside the station. (Be sure to take a "Shady Grove" train; trains at the same platform marked "Grosvenor" do not go all the way to Twinbrook.)

Re: White House Electronic Mail

Nick Rothwell <cassiel@cassiel.demon.co.uk>
Wed, 9 Jun 1993 07:33:18 +0000

<> ... The White House will be connected to the Internet as well as
<> several on-line commercial vendors, thus making us more
<> accessible and more in touch with people across this country.

Only a minor item of risk-interest, perhaps, but: which people and which country? I have an email address ending in ".uk", but the more generic ".com" is available to people outside the US for a small sum (I'll have access to one soon). I don't see anything to stop (for example) groups from outside the US lobbying this email service by pretending to be "the people" from "this country." The Internet is international.

Nothing to lose sleep over, I don't think, but I did sense a wee bit of parochialism in this announcement and thought I'd point out something that's probably obvious.

Nick Rothwell | cassiel@cassiel.demon.co.uk
CASSIEL Contemporary Music/Dance | cassiel@cix.compulink.co.uk

[By the way, jim@mpl.UCSD.EDU (Jim Easton) reported that mail to

vice.president@whitehouse.gov was rejected. Let him know
if you have a good address. And thanks to all of you who
reported on Gedanken Experiments with the the White House
Internet connections. They are vastly too numerous (and some
to off-color) to be included here. PGN]

Cryptography, Free Speech, and so on

Jerry Leichter <leichter@lrw.com>
Fri, 4 Jun 93 17:32:38 EDT

In RISKS-14.69, Peter Junger responds to comments I'd made earlier. I'd like to look a bit at the broader issues.

The Constitution may protect speech, but espionage, a crime which may involve "nothing more" than speech, has been illegal since before the Constitution was written, and you wouldn't have much success challenging it on First Amendment grounds.

There are two interesting things about cryptography:

- It's one of only two examples of cases where things can be treated as secret even if you invent them yourself. (The other is information about nuclear technology.) If you were to become aware of classified information about existing cryptosystems, the espionage statutes would apply to you just as they would were you to come into possession of plans for a fighter plane. If you can be forbidden from discussing one, you can be forbidden from discussing the other. (Actually, "discussing" for espionage purposes doesn't even have to be with foreign nationals, but it does have to be with the intent of making the information available to foreign nationals, or something like that.)

  So what we come down to is the claim that the fact that you invented something yourself automatically gives it First Amendment protection, even though had you gotten it by other means it might not be so protected. Well, maybe. It's an argument worth making, but personally I think more on social policy grounds than Constitutional ones - I see nothing in the Constitution that makes a distinction based on authorship, and in fact such distinctions can be very hazardous: If I have a right to say something, but my publisher does not have the right to publish it for me, my rights are being honored more in the breach than in reality.

- Cryptographic systems can easily be embodied as software. As Mr. Junger point out, software is inherently both speech and object. One gets the feeling on the net that people wish to see it purely as speech because that gets them to final results they like, right now. Along the way, they make various questionable assumptions, such as identifying the description

> of an algorithm with efficient (or just WORKABLE!) code for it. That was the point of my 500-man-year example. The code for such a monstrosity would clearly be a manufactured object, difficult to duplicate from scratch. A broad description of that object might help someone duplicate it to a very limited extent. A detailed design specification would help a lot more. But the code itself remains much more usable than any description.
>
> Building a fighter jet is difficult for many reasons. Even with the proper equipment and materials, detailed drawings and specifications remain necessary. Code is like those detailed drawings and specifications. It just happens that for programs, once you have the code, you don't need to do much more (while for a fighter you've still got a great deal of work). Plans for fighters have always been considered very sensitive. I see no reason why code, or specifications for code, should not be.
>
> Our ideas about free speech were developed at a time when "information" and "objects" were separate universes. Speech might affect PEOPLE, but it could not directly affect the physical world. It's exactly because of its effect on people that dictatorships wish to control it; and it's exactly because our system of government is based on the idea that people, in effect, have the right to be affected, that we so strongly protect speech rights.
>
> These days, the borderline between "information" and "object" is getting fuzzy. A computer virus is "information", but it can pretty directly affect the real, physical world. Should it be given the same protection as speech that is aimed at people? People are moral actors, and are assumed to be responsible for the outcomes of their acting on speech they hear. A computer that "hears" a virus is NOT a moral actor; the responsibility for any damage it does lies entirely on the creator of the virus.
>
> Actions certainly have consequences. We like to say that ideas have consequences, too, but those consequences are always filtered through other people, other moral actors. This is very different from the growing potential for certain ideas, expressed in software rather than words, to have DIRECT consequences. I believe it's foolish to claim that just because we use the word "information" to describe both traditional speech and this new class of thing that we should automatically apply the same standards to each.

I have no love for the existing cryptographic export regulations. However, I refuse to close my eyes to the problems they are trying to solve. Rather than tossing our hands up and saying "there's no perfect solution, so let's not try to find ANY solution," we should try to come up with better approaches. Perhaps in the long run we are destined to fail; even so, we have to survive in the short run.

-- Jerry

Re: Denning on NIST/NSA Revelations

Kevin S. McCurley <mccurley@cs.sandia.gov>
Wed, 19 May 93 22:46:52 MDT

Let's review a RISKS discussion that's gotten out of hand:

David Sobel, originally wrote in RISKS DIGEST 14.59:
<> The proposed DSS was widely criticized within the computer
<> industry for its perceived weak security and inferiority to an
<> existing authentication technology known as the RSA algorithm.
<> Many observers have speculated that the RSA technique was
<> disfavored by NSA because it was, in fact, more secure than the
<> NSA-proposed algorithm and because the RSA technique could also
<> be used to encrypt data very securely.

Dorothy Denning responded in RISKS 14.60:
> This is terribly misleading. NIST issued the DSS proposal along with a
> public call for comments as part of their normal practice with proposed
> standards. The community responded, and NIST promptly addressed the
> security concerns. Among other things, the DSS now accommodates longer
> keys (up to 1024 bits). As a result of the revisions, the DSS is now
> considered to be just as strong as RSA.

Marc Rotenberg commented in RISKS 14.62:
> Denning has to be kidding. The comments on the proposed DSS were uniformly
> critical. Both Marty Hellman and Ron Rivest questioned the desirability of
> the proposed standard.

Most recently, Eric Raymond wrote in RISKS 14.64:
> As a long-time RISKS reader and contributor, I observe that that this is not
> the first time that Ms. Denning has apparently operated as a mouthpiece for
> the NSA's anti-privacy party line on DES and related issues.
>
>I believe Ms. Denning's remarks must be understood as part of a continuing
>propaganda campaign to marginalize and demonize advocates of electronic
>privacy rights.

I have no link to the FBI, NSA, or NIST, and I agree with this particular statement of Dorothy's, that DSS is regarded to be as strong as RSA. Mobs often believe the words that are shouted the loudest, and this may have warped the public perception of DSS. Some people will refuse to accept DSS because of where it came from, but let's be clear on this specific issue:

NOBODY HAS PRESENTED A CREDIBLE SCIENTIFIC ARGUMENT THAT DSS CAN BE BROKEN!

I spent a couple of years using some of the most powerful machines in the world to compute discrete logarithms, and I published a survey paper in 1990 on the discrete logarithm problem. I am quite sure that there is no publicly known technique that will compromise DSS with 1024 bit keys, and I think both

Rivest and Hellman will agree on this point. There are technical issues of some dispute, but this issue is not among them. If anything, factoring is regarded as easier than computing discrete logarithms because of the linear algebra involved.

People are apparently getting so steamed over Clipper and the notion of key escrowing that their glasses are getting fogged. It's gotten so no matter what Dorothy says, she is demonized as a stooge of the Feds. It appears that there are legitimate issues to be debated here, but let's try to clean up the discussion surrounding Clipper, Skipjack, Capstone, DSS, SHA, NSA, NIST, and RSA, to distinguish between the different scientific, business, and governmental policy issues.

If you disagree with Dorothy's statements regarding key escrow policy, then say so explicitly. If you believe that DSS is cryptographically weak, then let's see somebody break it. I maintain that unless somebody pulls a new algorithmic trick out of their sleeve, we won't see a 1024-bit DSS signature forged until long after we are all pushing up daisies.

Kevin S. McCurley
Massively Parallel Computing Research Laboratory
Sandia National Laboratories

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 73

Saturday 12 June 1993

Contents

Palo Alto library computer system calamity

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 12 Jun 93 11:24:09 PDT

On 13 May 1993, the computer system used by the Palo Alto Library's six branches began to make a few small errors in processing requests. The staff considered the errors not too serious at that time. However, by 22 May, the problems had escalated seriously, and the service folks were called in.

The system is an eight-year-old Ultimate System from Honeywell. Only used or reconditioned replacement parts are available. Unfortunately, the replacement parts turned out to be lemons, which further aggravated the situation. As a backup, the staff resorted to a read-only file that tells only what books the library owns, but not what is supposedly on the shelves. Consequently, all book-borrowing transactions had to be done by hand, while no returned books could be reshelved. A power surge on 25 May did further damage to the system, and on the 26th, the system was shut down completely for another week. Finally, the system was available again on 2 June, although considerable effort had to be devoted to processing the accumulation of returned books before operations returned to normal.

[Source: an article by Rufus Jeffris in the Palo Alto Weekly, 9 June 1993,
p. 11]

Computer errors in Spanish elections

"(Miguel Gallardo)" <gallardo@batman.fi.upm.es>
Fri, 11 Jun 1993 14:21:14 UTC+0200

On 6th of June several Spanish cities and towns had too high number of people that could not vote because their name were not in the right list.

In Spain, Instituto Nacional de Estadistica (INE) is responsible for computing and updating the polling lists.

As the election was nation wide, these mistakes did not change any parliament member. However, next election will be a local one, and it seems that INE will not perform better, it will be much more difficult to explain to the people why they will not have the chance to change their majors.

Miguel A. Gallardo Ortiz, PX86 Engineer UNIX&C freelance working on RSA crypto
P.O. Box 17083 - E-28080 Madrid (Spain) Tel: (341) 474 38 09 - FAX: 473 81 97
gallardo@batman.fi.upm.es President of APEDANICA (Spanish Legal Computer Crime
Research Association) ASOCIACION PARA LA PREVENCION Y ESTUDIO DE DELITOS
ABUSOS Y NEGIGENCIAS EN INFORMATICA Y COMUNICACIONES AVANZADAS

Seattle hackers fined (from Reuters via the NYTimes)

the person your mother warned you about <phydeaux@cumc.cornell.edu>
Fri, 11 Jun 1993 09:20:36 -0500

I found this little piece buried in the NYTimes, 11 June 1993. No real mention is made of what the "hackers" (I suppose the word will never be rescued) did. Is anyone on RISK familiar with the details?

And you have to wonder, given the size of notebook computers, and the ease of purchasing and storing them secretly, how the last clause mentioned could possibly be enforced.

COMPUTER HACKERS ARE GIVEN FINES AND 5 YEARS' PROBATION

SEATTLE, June 10 (Reuters) -- Two hackers who illegally infiltrated the computer systems last fall at the Boeing Company and the United States District Court here were each sentenced to five years of probation and 250 hours of community service, a clerk at the court said Wednesday.

Magistrate David Wilson also ordered the two Seattle residents, Charles Anderson and Costa George Katsaniotis to pay a combined $30,000 in restitution. Boeing, which said at the time that none of its systems or data had been damaged by the unauthorized access, will get $28,000 of the fine and the court $2000 to defray costs of changing security and checking files. "As part of the probation they're not allowed to own a computer or computer accounts without the permission of the probation officer," the clerk added.

73 de Dave Weingart KB2CWF phydeaux@cumc.cornell.edu
phydeaux@src4src.linet.org

Re: Flight control computers 'to bypass pilots' (RISKS-14.65)

<timothy@tbucks.com>
Thu, 10 Jun 93 09:18 MDT

I would like to address this subject; I am an Air Traffic Controller with 13 years experience in most control functions, including Radar and Oceanic Non-Radar.

Most communications with pilots over or near land take place under VHF or UHF A/G radio. If, for example, I want to descend a flight to FL 240 (24,000 feet) I say "Flight No., descend and maintain flight level two four zero." The pilot will acknowledge by repeating his flight number and the assigned altitude, then begin a descent. (Well, lots of times they will question the altitude but let's not get into that <g>).

At the same time I'm speaking, I will punch the flight id and altitude into my computer, and the assigned altitude will be displayed on the scope. But that bears no relation to what I've said, or the pilot heard or said back to me.

I might be thinking 240, punch 240 into the computer, but say 220. I should catch the error when the pilot reads back the clearance, but I might not. I might say 240, but the pilot hears 220, and I don't catch the error on read-back. He might read back 240, but put 220 into his flight director. Each of these errors happens from time to time, and can cause problems.

Using Mode S, I would enter the flight id and altitude and that would be sent to the cockpit, where the pilot would acknowledge by pressing a button. My display would indicate the acknowledgement. The pilot could still question the clearance via voice radio.

Mode S would not eliminate errors; I might for example punch in the wrong flight id or altitude. But it should reduce greatly incidents in which the pilot is doing something other than what is shown on my display. Since I am continually scanning that display for potential conflicts, it is vital that it accurately reflect the intentions of the pilots.

There will, I think, always be a pilot (though perhaps someday only one) but the pilot in command already leaves many tasks to the computer. A commercial airliner is on auto-pilot most of the time after take-off, and can begin a landing approach. The most advanced systems can make a landing in zero visibility conditions, which a human pilot cannot.

Timothy Buchanan

Across the Computer Divide, NY Times

Marty Leisner x71348 <leisner@hydrus.WRC.Xerox.COM>
Fri, 11 Jun 1993 21:28:03 GMT

"Across the Computer Divide, The Nerds face the Dummies" (Sunday NY Times, 6 June, p. 1) talked about "DOS for Dummies", and the lack of training. This has to do with productivity (computers with out training and expertise don't improve productivity).

Marty Leisner   leisner@eso.mc.xerox.com   leisner.henr801c@xerox.com

The Internet is international (Rothwell, RISKS-14.72)

Frederick Roeber <roeber@vxcrna.cern.ch>
Thu, 10 Jun 1993 10:50:34 GMT

A little while ago someone at tis.com announced (on alt.security, among other places) that a reference PEM implementation was "freely" [sic] available for ftp in the US and Canada.

Just for kicks, I tried it from here (the evil CH empire):

```
% ftp ftp.tis.com
Connected to AZALEA.TIS.COM.
530 Only DNS registered hosts in the US/Canada can use this server.
```

I haven't extensively played with their system, but I'd suspect they
are reverse-resolving the IP address to a fully-qualified domain name,
and seeing if the top-most domain is an old three-letter type (or
possibly ".us" or ".ca"), or an international two-letter (e.g, ".uk" or
".ch"). I'm sure we can all evaluate the security of this method.

> I don't see anything to stop (for example) groups from outside the US
> lobbying this email service by pretending to be "the people" from "this
> country."

Well, the system for the USA's House of Representatives requires that any
would-be e-mail sender first send a (real) postcard to their rep, listing
their actual address and their e-mail address. This would provide a link from
any e-mail message to a real location in the rep's district. All replies are
via real mail, anyway, presumably to the address on the postcard.

BTW, ftpmail to ftp.tis.com works ;-)

Frederick G. M. Roeber | CERN -- European Center for Nuclear Research
CERN/PPE, 1211 Geneva 23, Switzerland roeber@cern.ch +41 22 767 31 80

[Postcard scheme also noted by bruner@csrd.uiuc.edu (John Bruner).
REAL SECURITY, eh? PGN]

Re: Whitehouse mail -

Marcus J Ranum <mjr@TIS.COM>
Wed, 9 Jun 93 21:41:59 EDT

It is possible that some whitehouse mail that is "correctly" addressed
is being rejected because the recipient addresses contain mail metacharacters.
This is a draconian mechanism to prevent folks from routing mail so it appears
to have originated from whitehouse.gov, by talking to the SMTP port, I.e.:

```
sol-> telnet whitehouse.gov 25
Trying 198.137.240.100 ...
Connected to whitehouse.gov.
Escape character is '^]'.
220 whitehouse.gov SMTP/smap Ready.
helo whitehouse.gov
250 (whitehouse.gov) pleased to meet you.
mail From: clinton
250 clinton... Sender Ok
rcpt To: mjr@tis.com
550 Recipient must be in form of: user, user@eop.gov, or user@whitehouse.gov
```

This has the unfortunate side effect that mailers that generate cruft
like IN%president@whitehouse.gov will run afoul of the destination check.

Re: Grassroots vs. Astroturf Movements (RISKS-14.72)

Max Stern 310-524-6152 <lms@ncrtory.torreypinesca.ncr.com>
Thu, 10 Jun 93 09:17:38 PDT

I also heard the NPR report cited in 14.72 by Shyamal Jajodia <SHYAM@mitvmc.mit.edu>. NPR described more than the preparation of lobbying letters for targeted mailing lists to send on to their representatives. The new Astroturf (r) lobbying techniques also include the following horror:

> The consulting outfit contracts with a lobbyist to generate not mail, but PHONE CALLS, to congressional offices. They then telephone "grass roots" citizens and, having given them a sketch of the issue, say "If you agree with us that this issue is important, we can connect you with Congressman Wintergreen right now, so that you can express your opinion to him." Then they "patch" the callee through to the congressperson's office, get off the line, and it's on to the next call. In this way they can generate a constant flux of phone calls, seemingly spontaneous, from private citizens, in support of any issue.

The more sophisticated congressional staffs have already learned to detect this kind of lobbying; they ask a few detailed questions about the issues and find that the caller completely lacks any substantive background information. The RISK is that it becomes increasingly difficult for the congressional staff to winnow the wheat (sincere opinion from concerned citizens) from the Astroturf chaff, and that modern information technology is what enables the consulting firm to provide this "service."

Max.Stern@TorreyPinesCA.ncr.com

Re: French Fry Robots! (McKay, RISKS-14.71)

Hugh JE Davies <hdavies@rx.xerox.com>
Thu, 10 Jun 1993 10:38:24 GMT

This [risk] has been routinely dealt with in the process control industry for decades. About 15 years ago, I was working on systems for the potato chip (US)/crisp (UK) manufacturing industry which handled hundreds of tons of sliced potato per hour being run through a fryer containing 3 tons of corn oil. As long as the oil level/oil pump/heater thermostat interlocks didn't fail spectacularly, there was no problem.

Admittedly, we had a rotating orange light and a *loud* siren on top of the control panel that was the "if all else fails, run away" warning.

And I won't mention the time a supervisor dropped a clipboard onto the fryer input belt (which ran at several hundred feet a minute.)

Cheese & onion clipboard, anyone?

Huge.wgc1@rx.xerox.com   Rank Xerox Technical Centre, WGC, UK.

Re: Citibank ATM risk (Kass, RISKS-14.72)

The Polymath <hollombe@polymath.tti.com>
Wed, 9 Jun 93 18:32:50 PDT

}... I've never made two transactions in a row on a Citibank ATM, so I
}can't be sure that the language question is routinely presented again ...

It isn't. Language is chosen at start of session. The only way to arrive at the situation you found is for someone to dip their card, then change their mind and walk away. Further, if you check I think you'll find the ATM asks for the PIN _after_ language selection (so the PIN entry screen will be in the correct language). Thus, what you saw was much less of a security risk than it seemed.

Jerry Hollombe, aka: hollombe@polymath.tti.com Head Robot Wrangler at Citicorp
Usual disclaimers [not Citicorp policy or official Citicorp anything]

ATM RISKS (Kass, RISKS-14.72)

the person your mother warned you about <phydeaux@cumc.cornell.edu>
Thu, 10 Jun 1993 09:30:32 -0500

Generally speaking (at least, among the many ATM's I've used in the NYMet area), if an ATM sits idle for a period of time (and this period seems to be less than one minute, admittedly a fairly long period of time), it will prompt you for your PIN again before allowing you to make a withdrawal, presumably as a protection against just such opportunistic attacks on your account. This protection is lessened if you aren't carful about shielding your PIN as you punch it in to the extremely large and easy-to-read display.

What's interesting to note about the Citibank ATM's (if not a RISK associated with them), is the braille strips around the slots. Since it's a touch screen, with no physical keypad, someone who's blind (ooops, pardon me..."optically challenged") can't use it anyway!

73 de Dave Weingart KB2CWF phydeaux@cumc.cornell.edu phydeaux@src4src.linet.org

---

Re: Citibank ATM Risk (Kass, RISKS-14.72)

Greg Brail <gjb@fig.citib.com>
Fri, 11 Jun 1993 18:35:27 -0400

To start with, I am a programmer and I do work at Citibank, but I don't know any more about the design of the ATMs than the average person. Nonetheless, I use them all the time.

Anyway, the ATMs, at least the ones in most of the Manhattan locations, ask "What language to you want to speak?" before asking for the PIN. Since the ATMs support languages that don't use the Roman alphabet (like Chinese and Japanese, although I don't know either so I can't tell which is which from the buttons) , the numbers on the PIN keypad would have to be different for those languages.

And even though the ATMs don't "eat the card," they ask for the PIN frequently. At the very least, they appear to ask before every "Get Cash" transaction, and I think they ask before money transfers as well. However, I don't know the exact algorithm, so I wonder if they also ask before one tries to see someone else's account balances or transaction history.

greg [Disclaimers...]

[Similar comments from Mark Eckenwiler eck@panix.com ...!cmcl2!panix!eck]

Re: Cryptography, Free Speech, and so on (Leichter, RISKS-14.72)

Carl Ellison <cme@ellisun.sw.stratus.com>
Thu, 10 Jun 93 15:13:38 EDT

If Jerry is trying to claim that cryptography is born classified, like nuclear technology, then I believe he is wrong. The NSA tried to push this concept back in the late 1970's and it was tossed out, as I recall. As a result, I am allowed to publish anything about cryptography in any international journal or speak at a conference giving details of my work without getting approval of any government agency.

The NSA, in the late 1970's, tried to make it otherwise: that a citizen had to get permission to publish or speak on cryptography and couldn't speak to any foreigners.

Re: Clipper

Dave Banisar <banisar@washofc.cpsr.org>
Sat, 12 Jun 1993 12:14:29 EST

On June 9, 1993, Congressman Edward Markey, Chairman of the House Subcommittee on Telecommunications and Finance held an oversight hearing on encryption and telecommunications network security. Panelists were Whitfield Diffie of Sun Microsystems, Dr. Dorothy Denning, Steven Bryen of Secure Communications, Marc Rotenberg of the CPSR Washington Office and E.R. Kerkeslager of AT&T.

Congressman Markey, after hearing the testimony presented, noted that the Clipper proposal had raised an *arched eyebrow among the whole committee* and that the committee viewed the proposal skeptically. This statement was the latest indication that the Clipper proposal has not been well received by policy makers. Last Friday, the Computer Systems Security and Privacy Advisory Board of NIST issued two resolutions critical of the encryption plan, suggesting that further study was required and that implementation of the plan should be delayed until the review is completed.

At the Third CPSR Cryptography and Privacy Conference on Monday, June 7, the Acting Director of NIST, Raymond Kammer, announced that the implementation of the proposal will be delayed and that a more comprehensive review will be undertaken. The review is due in the fall. Kammer told the Washington Post that maybe we won't continue in the direction we started out.

The full text is available by anonymous ftp from cpsr.org /cpsr/crypto/clipper

Re: health effects of VDTs (correction) (Hull-Richter, RISKS-14.72)

Kenneth R Foster <kfoster@eniac.seas.upenn.edu>
Thu, 10 Jun 93 07:03:49 -0400

The unit should have been mG (milligauss). The text had been "corrected" by a typist. I think that we corrected the error in the galleys. The book is _Phantom Risk_ (Foster,Bernstein, Huber, eds), MIT Press 1993.

Strictly speaking, the correct unit should be Tesla; in discussions of health effects of magnetic fields the unit Gauss is usually used. For nonmagnetic materials it is appropriate as well.

Kenneth R. Foster

Re: Errors in the correction of the error

Bruce Limber <blimber@cap.gwu.edu>
Thu, 10 Jun 1993 09:45:26 -0400 (EDT)

Please forgive me if any of what follows seems uncharitable; I truly don't mean it to be a personal attack, nor to I wish to appear non-humble.

Two corrections were posted in RISKS-14.72, pointing out errors in the RISKS-14.71 directions for getting to a conference by Metro (the DC subway system) from National Airport. There was indeed an error in the original directions.

I posted one set of corrections; that set is, to the best of my knowledge, reliable. I stand by my correction, and I'm more humble than you are! :-)

The other correction was posted by one of our esteemed colleagues, and in correcting the (one) error in the original directions, he regrettably introduced two new errors. (Perhaps we should stop before we're even farther behind?)

1. The yellow train to take from National Airport is labeled "Mt. Vernon Sq." It "does not--and never has--" gone to U Street/Cardozo. (He's thinking of the green train, which is irrelevant to our intent; when the end-of-track was extended from Gallery Place to U Street for the new green line, the yellow train's terminus was extended up the new track beyond Gallery Place, too--but only to Mt. Vernon Square.)

2. The blue train through Metro center (both of which are ideally irrelevant to our discussion) says "Addison Road," not "New Carrolton." The New Carrolton train is the orange line, which is--suffice it to say,

you don't want to hear about it. :-)

BTW, if you're at the National Airport station and see a blue train labeled "Addison Road," ignore it: it's a lot slower than the yellow train.

TRUST ME :-) --here are the correct directions, again:

Take the yellow train labeled "Mt. Verson Sq." to Gallery Place; there, transfer to a red train labeled "Shady Grove." Your destination is the Twinbrook station.

Piece of cake.

Unfortunately, the real tragedy of all this confusion is that it will probably put off lots of people who would otherwise have taken the subway, which really is an easy and enjoyable way to travel from National Airport to the hotel. It's also one of the cheapest. Buses cost more and probably take longer. And the less you have to deal with taxis in this area, the happier you'll be: the correct fare is a lot, and hacks here are notorious for overcharging (not all cabs here use meters).

Take the subway; you'll be glad you did.

You have my word on it. :-)

Re: And yet, a Risks report contains more errors!

BillV <billv@nafsa.org>
Fri, 11 Jun 93 09:41:25 EST

I don't find botched Metro directions at all surprising. For example, the Blue line train actually goes to, and is labelled, "Addison Road". It's the Orange Line that runs to New Carrolton, which theoretically does not run from the Airport.

Re: What's in it for the grocer? (Kristol, RISKS-14.72)

Geraint Jones <Geraint.Jones@prg.ox.ac.uk>
Thu, 10 Jun 93 09:54:00 BST

There is a hidden assumption that the use of cash is free to the supermarket. Whilst cash can be a moderately convenient means of exchange for the small sums in which individuals deal, or indeed for disguising huge transactions from the tax man, it is tremendously expensive to move it from place to place, and to protect it against both pervasive `evaporation' from the surface of the organisation, and from occasional shotgun-inspired haemorrhages.

I plead relevance to RISKS, because it sometimes seems that things get sent (t)here because they mention technology -- risky or not -- and we do seem to assume that the absence of technology must at worst not be a bad thing.

Re: What's in it for the Grocer?

David Carroll <BDCARRD1%BUDGET@CUNYVM.CUNY.EDU>
Thu, 10 Jun 93 10:11:09 EDT

Dollars, that's what! Dave Kristol posted asking if supermarket "price clubs" were used for building "buying profiles" detailed everything that you bought using that card. I have no way of knowing if this happens in other geographic areas, but in the Albany, NY area, the Price Chopper chain does exactly that. But wait; there's more (to shamelessly steal Popeil's ad line) the card for that "price club" is one and the same with the stores check cashing card. If you don't feel like having a business make a buck selling your personal information, you have to stand in line at the "courtesy" desk to get a check approved - amount of purchase only. Friends and I have each tried to get a card for the sole purpose of check cashing (I don't get their specials and they don't sell my information; sounds fair?) No way, Jose. So I have another solution - I won't shop there. Whenever my sad little Grand Union doesn't have some essential ingredient I must have, I go to Price Chopper and take the opportunity to complain about their policy (while pointing out that I spent c.$100 at Grand Union and $10 there.) The risk? that in an increasingly automated age, as checks become obsolete (very soon by all reports), they won't even need this extra card as the electronic hook to tie your purchase info to your demographic info. If you have to use a card to pay (whether credit or debit) they'll have the hook. Now is the time to get legislation passed to outlaw use of private information for purposes unrelated to a transaction that are not expressly approved. That principle has been advocated by the Privacy Commission and countless privacy experts for the past 25-30 years. Are we ready?

Dave Carroll, NYS Div. of the Budget bdcarrd1%budget@cunyvm.cuny.edu

Re: What's in it for the grocer? (Kristol, RISKS-14.72)

Mike Olson <mao@postgres.Berkeley.EDU>
Thu, 10 Jun 1993 10:58:13 -0700

Dr. Mike Stonebraker here at Berkeley consults for a bunch of big retailers on database management (Stonebraker started the Ingres project, which he subsequently commercialized, in the early '70's). I've heard him give a talk on exactly this topic. Here's the gist of his story:

Supermarkets will offer "frequent buyer discount" cards. If you use the card, they will automatically apply any manufacturer discount coupons that apply to your purchases. You don't need the paper coupons.

The benefit to the consumer is that his grocery bill is lower.

The store is able to track purchases by individual customers, which is good for the store in two ways. First, it can break down purchasing habits by whatever demographic information they can find, which may help them advertise and stock their shelves. Second, it can sell the names of all Coke purchasers to Pepsi, so that Pepsi can clutter up your mailbox with advertisements. This way, the store makes some extra money.

The benefit to the manufacturer is that it finds out about your buying habits and can develop ad campaigns directed at you.

The RISK, of course, is that previously anonymous transactions will be recorded, and details sold to people you don't know. If that bothers you, you should pay cash and not use any kind of discount card.

Stonebraker's talk on the future use of database systems by retailers is pretty interesting. Big retailers like K-mart and Walmart in the US capture every single item sold at every cash register they own. The data are loaded into an enormous central database, where they're used in "data mining" applications to plan future purchases by the store. The main problem the retailers have right now is storage space and techniques for digesting the volume of data they have. If they could do it, they'd keep all purchase data forever, and issue queries like "When will knee-length powder-blue dresses come back into style?"

Mike Olson, UC Berkeley (mao@cs.Berkeley.EDU)

Re: What's in it for the grocer?

<mc/G=Brad/S=Hicks/OU=0205925@mhs.attmail.com>
10 Jun 93 15:36:41 GMT

To protect my job, I have to put the disclaimer first. As you can see from my X.400 address and sig, I work for MasterCard International. I've read a lot on the subject in company newsletters, etc., but the following remarks should be interpreted as cocktail-party conversation, not official statements from MasterCard International, Inc.

Yes, the credit card companies are offering lower fees to grocers (also to movie theaters and fast food restaurants, as I recall). But there are fees, and as you say, grocers tend to have slender margins. So what's in it for them? Two things: (1) customers like having more payment options and some of them will pick a grocer who takes MasterCard over one who doesn't, and (2) people who are paying with plastic instead of "real money" run up higher bills. So customer traffic goes up and profit per customer transaction goes up. THAT's why MasterCard has been so successful in getting grocery stores to accept MasterCard.

If any grocer who accepts MasterCard (or Cirrus ATM cards, or Maestro debit cards) is tracking purchases vs. card number, I haven't heard of it. On, the other hand, unless you're buying huge amounts of booze or something, the total RISK of such a database (it seems to me) would be a bit more junk mail, which hardly seems like a big deal when offset against the benefit of not having to carry cash or wait while a check is approved. And actually, since I don't think that grocers subscribe to the service that lets you look up address against card number, it probably couldn't even be used for that.

(I know I've been doing all of my grocery shopping with my BankMate ATM/Maestro debit card for two years now; I love it.)

If anybody wants to try and get an official statment on the subject out of MasterCard, they could try the following people in our Public Relations department: mc!Marianne_Fulgenzi@mhs.attmail.com, mc!Richard_Woods@mhs.attmail.com, or mc!Jana_Weatherbee@mhs.attmail.com. (X.400: c=us, admd=attmail, prmd=mastercard, and fill in sn= and gn= from the above list.) [Peter, you're "the press," why don't you try?]

J. Brad Hicks   Internet: mc!Brad_Hicks@mhs.attmail.com
X.400: c=US admd=ATTMail prmd=MasterCard sn=Hicks gn=Brad

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 74

Tuesday 6 July 1993

Contents

Major New York Telephone outage: cable cut in Mount Vernon

John Hawkinson <jhawk@Panix.Com>
1 Jul 1993 00:06:21 -0400

According to New York Telephone, there has been a cut trunk (cable) in Mount Vernon, NY, causing a major service disruption. The estimated time for completion of repair is 5:00pm Friday! The disruption has the following effects:

* A large number (all?) of 914 (Westchester, including Yonkers, White Plains, etc.) numbers are unreachable from 212 (and perhaps other places). You get an ``all circuits busy'' message.

*   A large number (all?) of 212 numbers are unreachable from most of 914. You just get a fast busy.

*   At least some 914 numbers are unreachable from 914. Again, just a fast busy. This might be dependent on your switch (my switch, which covers 914-969 and some others, is a 1AESS).

*   Many phone services are unreachable from 914 (for me, at least), such as 411 and 555-1212 (directory assistance), 0 (the local operator), 211 (automated/manual credit), and in some instances, 611 (repair). I was successful getting through to repair via 890-6611, once, and via 611 once.

As I said above, New York Telephone's latest estimate is that the problem will be repaired by 5:00pm Friday. Apparently a construction firm cut a trunk (perhaps more than one) to cause this problem.

To go around the problem, you should be able to route your calls through AT&T, MCI, Sprint, or another long distance company, by dialing

```
   10XXX-1-nnn-mmm-mmmm
```

Where 10XXX is a carrier access code, like:

```
   10288 for AT&T
   10333 for Sprint
   10222 for MCI
and 10698 for NYTelephone (ha, ha)
```

nnn is the area code (might not be necessary if you're in the same area code as the number you're trying to reach), and mmm-mmmm is the phone number (exchange and unit #).

Followups to ny.general, please.

John Hawkinson, jhawk@panix.com

Another mobile phone RISK hits "Sunset Boulevard"

"Jonathan I. Kamens" <jik@gza.com>
Fri, 2 Jul 93 16:35:44 -0400

(Quoted from the "Names & Faces" column, by Michael Blowen, in the Friday, July 2, 1993 edition of The Boston Globe. I believe this is a short enough excerpt to constitute "fair use.")

Moving sets a musical mystery

The British opening of Andrew Lloyd Webber's $5 million musical, "Sunset Boulevard," was delayed 13 days because the scenery was mysteriously shifting on its own, as if -- dare we say it? -- there was a Phantom of the Theater. Webber discovered the glitch when he visited the theater. "I made a call on my mobile phone and the set moved," he told The New York Times. "I made a second call and it moved again." Hydraulic valves powering the sets were apparently touched off the the transmissions.

> [The RISKS Archives include a performance of A Chorus Line attended by President Ford that was plunged into darkness by a Secret Service walkie-talkie, wiping out the lighting board CMOS memory. PGN]

(Although it's not exactly a RISK, the following tidbit appears right before the one given above, and is perhaps worth mentioning because many RISKS readers will probably find it amusing:

Making a ruckus about silence

IBM wants a little credit for a room of quiet. The computer giant has applied to the Guinness Book of Records to get its echoless test chamber that eliminates 99.99 percent of noise listed as the quietest place on Earth. "With the door closed, this place is quieter than a morgue," said Bob Waters, an IBM acoustical engineer. Sound-absorbing fiberglass wedges cover the room's concrete walls, door and ceiling. IBM uses its chamber in Boca Raton for testing computer equipment. The "dead room" at Bell Telephone System laboratory in Murray Hill, N.J., holds the quietest-room record, according to the 1992 Guinness book. It eliminates 99.98 percent of noise.

Jonathan Kamens Geer Zolot Associates jik@GZA.COM

German Bundestag microphones still not working [RISKS-14.19]

Debora Weber-Wulff <dww@math.fu-berlin.de>
Thu, 24 Jun 1993 07:15:24 GMT

Hopes that the new chamber for the German parliament, the Bundestag, would be ready before the summer break have not been fulfilled. The computer controlled microphone system did not work as expected. The Tagespiegel in Berlin gleefully printed a picture this morning of the current testing in progress: to simulate a "full house" the company has put empty cardboard boxes at each place. [Can we deduce from this that if they now get it to work, the parliamentarians are analogous to empty boxes :-) ? -dww] It seems a major problem in the previous system was that it was only tested in the empty chamber.

Debora Weber-Wulff, Professorin fuer Softwaretechnik, Technische Fachhochschule Berlin, FB Informatik, Luxemburgerstr. 10, 13353 Berlin,

Strasbourg A320 crash: "Pilot Error" - Official!

Pete Mellor <pm@csr.city.ac.uk>
Mon, 28 Jun 93 12:16:47 BST

In France-Soir of Monday 10th May (which was recently sent to me by a friend) there is a report that the Commission of Enquiry into the crash of an A320

near Strasbourg on 20th January 1992 is about to deliver its final report.
(Given the date of the report, it has probably already done so.)

The conclusion on the cause of the accident is "pilot error".

The main error was the confusion of the "flight-path angle" (FPA) and "vertical speed" (V/S) modes of descent, selected on the Flight Management and Guidance System (FMGS) console. The pilots were inadvertently in V/S when they should have been in FPA mode.

The error was not noticed on the console itself, due to the similarity of the number format display in the two modes. The other cues on the Primary Flight Display (PFD) screen and elsewhere (e.g., altitude and vertical speed indicator) were not noticed since the pilots were overloaded following a last-minute change of flight plan, and presumably were concentrating on the Navigational Display.

The actions of the ATC did not help the situation.

The result was that the aircraft descended at a vertical speed of 1100 metres/minute when it was only 1500 metres above the terrain.

Following the accident, the rescue teams took 2 hours to find the crash site, which probably led to the deaths of between 6 and 20 passengers who had survived the impact, and could have been saved by prompt attention.

This in turn was partly due to chaotic organisation, plus the fact that the emergency radio beacon was destroyed on impact.

Further details when I have had time to translate the report properly, or get hold of a copy of the final report.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, Tel: +44(0)71-477-8422, JANET: p.mellor@csr.city.ac.uk

The great bancard network breakdown

Bertrand Meyer <bertrand@eiffel.com>
Wed, 30 Jun 1993 11:22:28 -0700

The following is excerpted from Le Monde dated Tuesday, 29 June 1993, page 18. Translation and ellipses by Bertrand Meyer.

A Black Week-End for Automatic Teller Machines

THE GREAT BANKCARD NETWORK BREAKDOWN

Background (from the end of the article)

[All bankcards issued in France, but in France only, now have a built-in chip.] The famous [bankcard chip] has suffered many infantile problems. And for several months the Anglo-Saxon press has criticized French merchants, who sometimes reject foreign bankcards under the pretext that they don't have a chip.

[Note by BM: I have a ``foreign'' card but have not encountered such a problem.]

- -

Now for the recent incident:

Last week-end was tough for many of the 21 million French people who have a bankcard. They had the unpleasant surprise of being almost unable to use it on Saturday the 26th and Sunday the 27th, whether to withdraw money from ATMs or to pay merchants. All because the computers in charge of authorizing payments to close to 40% of current cards were down for almost thirty hours. The loss to businesses, already hurt by the recession, is hard to evaluate; but the French bankcard system, touted as a little marvel of technology and safety, has just shown its limits.

[...] The collapse was caused by a breakdown of the Sligos company's computers, which manage withdrawal and payment authorizations for close to half of the cards.

Banks such as BNP and Societe Generale, which have their own computer servers for bankcard processing, were not affected.

[Several paragraphs describe how various businesses tried to cope with the problem, with examples from Air France, Eurodisney etc.]

On an average day transactions amount to five million operations amounting to 2 billion francs.

The bankcard system has been presented as a symbol of the edge that French banks have acquired. What characterizes it in principle is both safety, thanks to the built-in chip, and flexibility, thanks to the ability for cardholders to withdraw money from 17,400 ATMs and buy from 520,000 merchants. But the system had already shown worrying signs of fragility. Last autumn [...] some operations were charged twice.

The history of bankcards in France goes back to the beginning of the seventies with the creation of the GIE [consortium] ``Carte Bleue'', followed in 1984 by another GIE called Carte Bancaire [Bank Card]. [...] In ten years of constant investments amounting to several billion francs, the little plastic card has acquired a hologram and a chip and [...] has become indispensable.

It seems incredible, then, that safety and relay mechanisms, as present in all sensitive computer systems, were not able to prevent last weekend's giant breakdown. Aside from a few isolated cases [DETAILS PLEASE! BM] the 30-hour service interruption has not had any really tragic consequences; it could have if the system's functioning had been interrupted for a longer period. One

may indeed wonder whether the forced-march development of electronic
money, ``monetics'', does not put a country's economy at the mercy
of a breakdown. Last year more than two billion operations were
performed in France with bankcards, for a total amount of 718 billion
francs, 475 billion for payments and 243 billion for withdrawals.

UK National Savings "computer problem"

<Jonathan.Bowen@prg.ox.ac.uk>
Thu, 24 Jun 93 15:55:22 BST

Yesterday I received a printed letter from the UK government National Savings Deposit Bonds centre:

> Dear Customer,
>
> I am sorry to tell you that the most recent Anniversary Certificate you received for this bond is incorrect.
>
> The Deposit Bond interest rate changed from 8% to 7% on 26 December 1992. But because of a computer problem this change was not reflected on your certificate. So the amount of interest and the bond value shown are higher than they should be.
>
> I enclose a replacement certificate ...

I suspect this letter and replacement certificates must have been sent to a great many people. As usual the computer rather than the programmer is blamed for the error. It's a hard life with not much redress being a computer!

Jonathan Bowen, Oxford University

An extreme risk of poor computer security

<Ross.Anderson@cl.cam.ac.uk>
Tue, 22 Jun 1993 16:11:19 +0100

A couple of weeks ago, Michelle and Lisa Taylor were acquitted (on appeal) of the murder of Alison Shaughnessy. This judgment freed them from serving life imprisonment.

An automatic teller machine transaction (since believed to have been a fraud or a processing error) placed the sisters near the scene of this murder. The police did the rest; the appeal court found that they had framed the sisters, and had deliberately suppressed a witness statement which cleared them (this witness had stated that one of the two suspects seen leaving the scene of the crime was black, while the Taylors are white). Thus Michelle and Lisa ended up being convicted of murder in the lower court.

During the appeal, their counsel did not raise the issue of the bogus ATM transaction which caused the trouble, as he was already accusing the police of lying about the evidence and did not want to complicate matters by accusing the banking industry of lying too.

Nonetheless the story is now out, and it shows that the risk of poor computer security at your bank is not just a financial one.

Ross Anderson, University Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, England rja14@cl.cam.ac.uk

2 Men Arrested in Bogus Connecticut ATM Fraud (RISKS-14.59 et seq.)

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 6 Jul 93 11:34:29 PDT

Alan Scott Pace, 30, and Gerald Harvey Greenfield, 50, were arrested on charges of credit card fraud, wire fraud, interstate transportation of stolen property, and conspiracy to commit a felony. Mr. Greenfield was also charged with bank fraud. (The planting of a bogus ATM in the Buckland Hills Mall in Manchester, Connecticut, was reported in RISKS-14.59.) Their arrest on 29 June was based on routine films of their having used genuine ATMs from which they allegedly withdrew more than $100,000, from the accounts whose numbers and PINs their Trojan-horse ATM had captured. Also seized were software, three handguns, bank-network stickers, a police scanner, and equipment to make phony bank cards, credit cards and passports. [Source: Article by Ari L. Goldman, N.Y. Times, 30 June 1993, B6.]

New Hampshire subsequently informed Connecticut that Pace was wanted in New Hampshire for a string of nine jewelry scams in 1987. He had been under indictment in 1989 for running a fake jewelry store, but never showed up for arraignment. [From an AP item in the Boston Globe, 2 Jul 1993, p. 19.]

Digital Signature Scandal

Noah Friedman <friedman@gnu.ai.mit.edu>
Mon, 28 Jun 1993 07:48:33 GMT

[The following is an official announcement from the League for Programming Freedom. Please redistribute this as widely as possible. [NF]]

> [Taking Noah at his word, several of you forwarded Noah's message to RISKS, including Paul Robinson <TDARCOS@MCIMAIL.COM>,
> Roland B Roberts <ROBERTS@curie.nsrl.rochester.edu>, and
> Sarah_M._Elkins.Wbst139@xerox.com. PGN]

Digital Signature Scandal

Digital signature is a technique whereby one person (call her J. R. Gensym) can produce a specially encrypted number which anyone can verify could only have been produced by her. (Typically a particular signature number encodes additional information such as a date and time or a legal document being signed.) Anyone can decrypt the number because that can be done with information that is published; but producing such a number uses a "key" (a password) that J. R. Gensym does not tell to anyone else.

Several years ago, Congress directed the NIST (National Institute of Standards and Technology, formerly the National Bureau of Standards) to choose a single digital signature algorithm as a standard for the US.

In 1992, two algorithms were under consideration. One had been developed by NIST with advice from the NSA (National Security Agency), which engages in electronic spying and decoding. There was widespread suspicion that this algorithm had been designed to facilitate some sort of trickery.

The fact that NIST had applied for a patent on this algorithm engendered additional suspicion; despite their assurances that this would not be used to interfere with use of the technique, people could imagine no harmless motive for patenting it.

The other algorithm was proposed by a company called PKP, Inc., which not coincidentally has patents covering its use. This alternative had a disadvantage that was not just speculation: if this algorithm were adopted as the standard, everyone using the standard would have to pay PKP.

(The same patents cover the broader field of public key cryptography, a technique whose use in the US has been mostly inhibited for a decade by PKP's assiduous enforcement of these patents. The patents were licensed exclusively to PKP by the Massachusetts Institute of Technology and Stanford University, and derive from taxpayer-funded research.)

PKP, Inc. made much of the suspect nature of the NIST algorithm and portrayed itself as warning the public about this.

On June 8, NIST published a new plan which combines the worst of both worlds: to adopt the suspect NIST algorithm, and give PKP, Inc. an *exclusive* license to the patent for it. This plan places digital signature use under the control of PKP through the year 2010.

By agreeing to this arrangement, PKP, Inc. shows that its concern to protect the public from possible trickery was a sham. Its real desire was, as one might have guessed, to own an official national standard. Meanwhile, NIST has justified past suspicion about its patent application by proposing to give that patent (in effect) to a private entity.

Instead of making a gift to PKP, Inc., of the work all of us have paid for, NIST and Congress ought to protect our access to it--by pursuing all possible means, judicial and legislative, to invalidate or annul the PKP patents. If that fails, even taking them by eminent domain is better (and cheaper in the long run!) than the current plan.

You can write to NIST to object to this giveaway. Write to:

Michael R. Rubin
Active Chief Counsel for Technology
Room A-1111, Administration Building,
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
(301) 975-2803.

The deadline for arrival of letters is around August 4.

Please send a copy of your letter to:

League for Programming Freedom
1 Kendall Square #143
P.O.Box 9171
Cambridge, Massachusetts 02139

(The League for Programming Freedom is an organization which defends the freedom to write software, and opposes monopolies such as patented algorithms and copyrighted languages. It advocates returning to the former legal system under which if you write the program, you are free to use it. Please write to the League if you want more information.)

Sending copies to the League will enable us to show them to elected officials if that is useful.

This text was transcribed from a fax and may have transcription errors. We believe the text to be correct but some of the numbers may be incorrect or incomplete.

- -

** The following notice was published in the Federal Register, Vol. 58, No. 108, dated June 8, 1993 under Notices **

National Institute of Standards and Technology

Notice of Proposal for Grant of Exclusive Patent License

This is to notify the public that the National Institute of Standards and Technology (NIST) intends to grant an exclusive world-wide license to Public Key Partners of Sunnyvale, California to practice the Invention embodied in U.S. Patent Application No. 07/738.431 and entitled "Digital Signature Algorithm." A PCT application has been filed. The rights in the invention have been assigned to the United States of America.

The prospective license is a cross-license which would resolve a patent dispute with Public Key Partners and includes the right to sublicense. Notice of availability of this invention for licensing was waived because it was determined that expeditious granting of such license will best serve the interest of the Federal Government and the public. Public Key Partners has provided NIST with the materials contained in Appendix A as part of their proposal to NIST.

Inquiries, comments, and other materials relating to the prospective license shall be submitted to Michael R. Rubin, Active Chief Counsel for Technology, Room A-1111, Administration Building, National Institute of Standards and Technology, Gaithersburg, Maryland 20899. His telephone number is (301) 975-2803. Applications for a license filed in response to this notice will be treated as objections to the grant of the prospective license. Only written comments and/or applications for a license which are received by NIST within sixty (60) days for the publication of this notice will be considered.

The prospective license will be granted unless, within sixty (60) days of this notice, NIST receives written evidence and argument which established that the grant of the license would not be consistent with the requirements of 35 U.S.C. 209 and 37 CFR 404.7.

Dated: June 2, 1993.

Raymond G. Kammer
Acting Director, National Institute Standards and Technology.

Appendix "A"

The National Institute for Standards and Technology ("NIST") has announced its intention to grant Public Key Partners ("PKP") sublicensing rights to NIST's pending patent application on the Digital Signature Algorithm ("DSA").

Subject to NIST's grant of this license, PKP is pleased to declare its support for the proposed Federal Information Processing Standard for Digital Signatures (the "DSS") and the pending availability of licenses to practice the DSA. In addition to the DSA, licenses to practice digital signatures will be offered by PKP under the following patents:

```
        Cryptographic Apparatus and Method ("Diffie-Hellman")
             No. 4,200,770
        Public Key Cryptographic Apparatus and Method
             ("Hellman-Merkle")   No. 4,315,552
        Exponential Cryptographic Apparatus and Method
             ("Hellman-Pohlig")   No. 4,434,414
        Method For Identifying Subscribers And For Generating
             And Verifying Electronic Signatures In A Data Exchange
             System ("Schnorr")   No. 4,995,082
```

It is PKP's intent to make practice of the DSA royalty free for personal, noncommercial and U.S. Federal, state and local government use. As explained below, only those parties who enjoy commercial benefit from making or selling products, or certifying digital signatures, will be required to pay royalties to practice the DSA.

PKP will also grant a license to practice key management, at no additional fee, for the integrated circuits which will implement both the DSA and the anticipated Federal Information Processing Standard for the "key escrow" system announced by President Clinton on April 16, 1993.

Having stated these intentions, PKP now takes this opportunity to publish its guidelines for granting uniform licenses to all parties having a commercial interest in practicing this technology:

First, no party will be denied a license for any reason other that the following:

(i) Failure to meet its payment obligations,
(ii) Outstanding claims of infringement, or
(iii) Previous termination due to material breach.

Second, licenses will be granted for any embodiment sold by the licensee or made for its use, whether for final products software, or components such as integrated circuits and boards, and regardless of the licensee's channel of distribution. Provided the requisite royalties have been paid by the seller on the enabling component(s), no further royalties will be owned by the buyer for making or selling the final product which incorporates such components.

Third, the practice of digital signatures in accordance with the DSS may be licensed separately from any other technical art covered by PKP's patents.

Fourth, PKP's royalty rates for the right to make or sell products, subject to uniform minimum fees, will be no more than 2 1/2% for hardware products and 5% for software, with the royalty rate further declining to 1% on any portion of the product price exceeding $1,000. These royalty rates apply only to noninfringing parties and will be uniform without regard to whether the licensed product creates digital signatures, verifies digital signatures or performs both.

Fifth, for the next three (3) years, all commercial services which certify a signature's authenticity for a fee may be operated royalty free. Thereafter, all providers of such commercial certification services shall pay a royalty to PKP of $1.00 per certificate for each year the certificate is valid.

Sixth, provided the foregoing royalties are paid on such products or services, all other practice of the DSA shall be royalty free.

Seventh, PKP invites all of its existing licensees, at their option, to exchange their current licenses for the standard license offered for DSA.

Finally, PKP will mediate the concerns of any party regarding the availability of PKP's licenses for the DSA with designated representatives of NIST and PKP. For copies of PKP's license terms, contact Michael R. Rubin, Acting Chief Counsel for Technology, NIST, or Public Key Partners.

Dated: June 2, 1993.

Robert B. Fougner, Esq.,
Director of Licensing, Public Key Partners,
310 North Mary Avenue, Sunnyvale, CA 94033

[FR Doc. 93-13473 Filed 8-7-93; 8:45 am]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 75

Wednesday 14 July 1993

Contents

Bugs in the computer

Clive Feather <clive@x.co.uk>
Wed, 14 Jul 93 11:11:11 BST

The following appeared in Unigram.X (a UK newsletter) and Market Watch
(an electronic news clippings service). On my request, permission has been
granted to reproduce this item in RISKS provided that the full text,
up to and including the line beginning with several = signs, is included.
Clive D.W. Feather, IXI Ltd, Vision Park, Cambridge   CB4 4ZR UK
clive@x.co.uk   Phone: +44 223 236 555   Fax: +44 223 236 466

- -

SUN MICROSYSTEMS INC KNOWS WHY BRAZIL IS KNOWN TO ITS NATIVE INHABITANTS
AS THE KINGDOM OF THE ANTS

Computergram via First! -- Sun Microsystems Inc knows why Brazil is known to its native inhabitants as the kingdom of the ants - it got an electronic mail message from its local representative down there asking how to get rid of bugs - ants nests to be precise: seems a user had turned his workstation off for a few days and on returning to power the thing up was greeted by some nasty crunching and popping sounds; opening the lid he was greeted by an army of ants whose nest-building had been rudely interrupted by his machine's Sparc CPU and disk subsystem coming to life; pest control was hurriedly dispatched and the system was soon up and running - Sun knows its stuff when it comes to bug-fixing.

[07-08-93 at 14:38 EDT, Copyright 1993, Apt Data Services., File: g0708183.437]

- -

Re: Important words in other fonts

Frederick G.M. Roeber <roeber@axcrnb.cern.ch>
Wed, 7 Jul 1993 09:44:07 +0200

Recently I have been working with the "World Wide Web," a project designed to unite the various data resources on the internet into a common web of information. The Web began a few years ago at CERN. I am working at CERN as well, and some people who saw my work or articles thought I was an official web project member.

So, on my 'signature' page (http://info.cern.ch/roeber/fgmr.html)
I included a disclaimer:

  Please note: <b>I am <i>not</i> an official member ...</b>.

The lingua franca of the web is HTML, or hypertext markup language, which is based on SGML. The codes in angle brackets above are SGML, and stand for bold and italics.

I looked at my page with my whiz-bang X-based web browser (NCSA Mosaic), and sure enough the line appeared with nice bold and italicised words.

A short time later, I got a call from a somewhat annoyed web project guy, demanding to know why I was claiming to be an offical member. It seems that on his NeXT browser, the word "not" was mysteriously absent.

The problem was that his browser didn't support italics.

Why? Well, when the Web began it was "hypertext" based. Everything was supposed to be simple, plain text accessible by everybody. Though HTML was based on SGML, this was more to be "standard" than to support fancy markups. The core team had a nice plan as to how they would expand, slowly and in step. Then the NCSA came along, with their elegant multimedia X-based browser. Suddenly the web became "hypermedia," and (as it supported much more of SGML), even plain text could be marked up in much fancier ways. So people started writing documents depending on the capabilities of NCSA Mosaic, leaving the earlier browsers behind. In this case, that lapse changed the entire meaning of a rather important sentence.

There are a few points here:

1) In important sentences of electronic documents, don't put important words (like "not") in other fonts or representations.

2) In fact, avoid needless font and representation twiddling.

3) Don't assume everybody has the same advanced tools you do.

4) If you're going to use a standard, use *all* of the standard. HTML is based on SGML. The <i> code is legitimate SGML.

5) If you can't represent a requested font, for pete's sake don't just ignore the text! Put it up however you can. In this case, when I protested my innocence, the other guy loaded up the page on the old line-mode browser on the VM system. This browser ignores virtually all markup commands, so the unadorned sentence -- including the 'not' -- appeared.

6) If you launch a project in to the public, be prepared for someone to take the ball and outrun you. You can't stay firmly in control. This emphasizes point 4 -- the whole point of "standards" is so that when this happens, things are still compatible.

Frederick G. M. Roeber, CERN/PPE, 1211 Geneva 23, Switzerland
roeber@cern.ch or roeber@caltech.edu | work: +41 22 767 31 80

IEEE Computer Magazine Article Analyzes Therac-25 Accidents

Jim Haynes <haynes@cats.UCSC.EDU>
Tue, 13 Jul 93 13:19:55 -0700

by Nancy G. Leveson, Professor of Computer Science and Engineering at University of Washington, and Clark S. Turner, doctoral student at University of California, Irvine. Pages 18 through 41 of the current (July 1993) issue of Computer.

[The report from which this paper is drawn was noted in RISKS-14.04. PGN]

Medical Reimbursements and Computer Glitches

Sanford Sherizen <0003965782@mcimail.com>
Thu, 24 Jun 93 10:45 GMT

I have been handling some of my elderly mother's bills after her recent hospitalization. Since she is in an HMO (Health Maintenance Organization), she should not have had any bills other than for personal incidentals (tv, etc.). Yet, she kept getting bills from one medical testing lab. When I made an inquiry, the lab told me that the bills should have been paid by the HMO and that I should notify them, which I did. Several more bills came from the lab and several more inquiry calls were made. Yesterday, a letter came indicating that the account is delinquent and that it will be turned over to a collection agency unless paid immediately. I called and was told that their records indicated that the bill had not been paid. After pushing them a lot to review their records, they suddenly discovered that the bill had been paid by the HMO s more than a month ago. The clerk told me that there had been a *number of cases* recently where the computer had not recognized that a payment had been made and bills were automatically sent out. He told me that the computer problem ws being worked on. When I complained that the lab continued to send out bills even though they knew that some of them were false, he told me that all people had to do was to call the accounts department (it was an 800 number) and any errors would be corrected. However, if I had not insisted several times that the HMO had been notified and that they had paid the bill, the money would be owed by my mother.

The end result is that this lab knows that there is a billing problem and they have continued to send out bills, some of which are erroneous. Their solution is that (often ill) people will know that the bill has been paid, will contact the billing office, will fight to ensure that the correct information is in the computer, and all will be resolved. Unfortunately, what will really happen is that some people will pay the bill even if they do not owe the money and others will have their credit history threatened if they cannot afford to pay the money.

While this does not seem to fall under the legal definition of fraud, it may be illegal if the lab is billing with knowledge of a computer problem of this sort. I suspect that this problem is more common than recognized and that the lab is only one of a number of organizations that have decided that orderly processing of accounts is more important than correct billing of people. Computer glitch has become an excuse for financial manipulation and harming of people.

Software Safety Workshop: Call for Papers and Participants.

"Dr. Lon D. Gowen" <gowen@sevmsa.cs.msstate.edu>
Wed, 23 Jun 1993 19:17:29 CDT

CALL FOR PAPERS AND PARTICIPANTS

The '93 International Software Safety Workshop

November 18-19, 1993
Computer Science Department
Mississippi State University
MS State, MS 39762

Tentative Sponsors:
The National Science Foundation (NSF)
The Oak Ridge Associated Universities (ORAU)
Mississippi State University (MSU)

In Cooperation with:
The American Society of Safety Engineers (ASSE)

This workshop's goal is to bring together researchers and practitioners from academia, industry, and government in order to (1) enhance the transfer of technology and communication, (2) examine current problems relating to software safety research and practice, and (3) discuss and propose new directions for software safety research and practice. The workshop's organizers desire participation from all software-safety-impacted sectors such as aviation, medicine, transportation, manufacturing, the military, chemical processing, etc. The organizers also encourage participation by both industrial and governmental individuals who manage, specify, design, code, verify, or certify safety-critical software systems.

Additionally, this workshop seeks papers and presentations relating specifically to software safety. A partial list of topics follows:

* Standards for developing and certifying safety-critical software
* Techniques for static and dynamic verification & validation
* Managerial issues and methods
* Case studies in software safety
* Experience reports dealing with software safety
* Tools, techniques, and methodologies
* Technology transfer between researchers and practitioners
* Improving cooperation and communication between researchers and practitioners
* Software hazard analysis and safety-critical requirements
* Safety-critical designs
* Long-range goals and plans for software safety, and how best to achieve them
* Preliminary results from recent research or practice

Authors wishing to submit a manuscript for possible presentation and inclusion in the workshop's proceedings must submit five copies by 3-SEP-1993 of full-length papers (20 single-spaced pages maximum) or topics for presentation (2 single-spaced pages maximum) to the workshop's general chair at the address below:

Lon D. Gowen, Ph.D.
ISSW '93
Computer Science Department

Mississippi State University
P.O. Drawer CS
MS State, MS 39762

Phone: (601) 325-7508
Fax: (601) 325-8997
E-mail: gowen@cs.msstate.edu

In addition to the refereed papers and presentations, there will be several invited papers and presentations. The organizers anticipate presentations by the following organizations: FAA, FDA, FHWA, DoE, NASA, DLSF Systems, McKinlay and Associates, plus others. Additionally, there will be presentations by various academic researchers.

Application of Software Metrics and Quality Assurance in Industry

Pete Mellor <pm@csr.city.ac.uk>
Sat, 10 Jul 93 15:58:02 BST

The annual workshop of the Centre for Software Reliability will be held this year in Amsterdam from 29th September to 1st October, co-hosted with the Japanese Union of Scientists and Engineers.

The theme is "The Application of Software Metrics and Quality Assurance in Industry". Keynote speakers are Vic Basili, University of Maryland, and Yoshinori Iizuka, University of Tokyo.

Programme and application form can be supplied in paper or electronic form.

Under the Human Capital and Mobility scheme of the Commission for the European Community, 100% support is available for up to 15 delegates to attend from those areas of the EC which qualify for special support (which include Greece and Portugal).

Applications are therefore particularly invited from people in these areas (although naturally, all applicants are very welcome!).

Please respond preferably by e-mail. If you happen to know of anyone in one of the supported areas of Europe who might be interested but who does not receive e-mail or read the relevant lists, please pass the information on and ask them to respond by fax or snail-mail.

Peter Mellor, Centre for Software Reliability, City University, Northampton
Sq., London EC1V 0HB, UK. Tel: +44(0)71-477-8422 (Direct line to P. Mellor),
Tel: +44(0)71-477-8421 (Direct line to Ms. C.A. Allen, Centre Manager),
Fax: +44(0)71-477-8585 p.mellor@csr.city.ac.uk, c.a.allen@csr.city.ac.uk

"Russian Day" in St.Petersburg

<brunnstein@rz.informatik.uni-hamburg.d400.de>

Wed, 7 Jul 1993 18:36:46 +0200

In addition to the announcements in Risk Forum 14.60 (May 12,1993), concerning

```
      SECURITY AND CONTROL OF INFORMATION TECHNOLOGY IN SOCIETY
        IFIP WG 9.6 Working Conference, August 12-17, 1993
  Venue: the conference ship M/S Ilich between Stockholm and St.Petersburg
```

here is an updated program of the "Russian Day" (St.Petersburg, August 14,1993) To my knowledge, this is the first time where plans for "Russian ITSEC" may be compared to other suggestions (ITSEC, FC/FIPS), eg in related contributions of Marshall Abrams and one EEC speaker. Klaus Brunnstein (May 28, 1993)

```
    Saturday August 14: "Russian Day"

    Part I:  "IT and Security in Russia. Experts view"
    -------------------------------------------------
    "IT and Security in Russia"
        E.V. Evtyushin (Russian Agency for New Information)

    "IT vs. Security in Russia"
        E.A. Musaev (Russian Agency for New Information Technologies)

    "Problems of information protection in the Northwestern region of Russia"
       P.A. Kuznetsov (Association for Information Protection "Confident")


    Part II: "IT and Security in Russia - Commercial sector"
    --------------------------------------------------------
    "Bank requirements for Information Security"
       TBD (Sberbank of Russia)

    "Insurance Companies and Information Security"
       TBD (Representative of an insurance company)


    Part III: "It and Security in Russia - Public Sector"
    -----------------------------------------------------
    "The current state of INFOSEC legislation development in Russia"
       A.P. Kurilo (State Technical Committee of Russia)

    "The legal aspects of Digital Signature standardisation in Russian
     Federation"
       V.V. Markelov (Federal Agency of Government Communications and
       Information)

    "The Russian IT Security Evaluation Criteria"
       Y.A. Timofeev (National Sub-committee on IT Security Techniques
       Standardisation)


    Part IV: "Western Developments in IT-Security"
    ----------------------------------------------
```

R.Hackworth (U.K.): "The OECD Guidelines on IT Security"

M.Abrams (USA): "From Orange Book to new US Criteria"

P.White (U.K.): "Drafting Security Policies"

TBD "INFOSEC Security Issues in the EC"

Incident Response Workshop info

Gene Spafford <spaf@cs.purdue.edu>
8 Jul 1993 20:03:29 -0500

PRELIMINARY AGENDA
5th Computer Security Incident Handling Workshop
Sponsored by the Forum of Incident Response and Security Teams (FIRST)

August 10-13, 1993
St. Louis, MO

TUESDAY, August 10, 1993 Full-day Tutorials

1. Creating a Security Policy, presented by Charles Cresson Wood:
   [no abstract available at time of posting]

2. Vulnerabilities of the IBM PC Architecture: Virus, Worms, Trojan
   Horses, and Things That Go Bump In The Night
   presented by A. Padgett Peterson:

An intensive look into the architecture of the IBM-PC and MS/PC-DOS -- What it is and why it was designed that way. An understanding of assembly language and the interrupt structure of the Intel 80x86 processor is helpful.

The day will begin with the BIOS and what makes the PC a fully functional computer before any higher operating system is introduced. Next will be a discussion of the various operating systems, what they add and what is masked. Finally, the role and effects of the PC and various LAN configurations (peer-peer and client server) will be examined with emphasis on the potential protection afforded by login scripting and RIGHTS.

At each step, vulnerabilities will be examined and demonstrations made of how malicious software exploits them. Demonstrations may include STONED, MICHELANGELO, AZUSA, FORM, JERUSALEM, SUNDAY, 4096, and EXEBUG viruses depending on time and equipment available.

On completion attendees will understand the vulnerabilities and how to detect attempted exploitation using simple tools included with DOS such as DEBUG and MEM.

3. Unix Security
presented by Matt Bishop:

Unix can be a secure operating system if the appropriate controls and tools are used. However, it is difficult for even experienced system administrators to know all the appropriate controls to use. This tutorial covers the most important aspects of Unix security administration, including internal and external controls, useful tools, and administration techniques to develop better security.

Upon completion, Unix system administrators will have a better understanding of vulnerabilities in Unix, and of methods to protect their systems.

WEDNESDAY, August 11, 1993

8:30 - 8:45 Opening Remarks - Rich Pethia (CERT/CC)

8:45 - 9:30 Keynote Speaker - Dr. Vinton Cerf (XXXX)

9:30 - 10:00 Break

10:00 - 12:00 International Issues - Computer networks and communication lines span national borders. This session will focus on how computer incidents may be handled in an international context, and on some ways investigators can coordinate their efforts.
SPEAKERS:
Harry Onderwater (Dutch Federal Police)
John Austien (New Scotland Yard)
other speakers pending

12:00 - 1:30 Lunch with Presentations by various Response Teams

1:30 - 3:00 Professional Certification & Qualification - how do you know if the people you hire for security work are qualified for the job? How can we even know what the appropriate qualifications are? The speakers in this session will discuss some approaches to the problem for some segments of industry and government.
SPEAKERS:
Sally Meglathery ((ISC)2)
Lynn McNulty (NIST)
Genevieve Burns (ISSA)

3:00 - 3:30 Break

3:30 - 6:00 Incident Aftermath and Press Relations - What happens after an incident has been discovered? What are some of the consequences of dealing with law enforcement and the press? This session will feature presentations on these issues, and include a panel to answer audience questions.
SPEAKERS:
Laurie Sefton (Apple Computer)
Jeffrey Sebring (MITRE)
Terry McGillen (Software Engineering Institute)
John Markoff (NY Times)

Mike Alexander (InfoSecurity News)

7:00 - 9:00 Reception

THURSDAY August 12

8:30 - 10:00 Preserving Rights During an Investigation - During an investigation, sometimes more damage is done by the investigators than from the original incident. This session reinforces the importance of respecting the rights of victims, bystanders, and suspects while also gathering evidence that may be used in legal or administrative actions.
SPEAKERS:
Mike Godwin (Electronic Frontiers Foundation)
Scott Charney (Department of Justice)
other speaker pending

10:00 - 10:30 Break

10:30 - 12:00 Coordinating an Investigation - What are the steps in an investigation? When should law enforcement be called in? How should evidence be preserved? Veteran investigators discuss these questions. A panel will answer questions, time permitting.
SPEAKER:
Jim Settle (FBI)
other speakers pending

12:00 - 1:30 Special Interest Lunch

1:30 - 3:00 Liabilities and Insurance - You organize security measures but a loss occurs. Can you somehow recover the cost of damages? You investigate an incident, only to cause some incidental damage. Can you be sued? This session examines these and related questions.
SPEAKERS:
Mark Rasch (Arent Fox)
Bill Cook (Willian, Brinks, Olds, Hoffer, & Gibson)
Marr Haack (USF&G Insurance Companies)

3:00 - 3:15 Break

3:15 - 5:30 Incident Role Playing -- An exercise by the attendees
to develop new insights into the process of
investigating a computer security incident.
Organized by Dr. Tom Longstaff of the CERT/CC.

7:30 - ? Birds of a Feather and Poster Sessions

FRIDAY August 13

8:30 - 10:00 Virus Incidents - How do you organize a successful virus analysis and response group? The speakers in this session have

```
            considerable experience ans success in doing exactly this.  In
            their talks, and subsequent panel, they will explain how to
            organize computer virus response.
            SPEAKERS:
        Werner Uhrig (Macintosh Anti-virus Expert)
        David Grisham (University of New Mexico)
        Christoph Fischer (CARO)
        Karen Picharczyk (LLNL/DoE CIAC)
        Ken van Wyk (DISA/Virus-L)

10:00 - 10:15  Break

10:15 - 11:15  Databases - How do you store incident, suspect, and
            vulnerability information safely, but still allow the
            information to be used effectively?  The speakers in this
            session will share some of their insights and methods on this
            topic.
            SPEAKERS:
        John Carr (CCTA)
        Michael Higgins (DISA)
        speaker pending

11:15 - 12:15  Threats - Part of incidence response is to anticipate riska and
            threats.  This session will focus on some likely trends and
            possible new problems to be faced in computer security.
            SPEAKERS:
        Karl A. Seeger
        speakers pending


12:15 - 12:30  Closing Remarks - Dennis Steinauer (NIST/FIRST)

12:30 -  2:00  Lunch

 2:00 -  3:00  FIRST General Meeting and the Steering Committee Elections

 3:00 -  4:00  FIRST Steering Committee Meeting

^^^^^^^^^^^^^^^^^^^^Registration Information/Form Follows^^^^^^^^^^^^^^^^^^^^

INQUIRES:

Direct questions concerning registration and payment to:  Events at 412-268-6531

Direct general questions concerning the workshop to:  Mary Alice "Sam" Toocheck
                                          at 214-268-6933

Return to:   Helen E. Joyce
          Software Engineering Institute
          Carnegie Mellon University
          Pittsburgh, PA  15213-3890
          Facsimile:  412-268-7401
TERMS:
```

Please make checks or purchase orders payable to SEI/CMU. Credit cards are not accepted. No refunds will be issued, substitutions are encouraged.

The registrations fee includes materials, continental breakfast, lunches (not included on August 13), morning and afternoon breaks and an evening reception on August 11. Completed registration materials must be received by the SEI no later than July 10, 1993.

A minimum of 7 attendees are needed for each tutorial and there will be limit of 50 attendees. You MUST indicate which tutorial you would like to attend and an alternate if your first choice is full.

GOVERNMENT TERMS:

If your organization has not made prior arrangements for reimbursement of workshop expenses, please provide authorization (1556) from your agency at the time of registration.

GENERAL REGISTRATION INFORMATION:

Workshop................................ ....$300.00
All registrations received after July 10, 1993.........$350.00
Tutorials (Must be registered by July, 10, 1993)........$190.00
    [Yes, I know ...   If you call today, tell them a RISKS issue with
    this info did not come out until today. Maybe they can bend. PGN]

NAME:

TITLE:
COMPANY:

DIVISION:

ADDRESS:

CITY:

STATE:

ZIP:

BUSINESS PHONE:

EMERGENCY PHONE:

FACSIMILE NUMBER:

E-MAIL ADDRESS:
DIETARY/ACCESS REQUIREMENTS:

CITIZENSHIP: Are you a U.S. Citizen?   YES/NO

Identify country where citizenship is held if not the U.S.:

(Note: there will be no classified information disclosed at this workshop.
There is no attendance restriction based on citizenship or other criteria.)

GENERAL HOTEL INFORMATION:

RATES: A block of rooms has been reserved at the Hyatt Regency at Union Station, One St. Louis Union Station, St. Louis, Missouri 63103. The hotel will hold these rooms until July 10, 1993. Hotel arrangements should be made directly with the Hyatt, 314-231-1234. To receive the special rate of $65.00 per night, please mention the Fifth Computer Security Incident Handling Workshop when making your hotel arrangements.

ACCOMMODATIONS: Six-story hotel featuring 540 guest rooms, including 20 suites. All rooms have individual climate control, direct-dial telephone with message alert, color TV with cable and optional pay movies. Suites available with wet bar. Hotel offers three floors of Regency accommodations, along with a Hyatt Good Passport floor, and a special floor for women travelers.

LOCATION/TRANSPORTATION FACTS: Downtown hotel located in historic Union Station one mile from Cervantes Convention Center and St. Louis Convention Center and St. Louis Arch. Fifteen miles (30 minutes) from St. Louis Zoo.

DINING/ENTERTAINMENT: Italian Cuisine is features at Aldo's, the hotel's full-service restaurant. Enjoy afternoon cocktails in the Grand Hall, an open-air, six-story area featuring filigree work, fresco and stained glass windows. The station Grille offers a chop house and seafood menu.

RECREATIONAL/AMUSEMENT FACILITIES: Seasonal outdoor swimming pool. Full health club; sauna in both men's and women's locker rooms. Jogging maps are available at the hotel front desk.

SERVICES/FACILITIES/SHOPS: Over 100 specialty shops throughout the hotel, including men's and women's boutiques, children's toy shops and train stores.

Gene Spafford, COAST Project Director
Software Engineering Research Center & Dept. of Computer Sciences
Purdue University, W. Lafayette IN 47907-1398
Internet: spaf@cs.purdue.edu phone: (317) 494-7825

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 76

Tuesday 20 July 1993

Contents

Earthquake `early' warning system

Bill Owens <owens@desperado.cc.rochester.edu>
Wed, 14 Jul 1993 22:02:28 -0400 (EDT)

The latest Scientific American has a short piece in the Science and the Citizen department titled 'Fast Moves: Instant earthquake analysis may beat the waves' (August 1993, pp. 22-24). The primary topic is a system being developed at the California Institute of Technology which attempts to analyze seismological data immediately upon receipt, locating the quake and providing information to interested parties within minutes or even seconds. To achieve this, they are building a network of seismological labs in southern California. They appear to be thinking about the risks:

> Fast-analysis systems like the one at Harvard need not worry about small errors, because "they're not intended to support emergency operations... CUBE [the network] cannot afford to make mistakes"

But the real danger becomes apparent from the first paragraph of the article:

> ...researchers may soon be able to anticipate the effects of an initial tremor, enabling railroads to stop or slow their trains and permit [sic] elevator systems to halt at the nearest floor.

While that sort of automatic response would have the potential to be very helpful, it's obviously worrisome. Unfortunately, the system appears to require automation to achieve sufficiently fast response time. It would seem to be a difficult problem to not only analyze tremors without false alarms, but to predict damage well enough to activate only those safety measures necessary...

owens@cc.rochester.edu
Bill Owens, 727 Elmwood Avenue, Rochester, NY 14620 716/275-9120

DSS as a stamp tax

Mark Seecof <marks@wimsey.latimes.com>
Tue, 20 Jul 93 17:05:57 -0700

Many people raised in the U.S. are unfamiliar with general stamp taxes. We know about excise taxes (e.g., liquor) with payment evidenced by stamps, and tax stamps to validate specific documents (e.g., hunting licenses). But (to my perhaps inadequate knowledge) the U.S. hasn't had a general stamp tax since the War of Independence. England had one years ago... most signatures on receipts for money or bills of sale were invalid unless scrawled across postage stamps. England still imposes stamp taxes on some business transactions, e.g., transfer of real property.

NIST's proposal to "license" the DSS to PKP, forcing "the rest of us" including all who wish to transact business with the U.S. government to pay PKP every time we sign something digitally amounts to the imposition of a general stamp tax. Worse, it is a tax imposed by the government for the benefit of private persons (those who are paid by PKP).

Attempts by George III's government to impose various stamp taxes on American colonists 200-odd years ago fueled revolutionary sentiment among them...

Privacy report in Canada

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
15 Jul 93 10:02:09 EDT

A report in the Globe and Mail newspaper in Canada (Wed, 14 July 1994; #44801, page 1) by Geoffrey York of the Parliamentary Bureau is entitled "Privacy report warns of `Big Brother' computer; Linked government databases called ominous." Here is a summary.

> The Canadian federal government's privacy commissioner, Bruce Phillips, submitted a report warning that electronic data interchange among government computers could bring Orwellian Big Brother consequences to society. The government is proposing to establish booths where residents could transact government business; however, users would have to provide personal identification numbers, photographs, and fingerprints to be permitted to use these booths.
>
> The commissioner is concerned about the routine exchange of private information among people "whose right to the information is, at best, debatable." He also criticized the growing use of electronic surveillance and monitoring in the workplace. He urged Canadians to push for broader privacy rights and guidelines to control government use of electronic networks.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn.

Remote Control Car Locks

David Plumpton <plumpton@cc.uow.edu.au>
Thu, 15 Jul 1993 13:48:44 +1000

There was an article on the news the other night featuring a rather homemade looking device that a man had purchased for A$150 in Malaysia. This gizmo records and then transmits the codes that unlock car doors (or garages etc). A thief loiters around with the device set to receive as somebody is leaving their expensive looking car. When a remote control is used to lock the car, the signal is picked up and recorded by the device. The car owner wanders off, thinking that the car is secure. The thief sets the device to transmit, and hey presto the car unlocks itself for the thief.

Such an elegant and simple idea; I'm surprised that it took this long for someone to think of it (I certainly didn't). [*] The Australian police want the device made illegal (possession of it, I guess). What's the bet that the police will have legal use of it, though. Looks like pretty soon, remote controls will need time-stamped encryption techniques...

> [* Remember the movie *WarGames*, and the door-control touch-tones beaten by a record-and-playback attack? It's an old form of vulnerability for fixed authenticators. However, remember that even one-time tokens may be compromised if they are not properly incorporated into the system. PGN]

Airline entertainment systems - a true captive audience

Jon Leech <leech@cs.unc.edu>

Tue, 20 Jul 93 14:23:27 -0400

An article "Bottom Line Key In Video Systems" (Aviation Week, July 19, 1993, page 53) describes upcoming per-seat interactive video systems which will be eventually be installed in many aircraft. The last paragraph touches on privacy concerns:

> "On-board passenger entertainment systems also offer airlines a powerful marketing research tool. Master control unit software can be modified to log passenger viewing habits and game use. Inventory records can be adjusted automatically as meals and beverages are served. Passengers also can be asked to provide selected demographic data."

This is similar to the credit-card supermarket checkout systems, with the added bonus (for the airline) that they know just who is sitting in every seat - even the fact that someone *doesn't* watch TV will be noted.

Not that this seems like a significant privacy concern. But it's bad enough that we have to put up with advertisements for the airline blasting out of the speakers and garrulous twits who rattle away on Airphones in the next seat, without new annoyances such as this.

Jon (leech@cs.unc.edu)

Re: Strasbourg A320 crash: "Pilot Error" (Mellor, RISKS-14.74)

Flint Pellett <flint@gistdev.gist.com>
9 Jul 93 14:22:04 GMT

> The conclusion on the cause of the accident is "pilot error".

More of a user-interface design error, if you ask me. If you overload a person with things to do and input to consider to the point where they can no longer keep up, it is hardly reasonable to simply brush it off as "human error" when they fail to keep up.

This particular risk is one in which I think more computerization ought to be possible, and even good. A computer in the cockpit ought to be able to monitor the fact that "we're dropping 1100 m/s and we're only at 1500 m altitude" (along with quite a number of other things as well), prioritize potential problems, and then issue a verbal warning to the pilots if any problem gets life threatening like this. (Hopefully before it is too late to do anything.) The frequency of warnings are critical of course: if it cries "wolf" too often, it will get ignored.

Flint Pellett, Global Information Systems Technology, Inc., 100 Trade Centre Drive, Suite 301, Champaign, IL 61820 (217) 352-1165 flint@gistdev.gist.com

System Dynamics of Medical Reimbursements

Dan Yurman <dyurman@igc.apc.org>

Thu, 15 Jul 93 10:30:03 PDT

SYSTEM DYNAMICS OF MEDICAL REIMBURSEMENT PROBLEMS

Sanford Sherizen (3965782@mcimail.com) writes in Risks Digest 14.75 regarding the risks of incomplete management processes as well as faulty computer systems regarding medical reimbursement systems. The emphasis is more on the dynamics of the system than any particular computer risk.

1st: many physician practices "offload" their entire billing operation to service bureaus. 2nd: these service bureaus earn a fee for timely payment regardless of source, e.g., the patient or his/her insurance carrier. 3rd: some group practices, and large practices like HMOs, offer their service bureaus incentives for timely turnaround on receivables as well as penalties for failure to produce.

This creates an incentive for the service bureau to aggressively bill both the patient and the insurance carrier and worry about sorting out double payments, if at all, later on. The reinforcing loop for the service bureau is to churn payments as fast as possible regardless of source. The more quickly their doctor customers get paid, the more robust their incentive fee. From a systems perspective there is no balancing loop to insure integrity in the service bureau's records with regard to the source of the payment, only that an amount has been tallied and the client physician office has covered its receivables.

The service bureau cheerfully "offloads" the issue of reconciling mistakes in the source of payment to the patient. Their view is that patients will "know" and have "proof" that the bill for service has been covered. Here is tiny (pop. 45,000) Idaho Falls, ID, we have one such service bureau which exactly follows this model of aggressive practice in double billing the patient and the insurer. Further, there is an long lag (60+ days) in reconciling payments from insurers with copayments from patients.

Complaints to the provider have little effect. Once billing is offloaded to the service bureau, there is no one left in the doctor's office who is able, besides the doctor, to deal with the problem. As long as he/she is getting paid, the doctor has no special interest in patient billing problems with the service bureau. Typically, the doctor's office computer system is tied in directly to the service bureau. When the doctor looks at the system, the accounts are ok, and problems of double billing to the patient are invisible.

Patients have an opportunity to create a balancing loop if it is external to the doctor/service bureau system. Patients could form a consumer action organization which would intervene on their behalf, privately and publically, with service bureaus and their customers. The annual cost to a patient, e.g, on the order of $25/year, would be cost effective when compared to the average annual health bill of a family of four, e.g, $2,000-3000/year at a minimum.

Insurance companies, which are probably also fed up with aggressive double billing from service bureaus, might have an incentive to support such organizations. This would be especially true for those employers who self-insure and hire companies like Mutual of Omaha or Prudential to simply process the paperwork. The reference to these firms is for example purposes only, and is not intended to imply any connection to service bureau practices.

Dan Yurman, PO Box 1569, Idaho Falls, ID 83403 dyurman@igc.apc.org
3641277@mcimail.com

Re: Medical Reimbursements and Computer Glitches

Amos Shapir <amos@CS.HUJI.AC.IL>
Sun, 18 Jul 1993 17:02:38 +0300

This indeed may be quite common - an almost exactly identical incident happened to me -- about 10 years ago. It seems the lab bill is handled separately, and the lab computer (or their collection agency's computer) is not informed that the bill has been paid.

Amos Shapir, The Hebrew Univ. of Jerusalem, Dept. of Comp. Science.
Givat-Ram, Jerusalem 91904, Israel amos@cs.huji.ac.il Tel: +972 2 585706

Re: Medical Reimbursements and Computer Glitches

<Bob_Frankston@frankston.com>
Wed, 14 Jul 1993 23:50 -0400

I've long tried to track medical insurance payments. It isn't easy. In this example the user relied on the lab to assure that there records were correct and become aware of a specific case where they were probably wrong and followed through.

In general, however, each component system is designed in isolation with no thought being given to auditability on the part of the user. There are lots of uncorrelated pieces of paper mailed around with payments in varying amounts according to arcane rules going to various parties including the patient. The insurance companies seem to have some concept of medical events in an attempt to avoid double payments. But there is never a summary so the user can understand what is happening without collecting every slip of paper into one central set of records that correspond to the insurance company's representation.

One particular offender locally is Newton-Wellesley Hospital where each entity seems to be a separate corporation that does its own billing for each aspect of each procedure for combination of locations. This is compounded by having multiple members of a family with slightly differing names. And then there are lab tests...

Simple ideas like replacing bills that contain a single amount past do with summaries of payments and events and some common identification of events would go a long way. Such a system would be in the interest of the insurance agents as a way to discover errors and fraud.

In the meantime, I'll continue to use standard system methodology. Whenever things are confused let things quiesce. Don't pay bills until the insurance company and the doctors have had their chance to go around a few times and then take a guess at whether what remains to be paid is appropriate.

ATM Fraud/Databases/Ouch!

Russ Smith <e3urcs@fnma.com>
Mon, 19 Jul 93 13:14:30 EDT

To extend the much-trod ATM-fraud path...

My MasterCard number was recently used to fraudulently make $8000 worth of ATM cash advances over a 4 day period. Seems that the number itself was obtained via some standard illegal route which by now has undoubtedly been discussed (just the number was obtained, not the card itself) thus will not be addressed further in this note.

Much more interesting, however, was how my PIN was obtained, allowing the perpetrators of the fraud to use a fake MasterCard in an ATM 4 times a day, 4 days in a row, $500 each time...

Seems a written request for change-of-address was received by my Credit Union (backers of the MasterCard); this change was processed sometime on Wednesday, July 7th. The request included all sorts of identity-confirming information such as date of birth, social security number, and my mother's maiden name. The address was changed to a Brooklyn NY apartment (I live in a single-family house in Virginia).

IN THE SAME LETTER a request was made for a copy of the PIN for the MasterCard (not unusual for people to forget a PIN and request it again). The PIN, the most important secret piece of information for the card, was dutifully mailed off to the fraudulent address in Brooklyn.

Starting Monday, the 12th, the fraudulent cash advances were made from two different Brooklyn banks' ATMs.

Upon finding out about the fraud (tried to use the card myself and was declined for the first time in my life), I immediately called every financial institution I do business with -- fortunately, they all require some crucial bit of information for phone account manipulations (like a mother's maiden name...), send a change-of-address notice to BOTH the new AND old addresses, and won't send money/crucial info to the NEW address for 30 days.

Hope YOUR financial institutions protect your PINs as well...

Oh yeah, one more thing...on calling my MasterCard Service Center I was told that requests for PINs are handled by regenerating the same PIN and mailing it off to the address -- the SAME PIN is -always- regenerated (not just retrieved) from the same MasterCard #; if you want a DIFFERENT PIN, you have to get an entirely new MasterCard number...hmmm...

Russ <Smith@ur-guh.com>

ATM Fraud/Databases/Ouch!, Part II

Russ Smith <e3urcs@fnma.com>
Tue, 20 Jul 93 10:41:44 EDT

After many calls and faxes I've found out a little more about the mechanisms
behind ATM transactions and the fraudulent use of a MasterCard number of mine.

It turned out that the previously-related fraud was done using an
EXPIRED MasterCard number to withdraw cash from an ATM machine, not my
current MasterCard number. When the request for both the
change-of-address and the PIN number came via a letter, an old EXPIRED
MasterCard number was used (had expired more than a month earlier).
The change-of-address and PIN number for the expired card were
processed and sent off to the fake address The perpetrators then used the
expired card number and its PIN number to make the cash advances.

How is it possible to use an EXPIRED card to make $8000 in cash advances?

It's possible because the ATM's verification center ONLY checks if the
card number is on a list of STOLEN/LOST cards. If the card is not
stolen/lost, the verification center then performs a verification
check of the information FROM THE CARD ITSELF, not from some other
database.

So the perpetrators just wrote a new expiration date on the magnetic
stripe of their fake card; the ATM verification center verified that
the date hadn't yet passed and that was that.

Russ "Cancelled Credit" <Smith@ur-guh.com>

CFP94 (Sent to RISKS via Willis Ware)

George Trubow, John Marshall Law School <CFP94@jmls.edu>
14 Jul 93 11:04:30 CST

Conference Announcement and Call for Papers
Computers, Freedom, and Privacy 1994
23-26 March 1994

The fourth annual conference, "Computers, Freedom, and Privacy," will be
held in Chicago, Il., March 23-26, 1994. This conference will be jointly
sponsored by the Association for Computing Machinery (ACM) and The John
Marshall Law School. George B. Trubow, professor of law and director of the
Center for Informatics Law at The John Marshall Law School, is general
chairman of the conference.

The series began in 1991 with a conference in San Francisco\Burlingame,
and subsequent meetings took place in Washington, D.C. and again in San
Francisco\Burlingame, in successive years. Each conference has addressed a
broad range of issues confronting the "information society" in this era of the

computer revolution.

The advance of computer and communications technologies holds great promise for individuals and society. From conveniences for consumers and efficiencies in commerce to improved public health and safety and increased knowledge of and participation in government and community, these technologies are fundamentally transforming our environment and our lives.

At the same time, these technologies present challenges to the idea of a free and open society. Personal privacy is increasingly at risk from invasions by high-tech surveillance and monitoring; a myriad of personal information data bases expose private life to constant scrutiny; new forms of illegal activity may threaten the traditional barriers between citizen and state and present new tests of Constitutional protection; geographic boundaries of state and nation may be recast by information exchange that knows no boundaries as governments and economies are caught up in global data networks.

Computers, Freedom, and Privacy '94 will present an assemblage of experts, advocates and interested parties from diverse perspectives and disciplines to consider the effects on freedom and privacy resulting from the rapid technological advances in computer and telecommunication science. Participants come from fields of computer science, communications, law, business and commerce, research, government, education, the media, health, public advocacy and consumer affairs, and a variety of other backgrounds. A series of pre-conference tutorials will be offered on March 23, 1994, with the conference program beginning on Thursday, March 24, and running through Saturday, March 26, 1994.

The Palmer House, a Hilton hotel located at the corner of State Street and Washington Ave. in Chicago's "loop," and only about a block from The John Marshall Law School buildings, will be the conference headquarters. Room reservations should be made directly with the hotel, mentioning The John Marshall Law School or "CFP'94" to get the special conference rate of $99.00, plus tax.

The Palmer House Hilton
17 E. Monroe., Chicago, Il., 60603
Tel: 312-726-7500; 1-800-HILTONS; Fax 312-263-2556

Call for Papers and Program Suggestions

The emphasis at CFP'94 will be on examining the many potential uses of new technology and considering recommendations for dealing with them. Specific suggestions to harness the new technologies so society can enjoy the benefits while avoiding negative implications are solicited.

Proposals are requested from anyone working on a relevant paper, or who has an idea for a program presentation that will demonstrate new computer or communications technology and suggest what can be done with it. Any proposal must: state the title of the paper or program; describe the theme and content in a short paragraph; set out the credentials and experience of the author or suggested speakers; and should not exceed two pages. If an already completed paper is being proposed for presentation, then a copy should be included with the proposal.

Student Papers and Scholarships

It is anticipated that announcement of a student writing competition for CFP'94 will be made soon, together with information regarding the availability of a limited number of student scholarships for the conference.

Timetables

Proposals for papers and programs are being accepted at this time. It is intended that program committees will be finalized by August 1, 1993. Proposals must be received by October 1, 1993.

Communications

Conference communications should be sent to:

CFP'94
The John Marshall Law School
315 S. Plymouth Ct.
Chicago, IL 60604

(Voice: 312-987-1419; Fax: 312-427-8307; E-mail: CFP94@jmls.edu)

STSF WORKSHOP

Miquel Barcelo <blo@lsi.upc.es>
Thu, 15 Jul 1993 14:24:18 UTC+0100

CALL FOR PAPERS
SCIENCE AND TECHNOLOGY THROUGH SCIENCE FICTION
workshop next summer in Barcelona, Spain (22nd and 23rd, June 1994)

This will be the first edition of such a Workshop. If you know more people that could be interested, please help in making this information available by forwarding this message.

If you need more information, please feel free to contact
blo@lsi.upc.es, Dr. Miquel Barcels, Software Department - UPC
Pau Gargallo, 5, E 08028 BARCELONA (Spain)

- -

First Announcement and CALL FOR PAPERS
STSF '94

An International Workshop on
SCIENCE and TECHNOLOGY through SCIENCE FICTION
22nd-23rd June 1994 - BARCELONA (Spain)

Organized by CONSELL SOCIAL (Board of Trustees)
of Universitat Polithcnica de Catalunya (UPC)

in cooperation with:
Software Department (UPC)
Physics and Nuclear Engineering Department (UPC)
WORLD SF (Hispanic Chapter)

THE WORKSHOP

A good working definition of science fiction is "speculative extrapolation about the effect of science and technology on society". The aim of this International Workshop is to provide a forum for identifying, encouraging and discussing research about science and technology, or their consequences, as portrayed in science fiction. The Workshop will bring together researchers, scientists, and other academics with science fiction professionals to share information and explore new ideas about the relationship between science fiction, science and technology.

TOPICS OF INTEREST

The topics of interest include but are not limited to:

- Biotechnology, genetic engineering
- Computer science, robotics, artificial intelligence
- Macroengineering
- Nanotechnology
- Physics, astronomy, cosmology
- Professional activity of scientists and engineers
- Social impact of science and technology
- Teaching science and technology with science fiction

PROGRAM COMMITTEE

* Miquel Barcels (Software Dept., UPC, SPAIN)
* Joe Haldeman (SFWA president, M.I.T. Associate Professor, USA)
* Elizabeth A. Hull (SFRA past-president, USA)
* Frederik Pohl (SFWA and WSF past-president, USA)
* Vernor Vinge (Dept. of Math Sciences, SDSU, USA)

ORGANIZING COMMITTEE

* Miquel Barcels (Software Dept., UPC)
* Laura Cabarrocas (Board of Trustees (secr.), UPC)
* Gay Haldeman (Writing Program, M.I.T.,USA)
* Pedro Jorge (Hispanic Chapter of WORLD SF)
* Jordi Josi (Physics and Nuclear Engineering Dept., UPC)
* Louis Lemkow (Sociology Dept., UAB)
* Manel Moreno (Physics and Nuclear Engineering Dept., UPC)

INSTRUCTIONS TO AUTHORS

Paper submissions must be in English and no more than 6000 words long. The Proceedings of the Workshop will be published by the organizing institution. Authors are requested to submit a "Letter of Intention" with the title of the paper and a short abstract (less than one page) before November 30, 1993. Authors must submit five copies of each paper, before January 31, 1994, to the Program Chairperson: Miquel Barcels

Facultat d'Inform`tica
Universitat Polithcnica de Catalunya
Pau Gargallo, 5
E 08028 BARCELONA (Spain)
Tel: 34.3.401.6958
Fax: 34.3.401.7113
E-mail: blo@lsi.upc.es

IMPORTANT DATES

* Deadline for Letter of Intention: November 30, 1993
* Deadline for Paper Submission: January 31, 1994
* Notification of Acceptance: March 15, 1994
* Camera Ready Papers Due: April 30, 1994
* Workshop: June, 22-23, 1994

Search RISKS using swish-e ▭

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 77

Wednesday 21 July 1993

Contents

Another "time bomb" -- MOSS

Dave Horsfall <dave@eram.esi.com.au>
Wed, 21 Jul 93 21:39:48 EST

A colleague has just informed me that thousands of MOSS systems (a graphics package) all over the world crashed on 15 Jul, due to some authentication problem to do with the date. The "quick fix" was to set the date backwards, but this introduces its own problems; a lot of software rely on monotonically-increasing timestamps (were there any problems reported at the

Leap Second on 0000 UTC 1st July?), and some Apollo systems use the time value to generate "unique" (sic) file system descriptors...

Dave Horsfall (VK2KFU)   VK2KFU@VK2RWI.NSW.AUS.OC
dave@esi.COM.AU   ...munnari!esi.COM.AU!dave

Flood forecast risks

Douglas W. Jones <jones%pyrite@uunet.uu.net>
Wed, 21 Jul 1993 16:48:42 GMT

Living on the edge of the flooded Iowa River, I've been following the river reports from the Corps of Engineers quite regularly in recent weeks. They offer a recording you can call at their local office that gives the current river flow (in cubic feet per second), the current river stage in town, and the current statistics for the Coralville Reservoir ten miles upstream from my house.

This recording was well maintained until the reservoir went over the emergency flood spillway for the first time ever on the night of Monday, July 5, and then things began to break down. Normally, the recording is a deadpan recital of the numbers, but that night, the woman who recorded the message sounded like she was in a state of panic, and soon after that, they discontinued the recording for a week.

By midweek, even the data they were giving to the newspapers was sketchy, they were reporting the outflow of the reservoir and the current water level, but not the inflow. Furthermore, their predictions began to get very sketchy -- it turns out that lightning hit the gauging station upstream from the reservoir that they use to measure inflow, and without that data, they couldn't run their computer models to predict outflow. To quote one corps official I chatted with while he was looking at the floodwaters down the block from my house, they'd come to rely too much on their computer models and on their automatic data collection system.

Another problem they face is that they know the capacity of their reservoir up to the emergency flood spillway, but nobody every bothered to calculate the capacity of the reservoir when the water is 4 feet above the spillway; I gather that the working assumption has been that once water spilled over the spillway, it would stop rising. The spillway is 400 feet wide, so that seemed intuitive, but this is an awfully big flood!

Clearly, the hydraulic models of river systems that the corps uses to manage their flood control reservoirs need to be made more robust so that they can handle missing data, and the assumption that water will never rise significantly over dam spillways needs to be modified!

The Des Moines Register reported a similar but even more disastrous story about the floods in Des Moines in their Sunday July 18 chronology of the flood. On the weekend of July 11, the waterworks director phoned the US Weather Service for a flood forecast. They apparently gave him a forecast of a 22 foot crest on Tuesday, and when the director then told them that the river was already over 23, they were taken by surprise.

In that case, there was no provision made to compare the flood forecast coming out of the computer model with the current river data. This data comes in from stream gauging stations around the United States by satellite, and to make a flood forecast, they combine this data with rainfall data. If flood forecasts could be computed instantly, there would be no problem, but they aren't instantaneous and there was apparently no provision made for such a sanity check on the forecast!

Doug Jones jones@cs.uiowa.edu

Re: Earthquake `early' warning system (Owens, RISKS-14.76)

Richard Stead <stead@seismo.CSS.GOV>
Wed, 21 Jul 93 15:09:23 EDT

Early warning systems have been kicking around the seismological community for a decade at least. Most studies of proposed early warning systems have shown the economic return to be too small to justify development. California commissioned a such a study and chose not to pursue early warning on that basis. Of course, such analyses cannot include intangibles such as peace of mind or people temporarily in hazardous situations (eg: holding a pot of boiling water).

It is true that the system must be automated to achieve any warning. The system depends on detecting and identifying the quake in close proximity to the source. Then it relies on the speed of light exceeding that of elastic waves. The most damaging waves will arrive no earlier than an average velocity of 4.5 km/s. This would appear to give 45 seconds warning at 100 km. However, the system itself takes time. Without getting into the details, it is safe to say that time from the quake to the sensors and then processing and communicating the results might typically take 30 seconds.

This means that sites closest to the quake, those most adversely affected by it, gain no benefit, and sites far away (more than 200 km or so in California's case) do not benefit because the shaking is probably manageable. So there is a narrow range of distance that benefits. Even so, the system may be justified.

To answer the risks mentioned - Of course, it would be a rare system that could truly function without false alarms. One need only keep the false alarm rate to a manageable level, and make sure that any actions taken on the basis of the alarm not be hazardous. Slowing a train or halting elevators once or twice a year should not be a problem. In fact, I would think periodic tests of the system would be important as well. Predicting the damage should be straightforward. The magnitude of the quake can be estimated to sufficient accuracy - then a standard magnitude/ distance relation will return a rough expected intensity. It would not be hard to be more accurate - one need only measure the site response at the place where an action will be taken based on the warning, then program a site correction into the receiver. It is entirely up to the receiver to determine expected intensity and at which intensity to take which actions. This receiver can be as sophisticated as needed, but it will receive only magnitude, location and time. (Later, "verification" broadcasts could be made that rely on more data but take longer to produce. Any actions taken at the first notice could be modified then.)

I see two risks. The first is that most of the scientists involved seem to be trying to pull a "dual-use" out of this system. They want to deploy sophisticated sensors that are good for seismological research, and save and process mountains of data. I think that if the system is to work well, such efforts should be dropped. Early warning long ago ceased to be a seismic problem, it is an engineering and political problem. The sensors to be deployed should be a simple, reliable and inexpensive as possible, and should transmit a minimum of data to cut communications costs. By cutting physical and communications costs, the number of sensors can be increased and the cost of the entire program reduced. More sensors mean more warning time and more people benefit (up to the limit of the depth of the quakes).

The second risk is that people may rely on the existence of the system. I would hate to see someone designing something and say "well, if there was a quake, this would be a problem, but we have the early warning".

Security will be seen by many as a risk, but I think that is addressable by isolating the system from phone communications and networks and encrypting all communications.

Richard Stead stead@seismo.css.gov

Re: Strasbourg A320 crash: "Pilot Error" (Mellor, RISKS-14.74)

Lars-Henrik Eriksson <lhe@sics.se>
Wed, 21 Jul 93 07:32:29 +0200

Such a device (ground proximity warning system - GPWS) already exists and is mandatory on international flights. The Strasbourg A320 was only used domestically in France - where GPWS is (was?) not required. For some reason the airline decided not to install that equipment (or even had it disabled - I have some recollection that GPWS is standard equipment on the A320).

GPWS will alert the pilot to five different conditions (modes) that are considered unsafe at low altitude. Excess rate of descent is one of them.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263
S-164 28 KISTA, SWEDEN +46 8 752 15 09 lhe@sics.se

ATM Fraud/Databases/Ouch! (Smith, RISKS-14.76)

Scott Schwartz <schwartz@groucho.cse.psu.edu>
Tue, 20 Jul 1993 21:47:48 -0400

> Hope YOUR financial institutions protect your PINs as well...

Hah. My brother lost his wallet six months ago. Since then he's been dealing with massive credit fraud, and he's been told that his easiest recourse is to get a new social security number and a new set of accounts.

Credit Cards on the Internet

"Tansin A. Darcos & Company" <0005066432@mcimail.com>
Wed, 21 Jul 93 01:54 GMT

I sent the following to the Privatising the Internet List in
response to a question about credit card transactions via E-Mail:

>From: Paul Robinson <TDARCOS@MCIMAIL.COM>
Organization: Tansin A. Darcos & Company, Silver Spring, MD USA

Marianne Sweet <sweet@alexia.lis.uiuc.edu>, writes:

> On 17 June 1993 I posted a request for information to this list
> regarding credit card payment over the Internet. Since I received
> no responses, I am trying one more time with a slightly different
> request.
>
> Does anyone know of (commercial) services on the Internet that
> accept online credit card payment. I am currently working on a
> commercial application for the Internet and am interested in
> discovering what other services' charge displays look like.

The simple fact of the matter is that using Internet to handle
charge-card transactions is not very common for several reasons:

(1) Soliciting CC transactions might violate the Acceptable Use
   Provisions (doesn't apply if your feed is from a commercial
   internet connection.)

(2) Electronic mail is sent *in the clear* across the network. While
   it is part of a series of packets, it still can be seen by
   (a) the administrator of your site (b) the administrator of the
   destination site (c) anyone having access to the network connections
   used between the two sites who wants to monitor traffic.

In theory, some bright boy could put a "mail scanner" on the system and
watch for any messages that contain a string of 12 or 16 digits beginning
with 4 or 5 and capture those messages.

This means that someone watching for a message where the text
contains:

I'd like to order a 300 meg hard drive. Ship to
  Hathan Nale,
  1 Patriot Lane,
  Fourth July, MD 21776

Charge 4000 1776 1492 1993 exp 7/4/2076

Now someone supposedly could watch for this and keep such information.
Rare, but it could happen.

For those who are paranoid, the answer, of course, is to have privacy-enhanced mail made freely available. Once people have the ability to send mail to someone encoded with their private key and the recipient's public key, so that only the recipient can decode it, and so the sender can't deny it was sent, we will have problems.

There is probably close to 100 megabytes of transfers going across Internet every day; 40 meg of this is usenet news alone. While your little message might never be noticed, the chance is it could. Or you could mis mail it.

For example, say you intended to mail this order to "info-fax@sdi.com" (For, example, Soft-Disk Inc., a hard-disk seller) and instead, you miss and send it to "info-vax@sri.com" (it's only off by two characters), instead of sending the message with your credit card number to the one person at Soft-Disk Inc, you've just mailed it to the 75,000 readers of Info-Vax, which is gatewayed into "comp.os.vms".

PS: the above credit card number is fictitious.

Paul Robinson - TDARCOS@MCIMAIL.COM

Re: Medical Reimbursements ... (Frankston, RISKS-14.76)

<m.t.palmer@LaRC.NASA.GOV>
Wed Jul 21 09:01:51 1993

Bob_Frankston@frankston.com wrote:
>Simple ideas like replacing bills that contain a single amount ...

Actually, one of our local doctors has initiated a billing system very close to what you desire (after years of confusing us with what insurance payment went with what service, etc). The general form of the bill now looks like:

Date	Date/Code	Description	Amount	Amount	Balance
01/01/93	123456	Office Visit	35.00		
	01/01/93	Patient Copayment	10.00CR		
	02/24/93	Insurance Payment	17.50CR		
	02/24/93	Write-off	7.50CR		
	234567	Laboratory Work	25.00		
	02/24/93	Insurance Payment	18.00CR		
		Coinsurance Due		7.00	7.00
02/10/93	345678	Consultation	50.00		
	04/02/93	Insurance Payment	37.50CR		
	04/02/93	Write-off	4.00CR		
		Coinsurance Due		8.50	15.50

Several features of this format deserve special mention. First, note that events are only listed in chronological order within each "block," and that the specific office code for each billable service is given. In the above example, even though the consultation occurred before the insurance payments for the original office visit, those payments are listed with the service that generated them. Also, notice the existence of explicit write-offs. Our doctor is a "preferred provider" with a major health insurance company, and has agreed to accept the company's Usual, Customary, and Reasonable (UCR) amounts as payment in full. Even though the insurer doesn't alway *pay* the UCR amount, which means we still have copayments and coinsurance, there is still usually a difference between what the doctor "charges" and what he will accept as full payment. This billing format makes that distinction explicit for the first time.

How does this format reduce RISK? Simple. A recent bill (the first in this new format) seemed a tad high (like $200 or so too much), so we re-created our entire service history with that doctor in a spreadsheet and used this format. We quickly noticed where he had overlooked a previous account credit, and where he had forgotten to include a write-off for a specific service. It's probably easy to appreciate the level of frustration and helplessness we had previously felt with regard to keeping track of the myriad of bills, copayments, coinsurance, insurance payments, etc. for a couple of doctors and a dentist (we don't even have KIDS yet!). I will now keep track of all health service accounts using the new billing format, and will encourage our other doctors to do the same.

Michael T. Palmer m.t.palmer@larc.nasa.gov

DSS as Stamp Tax - Other historical precedents (Seecof, RISKS-14.76)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Wed, 21 Jul 93 07:57:59 -0400

>From: Mark Seecof <marks@wimsey.latimes.com>
>Subject: DSS as a stamp tax

Possibly a more exact parallel might be found in the "Teapot Dome" incident during the early 1900's in which Harry Sinclair and a group of oil magnates induced interior secretary Albert Bacon Fall to grant an exclusive license for federal oil reserves to their companies (remember Dino the Sinclair dinosaur ? Sinclair is now part of BP).

Mr. Fall was subsequently sentenced to prison for his part in the activities

Padgett

DSS as a stamp tax

<smb@research.att.com>
Wed, 21 Jul 93 12:00:12 EDT

There seems to be a lot of misunderstanding about what happened between NIST and PKP. NIST didn't ``give away'' anything to PKP. Rather, PKP had NIST over a legal barrel; some sort of deal was necessary. You can argue over the specific terms, but practically speaking, NIST had little choice.

The problem is this: the DSS appears to infringe several different patents owned by PKP. (I'm not going to discuss the propriety of algorithm patents here, a decision that I'm sure our esteemed moderator will applaud, given his comments about the load.) These include the Diffie-Hellman exponential key exchange patent and the Schnorr digital signature patent. It could be argued that for various reasons, these don't apply. Maybe -- but that's far obvious. At the very least, the standard would be tied up in court for many years.

NIST can't ignore such patents. Their own policy supports the propriety of such things (DSS itself is being patented.) And the government is not allowed to ignore private patent rights; that would, I'm told, constitute an illegal taking of property, as per the Fifth Amendment.

That left NIST with several choices, none great. They could do nothing, and not promulgate any standard. But that wouldn't meet the government's own need for one. They could adopt RSA, since the government has free rights to that patent. The rest of us would still have to pay royalties for its use. Besides, RSA can be used for secrecy, which NIST didn't want. (They cite exportability; others cite NSA's desire to spy. Pick your rationale.) Or they could ask NSA for a totally new signature scheme. Maybe NSA has one -- but I doubt very much they're going to reveal a totally new way to do cryptographic operations.

Finally, NIST could cut a deal with PKP. That's what they chose to do. It's not in any way a plot to enrich PKP; it's simply the only way to preserve the DSS.

--Steve Bellovin

Re: DSS as a stamp tax

Jim Bidzos <jim@RSA.COM>
Wed, 21 Jul 93 13:38:09 PDT

Mark Seecof should really should have read the DSS announcement more carefully before drawing any conclusions. The announcement said that DSS would be royalty-free for government use. Only private-sector use would require licensing. He compares it to a "tax."

He writes:

> forcing us to pay PKP everytime we sign something digitally ...

Very wrong. When someone in the private sector licenses DSS, they pay a royalty once for the manufacture and sale of the product, not its use. (It says you can license even the chips, the lowest cost component of a system.

There is quite a difference between a "use tax" and a "royalty.")

If he was referring to the $1 per certificate, that comes only from those who provide certificates as a service as a service, not from the user, and not for "use" of a signature product.

CPSR Secrecy Statement

Dave Banisar <banisar@washofc.cpsr.org>
Fri, 16 Jul 1993 8:27:56 EST

CPSR Secrecy Statement

Computer Professionals for Social Responsibility (CPSR) has called for a complete overhaul in the federal government's information classification system, including the removal of cryptography from the categories of information automatically deemed to be secret. In a letter to a special Presidential task force examining the classification system, CPSR said that the current system -- embodied in an Executive Order issued by President Reagan in 1982 -- "has limited informed public debate on technological issues and has restricted scientific innovation and technological development."

The CPSR statement, which was submitted in response to a task force request for public comments, strongly criticizes a provision in the Reagan secrecy directive that presumptively classifies any information that "concerns cryptology." CPSR notes that "while cryptography -- the science of making and breaking secret security codes -- was once the sole province of the military and the intelligence agencies, the technology today plays an essential role in assuring the security and privacy of a wide range of communications affecting finance, education, research and personal correspondence." With the end of the Cold War and the growth of widely available computer network services, the outdated view of cryptography reflected in the Reagan order must change, according to the statement.

CPSR's call for revision of the classification system is based upon the organization's experience in attempting to obtain government information relating to cryptography and computer security issues. CPSR is currently litigating Freedom of Information Act lawsuits against the National Security Agency (NSA) seeking the disclosure of technical data concerning the digital signature standard (DSS) and the administration's recent "Clipper Chip" proposal. NSA has relied on the Reagan Executive Order as authority for withholding the information from the public.

In its submission to the classification task force, CPSR also called for the following changes to the current secrecy directive:

* A return to the "balancing test," whereby the public interest in the disclosure of information is weighed against the claimed harm that might result from such disclosure;

* A prohibition against the reclassification of information that has been previously released;

- * The requirement that the economic cost of classifying scientific and technical be considered before such information may be classified;

- * The automatic declassification of information after 20 years, unless the head of the original classifying agency, in the exercise of his or her non-delegatable authority, determines in writing that the material requires continued classification for a specified period of time; and

- * The establishment of an independent oversight commission to monitor the operation of the security classification system.

The task force is scheduled to submit a draft revision of the Executive Order to President Clinton on November 30.

The full text of the CPSR statement can be obtained via ftp, wais and gopher from cpsr.org, under the filename cpsr\crypto\secrecy_statement.txt.

CPSR is a national organization of professionals in the computing field. Membership is open to the public. For more information on CPSR, or a full copy of the July 14 letter from Marc Rotenberg (CPSR Washington Director) and David L. Sobel (CPSR Legal Counsel) to the Information Security Oversight Office, contact <cpsr@cpsr.org>.

Announcements of NIST documents

Dolores Wallace <wallace@swe.ncsl.nist.gov>
Wed, 21 Jul 93 12:09:48 EDT

To order any of the following three documents, contact the Superintendent of Documents, U.S. Government Printing Office (GPO), Washington, DC 20402, (202) 783-3238.

* Wendy W. Peng and Dolores R. Wallace, Software Error Analysis, NIST Special Publication 500-209, GPO Stock Number SN003-003-03212-3. $7.00.

This document provides guidance on software error analysis. Software error analysis includes error detection, analysis, and resolution. Error detection techniques considered in the study are those used in software development, software quality assurance, and software verification, validation and testing activities. These techniques are those frequently cited in technical literature and software engineering standards or those representing new approaches to support error detection. The study includes statistical; process control techniques and relates them to their use as a software quality assurance technique for both product and process improvement. Finally, the report describes several software reliability models.

* Dolores R. Wallace, Laura M. Ippolito, D. Richard Kuhn, High Integrity Software Standards and Guidelines, NIST Special Publication 500-204, GPO Stock Number is SN003-03171-2. $6.50.

This report presents results of a study of standards, draft standards, and guidelines (all of which will hereafter be referred to as documents) that provide requirements for the assurance of software in safety systems in nuclear power plants. The study focused on identifying the attributes necessary in a standard for providing reasonable assurance for software in nuclear systems. The study addressed some issues involved in demonstrating conformance to a standard. The documents vary widely in their requirements and the precision with which the requirements are expressed. Recommendations are provided for guidance for the assurance of high integrity software. It is recommended that a nuclear industry standard be developed based on the documents reviewed in this study with additional attention to the concerns identified in this report.

* Dolores R. Wallace, Wendy W. Peng, Laura M. Ippolito, Software Quality Assurance: Documentation and Reviews, NISTIR 4909, FREE (as available). Contact Dolores Wallace at (301) 975-3340 or wallace@swe.ncsl.nist.gov, or Laura Ippolito at (301) 975-5248 or ippolito@swe.ncsl.nist.gov or either at [FAX] (301) 590-0932.

This study examines the contents of a software quality assurance standard for nuclear applications. The study includes recommendations for the documentation of software systems. Background information on the standard, documentation, and the review process is provided. The report includes an analysis of the applicability, content, and omissions of the standard and compares it with a general software quality assurance standard produced by the Institute for Electrical and Electronics Engineers. Information is provided for the content of the different types of documentation. This report describes information for use in safety evaluation reviews. Many recommendations in this report are applicable for software quality assurance in general.

- -

* Dan Craigen, Susan Gerhart, Ted Ralston, NIST Formal Methods Report

The National Institute of Standards and Technology has published a survey of twelve case studies of the use of formal methods in industrial projects. The report is published as NIST GCR 93/626 and is available in paper form from the National Technical Information Service. It is also available in electronic form; for electronic version, contact wallace@swe.ncsl.nist.gov .

The formal methods report contains the complete final version of "An International Survey of Industrial Applications of Formal Methods" sponsored by the U.S. National Institute of Standards and Technology, the U.S. Naval Research Laboratory, and the Canadian Atomic Energy Control Board. This report consists of two separate volumes. Volume 1 describes the purpose, approach, analysis, and conclusions of the survey; Volume 2 describes the case studies.

ORDER FROM: National Technical Information Service,
    5285 Port Royal Road, Springfield VA 22161   Phone(703) 487-4650

YOU MUST Use the PB numbers to order:

"An International Survey of Industrial Applications of Formal
Methods Volume 1 Purpose, Approach, Analysis and Conclusions"
NIST GCR 93/626-V1   PB93-178556/AS
Hard Copy: A07/$27.00 Microfiche: A02 $12.50

"An International Survey of Industrial Applications of Formal
Methods Volume 2 Case Studies"

NIST GCR 93-626-V2   PB93-178564/AS
Hard Copy: A09/$27.00 Microfiche: A03/$12.50

For electronic version, contact wallace@swe.ncsl.nist.gov

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 78

Tuesday 27 July 1993

Contents

Computer-aided tax fraud

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
27 Jul 93 11:16:20 EDT

By Denise Lavoie, Associated Press Writer (from the AP)

> Norwalk, Conn. (AP) -- A day after its owner admitted cheating the
> government out of $6.7 million in taxes, Stew Leonard's dairy and produce
> store was accused Friday of mislabeling weights on hundreds of items.

It seems that almost half of 2,658 tested products were short-weighted or had no weight listed on the label. As for the tax fraud, the criminals apparently removed records of $17.1 million in sales figures "in a computer-aided tax fraud scheme." The data diddling meant they failed to pay $6.7 million in taxes. The penalty is that they must pay $15 million in back taxes and fines.

Would someone from that area of the country please post additional details on how the computer scam operated?

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Industrial Espionage

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
27 Jul 93 11:16:36 EDT

Lopez Said To Order GM Papers; Volkswagen Denies Receiving Documents
Washington Post, 23 July 1993
By Frank Swoboda and Rick Atkinson, Washington Post Staff Writers

> Secret General Motors documents seized recently at a Wiesbaden apartment
> by German investigators were prepared at the request of former GM executive
> Jose Ignacio Lopez de Arriortua before he joined rival Volkswagen, German
> prosecutors said yesterday.

The article goes on to explain that the documents included information about Opel (General Motors in Europe) new Vectra car and about a top-secret "O" car. Both Lopez and VW deny any impropriety and denounced the prosecutor's public announcement. An intensive search of VW's computer systems is apparently going on to see if GM proprietary data have been stored there.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Stingers

<Bob_Frankston@frankston.com>
Tue, 27 Jul 1993 11:53 -0400

There was a recent article about the US trying to buy back Stinger antiaircraft missiles before they got sold to others.

This sounds like another version of the stories about government installations being rather lax about complying with pollution control requirements. Similarly, security considerations should include a time limit on small powerful weapons. I presume that worry about the future is not a checklist item. Does anyone on this list know more about the issues involved?

Chinese Airline Crashed a British Aerospace-made 146 "Whisperjet"

Li Gong <gong@csl.sri.com>
Mon, 26 Jul 93 11:32:31 -0700

BEIJING (UPI, July 23, 1993) -- [PGN Excerpting Service]

A Chinese Northwest Airlines flight carrying 113 people bounced off the runway and plunged into a lake in Yinchuan, the capital of Ningxia province, in a remote part of west China, on 23 Jul 1993, killing 59 people. The airliner attempted two takeoffs. The first was aborted. On the second, it ran off the runway, dropped into a lake, and broke apart. Flight 2119, a British Aerospace 146, was on a scheduled flight to Beijing. Ian Watson, director of regional operations for British Aerospace, said that "In the 10 years since it came into service, the BA-146 has compiled one of the finest safety records in the world."

The last major airline disaster in China occurred in November when a China Southern Airlines Boeing 737 crashed into a mountain in the south China tourist city of Guilin, killing all 141 aboard. China has halted the establishment of new airline companies to improve air safety and tighten control over expansion in civil aviation. About 35 airline companies have sprouted up in China since CAAC relinquished control over the industry in 1988, faster growth than in any other country.

China has only 109 airports, a fraction of those in developed countries, but passenger volume rose more than 24 percent in the first half of this year over last year.

Biz Card Machine -- New Risk!

Dan Hartung <dhartung@chinet.com>
Mon, 26 Jul 93 12:55 CDT

An unusual (and probably unexpected) risk has appeared -- business card vending machines. I saw my first one at a service plaza on the Indiana Toll Road (I-80/90). Basically, it's a simplified desktop publisher that will print out a variety of business card formats; you just enter your information. The prices were, of course, outrageous -- whereas I paid something less than 2 cents/card last time I had some printed professionally, this was at least 10 times that, even in quantity. Well, I suppose that a traveling salesman in an emergency ....

Anyway, the risk comes in here: the instructions suggest that you first purchase a small number of cards to be sure they print correctly; you can later put in more money and print out a larger quantity if you like what you see. Then this: "The machine stores your information for several minutes."

So, presumably, one could walk away from one of these machines with your cards reading "John Smith, Computer Consultant, 10 Takeita Way, Suckerstown, MD" and return from your business trip to find your house burgled of everything resembling a computer ... simply because someone went up to the machine after you left and printed out a set of their own. Or a woman could give away, unwittingly, her otherwise unlisted home phone number to a deep breather. And so on.

Again, as with so many of the risks discussed here, there is a debatable amount of privacy invasion on what is basically public information ... but information that is given to people you would otherwise NOT want to have it.

Postscript: another risk was illustrated here -- a sample "business card" inscribed with a semiliterate harangue along the lines of "You shouldn't park here, your license plate has been recorded by an anal-retentive mentally unstable person, and if you park here again a pickup truck with no insurance will wipe it back and forth along that nearby concrete wall." More or less identical in demeanor to the mail one gets for mis-posting. Three times as long, of course, and partly CAPITALIZED in TIME-HONORED Usenet NEWBIE style. Yet I believe that such a card, slipped under someone's wiper, would constitute legal assault. (IANAL.) And these people are *advocating* this? Yikes.

Re: Earthquake "early warning" systems

Lauren Weinstein <lauren@cv.vortex.com>
Wed, 21 Jul 93 21:17 PDT

Living here in the L.A. area, where earthquakes are certainly more than an academic concern, I can't help but question the usefulness of a warning system that gives, perhaps, 15 to 30 seconds of panic time. And I do mean panic time--because that's what most people would do. Primarily, most folks would probably try to rush out of buildings (just like they do when quakes start, even though they should know better). Lots of them will get out the door just in time to get hit by falling debris when the quake hits, which they could have avoided if they had just stayed inside.

That's all assuming that the quake *does* hit. If the alarm is false, you can bet that the *next* time the alarm fires it will be generally ignored--for better or worse.

One can certainly argue that the solution is education and training and such--but human nature being what it is, you can bet that if people believe the alarm, most of them are going to do pretty much the wrong thing in response, especially when the duration in which to act is very short. The real effort should go into upgrading of older buildings that predate modern earthquake area construction standards-- it's with those buildings that most injuries and deaths are likely to occur.

I'm reminded of an old "Saturday Night Live" skit. It was a fake commercial for a device passengers could carry on planes that would give them 10 seconds warning (or some such) of midair collisions. The guy is sitting calmly in his seat when the box starts beeping. He grabs it and stares at its display. He yells:

"We're going to be hit by a 747! (SCREAM!)"

--Lauren--

Re: Earthquake `early' warning system (Stead, RISKS-14.77)

Brian Herzog - SunSoft Product Engineering <herzog@dobbs.eng.sun.com>
Sun, 25 Jul 1993 13:45:40 +0800

>The most damaging waves will arrive no earlier than an average
>velocity of 4.5 km/s. This would appear to give 45 seconds warning at 100 km.

Er, my calculator says this would give 22 seconds warning at 100 km, which makes the economic feasibility of an early warning system even worse than stated. I do hope the quote above is a typical email typo, and not an accurate extraction from the California study!

Brian Herzog <herzog@eng.sun.com>

Re: Credit Cards on the Internet

Blake Sobiloff <sobiloff@lap.umd.edu>
Thu, 22 Jul 1993 13:47:26 -0500

(I hope this doesn't sound too much like an advertisement...) Reiter's Scientific & Professional Books, a great bookstore in Washington, D.C., is now on the Internet and is accepting credit card orders over the Internet for book orders. Orders and inquiries can be sent to "books@reiters.com" while comments can be sent to "rbaker@reiters.com".

I enquired about exactly how they wanted me to give them my credit card number, and they replied that they actually prefer to set up an account over the phone with the pertinent information, and then give you an account number. You then transmit the account number to them via email to place an order. They did not, however, reject the possibility of conducting business via email without voice verification.

My suggestion to look into public key encryption went unanswered...

Blake Sobiloff, Laboratory for Automation Psychology, Department of Psychology
University of Maryland, College Park, MD 20742-4411 <sobiloff@lap.umd.edu>

Credit Cards on the Internet

<nandu@cs.clemson.edu>
Thu, 22 Jul 93 12:56:26 EDT

This is further to the ongoing discussion on using credit cards over the

internet. To ensure security and escape the (possibly) prying eyes of
administrators at the sites through which a mail (ordering a product to
be paid through a credit card) passes, the sender could encrypt his/her
request. The key used for encryption could be a special INTERNET PIN that
the credit card company assigns while issuing the card, just like the one
assigned for ATM transactions through the card.

at the receiving end, the dealer simply forwards the mail to the credit
card company and waits for authorization from them. the dealer does not
know the card number since the mail is encrypted.

the credit card company could decrypt the mail, since they know the sender's
name and maybe the ZIP code (of course when the mail is encrypted, this
information should not be) and hence can find out the card number and the
special INTERNET PIN. once they decrypt the mail, they can verify if the
original sender listed the correct card number in his/her mail. once verified,
they can authorize the dealer to accept the request depending on the cost of
the product and the balance on the customer's account.

Nandakumar Sankaran, G34, Jordan Hall, Clemson University, Clemson, SC 29634
(803) 656 6979 nandu@cs.clemson.edu

Re: Credit Cards on the Internet (Robinson, RISKS-14.77)

Matt Crawford <matt@severian.chi.il.us>
Thu, 22 Jul 93 20:17:46 CDT

> (1) Soliciting CC transactions might violate the Acceptable Use
>   Provisions (doesn't apply if your feed is from a commercial
>   internet connection.)

I believe the parenthetical remark is quite incorrect. Traffic on sponsored
networks must conform to the AUPs, even if it originates on a commercial net.
I know I received a couple of solicitations out of the blue from people who
didn't understand this, and who now know better.

Matt Crawford

Seecof's reading ability

Mark Seecof <marks@wimsey.latimes.com>
Wed, 21 Jul 93 16:26:48 -0700

Despite Bidzos' attempt to bolster his DSS royalty defense by attacking my
literacy (he's wrong, BTW) and by weaseling that a "royalty" is not a "tax" (I
only said an unavoidable royalty "amounted to" a tax) I think he fails to show
that my comparison of NIST/PKP's proposal to a tax is invalid. Bidzos could
have argued that it was overdrawn, less apt than another analogy, or even
wrong on some concrete grounds. But his complaints are weak if strident. And
talk about charging for DSS implementations rather than uses (at least for the
nonce) draws a distinction without a difference. The U.S. taxes bottles of

liquor, not individual drinks poured at home, but economists will agree that you pay every time you swallow. Whether a tax is mills per ton or dollars per ounce is not the point, anyway. As for that $1 per certificate... Bidzos says users won't pay it--I think he's wrong. Users pay for everything in the end.

Also, the stuff about "free for government use" is smokescreen. It's private use that matters, including, especially, private use to communicate with the government. I cannot find, even by the closest scrutiny of the NIST/PKP announcement, any promise to relieve users of royalties on products they use to communicate with the government. (Possible loophole: gov't could supply DSS implementations to users royalty free; but that would depart from custom.)

Mark Seecof

Dependability conference; call for participants

<Jeremy.Jacob@prg.ox.ac.uk>
Tue, 27 Jul 93 08:59:08 BST

Institute of Mathematics and Its Applications
Conference on THE MATHEMATICS OF DEPENDABLE SYSTEMS
1--3 September 1993
Royal Hollway, University of London, Egham, Surrey, England

Invited speakers:
Prof. David Parnas (McMaster University)
Dr. Charles Pfleeger (Trusted Information Systems (UK))
Dr. John Rushby (SRI International)
Mr. Martyn Thomas (PRAXIS)

Conference fees (pounds sterling), includes lectures, abstracts, coffee, lunch and tea:

IMA members	#185.00
Non-members	#245.00
IMA student members	#145.00
Student non-members	#185.00

Residential fees (pounds sterling), includes bed, breakfast and dinner for 3 nights:
#110, #130 or #150 depending on accommodation booked.

Further details are available from:
Mrs Pamela Irving, Conference Officer
The IMA, 16 Nelson Street, SOUTHEND-ON-SEA
Essex SS1 1EF England
Telephone: +44 702 354020 Facsimile: +44 702 354111

High-assurance software courses

Nancy Leveson <leveson@cs.washington.edu>

Mon, 26 Jul 93 08:13:27 -0700

Announcing two courses in high assurance Software:

An Introduction to Software System Safety, Oct. 25-27
Nancy Leveson

A Tutorial on Software Testing, Oct. 28-29
Debra Richardson

Location: University of California, Irvine, CA

AN INTRODUCTION TO SOFTWARE SYSTEM SAFETY, Oct. 25-27

In order to ensure and certify that software will execute without resulting in unacceptable risk, changes to normal software development practices are necessary. This tutorial will focus on the unique problems involved in building safety-critical software and describe some techniques that can be used to enhance the safety of software-controlled systems. Emphasis will be on procedures and techniques that are practical enough to be applied to projects today. Real-project experiences with these techniques in different application areas will be described.

Topics:

Basic Principles of Risk
- Basic concepts in risk
- Why technological fixes may not reduce risk
- Using past experience to prevent future accidents
- How safe is safe enough?
- Do computers reduce or increase risk?

System Safety Engineering and other Approaches to Engineering Safety
- What is system safety
- The system safety process and tasks
- Software system safety
- Application-specific approaches
- Standards

Management Issues for Safety-Critical Projects
- Instituting a safety culture into the organization
- How management contributes to accidents
- Role of safety management (including software)
- Place in the organizational structure
- General process (for small and large organizations)
- Documentation
- Cost and resource requirements

Models of Accidents and Hazard Analysis
- General types of analysis techniques
- Limitations and sources of uncertainty
- Software Hazard Analysis
- Software Requirements Analysis
- Qualitative vs. quantitative analysis

Principles of Safe Design
- The design process
- Issues in safe design

  The relationship between software design and safe system design
  System safety design techniques and their application to software design
  Software safety design analysis
Verification and Validation of Safety
  Testing for safety
  Static software analysis including Software Fault Tree Analysis
Design of Human/Machine Interaction for Safety
  The role of humans in accidents
  The role of the HMI in accidents
  The need for and role of human operators in automated systems
  Human error models
  General design principles and approaches
  Software design issues

A TUTORIAL ON SOFTWARE TESTING, Oct. 28-29

The intent of this tutorial is to equip managers, software engineers, and test engineers with an understanding of testing technology to enable them to promote software testing in their organizations from an ad hoc, labor intensive, error-prone activity to a disciplined, technology-supported process. Emphasis is on techniques that are practical today. Some underlying testing theory will be presented to provide a foundation for evaluating testing technology, and several new approaches will be discussed. Issues of selecting complementary techniques and integrating them to achieve a comprehensive testing process are also addressed.

Topics:
 Software Testing Principles
  Definitions and basic principles
  Testing concepts
  Psychological factors
  Economic impacts
 Managerial Considerations
  Views of software testing
  Contributions to quality
  Testing phases and activities
 Test Planning
  Goals and objectives
  Developing a test strategy
  Test specifications and procedures
  Evaluating and reporting results
  Test process improvement
 Proactive Software Testing
  Technical Reviews
  Rapid Prototyping
 Software Testing Techniques
  Functional testing
  Structural testing
  Error-Oriented testing
  Integration testing
  Software system testing
  Evolution testing
  Developing test oracles

Tools and Environments
  Static/dynamic analysis tools
  Test generation tools
  Test Management tools
Methodology and Process
  Hybrid testing techniques
  Technique integration
  Formalized process
Test Set Adequacy and Metrics
  A theoretical view
  Software metrics in testing
Process Assessment/Improvement
  Process performance measures
  Test process assessment
  Improving the testing process

[For bios of Leveson and Richardson, and registration information,
send E-Mail to leveson@cs.washington.edu (Nancy Leveson).]

CSR Workshop 1993

Pete Mellor <pm@csr.city.ac.uk>
Sat, 24 Jul 93 17:02:26 BST

CSR (Centre for Software Reliability)
TENTH ANNUAL WORKSHOP
CO-HOSTED WITH JUSE
Japanese Union of Scientists and Engineers

APPLICATION OF SOFTWARE METRICS AND
QUALITY ASSURANCE IN INDUSTRY

PROVISIONAL PROGRAMME

Supported by the CEC under the Human Capital and Mobility Programme
The Grand Hotel, Oudezijds Voorburgwal 197, 1001 EX Amsterdam, The Netherlands
29th September - 1st October, 1993

CENTRE FOR SOFTWARE RELIABILITY

Tenth Annual Workshop

Application of Software Metrics and Quality Assurance in Industry

WEDNESDAY 29TH SEPTEMBER

08.30-0930   REGISTRATION AND REFRESHMENTS

Chair: Norman Fenton, City University, UK

09.30-10.30 Keynote Address: "Applying the Goal/Question/Metric
Paradigm in the Experience Factory"

```
   Vic Basili, University of Maryland, USA

11.00-13.00 Tutorial:  "Management Aspects of Software Reuse"
   Sadahiro Isoda, Nippon Telegraph and Telephone Corp., Japan

13.00-14.15 LUNCH

Chair:  Bev Littlewood, City University, UK

14.15-15.15 Keynote Address:  "Now it's the turning point
                          for the Japanese Software Industry"
   Yoshinori Iizuka, The University of Tokyo, Japan

15.45-17.45 Tutorial: "Setting up a Software Metrics Programme in Industry"
   Shari Lawrence-Pfleeger, Systems/Software, USA
   and City University, UK

THURSDAY 30TH SEPTEMBER

Chair:  Robin Whitty, South Bank University, UK

09.00-09.30 "The Role of Quality Staff in Software Development"
       Masanobu Hattori, Fujitsu Ltd, Japan

09.30-10.00 "Making Software Metrics and QA happen:  practical
          experiences in Italy"
   Gualtiera Bazzano, ETNOTEAM, Italy

10.00-10.30 "Product Development and Quality Assurance
          in the Software Factory"
   Katsuyuki Yasuda, Hitachi Ltd., Japan

11.00-11.30 "Industrial Experience - Working with AMI"
   Richard Espley, GEC-Marconi Avionics Ltd., UK

11.30-12.00 "Software Measurements - an Evolutionary Approach"
   Norbert Fuchs, Alcatel, Austria

12.00-12.30 Title to be announced
   Karl-Heinrich Mueller, Siemens, Germany

12.30-14.00 LUNCH

Chair:  Yoshinori Iizuka, University of Tokyo, Japan

14.00-14.30 "Using Function Points for Software Cost
             Estimation - Some Empirical Results"
   Barbara Kitchenham, NCC, UK

14.30-15.00 "Evaluating Effort Prediction Systems"
   Claude Stricker, University of Lausanne, Switzerland

15.00-15.30 "Use of Function Points for Estimation and Contracts"
   Jolyn Onvlee, Onvlee Opleidingen, The Netherlands
```

16.00-16.30 "Quality Practice in the Industry"
Roberto Ciampoli, O. Group SpA, Italy

16.30-17.00 "Beyond SEI's CMM - the BOOTSTRAP Approach for
Profiling and Measuring Software Engineering Processes"
Gunter Koch, 2i Industrial Informatics
GmbH, Germany

17.00 PANEL DISCUSSION: "Do Quality Assurance Procedures
Lead to Measurable Quality Improvements?"

Tom Anderson, Bev Littlewood (CSR, UK) Vic Basili (Maryland, USA) Bill Hetzel (SQE, USA) Sinclair Stockman (British Telecom, UK) Yoshinori Iizuka (University of Tokyo, Japan) Toshiro Ohno (Toshiba, Japan) Mitsuru.Ohba (IBM, Japan), Ayatomo Kanno (Science University, Tokyo, Japan)

19.30 WORKSHOP BANQUET

FRIDAY 1ST OCTOBER

PARALLEL SESSIONS

Chairs:		
	Norman Fenton, City University, UK	Tom Anderson, Univ. of Newcastle upon Tyne, UK

09.30-10.00

"Complexity Traces: an Instrument for Software Project Management" Christof Ebert, University of Stuttgart, Germany	"Introducing Metrics into Industry:a Perspective on GQM" Richard Bache, Infometrix, UK, & Martin Neal, Lloyd's Register, UK

10.00-10.30

"Measurement through the Software Life-cycle: a Comparative Case Study" Bob Cole and Derek Woods, Glasgow Caledonian University	"Practical Implementation of Process Improvement Initiatives" Paul Goodman, Brameur, UK

10.30-11.00

"Integrating Software Quality Assurance into the Teaching of Programming" Edmund Burke, University of Nottingham, UK	"A Case History of Automated Incremental Improvement of Software Product Quality" Les Hatton, Programming Research Ltd., UK

11.30-12.00

"QUANTUM - A Measurement-based Framework for Software Quality Assurance"	"Experience of Introducing Quality and Measurement in Telecommunication Software Development"

Chris Miller, Praxis, UK   Sinclair Stockman,
British Telecom, UK

12.00-12.30

Title to be announced   Title to be announced
Francois de Nazelle,   Yannis Kliafis, Greece
Q-Sys, France

12.30-13.45 LUNCH

Chair: Barbara Kitchenham, NCC, UK

13.45-14.45 "Measuring the Measurements: the Technology for
Measuring Software Practice"
Bill Hetzel, Software Quality Engineering, USA

14.45-15.15 "A Framework for System Development Activities and
Responsibilities - Quality Improvement by filling up the
Communication Gap"
Minoru Itakura, Fujitsu Ltd., Japan

15.45-16.15 "Situational Measurement"
Hans van Vliet, Vrije Universiteit, The Netherlands

16.15-16.45 "The Behavioural Analysis makes the Company Mature"
Ryuzo Kaneko, NEC Corp., Japan

16.45-17.15 "Function Points" (exact title to be announced)
Martin Hooft van Huysduynen, Ing Bank,
The Netherlands

[The full registration materials were too long for RISKS, and have been pared down. Request on-line registration information and other information by E-Mail from c.allen@csr.city.ac.uk , or contact Ms. Carol Allen, Centre Manager, Centre for Software Reliability, The City University, Northampton Square, London EC1V OHB UK, Tel: +44 71 477 8421, Fax: +44 71 477 8585]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 79

Tuesday 10 August 1993

Contents

Industrial espionage

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
27 Jul 93 17:54:16 EDT

Car wars: VW strikes back

BONN (UPI, 27 Aug 1993) -- Volkswagen Tuesday fired back at General Motors, challenging its claims of industrial espionage and suggesting that evidence found by investigators may have been tampered with. [...] "This is

> a battle between two major auto firms against the background of a trade war.
> We did not start start it but we will fight back," Piech said.

The language being used fits right in with the warnings of such experts as Winn Schwartau that information will be the battleground of the new millenium. Interpersonal, intercompany, and international hostilities are already including components of information warfare.

In addition to the risks from accident, we must increase our countermeasures to reduce the risks from deliberate sabotage and data leakage.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Criminal record data leakage and tampering

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
29 Jul 93 16:07:36 EDT

Criminal Records, By LAWRENCE L. KNUTSON, Associated Press Writer

> WASHINGTON (AP, 29 July 1993) -- Data in the computer files of the FBI's National Crime Information Center is increasingly being misused by law enforcement insiders, often for personal gain, congressional auditors say.

Criminal records are being sold to private detectives, lawyers and politicians in defiance of right-of-privacy laws.

The article mentions the following specific cases:

--In Arizona, an angry ex-policeman used FBI databanks to track down and murder a woman. [actually, his "estranged girlfriend" --- PGN]

--In Pennsylvania, the friend of a drug-dealer used police computers to verify the background of potential new clients (tracking down police undercover agents).

The III file includes 17 million records about criminal histories and is available to 19,000 law enforcement agencies [AGENCIES, not agents!] with over 97,000 terminals able to tap into the system directly.

All the reported abuse was by inside workers, not criminal hackers.

The GAO recommended that strong criminal sanctions be instituted to punish misuse of criminal records files.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Billion-dollar tax bills

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>

29 Jul 93 16:08:18 EDT

07/28 1143 IRS sends Midwesterners multibillion-dollar tax bills

  MINNEAPOLIS (UPI, 28 July, 1993) -- The Internal Revenue Service has some explaining to do.

  An IRS computer developed a glitch and sent out tax bills for as much as $68 billion to about 1,000 people in Minnesota, Wisconsin, Illinois, Missouri and Iowa.

The IRS was trying to remove the names of Midwest flood victims from its tax rolls. In an unexpected side-effect, other people got enormous random tax bills.

I wonder if we could convince the IRS of the value of quality assurance methodologies if they issued billion-dollar _refunds_ instead of bills?

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

---

More data remanence

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
02 Aug 93 06:11:16 EDT

Canadian Press report on page 1 of _Globe and Mail_ on Monday, 2 Aug 93:

Summary follows:

    DISK SLIPPED INTO WRONG HANDS.

    A used hard disk sold to an Edmonton man contained two years of detailed and confidential personnel files about 166 employees of the Alberta land-titles employees.

    An investigation is to be ordered by the Deputy Justice Minister.

Another example of failing to consider information as an asset requiring protection....

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

---

Pizza RISK

Dale Drew <ddrew@Tymnet.COM>
Tue, 3 Aug 93 12:24:57 PDT

The RISKs of propagating databases used by companies has been covered many, many times. It is a fairly well known fact that companies are massing great amounts of information on individuals for marketing purposes.

For the past several years, I have been identifying the numerous companies
that create, pass, trade, sell, distribute, and correlate my information.
During this process I identified several possible RISKs. One of which I
thought I'd pass along:

I discovered that an individual was attempting to gain access to my personal
information by calling Pizza Hut and attempting to order a pizza under my
name. Pizza Hut just happens to maintain a database of all its customers to
make deliveries easier. The culprit identified himself as me and ordered a
small pizza, and then attempted to verify my mailing address.

Fortunately, I had taken advanced precautions and the information was not
accessible. However, it raises the question of identification and
authorization when it comes to releasing confidential and/or sensitive
information. This process does not exist in the industry, and opens a wide
area of exposure for individuals wishing to gain information for whatever use.

It also raises the question of liability. Most companies make no attempt to
inform the "end user" that they are collecting "such-and-such" information and
intend on using it in "such-and-such" manner, it is up to the individual to
go on a mass writing campaign to identify where, exactly his/her information
is, and what it's being used for.

If the information had been released, and was used against me in some manner,
would Pizza Hut be liable for that release? Probably not. What motivation do
they have in performing identification and authorization checks? Probably
nothing.

[I wonder if Pizza Hut would deliver to a PO box?]

Dale Drew, BT North America, Inc., Global Network Security
Business Information Security (408) 922-6004 ddrew@druid.Tymnet.COM

Yet another lottery screwup

Reva Freedman <freedman@delta.eecs.nwu.edu>
Fri, 6 Aug 93 14:46:24 CDT

Even if you're opposed to state lotteries, if we're going to have them, don't
you wish they'd design the hardware and software better? Here follows a
summary of an incident in Illinois based on a Chicago Tribune article by Peter
Kendall (8/4/93, sec. 2, p.3).

> The only sure winners of last weekend's $11 million lottery drawing are the
> lawyers. The other winners are likely to be determined in court. The story
> started last week when office worker Carol Stonecipher attempted to buy a
> lottery ticket from the mini-mart at a Pride Petroleum gas station. She
> marked off six numbers on a card and handed it to the clerk, who was
> supposed to stick it into the lottery terminal.
>
> But the terminal was temporarily inactive, so the clerk, John Warford, kept
> re-inserting the card to print Ms. Stonecipher's ticket. When the terminal

became active again a few seconds later, it printed out six tickets, one for each stored request.

According to state lottery regulations, the store is required to pay for tickets printed by mistake unless someone else pays for them. The clerk gave Stonecipher the opportunity to buy the extra tickets, but she declined. None of this would have been of any importance except that Stonecipher holds the only winning number for last weekend's drawing.

Stonecipher says that the clerk told her that he was going to invalidate the extra tickets. Both the mini-mart owners and the clerk are claiming that they are the true owners of the extra tickets.

Gives new meaning to the term "printing money," huh?

Reva Freedman <freedman@eecs.nwu.edu>
Dept. of EECS, Northwestern University, Evanston, IL

"Terminal Compromise" on the Net

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Thu, 22 Jul 93 10:06:17 -0400

Though commercial in nature, I find this an important announcement since the novel is an excellent read about potential RISKS of widespread computer use and possible terrorism attacks AND since it is available electronically (ARCHIE found the 617K/560 page novel at knot.queensu.ca as /wuarchive/doc/misc/termcomp.zip. More sites are probably available by now). Note that the novel also predates (1991) "Rising Sun".

Padgett

!!!!POST EVERYWHERE!!!!
THE WORLD'S FIRST NOVEL-ON-THE-NET (tm) SHAREWARE!!!
By Inter.Pact Press
"TERMINAL COMPROMISE"
by Winn Schwartau

A high tech thriller that comes from today's headlines!

"The Tom Clancy of computer security."
Assoc. Prof. Dr. Karen Forcht, James Madison University

"Terminal Compromise" is a highly praised novel about the invasion of the United States by computer terrorists.

Since it was first published in conventional print form, (ISBN: 0-962-87000-5) it has sold extremely well world-wide, but then again, it never hit the New York Times Bestseller List either. But that's OK, not many do.

Recently, someone we know very well came up with a real bright idea. They suggested that INTER.PACT Press take the unprecedented, and maybe slightly crazy, step to put "Terminal Compromise" on the Global Network thus creating a new category for book publishers. The idea is to offer "Terminal Compromise," and perhaps other titles at NOVEL-ON-THE-NET SHAREWARE(tm) rates to millions of people who just don't spend a lot of time in bookstores. After discussions with dozens of people - maybe even - more than a hundred - we decided to do just that. We know that we're taking a chance, but we've been convinced by hackers and phreakers and corporate types and government representatives that putting "Terminal Compromise" on the net would be a fabulous step forward into the Electronic Age, (Cyberspace if you will) and would encourage other publishers to take advantage of electronic distribution. (It's still in the bookstores, though.)

NOVEL-ON-THE-NET SHAREWARE Fees For The People:

The suggested donation for individuals is $7. If you hate Terminal Compromise after reading it, then only send $6.50. If you're really, really broke, then tell a hundred other people how great it was, send us a rave review and post it where you think others will enjoy reading it, too. If you're only a little broke, send a few dollars. After all, this is how we stay in business. With each registration, we will also send a FREE! issue of "Security Insider Report," a monthly security newsletter also published by Inter.Pact Press.

Please forward all NOVEL-ON-THE-NET SHAREWARE fees to:

INTER.PACT PRESS
11511 Pine St. N.
Seminole, FL., 34642

Communications:

Phn: 813-393-6600
Fax: 813-393-6361
E-Mail: p00506@psi.com
wschwartau@mcimail.com

[Archie only reported TERMCOMP.ZIP at knot.queens.ca but the opening screen there recommends that outsiders use wuarchive.wustl.edu. I can verify that right now it is there as /doc/misc/termcomp.zip . Padgett]

ATM MODEM INSECURE?

"MARCHANT-SHAPIRO, ANDREW" <MARCHANA@gar.union.edu>
22 Jul 93 13:40:00 EST

Hey, how hard can it be to break into an ATM? It's easier than you think...

Today, needing a little cash, I wandered over to the College Center (nope, they don't call it a UNION here) to use the ATM. To my surprise, there was a little box sitting on top of the ATM with a lot of blinking lights -- a modem. A General Datacom NMS 2400, to be specific. It had a standard DB-25 on the back and was plugged into the ATM's serial port.

I should note that I've been out of town for a couple of months, and, when I left, there was no modem sitting on top of the box like that. So this MAY be temporary (let's hope). Anyway.

I do not believe that this modem is a secure device... It had no obvious security system, and there was no one around watching. Had I needed a 2400 baud modem, I could have picked it up and walked away with it (it wasn't screwed down). Far more interesting, however, would be the possibility of opening the box while it was running, attaching a wire or two, and getting a nice record of the codes sent from and received by the ATM. I didn't do it, of course.

I suppose there must be some kind of internal security in the ATM so that it will only dispense cash when it has a card in place (I don't know much about how they work), but it scares me to realize just how unsecure the link really is. For a few dollars, I could have had a printout (or a file) of the data stream between the ATM and its masters. Even if the stream were encoded, it would be a simple matter to watch what was being done by ATM customers and match it to the codes.

I had been getting complacent about RISKs lately -- "oh, yeah, another scare story about (phones, ATMs, aircraft, you name it)." Maybe it shouldn't, but this shook me out of that. Again an avid reader...

Andrew Marchant-Shapiro   Depts of Sociology and Political Science
USmail: Union College, Schenectady NY 12308   AT&T: (518) 388-6225*
INTERNET: marchana@gar.union.edu   BITNET: marchana@union.bitnet

Jurassic Park Networks

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
29 Jul 93 16:09:39 EDT

The following is the text as submitted to Network World. It was slightly edited and then published as "Jurassic Park's net security policies are prehistoric," _Network World_ 10(30):89 [26 July 93].

Velocihackers and Tyrannosaurus superior

by M. E. Kabay, Ph.D., Director of Education
National Computer Security Association
10 South Courthouse Avenue, Carlisle, PA 17013
Tel 717-258-1816 Fax 717-243-8642

The current hit movie "Jurassic Park" stars several holdovers from 65 million years ago. It also shows errors in network security that seem to be as old.

For those of you who have just returned from Neptune, "Jurassic Park" is about a dinosaur theme park that displays live dinosaurs created after scientists cracked extinct dinosaur DNA code recovered from petrified mosquitos. The film has terrific live-action dinosaur replicas and some heart-stopping scenes. It also dramatizes awful network management and security. Unfortunately, the policies are as realistic as the dinosaurs.

Consider a network security risk analysis for Jurassic Park. The entire complex depends on computer-controlled electric fences and gates to keep a range of prehistoric critters from eating the tourists and staff. So at a simple level, if the network fails, people turn into dinosaur food.

Jurassic Park's security network is controlled by an ultramodern Unix system, but its management structures date from the Stone Age. There is only one person who maintains the programs which control the security network. This breaks Kabay's Law of Redundancy, which states, "No knowledge shall be the property of only one member of the team." After all, if that solitary guru were to leave, go on vacation, or get eaten by a dinosaur, you'd be left without a safety net.

Jurassic Park's security system is controlled by computer programs consisting of two million lines of proprietary code. These critical programs are not properly documented. An undocumented system is by definition a time bomb. In the movie, this bomb is triggered by a vindictive programmer who is angry because he feels overworked and underpaid.

One of the key principles of security is that people are the most important component of any security system. Disgruntled and dishonest employees cause far more damage to networks and computer systems than hackers. The authoritarian owner of the Park dismisses the programmer's arguments and complaints as if owning a bunch of dinosaurs gives him the privilege of treating his employees rudely. He pays no attention to explicit indications of discontent, including aggressive language, resentful retorts, and sullen expressions. If the owner had taken the time to listen to his employee's grievances and take steps to address them, he could have prevented several dinosaur meals.

Bad housekeeping is another sign of trouble. The console where the disgruntled programmer works looks like a garbage dump; it's covered in coffee-cup fungus gardens, historically significant chocolate bar wrappers, and a treasure trove of recyclable soft drink cans. You'd think that a reasonable manager would be alarmed simply by the number of empty calories per hour being consumed by this critically important programmer. The poor fellow is so overweight that his life expectancy would be short even if he didn't become dinosaur fodder.

Ironically, the owner repeats, `No expense spared' at several points during the movie. It doesn't seem to occur to him that with hundreds of millions of dollars spent on hardware and software--not to mention the buildings and grounds and an entire private island--modest raises for the staff would be trivial in terms of operating expenses but significant for morale.

In the movie, the network programmer is bribed by competitors to steal dinosaur embryos. He does so by setting off a logic bomb that disrupts network operations completely. The network outage causes surveillance and containment systems to fail, stranding visitors in, well, uncomfortable situations. Even though the plot is not exactly brilliant, I'd like to leave at least something to surprise those who haven't seen the movie yet.

When the systems fail, for some reason all the electric locks in the park's laboratory are instantly switched to the open position. Why aren't they automatically locked instead? Normally, when a security controller fails, the default should be to keep security high, not eliminate it completely. Manual overrides such as crash bars (the horizontal bars that open latches on emergency exits) can provide emergency egress without compromising security.

As all of this is happening, a tropical storm is bearing down on the island. The contingency plan appears to consist of sending almost everyone away to the mainland, leaving a pitifully inadequate skeleton crew. The film suggests that the skeleton crew is not in physical danger from the storm, so why send essential personnel away? Contingency plans are supposed to include redundancy at every level. Reducing the staff when more are needed is incomprehensible.

At one point, the systems are rebooted by turning the power off to the entire island on which the park is located. This is equivalent to turning the power off in your city because you had an application failure on your PC. Talk about overkill: why couldn't they just power off the computers themselves?

Where were the DPMRP (Dinosaur Prevention, Mitigation and Recovery Planning) consultants when the park was being designed? Surely everybody should know by now that the only way to be ready for dinosaurs, uh, disasters, is to think, plan, rehearse, refine and update. Didn't anyone think about what would happen if the critters got loose? Where are the failsafe systems? The uninterruptible power supplies? The backup power generators? Sounds like Stupidosaurians were in charge.

We may be far from cloning dinosaurs, but we are uncomfortably close to managing security with all the grace of a Brontosaurus trying to type.

I hope you see the film. And bring your boss.

Best wishes, Mich

Michel E. Kabay, Ph.D.
Director of Education
National Computer Security Association

Intrusion Detection workshop

Teresa Lunt <lunt@csl.sri.com>

Thu, 5 Aug 93 11:05:26 -0700

TWELFTH INTRUSION DETECTION WORKSHOP
CALL FOR PARTICIPATION

SRI is holding a one-day workshop on intrusion detection at the Baltimore Convention Center in Baltimore MD on Thursday, September 23, 1993, which is the final day of the 15th National Computer Security Conference. This will be the twelfth in a series of intrusion-detection workshops. The NCSC conference organizers have kindly provided us with a room at the convention center.

If you and/or your colleagues wish to attend, please let us know using the attached reply form. For other questions, please call Liz Luntzel at 415-859-3285 or send us a fax at 415-859-2844 or email at luntzel@csl.sri.com.

The workshop will consist of several short presentations as well as discussion periods. To help me in preparing the agenda, I would be interested in knowing whether you have any progress to report on an intrusion-detection project or some related work that would be appropriate for a brief presentation. If so, please indicate the title and a paragraph describing your proposed talk on the enclosed form. Please also indicate there your suggestions for discussion topics. Please mail the completed form to Liz Luntzel at the address below:

Liz Luntzel EL250
SRI International
Computer Science Laboratory
333 Ravenswood Avenue
Menlo Park, California USA 94025

You may also email the completed form to: luntzel@csl.sri.com

There is no charge for the workshop, and meals are not included. There are numerous places in the surrounding Baltimore Harbor area for breakfast and lunch. The workshop will begin at 9am and will conclude at 4pm. At the request of the organizers of the National Computer Security Conference, we will break at 11am to allow you to attend the closing plenary session of the conference, and resume at 2pm after lunch.

I look forward to seeing you at the workshop!

Teresa Lunt lunt@csl.sri.com

------------------------------ cut here ---------------------------------

TWELFTH INTRUSION DETECTION WORKSHOP

Yes! I will attend the Intrusion-Detection Workshop September 23 at the Baltimore Convention Center.

Please complete the following:

Name: Title: Affiliation: Address:

Indicate one:

I am / am-not interested in presenting a talk.

If your are interested, please complete the following:

Title of Proposed Talk:
Abstract:

Suggestions for Discussion Topics:

cfp'94 announcement

</G=G/S=TRUBOW/O=COMPMAIL/ADMD=TELEMAIL/C=US/@sprint.com>
Wed, 4 Aug 1993 10:51:52 -0700

Conference Announcement
Computers, Freedom, and Privacy 1994
23-26 March 1994

The fourth annual conference, "Computers, Freedom, and Privacy," (CFP'94) will be held in Chicago, Il., March 23-26, 1994. The conference is hosted by The John Marshall Law School; George B. Trubow, professor of law and director of the Center for Informatics Law at John Marshall, is general chair of the conference. (E-Mail: 7trubow@jmls.edu). The program is sponsored jointly by these Association for Computing Machinery (ACM) Special Interest Groups: Communications (SIGCOMM); Computers and Society (SIGCAS); Security, Audit and Control (SIGSAC).

The advance of computer and communications technologies holds great promise for individuals and society. From conveniences for consumers and efficiencies in commerce to improved public health and safety and increased participation in government and community, these technologies are fundamentally transforming our environment and our lives.

At the same time, these technologies present challenges to the idea of a free and open society. Personal privacy is at risk from invasions by high-tech surveillance and monitoring; a myriad of personal information data bases expose private life to constant scrutiny; new forms of illegal activity may threaten the traditional barriers between citizen and state and present new tests of Constitutional protection; geographic boundaries of state and nation may be recast by information exchange that knows no boundaries in global data networks.

CFP'94 will present an assemblage of experts, advocates and interest groups from diverse perspectives and disciplines to consider freedom and privacy in today's "information society." A series of preconference tutorials will be offered on March 23, 1994, with the conference program beginning on Thursday, March 24, and running through Saturday, March 26, 1994.

The Palmer House, a Hilton hotel located in Chicago's "loop," and only about a block from The John Marshall Law School, is the conference headquarters. Room reservations should be made directly with the hotel after September 1, 1993, mentioning John Marshall or "CFP'94" to get the special conference rate of $99.00, plus tax.

The Palmer House Hilton
17 E. Monroe., Chicago, Il., 60603
Tel: 312-726-7500; 1-800-HILTONS; Fax 312-263-2556

Communications regarding the conference should be sent to:
CFP'94
The John Marshall Law School
315 S. Plymouth Ct.
Chicago, IL 60604-3907
(Voice: 312-987-1419; Fax: 312-427-8307; E-mail: CFP94@jmls.edu)

CALL FOR CFP'94 PARTICIPATION AND PROGRAM SUGGESTIONS

It is intended that CFP'94 programs will examine the potential benefits and burdens of new information and communications technologies and consider ways in which society can enjoy the benefits while minimizing negative implications.

Proposals are requested from those who desire to present an original paper in a relevant area of technology, policy analysis or law, or to suggest a program presentation. Any proposal (1) should not exceed three typewritten double-spaced pages; (2) must state the title of the paper or program; (3) briefly describe its theme and content; and (4) set out the name, address, credentials and experience of the author or suggested speakers. If a proposed paper has already been completed a copy should be attached to the proposal.

STUDENT PAPER COMPETITION

Full time college or graduate students are invited to enter the student paper competition. Papers must not exceed 2500 words and should address the impact of computer and telecommunications technologies on freedom and privacy in society. Winners will receive a scholarship to attend the conference and present their papers. All papers should be submitted by November 1, 1993 (either as straight text via e-mail or 6 printed copies) to:

Prof. Eugene Spafford
Department of Computer Science
Purdue University
West Lafayette, IN 47907-2004
E-Mail: spaf@cs.purdue.edu; Voice: 317-494-7825

REGISTRATION

Registration information and fee schedules will be announced by September 1, 1993. Inquiries regarding registration should be directed to RoseMarie Knight, Registration Chair, at the JMLS address above; her voice number is 312-987-1420.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 80

Wednesday 11 August 1993

Contents

Article by Dorothy Denning on Clipper Chip

Al Stangenberger <forags@nature.berkeley.edu>
Wed, 4 Aug 93 10:35:05 PDT

The July-August issue of American Scientist (Amer. Scientist 81:319-323) has a column by Dorothy Denning describing the Clipper Encryption System. It is written from the Administration and law enforcement viewpoint and does not discuss the serious privacy issues which have been raised in RISKS. However, it does present a clear discussion of the system and might be useful in explaining the system to colleagues.

Al Stangenberger   Dept. of Env. Sci., Policy, & Mgt.
forags@nature.berkeley.edu 145 Mulford Hall, Univ. of Calif. Berkeley CA 94720

SKIPJACK Review

Dorothy Denning <DENNING@guvax.acc.georgetown.edu>
Sun, 01 Aug 1993 21:16:56 -0400 (EDT)

SKIPJACK Review
Interim Report
The SKIPJACK Algorithm

Ernest F. Brickell, Sandia National Laboratories

Dorothy E. Denning, Georgetown University
Stephen T. Kent, BBN Communications Corporation
David P. Maher, AT&T
Walter Tuchman, Amperif Corporation

July 28, 1993
(copyright 1993)

Executive Summary

The objective of the SKIPJACK review was to provide a mechanism whereby persons outside the government could evaluate the strength of the classified encryption algorithm used in the escrowed encryption devices and publicly report their findings. Because SKIPJACK is but one component of a large, complex system, and because the security of communications encrypted with SKIPJACK depends on the security of the system as a whole, the review was extended to encompass other components of the system. The purpose of this Interim Report is to report on our evaluation of the SKIPJACK algorithm. A later Final Report will address the broader system issues.

The results of our evaluation of the SKIPJACK algorithm are as follows:

1. Under an assumption that the cost of processing power is halved every eighteen months, it will be 36 years before the cost of breaking SKIPJACK by exhaustive search will be equal to the cost of breaking DES today. Thus, there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.

2. There is no significant risk that SKIPJACK can be broken through a shortcut method of attack.

3. While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.

1. Background

On April 16, the President announced a new technology initiative aimed at providing a high level of security for sensitive, unclassified communications, while enabling lawfully authorized intercepts of telecommunications by law enforcement officials for criminal investigations. The initiative includes several components:

A classified encryption/decryption algorithm called "SKIPJACK."

Tamper-resistant cryptographic devices (e.g., electronic chips), each of which contains SKIPJACK, classified control software, a device identification number, a family key used by law enforcement, and a device unique key that unlocks the session key used to encrypt a particular communication.

A secure facility for generating device unique keys and programming the devices with the classified algorithms, identifiers, and keys.

Two escrow agents that each hold a component of every device unique key. When combined, those two components form the device unique key.

A law enforcement access field (LEAF), which enables an authorized law enforcement official to recover the session key. The LEAF is created by a device at the start of an encrypted communication and contains the session key encrypted under the device unique key together with the device identifier, all encrypted under the family key.

LEAF decoders that allow an authorized law enforcement official to extract the device identifier and encrypted session key from an intercepted LEAF. The identifier is then sent to the escrow agents, who return the components of the corresponding device unique key. Once obtained, the components are used to reconstruct the device unique key, which is then used to decrypt the session key.

This report reviews the security provided by the first component, namely the SKIPJACK algorithm. The review was performed pursuant to the President's direction that "respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their finding." The Acting Director of the National Institute of Standards and Technology (NIST) sent letters of invitation to potential reviewers. The authors of this report accepted that invitation.

We attended an initial meeting at the Institute for Defense Analyses Supercomputing Research Center (SRC) from June 21-23. At that meeting, the designer of SKIPJACK provided a complete, detailed description of the algorithm, the rationale for each feature, and the history of the design. The head of the NSA evaluation team described the evaluation process and its results. Other NSA staff briefed us on the LEAF structure and protocols for use, generation of device keys, protection of the devices against reverse engineering, and NSA's history in the design and evaluation of encryption methods contained in SKIPJACK. Additional NSA and NIST staff were present at the meeting to answer our questions and provide assistance. All staff members were forthcoming in providing us with requested information.

At the June meeting, we agreed to integrate our individual evaluations into this joint report. We also agreed to reconvene at SRC from July 19-21 for further discussions and to complete a draft of the report. In the interim, we undertook independent tasks according to our individual interests and availability. Ernest Brickell specified a suite of tests for evaluating SKIPJACK. Dorothy Denning worked at NSA on the refinement and execution of these and other tests that took into account suggestions solicited from Professor Martin Hellman at Stanford University. NSA staff assisted with the programming and execution of these tests. Denning also analyzed the structure of SKIPJACK and its susceptibility to differential cryptanalysis. Stephen Kent visited NSA to explore in more detail how SKIPJACK compared with NSA encryption algorithms that he already knew and that were used to protect classified data. David Maher developed a risk assessment approach while continuing his ongoing work on the use of the encryption chip in the AT&T Telephone Security Device. Walter Tuchman investigated the anti-reverse engineering properties of the chips.

We investigated more than just SKIPJACK because the security of communications encrypted with the escrowed encryption technology depends on the security provided by all the components of the initiative, including protection of the keys stored on the devices, protection of the key components stored with the escrow agents, the security provided by the LEAF and LEAF decoder, protection of keys after they have been transmitted to law enforcement under court order, and the resistance of the devices to reverse engineering. In addition, the success of the technology initiative depends on factors besides security, for example, performance of the chips. Because some components of the escrowed encryption system, particularly the key escrow system, are still under design, we decided to issue this Interim Report on the security of the SKIPJACK algorithm and to defer our Final Report until we could complete our evaluation of the system as a whole.

2. Overview of the SKIPJACK Algorithm

SKIPJACK is a 64-bit "electronic codebook" algorithm that transforms a 64-bit input block into a 64-bit output block. The transformation is parameterized by an 80-bit key, and involves performing 32 steps or iterations of a complex, nonlinear function. The algorithm can be used in any one of the four operating modes defined in FIPS 81 for use with the Data Encryption Standard (DES).

The SKIPJACK algorithm was developed by NSA and is classified SECRET. It is representative of a family of encryption algorithms developed in 1980 as part of the NSA suite of "Type I" algorithms, suitable for protecting all levels of classified data. The specific algorithm, SKIPJACK, is intended to be used with sensitive but unclassified information.

The strength of any encryption algorithm depends on its ability to withstand an attack aimed at determining either the key or the unencrypted ("plaintext") communications. There are basically two types of attack, brute-force and shortcut.

3. Susceptibility to Brute Force Attack by Exhaustive Search

In a brute-force attack (also called "exhaustive search"), the adversary essentially tries all possible keys until one is found that decrypts the intercepted communications into a known or meaningful plaintext message. The resources required to perform an exhaustive search depend on the length of the keys, since the number of possible keys is directly related to key length. In particular, a key of length N bits has 2^N possibilities. SKIPJACK uses 80-bit keys, which means there are 2^80 (approximately 10^24) or more than 1 trillion trillion possible keys.

An implementation of SKIPJACK optimized for a single processor on the 8-processor Cray YMP performs about 89,000 encryptions per second. At that rate, it would take more than 400 billion years to try all keys. Assuming the use of all 8 processors and aggressive vectorization, the time would be reduced to about a billion years.

A more speculative attack using a future, hypothetical, massively parallel machine with 100,000 RISC processors, each of which was capable of 100,000 encryptions per second, would still take about 4 million years. The cost of such a machine might be on the order of $50 million. In an even more speculative attack, a special purpose machine might be built using 1.2 billion $1 chips with a 1 GHz clock. If the algorithm could be pipelined so that one encryption step were performed per clock cycle, then the $1.2 billion machine could exhaust the key space in 1 year.

Another way of looking at the problem is by comparing a brute force attack on SKIPJACK with one on DES, which uses 56-bit keys. Given that no one has demonstrated a capability for breaking DES, DES offers a reasonable benchmark. Since SKIPJACK keys are 24 bits longer than DES keys, there are 2^24 times more possibilities. Assuming that the cost of processing power is halved every eighteen months, then it will not be for another 24 * 1.5 = 36 years before the cost of breaking SKIPJACK is equal to the cost of breaking DES today. Given the lack of demonstrated capability for breaking DES, and the expectation that the situation will continue for at least several more years, one can reasonably expect that SKIPJACK will not be broken within the next 30-40 years.

Conclusion 1: Under an assumption that the cost of processing power is halved every eighteen months, it will be 36 years before the cost of breaking SKIPJACK by exhaustive search will be equal to the cost of breaking DES today. Thus, there is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.

4. Susceptibility to Shortcut Attacks

In a shortcut attack, the adversary exploits some property of the encryption algorithm that enables the key or plaintext to be determined in much less time than by exhaustive search. For example, the RSA public-key encryption method is attacked by factoring a public value that is the product of two secret primes into its primes.

Most shortcut attacks use probabilistic or statistical methods that exploit a structural weakness, unintentional or intentional (i.e., a "trapdoor"), in the encryption algorithm. In order to determine whether such attacks are possible, it is necessary to thoroughly examine the structure of the algorithm and its statistical properties. In the time available for this review, it was not feasible to conduct an evaluation on the scale that NSA has conducted or that has been conducted on the DES. Such review would require many man-years of effort over a considerable time interval. Instead, we concentrated on reviewing NSA's design and evaluation process. In addition, we conducted several of our own tests.

4.1 NSA's Design and Evaluation Process

SKIPJACK was designed using building blocks and techniques that date back more than forty years. Many of the techniques are related to work that was evaluated by some of the world's most accomplished and famous experts in combinatorics and abstract algebra. SKIPJACK's more immediate heritage dates to around 1980, and its initial design to 1987.

SKIPJACK was designed to be evaluatable, and the design and evaluation approach was the same used with algorithms that protect the country's most sensitive classified information. The specific structures included in SKIPJACK have a long evaluation history, and the cryptographic properties of those structures had many prior years of intense study before the formal process began in 1987. Thus, an arsenal of tools and data was available. This arsenal was used by dozens of adversarial evaluators whose job was to break SKIPJACK. Many spent at least a full year working on the algorithm. Besides highly experienced evaluators, SKIPJACK was subjected to cryptanalysis by less experienced evaluators who were untainted by past approaches. All known methods of attacks were explored, including differential cryptanalysis. The goal was a design that did not allow a shortcut attack.

The design underwent a sequence of iterations based on feedback from the evaluation process. These iterations eliminated properties which, even though they might not allow successful attack, were related to properties that could be indicative of vulnerabilities. The head of the NSA evaluation team confidently concluded "I believe that SKIPJACK can only be broken by brute force; there is no better way."

In summary, SKIPJACK is based on some of NSA's best technology. Considerable care went into its design and evaluation in accordance with the care given to algorithms that protect classified data.

4.2 Independent Analysis and Testing

Our own analysis and testing increased our confidence in the strength of SKIPJACK and its resistance to attack.

4.2.1 Randomness and Correlation Tests

A strong encryption algorithm will behave like a random function of the key and plaintext so that it is impossible to determine any of the key bits or plaintext bits from the ciphertext bits (except by exhaustive search). We ran two sets of tests aimed at determining whether SKIPJACK is a good pseudo random number generator. These tests were run on a Cray YMP at NSA. The results showed that SKIPJACK behaves like a random function and that ciphertext bits are not correlated with either key bits or plaintext bits. Appendix A gives more details.

4.2.2 Differential Cryptanalysis

Differential cryptanalysis is a powerful method of attack that exploits structural properties in an encryption algorithm. The method involves analyzing the structure of the algorithm in order to determine the effect of particular differences in plaintext pairs on the differences of their corresponding ciphertext pairs, where the differences are represented by the exclusive-or of the pair. If it is possible to exploit these differential effects in order to determine a key in less time than with exhaustive search, an encryption algorithm is said to be susceptible to differential cryptanalysis. However, an actual attack using differential cryptanalysis may require substantially more chosen plaintext than can be practically acquired.

We examined the internal structure of SKIPJACK to determine its susceptibility to differential cryptanalysis. We concluded it was not possible to perform an attack based on differential cryptanalysis in less time than with exhaustive search.

4.2.3 Weak Key Test

Some algorithms have "weak keys" that might permit a shortcut solution. DES has a few weak keys, which follow from a pattern of symmetry in the algorithm. We saw no pattern of symmetry in the SKIPJACK algorithm which could lead to weak keys. We also experimentally tested the all "0" key (all 80 bits are "0") and the all "1" key to see if they were weak and found they were not.

4.2.4 Symmetry Under Complementation Test

The DES satisfies the property that for a given plaintext-ciphertext pair and associated key, encryption of the one's complement of the plaintext with the one's complement of the key yields the one's complement of the ciphertext. This "complementation property" shortens an attack by exhaustive search by a factor of two since half the keys can be tested by computing complements in lieu of performing a more costly encryption. We tested SKIPJACK for this property and found that it did not hold.

4.2.5 Comparison with Classified Algorithms

We compared the structure of SKIPJACK to that of NSA Type I algorithms used in current and near-future devices designed to protect classified data. This analysis was conducted with the close assistance of the cryptographer who developed SKIPJACK and included an in-depth discussion of design rationale for all of the algorithms involved. Based on this comparative, structural analysis of SKIPJACK against these other algorithms, and a detailed discussion of the similarities and differences between these algorithms, our confidence in the basic soundness of SKIPJACK was further increased.

Conclusion 2: There is no significant risk that SKIPJACK can be broken through a shortcut method of attack.

5. Secrecy of the Algorithm

The SKIPJACK algorithm is sensitive for several reasons. Disclosure of the algorithm would permit the construction of devices that fail to properly implement the LEAF, while still interoperating with legitimate SKIPJACK devices. Such devices would provide high quality cryptographic security without preserving the law enforcement access capability that distinguishes this cryptographic initiative. Additionally, the SKIPJACK algorithm is classified SECRET NOT RELEASABLE TO FOREIGN NATIONALS. This classification reflects the high quality of the algorithm, i.e., it incorporates design techniques that are representative of algorithms used to protect classified information. Disclosure of the algorithm would permit analysis that could result in discovery of these classified design techniques, and this would be detrimental to national security.

However, while full exposure of the internal details of SKIPJACK would jeopardize law enforcement and national security objectives, it would not jeopardize the security of encrypted communications. This is because a shortcut attack is not feasible even with full knowledge of the algorithm. Indeed, our analysis of the susceptibility of SKIPJACK to a brute force or shortcut attack was based on the assumption that the algorithm was known.

Conclusion 3: While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.

[The appendix in LaTeX form is available from Dorothy. PGN]

The Rule of Law and the Clipper Escrow Project

Peter Wayner <pcw@access.digex.net>
Tue, 3 Aug 1993 09:40:00 -0400

Last Thursday, I attended the first day of the Computer System Ssecurity and Privacy Advisory Board in Washington. This is a group of industry experts who discuss topics in computer security that should affect the public and industry. Some of the members are from users like banks and others are from service providing companies like Trusted Information Services. Lately, their discussion has centered on the NSA/NIST's Clipper/Capstone/Skipjack project and the effects it will have on society.

At the last meeting, the public was invited to make comments and they were almost unanimously skeptical and critical. They ranged from political objections to the purely practical impediments. Some argued that this process of requiring the government to have the key to all conversations was a violation of the fourth amendment of the constitution prohibiting warrantless searches. Others noted that a software solution was much simpler and cheaper even if the chips were going to cost a moderate $25. There were many different objections, but practically everyone felt that a standard security system was preferable.

This meeting was largely devoted to the rebuttals from the government. The National Security Association, the Department of Justice, the FBI, the national association of District Attorneys and Sheriffs and several others were all testifying today.

The board itself runs with a quasi-legal style they make a point of making both video and audio tapes of the presentations. The entire discussion is conducted with almost as much gravity as Congressional hearings. The entire meeting was suffused with an air of ernest lawfullness that came these speakers. All of them came from the upper ranks of the military or legal system and a person doesn't rise to such a position without adopting the careful air of the very diligent bureaucrat. People were fond of saying things like, "Oh, it's in the Federal Register. You can look it up." This is standard operating procedure in Washington agencies and second nature to many of the day's speakers.

Dorothy Denning was one of the first speakers and she reported on the findings of the committee of five noted public cryptologists who agreed to give the Clipper standard a once-over. Eleven people were asked, but six declined for a variety of reasons. The review was to be classified "Secret" and some balked at this condition because they felt it would compromise their position in public.

The talk made clear that the government intended to keep the standard secret for the sole purpose of preventing people from making unauthorized implementations without the law enforcement back door. Dr. Denning said that everyone at the NSA believes that the algorithm could withstand public knowledge with no trouble. The review by the panel revealed no reason why they shouldn't trust this assessment.

Although lack of time lead the panel to largely rubberstamp the more extensive review by the NSA, they did conduct a few tests of their own. They programmed the algorithm on a Cray YMP, which incidentally could process 89,000 encryptions per second in single processor mode. This implementation was used for a cycling test which they found seemed to imply that there was good randomness. The test is done by repeatedly encrypting one value of data until a cycle occurs. The results agreed with what a random process should generate.

They also tested the system for strength against a differential cryptanalysis attack and found it worthy. There was really very little other technical details in the talk. Saying more would have divulged something about the algorithm.

My general impression is that the system is secure. Many people have played paranoid and expressed concerns that the classified algorithm might be hiding a trapdoor. It became clear to me that these concerns were really silly. There is a built-in trapdoor to be used by the government when it is "legal authorized" to intercept messages. The NSA has rarely had trouble in the past exercising either its explicitly granted legal authority or its implied authority. The phrase "national security" is a powerful pass phrase around Washington and there is no reason for me to believe that the NSA wouldn't get all of the access to the escrow database that it needs to do its job. Building in a backdoor would only leave a weakness for an opponent to exploit and that is something that is almost as sacriligeous at the NSA as just putting the classified secrets in a Fed Ex package to Saddam Hussein.

Next there was a report from Geoff Greiveldinger , the man from the Department of Justice with the responsibility of implementing the the Key Escrow plan. After the Clipper/Capstone/SkipJack chips are manufactured, they will be programmed with an individual id number and a secret, unique key. A list is made of the id, key pairs and this list is split into two halves by taking each unique key, k, and finding two numbers a and b such that a+b=k. (+ represents XOR). One new list will go to one of the escrow agencies and one will go to the other. It will be impossible to recover the secret key without getting the list entry from both agencies.

At this point, they include an additional precaution. Each list will be encrypted so even the escrow agency won't be able to know what is in its list. The key for decoding this list will be locked away in the evesdropping box. When a wiretap is authorized, each escrow agency will lookup the halves of the key that correspond to the phone being tapped and send these to evesdropping box where they will be decrypted and combined. That means that two clerks from the escrow agencies could not combine their knowledge. They would need access to a third key or an evesdropping box.

It became clear that the system was not fully designed. It wasn't obvious how spontaneous and fully automated the system would be. Mr. Greiveldinger says that he is trying to balance the tradeoffs between security and efficiency. Officers are bound to be annoyed and hampered if they can't start a tap instanteneously. The kidnapping of a child is the prototypical example of when this would be necessary.

The courts also grant authority for "roving" wiretaps that allow the police to intercept calls from any number of phones. A tap like this begs out for a highly automated system for delivering the keys.

I imagine that the system as it's designed will consist of escrow computers with a few clerks who have nothing to do all day. When a tap is authorized, the evesdropping box will be programmed with a private key and shipped to the agents via overnight express. When they figure out the id number of the phone being tapped, the evesdropping box will probably phone the two escrow computers, perform a bit of zero-knowledge authorization and then receive the two halves of the key. This would allow them to switch lines and conduct roving taps effectively. The NSA would presumably have a box that would allow them to decrypt messages from foreign suspects.

At this point, I had just listened to an entirely logical presentation from a perfect gentleman. We had just run though a system that had many nice technological checks and balances in it. Subverting it seemed very difficult. You would need access to the two escrow agencies and an evesdropping box. Mr. Greiveldinger said that there would be many different "auditting" records that would be kept of the taps. It was very easy to feel rather secure about the whole system in a nice, air-conditioned auditorium where clean, nice legally precise people were speaking in measured tones. It was very easy to believe in the Rule of Law.

To counteract this, I tried to figure out the easiest way for me to subvert the system. The simplest way is to be a police officer engaged in a stakeout of someone for whom you've already received a warrant. You request the Clipper eavesdropping box on the off chance that the suspect will buy a Clipper phone and then you "lend" it to a friend who needs it. I think that the automation will allow the person who possesses the box to listen in to whatever lines that they want. The escrow agency doesn't maintain a list of people and id numbers-- they only know the list matching the id number to the secret key.

There is no way that they would know that a request from the field was unreasonable. Yes, the audit trails could be used later to reconstruct what the box was used for, but that would only be necessary if someone got caught.

The bribe value of this box would probably be hard to determine, but it could be very valuable. We know that the government of France is widely suspected of using its key escrow system to eavesdrop on US manufacturers in France. Would they be willing to buy eavesdropping time here in America? It is not uncommon to see reports of industrial espionage where the spies get millions of dollars. On the other hand, cops on the beat in NYC have been influenced for much less. The supply and demand theory of economics virtually guarantees that some deals are going to be done.

It is not really clear what real effect the key escrow system is going to have on security. Yes, thieves would need to raid two different buildings and steal two different copies of the tapes. This is good. But it is still impossible to figure out if the requests from the field are legitimate-- at least within the time constraints posed by urgent cases involving terrorism and kidnapping.

The net effect of implementing the system is that the phone system would be substantially strengthened against naive intruders, but the police (and those that bribe them) would still be able to eavesdrop with impunity. Everyone needs to begin to do a bit of calculus between the costs and benefits of this approach. On one hand, not letting the police intercept signals will let the crooks run free but on the other hand, the crooks are not about to use Clipper phones for their secrets if they know that they can be tapped.

The most interesting speaker was the assistant director of the National Security Agency, Dr. Clint Brooks. He immediately admitted that the entire Clipper project was quite unusual because the Agency was not used to dealing with the open world. Speaking before a wide audience was strange for him and he admitted that producing a very low cost commercial competitive chip was also a new challenge for them.

Nevertheless, I found him to be the deepest thinker at the conference. He readily admitted that the Clipper system isn't intended to catch any crooks. They'll just avoid the phones. It is just going to deny them access to the telecommunications system. They just won't be able to go into Radio Shack and buy a secure phone that comes off the line.

It was apparent that he was somewhat skeptical of the Clipper's potential for success. He said at one point the possibilities in the system made it worth taking the chance that it would succeed. If it could capture a large fraction of the market then it could help many efforts of the law enforcement and intelligence community.

When I listened, though, I began to worry about what is going to happen as we begin to see the eventual blurring of data and voice communications systems. Right now, people go to Radio Shack to buy a phone. It's the only way you can use the phone system. In the future, computers, networks and telephones are going to be linked in much more sophisticated ways. I think that Intel and Microsoft are already working on such a technology.

When this happens, programmable phones are going to emerge. People will be able to pop a new ROM in their cellular digital phone or install new software in their computer/video game/telephone. This could easily be a proprietary encryption system that scrambles everything. The traditional way of controlling technology by controlling the capital intensive manufacturing sites will be gone. Sure, the NSA and the police will go to Radio Shack and say "We want your cooperation" and they'll get it. But it's the little, slippery ones that will be trouble in the new, software world.

The end of the day was dominated by a panel of Law Enforcement specialists from around the country. These were sheriffs, district attorneys, FBI agents and other officers from different parts of the system. Their message was direct and they didn't hesitate to compare encryption with assault rifles. One even said, "I don't want to see the officers outgunned in a technical arena."

They repeatedly stressed the incredible safeguards placed upon the wiretapping process and described the hurdles that the officers must go through to use the system. One DA from New Jersey said that in his office, they process about 10,000 cases a year, but they only do one to two wiretaps on average. It just seems like a big hassle and expense for them.

It is common for the judges to require that the officers have very good circumstantial evidence from informers before giving them the warrant. This constraint coupled with the crooks natural hesitation to use the phone meant that wiretaps weren't the world's greatest evidence producers.

One moment of levity came when a board member asked what the criminals favorite type of encryption was. The police refused to answer this one and I'm not that sure if they've encountered enough cases to build a profile.

At the end of all of the earnestness and "support-the-cop-on-the-beat", I still began to wonder if there was much value to wiretaps at all. The police tried to use the low numbers of wiretaps as evidence that they're not out there abusing the system, but I kept thinking that this was mainly caused by the high cost and relatively low utility of the technique.

It turns out that there is an easy way to check the utility of these devices. Only 37 states allow their state and local police to use wiretaps in investigations. One member of the panel repeated the rumor that this is supposedly because major politicians were caught with wiretaps. The state legislatures in these states supposedly realized that recipients of graft and influence peddlers were the main target of wiretaps. Eavesdropping just wasn't a tool against muggers. So they decided to protect themselves.

It would be possible to check the crime statistics from each of these states and compare them against the eavesdropping states to discover which has a better record against crime. I would like to do this if I can dig up the list of states that allow the technique. I'm sure that this would prove little, but it could possibly clarify something about this technique.

It is interesting to note that the House of Representative committee on the Judiciary was holding hearings on abuses of the National Crime Information Center. They came in the same week as the latest round of Clipper hearings before the CSAB. The NCIC is a large computer system run by the FBI to provide all the police departments with a way to track down the past records of people. The widespread access to the system makes it quite vulnerable to abuse.

In the hearings, the Congress heard many examples of unauthorized access. Some were as benign as people checking out employees. The worst was an ex-police officer who used the system to track down his ex-girlfriend and kill her. They also heard of a woman who looked up clients for her drug-dealing boyfriend so he could avoid the undercover cops.

These hearings made it obvious that there were going to be problems determining the balance of grief. For every prototypical example of a child kidnapped to make child pornography, there is a renegade police officer out to knock off his ex-girlfriend. On the whole, the police may be much more trustworthy than the criminals, but we need to ask how often a system like Clipper will aid the bad guys.

In the end, I reduced the calculus of the decision about Clipper to be a simple tradeoff. If we allow widespread, secure encryption, will the criminals take great advantage of this system? The secure phones won't be useful in rapes and random street crime, but they'll be a big aid to organized endeavors. It would empower people to protect their own information unconditionally, but at the cost of letting the criminals do the same.

Built-in back doors for the law enforcement community, on the other hand, will deny the power of off-the-shelf technology to crooks, but it would also leave everyone vulnerable to organized attacks on people.

I began to wonder if the choice between Clipper and totally secure encryption was moot. In either case, there would be new opportunities for both the law-abiding and the law-ignoring. The amount of crime in the country would be limited only by the number of people who devote their life to the game-- not by any new fangled technology that would shift the balance.

I did not attend the Friday meeting so someone else will need to summarize the details.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 81

Wednesday 11 August 1993

Contents

Colorado prison is escape-proof! (We'll see...)

303) 977-2052
Wed, 11 Aug 93 18:27:33 MDT

CANON CITY--They said it about Alcatraz, and they're saying it about Colorado State Penitentiary. (Excerpted from The Denver Post, Saturday, July 31, 1993, pp. 1A, 7A)

Nobody'll ever bust outta this place.

"Can't happen," said George Sullivan, deputy director for operations of the Colorado Department of Corrections. "If there is such a thing as an escape-proof prison, this is as close as you'll get."

From the outside, the new $44.9 million maximum-security penitentiary--which was dedicated on Thursday--actually appears less secure than some of the other prisons in the state system, such as Limon Correctional Facility. There's no guard tower, for one thing. And there's no perimeter fence yet.

But even when a 12-foot cyclone fence is completed in September, it will be designed to keep outsiders away from the building, not insiders from running away. The building is so secure, Sullivan said, that type of precaution isn't necessary. [...] Locks, lights and video cameras throughout the prison can be turned on and off at the touch of a computer screen in a bullet-proof central control room. Two doors separate each of four living units, or "security envelopes," one door controlled by a correctional officer inside the unit and the other controlled by an officer in the control room.

Lance Gatrell gatrell@den.mmc.com

Surprise! contained in tar file

Olaf Titz <olaf@bigred.ka.sub.org>
Wed, 11 Aug 1993 22:44:22 +0200

The RISK of trusting in software to save confidentiality has recently been exposed in a German newsgroup. On a debate whether DES is illegal in Germany (it is not, by the way) someone posted a tarred, compressed, uuencoded archive of DES code via an anonymizing service. (No discussion on the topic of anonymization, please.) Not only that he forgot to delete the object code before tarring (thus giving an indication which kind of hardware he uses). The next day someone else posted an explanation why this action was stupid, giving the anonymous poster's full real name and address. He found it out because the tar he used leaves user names (not only UIDs, which would suffice to restore file permission settings) in the tar file. Of course, this fact is not mentioned explicitly in the man page rsp. info file (but the average user wouldn't expect it in the first place...) where an explicit warning could be considered appropriate.

Olaf Titz - olaf@bigred.ka.sub.org - s_titz@ira.uka.de

Exploiting Medco's database

David J. States <states@ibc.wustl.edu>
4 Aug 1993 22:19:17 GMT

>From today's (August 4, 1993) Wall Street Journal, pg. B1:
"Merck to Eploit Medco's Database"

The article goes on to explain that Merck, the world's largest pharmaceutical manufacturer, recently purchased Medco, a chain of discount pharmacies to gain access to the Medco database of pharmacy purchases. Merck plans to use this information in a variety of ways to promote Merck products. Examples in the article include:

- a patient is taking a more expensive drug from a competitor so Merck would suggest a competitive Merck product to the physician

- based on his other medications a patient is likely to have a condition that could be treated pharmacologically by a Merck product so suggest it to the physician

The use of pharmacy purchase records as a de facto window into a patient's medical record, and the commercial exploitation of that information is a very unfortunate development. The examples noted above seem benign enough, and the article states that Merck does not plan to actually identify patient names when they contact physcians, but this opens the door to commercial exploitation of medical records data. Many other uses of this data are very worrisome.

A tremendous amount of information can be inferred from pharmacy transactions. Both dosage and duration of therapy can be determined from the purchase data, and most people tend to stick with a small number of pharmacies. There are many thousands of drugs now on the market, and most of them carry very specific indications for use. For example, a young adult who purchases certain antibiotics is likely to be treating a case of the clap; a previously healthy parent who begins buying insulin is likely to have a child just diagnosed with diabetes; a single male in his 30's who starts buying AZT almost certainly has been diagnosed as HIV positive.

How would you feel about Merck selling information about your recent case of VD to Trojan so they could start direct mail advertising to you? There is even some medical justification for doing so. How about if they sold it to Playboy/girl? Or the local televangelist looking for sinners to convert? Is there anything to stop Merck from selling a list of patients at high risk for expensive medical care to insurance companies (who probably have the information anyway) or to prospective employers?

David States, M.D.

SAAB JAS 39 "Gripen" crashed (from soc.culture.nordic)

Lars-Henrik Eriksson <lhe@sics.se>
Wed, 11 Aug 93 22:30:28 +0200

The SAAB JAS 39 "Gripen" crashed on Sunday, August 8, during an air display over central Stockholm. The following very preliminary account of the accident is based on commentaries and video recordings of the accident that I've seen on Swedish TV. Better information should be available in a few days.

The aircraft was flying straight and level at low altitude and moderate speed. It began a gentle rocking motion in roll, then the nose pitched up rapidly, passing the vertical in a manouver resembling Pugachev's cobra. When the nose was well past the vertical - the pitch-up angle appeared to be about 120 degrees (!) - the pilot ejected and landed unhurt. After some further manouvres, the aircraft settled in a vertical descent in about level attitude. From what I could see, the aircraft did not break up in the air.

The aircraft struck a small hill on an island (Laangholmen), exploding on impact. The crash site was only tens of metres from a major bridge (Vaesterbron) packed with spectators. Miraculously no one on the ground was killed. Three people got slight burns, one sprained his ankle while running away. The only damage on the ground was that a tree was struck down.

JAS39 is a statically unstable aircraft controlled by computers (called "fly-by-wire", or FBW). The FBW system was immediately suspected to be the reason for the crash. Indeed, the behaviour of the aircraft is about what you would expect after a major failure of the FBW system. A person listening on the radio frequency used by the aircraft during the display claims that the immediately before he lost control, the pilot reported that a circuit breaker had tripped.

This is in contrast with the previous JAS 39 crash where the FBW system was functioning correctly according to the control laws in force, but where these control laws were incorrect causing the aircraft to overreact to the pilot's control inputs when the aircraft was hit by a wind gust during landing.

The aircraft that crashed was the first one to be delivered to the Swedish Air Force. It was flown by the same SAAB display pilot that flew the first accident aircraft!

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263, S-164 28 KISTA, SWEDEN lhe@sics.se +46 8 752 15 09

[Also noted by Martin Minow <minow@apple.com>
and Jacob Palme DSV <jpalme@DSV.SU.se>. PGN]

MD-11 slat extension

Robert Dorsett <rdd@cactus.org>
Fri, 6 Aug 93 03:48:09 CDT

The August 1993 Airline Pilot (p. 19) warns pilots to watch the flap/slat handle on MD-11's. This was in reference to the much-publicised incident involving a China Eastern Airlines MD-11 on April 6, which experienced uncommanded slat extension and a series of violent oscillations. The plane lost 5000', and spooked the crew enough that they made a diversion to an air base in Alaska to inspect the airplane.

Subsequent commentary in RISKS and elsewhere speculated that the digital cockpit in the airplane might have been responsible for the deployment. Comments on sci.aeronautics.airliners tended to indicate that this aspect of the flight control system was conventional in nature, however.

The article notes:

"NTSB cautioned, in its safety recommendation issued June 29, that 'The cause of the slat deployment has not been determined However, preliminary evidence strongly suggests that the flap/slat handle became dislodged from the slat-retract position... because of inadvertent contact with the handle by a flightcrew member.'

"At least 10 other cases of inadvertent or uncommanded inflight slat deployments have occurred on MD-11's since April 1991 (!!!). NTSB said Douglas Aircraft Company has advised operators of those incidents, "is aware of the continuing nature of the problem, and is... working with FAA and MD-11 operators to redesign the [MD-11] flap/slat actuating system."

[Snide personal note: cargo doors, anyone?]

The article notes that the NTSB urges:

1. That the FAA establish an interim measure to prevent inadvertent slat extension.

2. MD-11 operators to inform crews of the danger.

3. That the revamped system be installed ASAP.

"The Safety Board said the incidents continued to occur 'despite several attempted fixes' by Douglas. The China Eastern Airlines airplane had been modified to meet all Douglas service bulletins and applicable slat system [airworthiness directives].

"The day after the first incident, [Douglas told operators about the problem]

"[...] 'Sharply striking the aft side of the handle [it is normally at the furthest-forward position when flaps are retracted] will allow the handle to move upward if a very light vertical force is applied,' Douglas said. 'Normal spring and cable tensions will move the handle aft once disengaged from the FLAP UP/SLAT RET detent and allow the slats to extend.'

"In August 1992, Douglas designed a protective cover for the zero-degree detent gate. FAA later mandated that air carriers use the cover."

"[...] Douglas will replace the current flap/slat handle and its cable system with an electrically operated system designed to eliminate the cable tension forces that bias the slat system to the extend position. [...]
The electrically operated flap/slat handle system should be available in mid-1994; the interim system, within several months.

"Meanwhile, don't bump that flap/slat handle."

[And stay away from DC-10's and MD-11's, as a guiding philosophy in life :-).
--rdd]

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

MD-11 slat extension

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
6 Aug 93 19:44:23 BST (Fri)

>uncommanded [or, rather, inadvertent] slat extension [causes a] series of
>violent oscillations. The [MD11] lost 5000', and spooked the crew enough that
>they made a diversion to an air base in Alaska to inspect the airplane.

It was not just crew spook. Two passengers were killed, and all passengers were injured, some severely.

>Subsequent commentary in RISKS and elsewhere speculated that the digital
>cockpit in the airplane might have been responsible for the deployment.

I sent a query to ata-watchers asking if anyone knew if digital systems were involved. Mary Shaw responded that the report will eventually cross her desk. I don't recall seeing anything in RISKS.

I found the MD-11 that I flew on (Swissair) a year ago very comfortable, but ..
> [And stay away from DC-10's and MD-11's, as a guiding philosophy in life :-)
why the smiley face? :-)

Peter.

Call forwarding with "remote code" feature

Reva Freedman <freedman@delta.eecs.nwu.edu>
Fri, 6 Aug 93 14:45:00 CDT

An article in the Chicago Tribune (8/2/93, sec. 2, p. 7, by Terry Wilson) will make you want to check your next phone bill more carefully. A summary follows.

A Chicago man named Jeff Baird was concerned because his phone had been acting funny for days, ringing once and then stopping. One day last month he was able to answer it in the middle of a ring, and he heard a recorded message saying that the call was collect from an inmate named Bill in the Illinois Department of Corrections [IDOC--the state prison system] and that the call was being recorded and monitored. The recorded voice told him he could say "yes" and accept the charges or hang up.

Although Baird was curious about how Bill, whom he did not know, had gotten his phone number, he did not accept the charges. The odd rings continued. Eventually the Bairds discovered that an IDOC inmate had ordered call forwarding for their telephone along with a remote access code, a new feature offered by Illinois Bell. With the remote access feature, you don't have to be home to change the number your calls will be forwarded to. Just dial your home number and type in the code, followed by the number you want your calls to be forwarded to! The inmate had apparently been given the three-digit code over the phone by an Illinois Bell employee.

When the inmate wanted to make a call, he simply started forwarding the

> Bairds' calls to the number he wanted to call. Then he dialed the Bairds' number. The person to whom the call was forwarded would hear the recorded message and accept the call. The call was billed to the Bairds because it was their number which was originally dialed. More than $200 worth of collect calls were made in a week, by several inmates. In spite of the fact that all the calls were supposedly recorded, IDOC officials claim they cannot identify any of the inmates.
>
> Presumably the inmate un-forwarded the phone when he was through or the Bairds would not have received any calls at all. Once, however, Jane Baird called home and found herself talking to a complete stranger who declined to identify herself or explain why she was answering the Bairds' telephone.
>
> Illinois Bell eventually discovered that the Bairds had not ordered call forwarding. The Bairds will not have to pay for the calls. Illinois Bell has decided to mail out the code number to the address where the phone is located.

Well, folks, it looks like the phone company has come up with something more aggravating than call waiting. Seriously, though, call forwarding was originally designed *without* remote forwarding to avoid precisely this problem.

Reva Freedman <freedman@eecs.nwu.edu>
Dept. of EECS, Northwestern University, Evanston, IL

"Terminal Compromise" on the Net

ESPEN ANDERSEN <EANDERSEN@HBS.HBS.HARVARD.EDU>
11 Aug 1993 11:15:20 -0400 (EDT)

This may be the first "Novel on the Net" (though the Gutenberg project may have some comments on that), but it is not the first book published as Shareware or commercially published through computer networks. "Computer Shock", an anthology of pieces about how computers and technology affect our lives and work, was published in 1987. Quite a few well-known writers were in it (Jacques Vallee, Robert Johansen, Barbara Garson, about 10 others.) The book was edited by Roger Bullis, professor at University of Wisconsin. The thing came in a ZIP (or rather ARC) file with the text files in a COM format (when you executed the program, the text was shown on the screen). A couple of the chapters were about privacy, by the way, as well as the nature of computerized communication.

My involvement in this was when I worked for the computer center at a business school in Norway, and we made a chapter of this book a part of the curriculum in the introductory computer course. Transferred the thing to Mac under Hypercard and also to an IBM VM/CMS mainframe with a small reading program in REXX. We explained the concept of ShareWare to the students, and suggested some amount of payment (I don't remember how much, but we cleared with the editor up front). Sad to say, not much money came out of it, but I still owe Roger a beer if he ever makes it to Norway.....

Espen Andersen (hbs.harvard.edu)

Re: Jurassic Park Networks (rebooting through power reset)

Lauren Weinstein <lauren@vortex.com>
Tue, 10 Aug 93 19:34 PDT

A recent posting to RISKS points out the undesirability of rebooting all the computers via cutting all power on the island in "Jurassic Park". Such power resets are a time-honored SF movie technique for trying to solve problems. For example, in "Westworld" (1973), not only was cutting the power unsuccessful in stopping rampaging robots ("They're running on stored charge out there!"), it also, when power couldn't be restored, locked the control staff in a hermetically sealed room with doors which could only be opened electrically. No overrides, so everyone suffocates.

Conceptually similar technical silliness can be observed in "The Andromeda Strain (1971)", "The Terminal Man" (1974), and "Looker" (1981). In all these cases, elementary technical points, unlikely to be overlooked in the real world, are used as major plot development elements.

By now, many of you have already discerned the pattern in the above. All of the films listed were written by Michael Crichton, and in somes cases directed by him. Michael is the king of what I call "pop-pseudo-technology" writing--which generally revels in making as many technical folks as possible look like complete idiots and incapable of even the most obvious observations. Given his recent contractual expansions in the wake of "Jurassic Park", there will be a lot more of the same attitudes coming down the line soon.

--Lauren--

Re: ATM modem insecure?

Lauren Weinstein <lauren@vortex.com>
Tue, 10 Aug 93 19:41 PDT

I wouldn't be too concerned about the *modem* being exposed--at least not from a data integrity standpoint (whether or not the modem will last long before being removed by sticky fingers is another matter). Virtually all modern ATM terminals use data encryption (typically DES-based) for end-to-end communications. The encryption is done within the terminal, so all of the data that reaches the modem, from either side, should already be "secured."

--Lauren--

Call for Papers, IEEE Symposium on Research in Security and Privacy

John Rushby <RUSHBY@csl.sri.com>
Wed 11 Aug 93 18:05:09-PDT

1994 IEEE Symposium on May 16--18, 1994
Research in Security and Privacy Oakland, California

Sponsored by
IEEE Computer Society Technical Committee on Security and Privacy
in cooperation with
The International Association for Cryptologic Research (IACR)

The Symposium on Security and Privacy is the premier forum for the presentation of developments in computer security, and for bringing together researchers and practitioners in the field. The focus of this, the 15th symposium in the series, will include technical aspects of security and privacy as they arise in commercial and industrial applications, as well in government and military systems. The symposium will address advances in the theory, design, implementation, analysis, and application of secure computer systems, and in the integration and reconciliation of security and privacy with other critical system properties such as reliability and safety. Topics in which papers and panel session proposals are invited include, but are not limited to, the following:

Secure systems Privacy Issues Access controls Security verification
Network security Policy modeling Information flow Authentication
Database security Data integrity Protocols Viruses and worms
Auditing and intrusion detection Commercial and industrial security
Security and other critical system properties Distributed systems

INSTRUCTIONS TO AUTHORS:

Send six copies of your paper and/or proposal for a panel session to John Rushby, Program Co-Chair, at the address given below. Papers and panel proposals must be received by November 15, 1993. Papers, which should include an abstract, must not exceed 7500 words. The names and affiliations of the authors should appear on a separate cover page only, as a ``blind'' refereeing process is used. Authors must certify prior to December 31, 1993 that any and all necessary clearances for publication have been obtained.

Papers must report original work that has not been published previously, and is not under consideration for publication elsewhere. Abstracts, overlength papers, electronic submissions, late submissions, and papers that cannot be published in the proceedings will be rejected without review. Authors will be notified of acceptance by February 1, 1994. Camera-ready copies are due not later than March 15, 1994.

Panel proposals should describe, in two pages or less, the objective of the panel and the topic(s) to be addressed. Names and addresses of potential panelists (with position abstracts if possible) and of the moderator should also be included.

The Symposium will also include informal poster sessions where preliminary or speculative material, and descriptions or demonstrations of software, may be presented. Send one copy of your poster session paper to Cristi Garvey, at

the address given below, by January 31, 1994, together with certification that
any and all necessary clearances for presentation have been obtained.

PROGRAM COMMITTEE

Ross Anderson, Cambridge University, UK
Tom Berson, Anagram Laboratories, USA
Leslie Chalmers, Bank of California, USA
Oliver Costich, CSIS, George Mason University, USA
Frederic Cuppens, ONERA/CERT, France
James Gray, University of Science & Technology, Hong Kong
Sushil Jajodia, George Mason University, USA
Dale Johnson, MITRE Corporation, USA
Steve Kent, BBN, USA
Sue Landauer, Trusted Information Systems, USA
Teresa Lunt, SRI International, USA
John McHugh, Portland State University, USA
Doug McIlroy, AT&T Bell Labs, USA
John McLean, Naval Research Laboratory, USA
Jon Millen, MITRE Corporation, USA
Sylvan Pinsky, National Security Agency, USA
Michael Reiter, AT&T Bell Labs, USA
Karen Sollins, MIT Laboratory for Computer Science, USA
Stuart Stubblebine, University of Southern California, USA
Gene Tsudik, IBM Research Laboratory, Switzerland
Yacov Yacobi, Bellcore, USA
Raphael Yahalom, Hebrew University, Israel

For further information concerning the symposium, contact:

Cristi Garvey, General Chair   John Rushby, Program Co-Chair
TRW, MS R2-2044   SRI International, EL254
One Space Park   333 Ravenswood Avenue
Redondo Beach, CA 90278, USA   Menlo Park, CA 94025, USA
Tel: +1 (310) 812-0566   Tel: +1 (415) 859-5456
FAX: +1 (310) 812-4310   FAX: +1 (415) 859-2844
Garvey@zoo.sdd.trw.com   rushby@csl.sri.com

Carl Landwehr, Vice Chair   Catherine Meadows, Program Co-Chair
Naval Research Lab., Code 5542   Naval Research Laboratory, Code 5543
4555 Overlook Ave., SW   4555 Overlook Ave., SW
Washington DC 20375, USA   Washington DC 20375, USA
Tel: +1 (202) 404-8888   Tel: +1 (202) 767-3490
FAX: +1 (202) 404-7942   FAX: +1 (202) 404-7942
landwehr@itd.nrl.navy.mil   meadows@itd.nrl.navy.mil

Frederic Cuppens, European Contact James Gray III, Asia/Pacific Contact
ONERA/CERT   Department of Computer Science
2 Avenue E. Belin   Hong Kong Univ. of Science & Technology
31400 Toulouse, France   Clear Water Bay, Kowloon, Hong Kong
Tel: +33 61 55 70 75   +852 358-7012
FAX: +33 61 55 71 32   +852 358-1477
cuppens@tls-cs.cert.fr   gray@cs.ust.hk

---snip here---

Obtaining the Call For Papers for the
1994 IEEE Symposium on Security and Privacy
by anonymous ftp

The CFP is available from ftp.csl.sri.com--note the ftp on the
front--(192.12.33.94) in directory /pub in the following forms

Plain Ascii text: sec-priv94.txt

Single-page for US-size (8.5x11) paper

LaTeX source:	sec-priv94.tex
LaTeX output:	sec-priv94.dvi (needs binary transfer)
Postscript:	sec-priv94.ps

Single-page for A4-size paper

LaTeX source:	sec-priv94-a4.tex
LaTeX output:	sec-priv94-a4.dvi (needs binary transfer)
Postscript:	sec-priv94-a4.ps

Two pages, big font, suitable for faxing

LaTeX source:	sec-priv94-big.tex
LaTeX output:	sec-priv94-big.dvi (needs binary transfer)
Postscript:	sec-priv94-big.ps

Send questions or problems to John Rushby (rushby@csl.sri.com).

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 83

Monday 16 August 1993

Contents

Dorney Park Hercules roller coaster injures 14

"Steve Walker via Peter G. Neumann" <neumann@csl.sri.com>
Mon, 16 Aug 93 18:48:54 PDT

On July 18 at Maryland's Dorney Park, an occupied train on the Hercules roller coaster ran into an empty train outside the loading platform, injuring 14 passengers. The trains operate with no brakes for the 1 minute and 50 second ride; once they leave the station are free-wheeling when not being towed uphill. A faulty sensor was blamed, which was supposed to detect the train leaving the station, which in turn would enable the computer system to release the restraints on the empty train so that it could move into the loading area.

Three new safety measures will be added.

* A backup sensor will be added where the first one failed. (Strangely, the

present sensor is the only one that did not have a backup.)

* The control panel will be modified to display all trains on the track.

* A manual brake will be added.

The temporary fix is to operate only one train on the track. [From an article by Chuck Ayers, *The Morning Call*, July 28, 1993, p. B5, sent to RISKS by Steve Walker.]

This accident sounds remarkably similar to the accident on the Timber Wolf roller coaster at Worlds of Fun in Kansas City, on March 31, 1990. The nature of the accident and the fixes were essentially the same! See RISKS-9.96.

About 'Terminal Compression'

"Tansin A. Darcos & Company" <0005066432@MCIMAIL.COM>
Sun, 15 Aug 1993 03:29:55 -0400 (EDT)

A company (Inter Pact) has run a number of advertisements on the Internet regarding their book 'Terminal Compression' which has been subsequently released in text form which can be downloaded via FTP, with the idea that if you read it you will send them a shareware donation. I probably would never have read the book if it hadn't been made available that way.

The copyright slugs on the text indicate publication years of 1991-1993, seemingly indicating a recently issued book. (One of the items in the book is the mention of the new E-Mail address for the White House, which was only created this year.)

The book has a number of holes in it which I could see through and I decided to comment. A shorter version of this message has gone to the Telecom Digest.

The book deals with the combined issues of some of the dangers of technology and the threats to the privacy of individuals, I have therefore posted this review to both the Risks List and the Privacy List.

I will mention one hole which is so obviously inaccurate as to be ridiculous: A government agency gets a court order telling the newspaper in the story, "The New York City Times" (note: not 'The New York Times' but the article makes clear that the paper on Sunday is '34 pounds') to not print any articles dealing with the ability to read CNG emissions (this is the leakage off a computer or monitor which can be read like a radio transmitter from a distance by electronic equipment.) A reporter writes an article from research, and an agency gets a prohibition not just against that article - which is a dubious issue to get a prior restraint order against in the absence of use of government material, anyway - but that this court order is not to stop a particular article, but to completely prohibit any articles regarding that particular *subject*! I've never heard of a judge that would even consider issuing that type of order, (an appeals court would tear him to shreds) and this assumes the paper wouldn't (1) print the article anyway and risk a contempt citation (2) print a _blank_ article and a copy of the court order. Apparently this order was never publicized; any time a government agency tries to suppress publication of something in a newspaper it usually makes _national_ headlines; the press takes threats to the 1st Amendment *very* seriously. CNN's use of the Noriega Tapes comes to mind, and, of course, the Pentagon Papers and the A-Bomb schematics cases.

Without intending to spoil the story, I wanted to point out that it mentions only AT&T as the national long distance carrier; a deafening silence exists about MCI and Sprint. Yet later in the book it mentions 'FTS-2000' the private network for government telephone calls that MCI has unsuccessfully been fighting ever since 1/2 went to AT&T and 1/2 went to Sprint, from the time of its creation.

At a point in the book, it mentions that the National Security Agency (NSA) uses its massive computer arrays to monitor - in real time - every telephone call connection made in the U.S., e.g. every dial call from and to any point and the call being forwarded, and to where. This seems to forget that despite there being some 200+ service points (called LATAs in the trade) in the U.S. where every call has to go into or out of, not to mention the private cellular carriers, plus local call forwarding setups and call forwarding through PBXs. Plus private cellular companies, trunked mobile radiotelephone companies, ham radio patches...

Even in the book it mentions that one of the calls made by some of the criminal elements in the book went to 'a Canadian Cellular Exchange'. I find it hard to believe that a Canadian telephone company is going to let a U.S. government agency inquire into its phone system without a court order issued by a Canadian judge. Is Pacific Bell going to allow someone from the Canadian Department of Revenue or Scotland Yard have the list of who owns what non-listed number without a U.S. Court Order? I think not. (I'll skip over the possibility of bribery for now.)

I find it a bit far fetched to believe that it is possible to put a 'pen register' on every telephone call made in the United States. If I call into General Electric's PBX in New York, or Northrop's in Los Angeles, is a call transferred out of it (one of perhaps 100 that go out at any minute) mine or someone else's?

Also, in the story it notes that voice, fax or data transmissions are detected and that encrypted ones are 'red flagged'. This is a crock. Bits are bits; there is no way to tell based on the bit stream going through a data call whether the Zmodem Binary transfer I make is a ZIP archive, an EXE file, a binary data file, a Word Perfect file, or a binary file which has been processed with PGP or RIPEM. Bits are Bits; there is no means to differentiate between a compressed, encrypted transmission (such as a file processed with PGP) and a binary data file. It could be possible due to echo cancellers to tell if someone is using a data transmission device; whether a fax or modem detection is possible is another thing. And it also assumes someone doesn't switch to a non-standard method of data transmission such as combined voice and data on a compressed transmission channel. Or local calls to non-telephone networks such as Compuserve. Or private long distance companies that don't use Feature Group service, but simply buy commercial inward lines in some cities and lease dedicated trunk space.

The virus issues are a little ridiculous too. Now a couple of years ago a man named William Harrison, I think, wrote a book called 'virus'. With the same basic idea: a series of rogue computer programs can be used to allow someone to commit crimes. Harrison's book was much better: I've had more than 12 years of computer experience as well as extensive use of MSDOS and there wasn't *a single* technical mistake in Harrison's book.

The virus issues are rather silly. For one thing, unless someone is careless on large machines, you can't create viruses for VMS or IBM mainframes; they have fully operational supervisor state protection against runaway programs. It might be possible to damage some data in some files if you contaminated them, but in general the kind of virus problems that are reported on PCs because every program that runs on a PC runs with unlimited privilege.

One of the viruses is mentioned that it fries the printer port and "causes smoke, then while the user checks that, damages the disk drive". Now, I know it's possible on very old Hercules cards to program them wrong and damage them, and some IDE drive cards have errors in them and miscommanding them could damage the card or the disk (due to errors in the design.) This one, however, is a little hard to believe.

I have said it many times: the only reason that viruses can even exist is because the operating system does not use the memory and task protection hardware built into every Intel x86 processor higher than the 80186. A criminally negligent practice, I would say. A person I know claims there are bugs in the 80286 task protection hardware, which I find hard to believe. In any case, 80386 hardware contains working task protection capability. If viruses became so serious that it was necessary to worry about them, it would be not too difficult to release the equivalent of the IBM VM/370 operating system for PCs: at the 80386 level, everything runs in user-mode protection and does not have of I have said it many times: the only reason that viruses can even exist is because the operating system does not use the memory segmentation and task protection hardware built into every Intel x86 processor higher than the 80186. A person I know claims there are bugs in the 80286 task protection hardware, which I find hard to believe. In any case, 80386 hardware contains working task protection capability. If viruses became so serious that it was necessary to worry about them, it would be not too difficult to release the equivalent of the IBM VM/370 operating system for PCs: at the 80386 level, everything runs in user-mode protection and does not have kernel privileges. It can refuse all disk I/O except from the ROM BIOS, any attempt to access any I/O ports is refused. Without that access - which requires privilege - a program cannot do damage and can't get access to the system. A user could well trust a program and allow it access to the screen ports. And the protection program could either allow certain access directly or trap access and emulate it. So there would be no means to get access to the disk drive hardware and no means to attach to other files. The hardware doesn't permit access without permission.

If you don't want the story spoiled, do not read this paragraph. At the end of the story, a character responsible for some of the problem meets with the Director of the NSA and we find out that the attacks were intentional with the knowledge of the NSA Director, to cause the country to increase security on its computers. Then, after the director speaks to the person, he has him arrested. Now, it's one thing to 'burn' one of your own people, but nobody is stupid enough to put someone involved with a covert agency in a public trial where he can - as a legitimate defense - expose an agency's dirty laundry. The argument of 'National Security' won't wash in a criminal case; if the defense has evidence that will exonerate it, it is entitled to present it, and if the government requires it to be suppressed, the court will dismiss the criminal complaint. If the man was tried in a secret trial or a military court where it could be hushed up, that's one thing: but a public trial in open court in these type of circumstances is hard to believe.

My sister is of the opinion that people don't notice technical errors in books, movies and TV shows. I do and I'm certain other people do, too.

Paul Robinson - TDARCOS@MCIMAIL.COM

Ghost in the machine

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
16 Aug 93 11:53:34 EDT

"Phone malfunction sends out 911 call."
Associated Press: Syracuse, NY.
Globe & Mail / Canada / 14 Aug 93, p. A7 [Summarized by MK]

The owner of a cordless phone was rudely awakened by police after his phone sent out a 911 call all by itself. AT&T spokesperson Steven Emery explained that older (> 5 years) cordless phones can accidentally pick up random frequencies and generate dial tones as a result. In this case, the tones happened to be 9, 1 and 1. The emergency response centre recorded the call and traced the address through the phone company.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

clusters and electromagnetism

Phil Agre <pagre@weber.ucsd.edu>
Thu, 10 Jun 1993 17:56:17 -0700

An article by Kenneth R. Foster <kfoster@eniac.seas.upenn.edu> in RISKS-14.70 surveys some literature on clusters of illness that have been associated with VDT use. Without wishing to question the author's integrity or methods, it might be useful to consider the point of view of the people who actually find themselves becoming statistics in a similar way. Paul Brodeur's article "The Cancer at Slater School" in the New Yorker (12.7.92, pages 86-119) is a very long and detailed account of the travails suffered by a group of elementary school employees who found themselves dying of cancer at a frightening rate. They suspected that the high-tension power lines running along the school playground might have something to do with it, and they called in the power company to help them investigate. The story concerns the astonishing lengths to which the power company, principally through the agency of fully accredited

scientists, went to stonewall, delay, obfuscate, and declare "inconclusive"
the study of these poor people. Granted that many in the relevant industries
revile Mr. Brodeur, nonetheless if his tale is even faintly representative
of the studies surveyed by Dr. Foster then I despair for the health both of
science and of everyone else.

Phil Agre, UCSD

Re: SKIPJACK Review

Brandon S. Allbery <bsa@kf8nh.wariat.org>
Wed, 11 Aug 93 12:28 EDT

>... Such devices would provide high quality cryptographic security
>without preserving the law enforcement access capability that distinguishes
>this cryptographic initiative. ...

Which, even to a non-crypto expert like myself and given that SKIPJACK is not the only foreseeable "high quality cryptographic security" algorithm, will only have the intended effect if all other cryptographic systems are banned; while you would lose the ability to talk to SKIPJACK-equipped devices, you could still communicate *without* using SKIPJACK and allow some other device or software program to perform the encryption/decryption.

Considering the current Congressional review revealing misuse of the NCIC database (mentioned in the following digest article by Peter Wayner), I see some other problems as well. The proposed key escrow system involves encrypting the escrowed keys in such a way that they can only be decrypted by LEAF devices, and therefore the escrow agencies will require access to LEAF devices to examine their own escrowed key lists. I see two problems with this:

(1) How are *these* keys encrypted? If the encryption algorithm is subject to exhaustive or "shortcut" searches, the keys may as well be in plaintext. If they are encrypted using SKIPJACK, we have either a chicken-and-egg situation or a back door to avoid the need to obtain keys from the key escrow agencies (just feed a LEAF device the conversation *as an encrypted key* and see what it comes back with).

(2) The only protection against the escrow agency decrypting its escrowed key list is to keep the agency from obtaining a LEAF device. I dare say there are ways around this, such as the one (also mentioned in Wayner's submission) of a less-than-honest policeman obtaining a LEAF device and "loaning it out". This is somewhat mitigated by the fact that the escrowed key is only useful when combined with the corresponding key from the other escrow agency, but is still a potential source of problems.

Brandon S. Allbery   kf8nh@kf8nh.ampr.org   bsa@kf8nh.wariat.org

Clipper & French key escrow

"Richard Schroeppel" <rcs@cs.arizona.edu>
Wed, 11 Aug 1993 11:30:57 MST

Peter Wayner's report on the Clipper system included the bone-jarring sentence:

> We know that the government of France is widely suspected
> of using its key escrow system to eavesdrop on US manufacturers in France.

I was under the (obviously naive) impression that the Clipper system was the first seriously proposed use of key escrow. Now I discover that France is using key escrow, right now, today. The French experience might be relevant to our own discussion. Could someone provide more information?

Rich Schroeppel rcs@cs.arizona.edu

Privacy Digests

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 16 Aug 93 18:49:15 PDT

Periodically I remind you of TWO useful digests related to privacy, both of which are siphoning off some of the material that would otherwise appear in RISKS, but which should be read by those of you vitally interested in privacy problems. RISKS will continue to carry higher-level discussions in which risks to privacy are a concern.

* The PRIVACY Forum Digest (PFD) is run by Lauren Weinstein. He manages it as a rather selectively moderated digest, somewhat akin to RISKS; it spans the full range of both technological and non-technological privacy-related issues (with an emphasis on the former). For information regarding the PRIVACY Forum, please send the exact line:

information privacy

as the BODY of a message to "privacy-request@vortex.com"; you will receive a response from an automated listserv system. To submit contributions, send to "privacy@vortex.com".

* The Computer PRIVACY Digest (CPD) (formerly the Telecom Privacy digest) is run by Dennis G. Rears. It is gatewayed to the USENET newsgroup comp.society.privacy. It is a relatively open (i.e., less tightly moderated) forum, and was established to provide a forum for discussion on the effect of technology on privacy. All too often technology is way ahead of the law and society as it presents us with new devices and applications. Technology can enhance and detract from privacy. Submissions should go to comp-privacy@pica.army.mil and administrative requests to comp-privacy-request@pica.army.mil.

There is clearly much potential for overlap between the two digests, although contributions tend not to appear in both places. If you are very short of time and can scan only one, you might want to try the former. If you are interested in ongoing detailed discussions, try the latter. Otherwise, it may well be

appropriate for you to read both, depending on the strength of your interests
and time available.

PGN

PDCS2 Open Workshop

Louise Heery <l.m.heery@newcastle.ac.uk>
Mon, 16 Aug 1993 10:17:56 GMT

[Apologies to those of you who have already seen this.]

Please find below the programme for the PDCS2 September Open Workshop, being held at LAAS-CNRS, Toulouse, 21 - 23 Sept. '93, together with a registration form. All attendees are subject to the registration fee unless specifically told otherwise.

Additional information such as hotels and maps of LAAS will be forwarded upon receipt of completed registration forms, which should be returned to me NO LATER THAN 10 September '93. However, as individuals are responsible for making their own hotel reservations, I would advise you to reply sooner so that I will then be able to send you a list of recommended hotels. Please also note that the number of places available at the workshop are limited and that I will, therefore, be working on a first-come-first-served basis with regard to receipt of registrations.

Regards,
Louise Heery

| PDCS2 Administrative Co-ordinator |
| Dept. of Computing Science, |
| Claremont Tower, |
| University of Newcastle upon Tyne, NE1 7RU |
| Tel: +44/091-222-7948 Fax: +44/091-222-8232 |
| E-mail: l.m.heery@newcastle.ac.uk |

PDCS2, as its acronym implies, aims to build on, and take significantly further the work of ESPRIT Basic research Action 3092, Predictably Dependable Computing Systems (PDCS), on the problems of making the process of designing and constructing adequately dependable computing systems much more predictable and cost-effective than at present. In particular it will address the problems of producing dependable distributed real-time systems and especially those where the dependability requirements centre on issues of safety and/or security. The planned programme of research concerns a number of carefully selected topics in fault prevention, fault tolerance, fault removal and fault forecasting. The work to be done ranges in nature from theoretical to experimental; in a number of cases it involves the acquisition or implementation, in prototype form, of software tools, and their experimental interconnection.

OPEN WORKSHOP TIMETABLE - TUE. 21 - THUR. 23 SEPT. '93.

Tuesday 21 Sept.

8.30-9.30:
REGISTRATION AND COFFEE
9.30-10.30:
Welcome: Alain Costes (10 mins)
PDCS OVERVIEW AND WORKSHOP
Introduction: Brian Randell (50 mins)
COFFEE
11.00-12.30:
REAL TIME FAULT TOLERANCE
Moderator: Alan Burns (University of York, York, UK).
Speakers: (1) Johannes Reisinger, "Real-time Interprocess Communications in MARS" (Technische Universitat, Vienna, Austria);
(2) Andrea Bondavalli, "Adaptable Fault Tolerance for Real-Time Systems" (CNR, Pisa, Italy).
LUNCH
14.00-15.30:
OBJECT-ORIENTED FAULT TOLERANCE
Moderator: Lorenzo Strigini (CNR, Pisa, Italy).
Speakers: (1) Jean-Charles Fabre, "Fault and Intrusion Tolerance in Object-oriented Applications by Fragmentation-Redundancy-Scattering" (LAAS-CNRS, Toulouse, France in conjunction with University of Newcastle, UK);
(2) Robert Stroud, "Object-oriented Techniques for Realising Fault Tolerance in Software" (University of Newcastle upon Tyne, Newcastle upon Tyne, UK).
COFFEE
16.00-17.30:
DEMONSTRATIONS

Room 1	Room 2	Room 3
Demo A	Demo C	Demo D
Demo B	Demo C	Demo D

Wednesday 22 Sept.
9.00-10.30:
INDUSTRIAL INVITED SPEAKERS:
Moderator: Alain Costes
Speakers: (a) Marc Guillemont (Chorus Systemes)
(b) Malcolm Mills (Software Sciences Limited)
(c) Peter Knezu (ALCATEL Austria)
COFFEE
11.00-12.30:
SECURITY ASSESSMENT
Moderator: Yves Deswarte (LAAS-CNRS, Toulouse, France).
Speakers: (1) Bev Littlewood & Tomas Olovsson, "A Pilot Experiment in the Modelling of Operational Security" (CSR, City University, London, UK and Chalmers University of Technology, Goteborg, Sweden);
(2) John McDermid, "Developing Secure Systems in a Modular Way" (University of York, York, UK).
LUNCH
14.00-15.30:
FAULT INJECTION
Moderator: Hermann Kopetz
Speakers: (1) Eric Jenn, "Fault-injection into VHDL Models: The MEFISTO Tool" (LAAS-CNRS, Toulouse/Chalmers University of Technology, Goteborg);

(2) Johan Karlsson, "Validation of the MARS System by Physical Fault
Injection," (Chalmers University of Technology, Goteborg).
COFFEE
16.00-17.30:
DEMONSTRATIONS
Room 1 Room 2 Room 3
Demo A Demo B Demo C
Demo A Demo B Demo D

Thursday 23 Sept.
9.00-9.30:
TESTING
Moderator: Tom Anderson (University of Newcastle upon Tyne, Newcastle
upon Tyne, UK)
Speakers: (1) Pascale Thevenod, "Functional Testing of Critical Software:
Formal and Statistical Approaches; A Case Study" (LAAS-CNRS, Toulouse and
LRI-Universite de Paris-Sud, France);
(2) Werner Schuetz, "A Statistical Approach for Testing the Execution Time
of Program Units" (LAAS-CNRS, Toulouse, France and Technische Universitat,
Vienna, Austria).
COFFEE
11.00-12.30:
SOFTWARE RELIABILITY EVALUATION
Moderator: Karama Kanoun (LAAS-CNRS, Toulouse, France).
Speakers: (1) Mohamed Kaaniche, "Discrete-time Software Reliability
Modelling and Evaluation" (LAAS-CNRS, Toulouse, France);
(2) Sarah Brocklehurst & David Wright,"General Methods for the Improvement
of Software Reliability Predictions" (City University, London, UK).
LUNCH
14.00-15.30:
ACADEMIC INVITED SPEAKERS AND CONCLUSION
Moderator: Jean-Claude Laprie
Speakers: (a) Jack Stankovic (University of Massachusetts)
(b) John Meyer (University of Michigan)
Closing Address: Jean-Claude Laprie (20 mins)
================
END OF TIMETABLE
================

DEMONSTRATIONS
A> "Object Oriented Fragmentation/Redundancy/Scattering" (University of
Newcastle upon Tyne, Newcastle upon Tyne, UK and (LAAS-CNRS, Toulouse,
France).

A distributed Electronic Diary system which has been designed using Eiffel design tools and implemented on top of the DELTA-4 Support Environment will be demonstrated. The system uses fragmentation-redundancy-scattering to provide means of achieving high reliability and security by tolerating both accidental faults and intentional intrusions.

B> R. Schlatterbeck, "Tool Integration by CDL" (Technische Universitat,
Vienna, Austria);

In the first phase we will explain the purpose, the structure and the
operation of CDL using a set of pictures. In the second phase we will
demonstrate the prototype implementation of our CDL tools.

C> "Analysis of Predictive Accuracy and Recalibration of Reliability Growth
Predictions" (City University, London, UK);

Some real software failure data will be analysed using reliability growth
models, an analysis of the accuracy of the resulting reliability
predictions, and their recalibration, will be conducted.

D.G. Leber, "Single Board Computer with High Error Coverage" (Technische
Universitat, Vienna, Austria);

Presentation of a single board computer with high error detection coverage:
We will explain the special mechanisms within the hardware and the
operating system of the new MARS nodes which are responsible for realizing
both the fail-silence property and a predictable timing behaviour

REGISTRATION FORM:
Fee 1800 FF (inclusive of VAT)

Last Name:____

First Name:____

Title: Prof/Dr/Mr/Ms/Mrs/Miss/Other:_________________

Address:____

____

____

Tel:_________________ Fax:_________________ E-mail:____________________

Delete as applicable:
Please reserve a place for me at the Open Workshop YES/NO
Date of arrival:____/09/93

Please add my name to the PDCS2 Technical Report mailing list YES/NO

I will attend the banquet dinner: Yes/No
I am vegetarian: Yes/No

Please indicate preferred method of payment (delete all methods EXCEPT the
method of payment chosen):
Fee 1800 FF (inclusive of VAT)

Bank Transfer:
(I will send out the details necessary for this upon receipt of
registration)
OR
French Bank cheque to the order of ADERMIP

OR
Order form for invoice
OR
Credit Card: Visa/Mastercard/ EuroCard
OR
On site payment by cash/credit card

Return form, to arrive no later than 10 September 1993, to: Louise Heery,
PDCS2 Administrative Co-ordinator, Department of Computing Science,
University of Newcastle upon Tyne, Newcastle upon Tyne, NE1 7RU, UK.
Fax: +44/091-222-8232; e-mail: l.m.heery@newcastle.ac.uk

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 82

Tuesday 17 August 1993

Contents

RISKS-14.83!!! and RISKS-%&#@!!

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 17 Aug 93 10:41:59 PDT

For those of you who wondered where RISKS-14.82 was when you saw RISKS-14.83, this is it. In one of the wonders of modern technology, RISKS-14.82 appears AFTER RISKS-14.83. This was unintentional, but Steve Smoliar pointed out to me that it offsets the fact that there were two different issues of Info-mac yesterday with the same issue number (vol 11, issue 110?), somehow preserving karmic parity. Perhaps it all comes out in the wash, but it seemed appropriate for me to quickly put out RISKS-14.82 to stave off further requests for the supposedly missing issue. (Surprisingly, I have had only one such request thus far this morning, from Jerry Leichter.)

Incidentally, the level of BARFmail and other addressing problems has been excruciating lately. The following all seem to be escalating in frequency:

 * Requests from E-mail addresses for which my answer is rejected by the
   originating host!
 * E-mail addresses that worked yesterday but not today, but then might
   work again tomorrow or some time in the future!
 * Requests to reinstate subscribers who think they were dropped from the
   list, where they had in fact been sent mail for weeks or months --- but
   their hosts had been merrily accepting their mail without actually
   delivering it or notifying anyone of nondelivery!
 * BITNET in general.

PGN

Re: Dorney Park Hercules roller coaster injures 14

Scott Walker <walker@eplrx7.es.duPont.com>
Tue, 17 Aug 1993 12:33:37 -0400 (EDT)

> Maryland's Dorney Park
          ^^^^^^^^^^
This park is actually in Allentown, Pennsylvania. Quite a ride, too!

  [Steve Walker's original item was a clipping from a very local
  newspaper that did not identify its city or state. I interpolated a
  mis-extrapolation. Sorry. Bad idea in general anyway. PGN]

Re: Surprise! contained in tar file (RISKS-14.81)

David Wittenberg <dkw@cs.brandeis.edu>
Tue, 17 Aug 1993 12:49:11 -0500 (EDT)

In Risks 14.81 Olaf Titz warns us that tar keeps information which can identify the person who tarred the file. I've seen two other simple failures of anonymous posting, the first a software "feature", the second a human's misunderstanding.

Many newsreader programs automatically include a .signature file in all postings. I've seen such files appear in what were supposed to be anonymous postings. Apparently the user didn't realize that he had to rename his .signature file or it would be appended to his message.

The other was a system where a few people offered to post messages anonymously if you sent them email. In one case, someone sent a message reading "Please post this anonymously. Thanks, John". The woman who posted it didn't notice that John had signed his note, so when she posted it, there was almost no doubt who it had come from.

The point here is that we usually spend a lot of effort insuring that the appropriate person gets credit for something. As a result, we leave "signatures" of various sorts scattered widely. It's very hard to make sure that we've removed all of them.

--David Wittenberg dkw@cs.brandeis.edu

Re: Terminal compression (Robinson, RISKS-14.83)

<csvcjld@nomvst.lsumc.edu>
17 Aug 93 06:41:24 -0700

>Also, in the story it notes that voice, fax or data transmissions are
>detected and that encrypted ones are 'red flagged'. This is a crock.
>Bits are bits; there is no way to tell...

If the bytes are uniformly distributed, there is a good chance they are encrypted.

[But NOT NECESSARILY. A simple compression code such as a Huffman code encodes into a random string of bits if the source text is chosen independently. But then, there would be no compression if there was not contextual dependence in the first place, so simplifications are tricky. PGN]

Terminal Compromise (Robinson, RISKS-14.83)

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
17 Aug 93 13:45:40 EDT

The book is entitled TERMINAL COMPROMISE.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Re: Clusters and electromagnetic fields

Kenneth R Foster <kfoster@eniac.seas.upenn.edu>
Tue, 17 Aug 93 14:15:34 -0400

I briefly respond to the recent posting by Phil Agre.

The posting that he referred to was my article on reproductive risk and use of VDTs, from _Phantom Risk_, MIT Press, June 1993. The clusters I discussed were reported clusters of miscarriage among women users of VDTs, that were reported around 1980. As I argue, the dozen epidemiologic studies that were performed in the decade following (virtually all negative) shows that the clusters were almost surely chance events, with no indication of reproductive risks from VDTs.

Mr. Agre brings up a totally different issue -- reports of clusters of childhood among California schoolchildren, as described in a _New Yorker_ article by Paul Brodeur. I had not previously expressed any opinion about this in my posting to this newsgroup and I object to Mr. Agre's inferring that I did.

For what it is worth, here are my comments on the issue.

Mr. Agre brings up a totally different issue, clusters of cancer cases in California schools supposedly associated with high power lines, as publicized by Paul Brodeur. Without offering any opinion about Brodeur or his motives, I note that the interpretation of these observed clusters is very unclear, far more so than he indicated in Brodeur's _New Yorker_ articles on the subject. The interpretation of "clusters" has been well discussed in the epidemiologic literature; whole issues of epi journals have been devoted to the matter. The question is not whether some kids in school near power lines got cancer (there are lots of kids in California schools, and invariably some of them will get cancer), but whether going to a school that is located near a power line conveys higher risk of childhood cancer. A few isolated cases does not allow one to draw any inferences one way or the other. Ray Neutra, a highly respected epidemiologist with the State of California, has investigated these clusters (of childhood cancer in California schools) and found no indication of any link with power lines. Given the large number of California schoolchildren, one would expect several "clusters" like those Brodeur reported every year, by chance alone.

For a good discussion how an epidemiologist would investigate a report of a cluster (and many clusters of various kinds are reported to health officials around the country, alleging all sorts of things) I refer you to a special issue on clusters published in (I recall) the American Journal of Epidemiology about 2 years ago.

I note that Brodeur also described the clusters of miscarriage among women VDT users in his _New Yorker_ articles, but gave neither a fair assessment of the difficulties of interpreting them, nor a fair and complete survey of the relevant epidemiological studies.

Gripen crash: pilot's view

Martyn Thomas <mct@praxis.co.uk>
Tue, 17 Aug 1993 10:34:15 +0100 (BST)

Flight International today quotes the pilot of the Gripen FBW fighter that crashed at the Stockholm display.

"It was like sitting on a big ball feeling like you're sliding off it. When I entered the turn, the computer overcompensated by roughly 10 degrees. When I then straightened out the aircraft, I got an undemanded pitch oscillation and, when I tried to compensate for that one, the aircraft kind of sat down and became impossible to control." He described the feeling of loss of control as being ".. like butter on a hot potato".

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk Fax: +44-225-465205

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 84

Tuesday 17 August 1993

Contents

Re: BARFmail and other list headaches (PGN in RISKS-14.82)

"Dennis G. Rears" <drears@Pica.Army.Mil>
Tue, 17 Aug 93 15:46:22 EDT

I guess you can say that one risks of BARFmail is that if it gets to a
certain point, volunteers will just say no.
 I run an exploder list for RISKS for all U.S. military and government sites.
I also run the mail list for the Computer Privacy Digest. In each case I have
seen an increasing amount of BARFmail, broken mailers, people with improper
addresses, and general incompetence among many postmasters.
 I use to spend 15-45 minutes a week in mail list maintenance. Now it
is close to three hours a week. With every Risks Digest that is sent out
I get back 3-4 error messages; with the Computer Privacy Digest, I get

about 10.

As a subscriber,

o You should ensure that you have enough space in your mailbox for the lists
  that you subscribe to.

o If you domain address changes, please let us know.

o If your account is canceled, please let us know.

The system administrator as part of his job should ensure that:

o All outgoing mail is stamped properly so that replies can be sent back.

  - Several times a month I get add requests from <name@host>
  as opposed to <name@host.domain>. I have to go through the
  received lines to get a valid email address.

o Send rejected mail to the right place:

  - It should go to the Errors-To, Reply-to, List-request
  address. I had to stop my notification service front the CPD
  thanks to a badly configured mailer.

o There are military machines that use subhosts, which is
   in violation of RFC 822. I have to source route these
   (name%subhost@realhost) in the mail list. I am talking about
   the Sperry hosts that a lot of military sites use. These
   STILL DON'T use DNS aka nameservers.

dennis

[I am exceedingly grateful to Dennis, who handles .mil and .gov
RISKS traffic for me, and also to Lindsay.Marshall@newcastle.ac.uk
who provides a similar indirection service for RISKS readers in the
U.K. Anything you can do to make their lives and mine simpler with
respect to E-mail addresses would be greatly appreciated. PGN]

Prototype voice-operated ATM

Malcolm Butler <malb@ee.uts.edu.au>
Mon, 16 Aug 93 1:25:39 EST

[RISKS readers may be interested in the following report from The Sydney
Morning Herald, August 13, 1993). Malcolm Butler (malb@ee.uts.edu.au)]

Your word is my command: ATM

Researchers at the University of Queensland unveiled yesterday a prototype of
what they say is the first voice-activated automatic teller machine (ATM).

But in an embarrassing moment during a media demonstration, a mock ATM
incorrectly accepted the voice od a female journalist and allowed her to
gain access to the "funds" of a male researcher.

It was quickly pointed out that the machines accuracy would improve with
fine-tuning and that security was the opposite of convenience. A second
imposter who tried to con the machine was unsuccessful. All he could
extract from it was a wicked cackle.

The system uses the new technology of artificial neural networks ... It
verifies customers' identities by comparing their voices with samples
that have been stored on a computer.

This aural equivalent of a fingerprint is good news for those who have trouble
remembering their personal identification numbers but, unfortunately, the
system, still has a few glitches. It accepts 10 per cent of imposters,
rejects 1 per cent of true customers and may not be sympathetic if you have a
cold, are drunk, or your voice sounds different.

``It may turn out that it would be a good idea for you to go in sometime and
leave a voice sample when you have a cold so that it can recognise you when
you are in that situation," said one of the project's researchers, Professor
Tom Downs.

[...] The researchers say the system could also be used for credit card or
banking transactions by telephone and for allowing entry into restricted
buildings. Their next project will be to develop a system which allows free
conversations between ATMs and customers.

Professor Downs said several voice-verification systems had been developed
overseas but were relatively unsophisticated.

Filling Station Ripoff

Matt Healy <matt@wardsgi.med.yale.edu>
Fri, 30 Jul 1993 00:45:52 GMT

On Thursday afternoon, 29 July, WCBS Radio (NYC) broadcast an interview with a
city official about a new scam: modifying the circuit board of a gas pump
controller so the pumps will deliver less gasoline than indicated by the
display.

He characterized this as "just old fashioned cheating, using new technology."
In one case, his inspector discovered that the pump delivered about 5 gallons
while indicating 7 gallons.

He said his department will be stepping-up inspections, but of course they
cannot check every filling station at once! He advised motorists to keep
records of gas purchases and odometer readings, and report any suspicious
sales immediately. He said several offenders have already been caught in this
manner--an alert citizen noticed the short delivery amounts.

Matt Healy matt@wardsgi.med.yale.edu   Dept of Genetics (WardLab-SHM I-148)
          333 Cedar Street   NEW HAVEN, CT 06510

President Clinton's Tax Plan

"Richard Schroeppel" <rcs@cs.arizona.edu>
Tue, 17 Aug 1993 11:28:11 MST

With the passage of the new budget, the IRS has shifted into high gear. One provision of the bill imposes the higher rates retroactively to Jan 1.

Last Thursday night (Aug 12) our local TV news did a story about a Tucson small-businessman who received a tax bill for $72G. They showed the bill, it looked real, including low order digits, properly placed commas & decimal point, etc. Apparently the man was a real slacker; about half the amount was for interest & penalties. The IRS had no immediate comment, but apparently this man was not the only recipient of such a bill.

Now it seems to me, that if this guy & his five friends would just pay their fair share, instead of whining to the media, we'd have this deficit thing licked in no time. Way to go, Prez!

The RISK here should be apparent to all programmers: When laying out your printed forms, be sure to allow extra space in the numeric fields. Always use double precision for money amounts. It's stupid to have a program break just because some intermediate value is unexpectedly large, or to not have room on the form for a big amount. The constants for interest rates & penalties should be specified to high enough precision, so that the cents are calculated accurately. Clearly the IRS hires pros: These guys really know their stuff! All their commas and periods lined up exactly, no extra punctuation, nothing out of place, even a properly placed floating dollar sign.

Too often, RISKS concentrates on the failures and screwups. It's high time that we recognized the people who do it right, and celebrate a job well done. The hard working programmers behind the tax bills often go unacknowledged. Let's show them our appreciation. Tax programmers, I take my hat off to you!

Rich Schroeppel rcs@cs.arizona.edu

Terminal Consternation (csvcjld, RISKS-14.82)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Tue, 17 Aug 93 15:40:21 -0400

>If the bytes are uniformly distributed, there is a good chance they
>are encrypted.

> [But NOT NECESSARILY. ... simplifications are tricky. PGN]

The whole subject is tricky. Functionally, there is no real difference between compression and encryption other than degree of difficulty in breaking 8*).

Run the compressed file through UUENCODE or a TEKHEX generator and we are back
to a non-random string. (BTW XXENCODE permits use of a user-supplied table --
is this Encryption ?).

I *suspect* that the telco filter is very simplistic - could just be
interrupting the connection on an XOFF (Ctrl-S or 13h). Might not even be
deliberate.

Point is that it is easy to disguise text as binary, slightly more difficult
to make binary look like text, but not impossible, engineers have been doing
it for years - "I didn't know you were *trying* to block binary, it just
looked like a faulty design."

Padgett

Preserving electronic memos -- a serious problem

<Bob_Frankston@frankston.com>
Mon, 16 Aug 1993 21:00 -0400

A recent New York Times featured a policy wherein all electronic correspondence among people at the White House must be preserved. As Oliver North discovered, email can be forever. More to the point is Richard Nixon's experience. Once he recorded all his phone conversations, he exposed himself to having them subpoenaed!

Here is an example where the reality of electronic communications and our legal systems are seriously out of step. Essentially all business records and, I wouldn't be surprised, all personal records, can be subpoenaed. In the government, many of the records must be supplied upon request. (A reader with more expertise can clarify the legal aspects of this).

It can be quite disconcerting to discover that a private memo citing the possibility that a chemical might cause cancer surfaces twenty years later to prove that your company knew about the danger and failed to act. On the other hand, such exposure is often necessary to uncover criminal behavior. Let's assume that a balance has been struck over the year between the publics need to know and the requirements of privacy for classic paper documents.

While this might be a big assumption, it is the status quo. One develops defenses such as a paperless office (i.e., never write anything down, just discuss it in person or on the phone) or shredding memos upon reading them. These aren't perfect as the Nixon experience shows and when participates choose to, or accidentally preserve information.

This all changes when the normal means of conversations leaves an indelible trail. While this policy cites email, bits is bits and as we shift to digital PBXes in which text, voice, images are all stored in the same pool, we have lost all privacy.

Unfortunately, this issue was not explicitly faced in the 1700's and thus there was no provision in the constitution.

There are those that argue that there is no right to privacy in a commercial setting, that an employer has a right to tape all conversations on premises and install video cameras in every nook and cranny. And some have. After all, who knows how many rest room visits were just a way to take a break without accomplishing anything.

But it also means a world that doesn't allow tentative thinking, questioning of the norm, diplomacy or correction. It is a world where all ones inner thoughts are exposed to analysis and criticism without a chance to refute or comment. It is a world where innocuous behavior might resurface twenty years later and be judged in an entirely different world. It is a world that guarantees mediocrity since any behavior that doesn't reinforce the popular images of the majority (even if it is not a real majority) will result in disgrace.

Sadly, the problem is not easy to solve. The opposite extreme of a world with no paper trail can be a conspiratorial world where all behavior is hidden and thus is suspect, if not corrupt. I don't have easy answers but am concerned that people should be aware that while email might be the successor to the paper memo, it is much more than that and extending an old policy can have serious, and unexpected, ramifications.

Is a world with perfect memory better than one without history?

Call for Clipper Comments

Dave Banisar <banisar@washofc.cpsr.org>
Tue, 17 Aug 1993 14:23:16 EST

The National Institute of Standards and Technology (NIST) has issued a request for public comments on its proposal to establish the "Skipjack" key-escrow system as a Federal Information Processing Standard (FIPS). The deadline for the submission of comments is September 28, 1993. The full text of the NIST notice follows.

CPSR is urging all interested individuals and organizations to express their views on the proposal and to submit comments directly to NIST. Comments need not be lengthy or very detailed; all thoughtful statements addressing a particular concern will likely contribute to NIST's evaluation of the key-escrow proposal.

The following points could be raised about the NIST proposal (additional materials on Clipper and the key escrow proposal may be found at the CPSR ftp site, cpsr.org):

* The potential risks of the proposal have not been assessed and many questions about the implementation remain unanswered. The NIST notice states that the current proposal "does not include identification of key escrow agents who will hold the keys for the key escrow microcircuits or the procedures for access to the keys." The key escrow configuration may also create a dangerous vulnerability in a communications network. The risks of misuse of this feature should be weighed against any perceived benefit.

* The classification of the Skipjack algorithm as a "national security" matter is inappropriate for technology that will be used primarily in civilian and commercial applications. Classification of technical information also limits the computing community's ability to evaluate fully the proposal and the general public's right to know about the activities of government.

* The proposal was not developed in response to a public concern or a business request. It was put forward by the National Security Agency and the Federal Bureau of Investigation so that these two agencies could continue surveillance of electronic communications. It has not been established that is necessary for crime prevention. The number of arrests resulting from wiretaps has remained essentially unchanged since the federal wiretap law was enacted in 1968.

* The NIST proposal states that the escrow agents will provide the key components to a government agency that "properly demonstrates legal authorization to conduct electronic surveillance of communications which are encrypted." The crucial term "legal authorization" has not been defined. The vagueness of the term "legal authorization" leaves open the possibility that court-issued warrants may not be required in some circumstances. This issue must be squarely addressed and clarified.

* Adoption of the proposed key escrow standard may have an adverse impact upon the ability of U.S. manufacturers to market cryptographic products abroad. It is unlikely that non-U.S. users would purchase communication security products to which the U.S. government holds keys.

Comments on the NIST proposal should be sent to:

Director, Computer Systems Laboratory
ATTN: Proposed FIPS for Escrowed Encryption Standard
Technology Building, Room B-154
National Institute of Standards and Technology
Gaithersburg, MD 20899

Submissions must be received by September 28, 1993. CPSR has asked NIST that provisions be made to allow for electronic submission of comments.

Please also send copies of your comments on the key escrow proposal to CPSR for inclusion in the CPSR Internet Library, our ftp site. Copies should be sent to <clipper@washofc.cpsr.org>.

[Federal Register Vol 58 No 145, NIST, Docket No. 930659-3159, RIN 0693-AB19, "A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)", 58 FR 40791, Friday, July 30, 1993 is available for anonymous FTP on CRVAX.SRI.COM in the RISKS: archive directory, with file name RISKS-14.84N, of from Dave Banisar <banisar@washofc.cpsr.org>. PGN]

Call for papers -- 2nd Workshop on Feature Interactions

Nancy Griffeth <nancyg@banshee.bellcore.com>
Wed, 11 Aug 93 16:22:54 GMT

Feature interactions can create security loopholes or even bring the public telephone network down. Since various critical systems -- emergency services and airport control towers -- depend on the telephone network, the subject is relevant to RISKS. For more information, I would refer readers to the August 1993 issues of Computer and Communications magazines, especially the introductory articles and the paper by Kuhn et. al., ``Improving Public Switched Network Security in an Open Environment'' in Computer, pp. 32-35. Also, Cameron and Lin published a paper in the Proceedings of the 1991 SIGSOFT Conference on Software for Critical Systems, ``A Real-Time Transition Model for Analyzing Behavioral Compatibility of Telecommunications Services''. Otherwise, little work has been published on approaches that can protect the network and its users from potential effects of feature interactions, so responses from people who have worked on other critical systems would be most welcome.

CALL FOR PARTICIPATION

Second International Workshop on Feature Interactions
in Telecommunications Software Systems

Amsterdam, The Netherlands
May 9-10, 1994

This workshop is the second in a series, whose mission is to encourage researchers from a variety of computer science specialties (software engineering, protocol engineering, distributed artificial intelligence, formal techniques, software testing, and distributed systems, among others) to apply their techniques to the feature interaction problem that arises in building telecommunications software systems (see the back page for a description of the problem). We welcome papers on avoiding, detecting, and/or resolving feature interactions using either analytical or structural approaches. Submissions are encouraged in (but are not limited to) the following topic areas:

- Classification of feature interactions.
- Modeling, reasoning, and testing techniques for detecting feature interactions.
- Software platforms and architecture designs to aid in avoiding, detecting, and resolving feature interactions.
- Tools and methodologies for promoting software compatibility and extensibility.
- Mechanisms for managing feature interactions throughout the service life-cyle.
- Management of feature interactions in PCS, ISDN, and Broadband services, as well as IN services.
- Management of feature interactions in various of the operations support functions such as Service Negotiation, Service Management, and Service Assurance.
- Feature Interactions and their potential impact on system Security and Safety.
- Environments and automated tools for related problems in other software systems.
- Management of Feature Interactions in various proposed

architectures such as TMN, INA, ROSA, CASSIOPEIA, SERENITE, or
PLATINA.

FORMAT

We hope to promote a dialogue among researchers in various related areas, as well as the designers and builders of telecommunications software. To this end, the workshop will have sessions for paper presentations, including relatively long discussion periods. Panel discussions and tool demonstrations are also planned.

ATTENDANCE

Workshop attendance will be limited to 90 people. Attendance will be by invitation only. Prospective attendees are asked to submit either a paper (maximum 5000 words) or a single page description of their interests and how they relate to the workshop. About 16-20 of the attendees will be asked to present talks. We will strive for an equal mix of theoretical results and practical experiences. Papers will be published in a conference proceedings.

SUBMISSIONS

Please send five copies of your full original paper or interest description to:

Wiet Bouma
PTT Research, Dr. Neher Laboratories
PO Box 421 or St. Paulusstraat 4
2260 AK Leidschendam 2264 XZ Leidschendam
The Netherlands The Netherlands
E-mail: L.G.Bouma@research.ptt.nl
Tel: +31 70 332 5457
FAX: +31 70 332 6477

IMPORTANT DATES:

November 15, 1993: Submission of contributions.
January 15, 1993: Notification of acceptance.
February 15, 1993: Submission of camera-ready versions.

WORKSHOP CO-CHAIRPERSONS

Wiet Bouma & Hugo Velthuijsen (PTT, The Netherlands)

PROGRAM COMMITTEE

Chair: E. Jane Cameron (Bellcore, USA) [Rest deleted. Request it. PGN]

Call for papers IFIP SEC'94 Caribbean

<fortrie@cipher.nl>

Wed, 11 Aug 1993 01:49 +0100

Call for Papers IFIP SEC'94 - updated information August 1993

Technical Committee 11 - Security and Protection in Information
Processing Systems - of the UNESCO affiliated INTERNATIONAL
FEDERATION FOR INFORMATION PROCESSING - IFIP,

announces:

Its TENTH INTERNATIONAL INFORMATION SECURITY CONFERENCE, IFIP SEC'94 TO BE HELD IN THE NETHERLANDS ANTILLES (CARIBBEAN), FROM MAY 23 THROUGH MAY 27, 1994.

Organized by Technical Committee 11 of IFIP, in close cooperation with the Special Interest Group on Information Security of the Dutch Computer Society and hosted by the Caribbean Computer Society, the TENTH International Information Security Conference IFIP SEC'94 will be devoted to advances in data, computer and communications security management, planning and control. The conference will encompass developments in both theory and practise, envisioning a broad perspective of the future of information security. The event will be lead by its main theme "Dynamic Views on Information Security in Progress".

Papers are invited and may be practical, conceptual, theoretical, tutorial or descriptive in nature, addressing any issue, aspect or topic of information security. Submitted papers will be refereed, and those presented at the conference, will be included in the formal conference proceedings. Submissions must not have been previously published and must be the original work of the author(s). Both the conference and the five tutorial expert workshops are open for refereed presentations.

The purpose of IFIP SEC'94 is to provide the most comprehensive international forum and platform, sharing experiences and interchanging ideas, research results, development activities and applications amongst academics, practitioners, manufacturers and other professionals, directly or indirectly involved with information security. The conference is intended for computer security researchers, security managers, advisors, consultants, accountants, lawyers, edp auditors, IT, adminiatration and system managers from government, industry and the academia, as well as individuals interested and/or involved in information security and protection.

IFIP SEC'94 will consist of a FIVE DAY - FIVE PARALLEL STREAM - enhanced conference, including a cluster of SIX FULL DAY expert tutorial workshops.

In total over 120 presentations will be held. During the event the second Kristian Beckman award will be presented. The conference will address virtually all aspects of computer and communications security, ranging from viruses to cryptology, legislation to military trusted systems, safety critical systems to network security, etc.

The six expert tutorial workshops, each a full day, will cover the following issues:

Tutorial A: Medical Information Security
Tutorial B: Information Security in Developing Nations
Tutorial C: Modern Cryptology
Tutorial D: IT Security Evaluation Criteria
Tutorial E: Information Security in the Banking and Financial Industry
Tutorial F: Security of Open/Distributed Systems

Each of the tutorials will be chaired by a most senior and internationally respected expert.

The formal proceedings will be published by Elsevier North Holland Publishers, including all presentations, accepted papers, key-note talks, and invited speeches.

The Venue for IFIP SEC'94 is the ITC World Trade Center Convention Facility at Piscadera Bay, Willemstad, Curacao, Netherlands Antilles.

A unique social program, including formal banquet, giant 'all you can eat' beach BBQ, island Carnival night, and much more will take care of leisure and relax time.

A vast partners program is available, ranging from island hopping, boating, snorkeling and diving to trips to Bonaire, St. Maarten, and Caracas.
A special explorers trip up the Venezuela jungle and the Orinoco River is also available.
For families a full service kindergarten can take care of youngsters.

The conference will be held in the English language. Spanish translation for Latin American delegates will be available.

Special arrangements with a wide range of hotels and appartments complexes in all rate categories have been made to accommodate the delegates and accompanying guests. (*)
The host organizer has made special exclusive arrangements with KLM Royal Dutch Airlines and ALM Antillean Airlines for worldwide promotional fares in both business and tourist class. (**)

(*)(**) Our own IFIP TC11 inhouse TRAVEL DESK will serve from any city on the globe.

All authors of papers submitted for the referee process will enjoy special benefits.

Authors of papers accepted by the International Referee Committee will enjoy extra benefits.

If sufficient proof (written) is provided, students of colleges, universities and science institutes within the academic community, may opt for student enrollment. These include special airfares, appartment accommodations, discounted participation, all in a one packet prepaid price.
(Authors' benefits will not be affected)

****
INSTRUCTIONS FOR AUTHORS

****

Five copies of the EXTENDED ABSTRACT, consisting of no more than 25 double spaced typewritten pages, including diagrams and illustrations, of approximately 5000 words, must be received by the Program Committee no later than November 15th, 1993.

We regret that electronically transmitted papers, papers on diskettes, papers transmitted by fax and handwritten papers are not accepted.

Each paper must have a title page, which includes the title of the paper, full names of all author(s) and their title(s), complete address(es), including affiliation(s), employer(s), telephone/fax number(s) and email address(es).
To facilitate the blind refereeing process the author(s)' particulars should only appear on the separate title page. The language of the conference papers is English.
The first page of the manuscript should include the title, a keyword list and a 50 word introduction. The last page of the manuscript should include the reference work (if any).

Authors are invited to express their interest in participating in the contest, providing the Program Committee with the subject or issue that the authors intend to address (e.g. crypto, viruses, legal, privacy, design, access control, etc.) This should be done preferably by email to < TC11@CIPHER.NL >, or alternately sending a faxmessage to +31 43 619449 (Program Committee IFIP SEC'94)

The extended abstracts must be received by the Program Committee on or before November 15th, 1993.

Notification of acceptance will be mailed to contestants on or before December 31, 1993. This notification will hold particular detailed instructions for the presentation and the preparation of camera ready manuscripts of the full paper.

Camera ready manuscripts must be ready and received by the Program Committee on or before February 28, 1994.

If you want to submit a paper, or you want particular information on the event, including participation, please write to:

IFIP SEC'94 Secretariat, Postoffice Box 1555, 6201 BN   MAASTRICHT
THE NETHERLANDS - EUROPE

or fax to IFIP SEC'94 Secretariat: +31 43 619449 (Netherlands)
or email to TC11@CIPHER.NL

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 85

Friday 20 August 1993

Contents

Child-Prodigy or Prodigy-Child? 14-year-old triggers alarms

<harrison@cs.ubc.ca>
Fri, 20 Aug 93 12:49:36 -0700

As a supposed joke, a 14-year-old Seattle-area girl sent a Prodigy message to her boyfriend in New Jersey containing a phony death threat against Baltimore Orioles' shortstop Cal Ripkin, Jr., who is getting ever closer to Lou Gehrig's record for consecutive games. Seattle and Baltimore were playing in the Kingdome in Seattle, and her boyfriend is an avid Orioles' fan. Known for its monitoring of messages, Prodigy alerted the police --- who tightened security at the Kingdome and also camped out waiting for the girl to return home. They apparently reprimanded the girl, but she was not charged. Police said she was ``very embarrassed and apologetic'' and added, ``By the time her [28-year-old] sister got done chewing her out, that was enough.'' [Source: A UPI item datelined Seattle, 19 Aug 93, PGN Excerpting and Extrapolating Service]

[The news on 20 Aug 93 noted that Kingdome officials are planning on charging the cost of the extra security assigned to Ripkin to the girl. - Jason]

IRS accounting bugs

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
18 Aug 93 15:13:41 EDT

See IRS's Books. Color Them Red.;
First Audit Ever Uncovers $752 VDT Valued at $5.6 Million
By Stephen Barr, Washington Post Staff Writer, Washington Post, 18 Aug 1993

The Internal Revenue Service, which has made many an American anxious over an audit, recently underwent a comprehensive audit of its own - its first. Among the findings:

A video display terminal costing $752 was valued in IRS inventory records at $5.6 million.

$36,000 was paid for a maintenance contract for a minicomputer that had been idle for three years.

32 duplicate payments and overpayments worth $500,000 were found in a review of 280 payments to vendors, and 112 payments totaling $17.2 million lacked complete supporting documentation.

The IRS examples are but a small slice of one of the federal government's most serious problems: financial books that are out of whack, perhaps by tens of billions of dollars."

The article goes on to detail a litany of egregious accounting blunders in various parts of the government:

"...more than $200 billion in accounting errors by the Army and Air Force,..."

"...more than $500 million worth of errors in NASA financial statements...."

In addition, the GAO's report was discussed in the Senate's Governmental Affairs Committee chaired by John Glenn (D-Ohio). The Committee was concerned "...about the disclosure that taxpayer privacy had been compromised by an internal breakdown in computer security."

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

IRS & security

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
20 Aug 93 10:37:39 EDT

IRS Computer Revamp Faulted By Study Panel; Privacy, Security Risks Seen
In Multibillion-Dollar Program,
By Stephen Barr, Washington Post Staff Writer, Washington Post, 20 Aug 1993

The Internal Revenue Service `has shown little progress' in addressing concerns about taxpayer confidentiality as it proceeds with a multibillion-dollar overhaul of its computer systems, a National Research Council panel said yesterday.

The Tax Systems Modernization program at IRS "can lead to a wide range of potentially disastrous privacy and security problems for the IRS unless the IRS develops effective, integrated privacy and security policies," the panel said."

The article continues to report that the program modernization will cost about $7.8 billion over the next 15 years.

Henry H. "Hank" Philcox said that the IRS has been studying security for at least the last 10 months, including both anti-hacker considerations and protection against abuse by employees.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Re: Dorney Park Hercules roller coaster ... (S.D.Walter, RISKS-14.83)

Gary Wright <gwright@world.std.com>
Wed, 18 Aug 1993 23:51:37 -0400

> This accident sounds remarkably similar to the accident on the Timber Wolf
> roller coaster at Worlds of Fun in Kansas City, on March 31, 1990. The
> nature of the accident and the fixes were essentially the same! See
> RISKS-9.96.

In fact, the Timber Wolf and Hercules were both built in 1989 and designed by the same firm, Curtis D. Summers, Inc. I believe the same construction company was used (Dinn). The material I have only lists designers. (Guide to Ride, American Coaster Enthusiasts, 1991).

[By the way, the identity of the original contributor was cited erroneously in RISKS-14.83. He is Steven D. Walter, of Bethlehem PA. Sorry for the error. Thanks to Steve for the SnailMail. PGN]

Remotely accessible answering machines may grant *too much* access

Tsutomu Shimomura <tsutomu@ariel.sdsc.edu>
Thu, 19 Aug 1993 13:34:23 -0700

Many telephone answering machines provide "remote access" features which permit the user to call and retrieve messages from elsewhere, often with the aid of a Touch-Tone(tm) telephone. There are often other functions provided, such as the ability to delete messages, change the outgoing message, and set various operating parameters for the machine. Some minimal degree of security is usually provided, typically a short "security code" to be sent via Touch-Tone to authenticate the user. The short "security code" is justified as a compromise between user convenience and security; after all, the worst thing that might reasonably happen is that someone else might retrieve and delete your messages, right?

The ability to change the outgoing message, in combination with the in-band signalling used in analog telephone systems, poses some interesting opportunities beyond the obvious juvenile pranks. If I have "cracked" the "security code", it is likely a simple matter to record an outgoing message which includes in-band signalling information (e.g., Touch-Tones) designed to be sent upon receipt of dialtone. Next, I must arrange for dialtone into which the answering machine can play its message; this can be accomplished by calling the machine and disconnecting just before it answers. We now have a manifestation of the classic telephone line "glare" race condition: the "answerer" does not realize that it is really an "originator", and has just initiated a call.

Numerous applications suggest themselves. The simplest are ones involving messages which call revenue-generating numbers (e.g., 1-900 for those of you in the NANP) or long distance call-forwarding for toll fraud purposes.

A more interesting possibility is the use of the answering machine as an "anonymous" messaging device. Suppose that the outgoing message is modified to dial a number, pause for an answer, and play a (voice) message? Having delivered its spiel, the machine will dutifully record a message from the called party. The answering machine can then be called in the "usual" manner and the message retrieved and erased. BTW, this *has* actually been tested, and found to work as described.

ISDN (out-of-band signalling), anyone? Perhaps we really need auditing and intrusion detection systems for home appliances ...

Note: If you work for an RBOC, you aren't allowed to use this note as a sales pitch for your CO-based voice-mail offerings. Oh yeah, and if you're a kidnapper, you can't use this to deliver your ransom note! ;-)

Tsutomu Shimomura tsutomu@ucsd.edu +1 619 534 5050
University of California at San Diego/San Diego Supercomputer Center, USA

ATM Scam (RISKS-14.60 to 74)

Gene Spafford <spaf@cs.purdue.edu>
Fri, 20 Aug 93 16:04:10 -0500

In recent RISKS, there have been some details on the fake ATM being set up in a shopping mall in New Haven.

Last week at the 5th FIRST Incident Response Workshop, an agent of the Secret Service regaled the audience with some details of the case:

* Several people were arrested
* One has admitted everything and is cooperating with authorities
* over 300 accounts at over 50 banks were hit by the counterfeit cards
* over 100K in fraudulent charges were made with the captured cards

This was not an isolated incident, but the latest in a 12-year string of fraud activity that may have netted over 12 million dollars. Included in this past history were computer-assisted forgeries of stocks, bonds, passports, military IDs, and even law enforcement IDs. On several occasions the people involved used forged ID documents to carry guns on-board airplanes.

[5th FIRST? Perhaps they drank a 5th FIRST? PGN]

High-speed password matching

Steve Stevenson <fpst@hubcap.clemson.edu>
Wed, 18 Aug 93 10:12:33 -0400

cross-post request from comp.parallel
To: comp-parallel@uunet.UU.NET
Newsgroups: comp.risks
From: unijbm@uts.uni-c.dk (J|rgen B. Madsen)
Subject: World record in password checking
Organization: UNI-C, Danish Computing Centre for Research and Education
Date: Wed, 18 Aug 1993 11:05:07 GMT
Summary: World record in password checking

A NEW WORLD RECORD IN PASSWORD CHECKING HAS BEEN SET:

Roch Bourbonnais, a Thinking Machines Corporation engineer, has ported and optimized the CM/2 port of the UFC-crypt to a CM/5 system.

The UFC-crypt (Ultra Fast Crypt) implementation on the CM/2 Connection Machine (parallel computer) is a UNIX password checking routine (crypt()) ported by Michael Glad at UNI-C.

The port, that is written in CM-fortran, utilizes the CM/5 vector units and is partly programmed in cdpeac (vector unit assembly language).

The package achieves 1560 encryptions/second/vector unit. This scales to

```
  6,4 million encryptions per second on a large  1024 node machine.
  800,000       -     -    -    - - small   128  -     -
```

With this impressive performance, all combinations of 6 letters can be
tried in less than an hour and all combinations of 6 lower-case letters
can be tried in less than one minute.

Congratulations, Jorgen Bo Madsen

Jorgen Bo Madsen, Security Consultant
UNI-C Lyngby, Danish Computing Centre for Research and Education
DTH, Building 305, DK - 2800 Lyngby,
Phone : +45-45-938355
Telefax: +45-45-930220
E-Mail : Jorgen.Bo.Madsen@uni-c.dk

Re: Crash of JAS 39 Gripen

Derrick Everett <derrick@dms.corena.no>
Fri, 20 Aug 93 21:19:47 DFT

I was in Stockholm the day after the JAS crash and read some of the
local papers, which were mostly filled with speculation. The
investigative commission has just made public their preliminary
findings. I enclose a translation of a local newspaper report.

>From Aftenposten (Oslo) 19 August 1993:

JAS AIR CRASH: BOTH TECHNICAL AND PILOT ERROR

Too rapid deflection in the control system and quick joystick movements by the pilot were the causes of the JAS accident in Stockholm on 8 August.

The Crash Investigative Commission into the JAS accident during the Water Festival, with ten thousand spectators around the crash location, presented their provisional report yesterday and have concluded that the technology and the pilot together caused the accident.

'The JAS crash was caused by the control systems high amplification of joystick deflections in combination with the pilots large and rapid joystick movements. This caused margins of stability to be exceeded`, the report says.

According to the Commission, 'the pilot flew below the minimum permitted altitude by an insignificant amount during the demonstration and exceeded by some amount the maximum permitted angle of attack.' The aircraft had no technical faults at the time of the accident and the motor continued to function normally right until the plane hit the ground. Everything happened very quickly: from the pilot losing control of the plane to his ejection and parachute descent took only 6.2 seconds.

The unthinkable consequences that would have followed if the JAS plane had crashed into the crowd have led to renewed and intense debate both in the political arena and among the Swedish public, about whether the JAS program

> should continue. It has so far cost 22 billion crowns [3.2 billion dollars].
>
> The Crash Investigative Commission asks the Air Force Chief of Staff to ensure that measures are taken to prevent any future occurrence similar to the JAS accident. When this has been done, the Commission expect there to be no reason for continued grounding of the JAS 39 Gripen, the report adds. But discussion continues about adding some inertia to the control system.
>
> The JAS project (JAS stands for search, attack, reconnaisance [jakt, angrep, spaning]) was announced in 1979 as the Swedish Defence Forces pride and an aircraft for the 1990s, even the leading edge of Swedish technological exports in military equipment. Both before and after the first aircraft left the production line this year, everybody from King Carl Gustaf through Prime Minister Carl Bildt to Defence Minister Anders Bjoerck done everything short of walking on their hands to get the plane sold to other countries. The Swedish establishment could hardly have received a more direct smack in the face.
>
> In aircraft jargon, what happened to the JAS plane on that fatal Sunday over Vaesterbron in the centre of Stockholm is called, 'Pilot Induced Oscillations (PIO)' - the pilots hand movements led to violent banking [actually, it looked more like pitching] of the plane. During the upswing, the nose of the aircraft came up too far, and so the pilot pushed the joystick forward to level the plane. At this, the nose came down but by more than the pilot had intended, because the control mechanism is so fine-tuned that even the smallest movement gives a large deflection. This has previously been the source of problems in the advanced JAS project. To stop the nose dropping too far, the pilot pulled back the joystick - at the same time as the computer [actually, a set of three processors] had given signals to lift the nose. The combined signals from the computer system and the joystick led to uncontrolled oscillation that became a vicious circle of signals and counter-signals until the aircraft was totally out of control. Because the plane was at a low altitude, there was no time to correct from the instability.

A few comments might be added from reading the Swedish newspapers. The JAS 39 Gripen is deliberately unstable. There are no ailerons on the main wings, but instead a pair of smaller wings located forward are used to actively correct the attitude of the aircraft. These are under the control of the three digital computers that presumably co-operate by majority voting. This system has to respond to signals within 200 milliseconds in order to maintain stability. If the digital system is disconnected, an analogue backup system ensures that the plane flies level but it is not then possible to manouevre. Since the centre of gravity lies behind the centre of lift, there is a tendency to lift the nose when control is lost.

Derrick Everett, Life*CDM Project Manager. CORENA A/S, Asker, Norway.

Risks of coming mass-communication capabilities

<Hiller@DOCKMASTER.NCSC.MIL>

Thu, 12 Aug 93 02:47 EDT

After reviewing several of the recent RISKS forum entries (Clipper articles, reports, etc.), I noticed that even these items quickly referenced the upcoming explosions of technology and capability being promised to us by AT&T, Time/Warner, MCI, and others. Along with the general trends coming through fruition of ISDN as well as these various cable and fiber based commercial offerings, which have been well-documented in newspapers and the like, I have been continually searching for a shred of evidence that ANYONE is pausing to look at the security and public policy issues that such offerings are bound to tax to the limit.

Through all the various channels, the RISKS forum included, it is clear that there is tremendous risk involved in such implementations. As our society is introduced to such capabilities, we will surely become orders of magnitude more dependent on information technology than we are today. Yet, we are light-years behind the capability curve in terms of protecting ourselves or even pretending to know how. Is anyone, commercially, governmentally, or otherwise looking at these impacts and advising the providers of these services on how to proceed

I'd be very interested to find out what sorts of steps anyone is taking, and the rapidity with which they are taking them. Please direct any such information to Hiller@DOCKMASTER.NCSC.MIL .

Thanks! Jim Hiller

Re: Computers Dialing 911 (Kabay, RISKS-14.93)

<wizard@moz.hookup.net>
Tue, 17 Aug 93 20:06:53 EST

In RISKS-14.83, Mich Kabay noted a cordless phone accidentally dialing 911.

That reminded me of two incidents I'd like to share here.

The first one occurred several years ago. I was doing technical support for a local software company. One of our users had a problem, and we were trying to get her to upload the problem to our BBS, so we could attempt to solve it. She was unfamiliar with telecomunication software, but had copied the directory off of her machine at work. She set up the modem, and the software, and entered the number to dial (1 519 ... .). Nothing seemed to happen. She tried again, several times. We were talking to her on a second phone line, when there was a loud knock on her door. She answered it, and there were a large number of police at the door! Apparently, the software had been configured to use the PBX at work, and all number's were prefixed with a 9 (for an outside line), and a 1 (for long distance). She had dialed 911 5 or 6 times!

The second incident occurred several weeks ago. A friend of mine runs a local BBS, and has set up a Call-Back-Verifier, to assure that people give there real phone number. Some one called in, and gave 911 as his number, hoping the

BBS would call it, and bring the cops in. Fortunately, my friend was watching at the time, and has since added 911 to the list of forbidden numbers.

Mark

Good news from the front lines

Jeremy Grodberg <jgro@netcom.com>
Thu, 19 Aug 1993 03:59:19 GMT

As we've heard over and over, our Social Security numbers are being used in dangerous ways. One particular example is that they are often used as authenticators in telephone transactions with financial institutions. In the past, it has been difficult to impossible to convince these institutions to use alternate authenticators, but I want to report that I have seen some progress.

Two years ago I sent a nastygram to Citibank complaining about them using my SSN to verify my identity in telephone transactions involving my credit card, and was told, in essence, "we don't have any alternative." Recently, I tried again, and found that not only Citibank, but also Chase, AT&T, and Bank of America will all accept alternate authenticators, at least in their credit card operations, in the guise of "Mother's Maiden Name", which can be any single pronounceable codeword. This is progress.

As for how I went about establishing this new protection, there were varying degrees of security. Citibank took the codeword over the phone, with only my SSN and account info as verification. BofA also took the new codeword over the phone and only required a little more info than Citibank, but nothing that wasn't on my monthly statement (if memory serves). Chase required the change in writing, required nothing but the account number in the letter, but did mail me a notification that the codeword had been changed. AT&T sent me a form to fill out to authorize the new codeword, although I don't know if they would have accepted a regular letter.

For those of you keeping score, IMHO AT&T in general, as in this particular case, seems to have the best security. At least the others are catching on.

Jeremy Grodberg jgro@netcom.com

Gideon Kunda, Engineering Culture

Phil Agre <pagre@weber.ucsd.edu>
Thu, 19 Aug 1993 15:45:40 -0700

Risks readers may be interested in Gideon Kunda's book "Engineering Culture: Control and Commitment in a High-Tech Corporation" (Temple University Press, 1992). It's an ethnographic study of a "corporate culture" program at a real but pseudonymous high-tech firm that Kunda calls "Tech". Immense effort goes into designing the symbolic aspects of work at Tech, including new-employee orientations, the ritual aspects of meetings, slogans and posters, company history, and so forth. Kunda gives many examples of these things and has some fascinating things to say about them, and particularly about the phenomenon of "burnout" among Tech employees.

A longer review of Kunda's book is available in issue #4 of the CPSR journal CPU, which can be obtained by ftp to cpsr.org in the directory /cpsr/work. To subscribe, send a message to listserv@cpsr.org with a blank subject and a single line in the body of the message:

SUBSCRIBE CPSR-CPU

Virus Catalog: new edition

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>
Fri, 20 Aug 1993 16:32:47 +0200

Computer Virus Catalog update July/August 1993

With it's July/August 1993 edition, Computer Virus Catalog describes more forms of Malicious Code = MalCodes (including chain letters, time bombs, trojan horses, viruses and worms) on multiple platforms (IBM and compatible PCs, Macintosh, IBM-MVS/VM, UNIX, Amiga and Atari).

Presently, ***340 MalCodes*** have been classified active on 6 platforms:

Amiga:	92 Viruses, 1 Trojan, 5 TimeBombs
Atari:	20 Viruses
Macintosh:	35 Viruses, 2 Trojans
MSDOS:	172 Viruses, 6 Trojans, 3 Virus Generators
MVS/VM:	1 Chain Letter
UNIX:	2 Viruses, 1 Worm

Entries for UNIX Internet Worm and IBM-VM CHRISTMA.EXEC are yet experimental (in "old" CVC format 1.2). A generalized format (2.0) for the Computer MalCode Catalog will be available, including descriptions of DEC-VMS worms (Father Christmas, WANK and OILZ), with next edition (planned: December 1993).

New CVC entries are available in ASCII, and all entries are available either via CVBASE.EXE (the electronic edition of CVC, for PCs) or as compressed (PKZIPPED) files. See Virus Test Center's FTP site.

The July/August 1993 CVC edition describes the following MalCodes:
- -
Macintosh: 3 new viruses:
    INIT 17, INIT M = WDEF M,
        MerryXmas Hypercard virus

IBM/compatible PCs: 26 new MalCodes:
    25 new viruses: (Goddam) Butterflies, Chinese_Fish=Fish Boot,
        Clone, Dec_Year=Last_Year(.604), Dudley, F-Word,
        Gnat (1.0), Horns, Invisible, Involuntary, Junior,
        Little Red, Loren, Mabuhay, Nguyen,

No_Int=Stoned.No_Int.A (Stoned Strain), Peter, QRRY,
Requires=Requires.981=Demise=Later, RMBD,
Runtime=Runtime-err412, Su=Susan, Terminator II,
Tonya, Warlock Virus.
1 Virus Generator: PS-MPC G2 Virus Generator
Update: Parity_Boot (A-C)=P-Check Virus (Parity_Boot Strain),
14 Minimal viruses renamed Trivial viruses.

Amiga: 24 new MalCodes:
19 viruses: AMIGA KNIGHT, CCCP,
COMPUPHAGOZYTE 1 (CompuPhagozyte Strain), CRIME'92,
DARTH VADER (V1.1), FICA, HOCHOFEN=TRABBI,
SADDAM_BOOT, SCA.D&A_dropper=SCA Dos kill=D&A
(SCA Virus Strain), TOMATES GENTECHNIC, TURK,
VIRCONSET2, WARSHAW AVENGER Virus
and the following SADDAM Strain viruses:
SADDAM (Hussein)=IRAK=DISK-Validator, SADDAM.ANIMAL,
SADDAM_FILE, SADDAM.KICK, SADDAM.LOOM, SADDAM.NATO,
SADDAM.RISK, SADDAM.][Virus
1 Trojan dropper: TURK Color Dropper Trojan
4 (Time) Bombs: EXCREMINATOR_1, STARLIGHT, TIMEBOMB_09,
VIRUSTEST_BOMB_936 Bomb

UNIX: 1 new virus, 1 worm (experimental):
1 virus: VMAGIC virus
1 worm: INTERNET worm

IBM-MVS/VM: 1 chain letter (experimental): CHRISTMA.EXEC (G1,G2)

The following files may be downloaded from our ftp site:

INDEX.793	(36 kBytes): Overview of CVC entries
AMIGAVIR.793	(92 kBytes): new Amiga viruses
MACVIR.793	(18 kBytes): new Mac viruses
MSDOSVIR.793	(84 kBytes): new MSDOS viruses (part 1)
MSDOSVIR.893	(77 kBytes): new MSDOS viruses (part 2)
MVSVIR.793	(8 kBytes): CHRISTMA.EXEC chain letter
UNIXVIR.793	(11 kBytes): VMAGIC, INTERNET worm

The following files contain ALL entries published in the respective
domain (since July 1989) in compacted (PKZIPPED) form:

AMIGAVIR.ZIP	All Amiga viruses
ATARIVIR.ZIP	All Atari viruses
MACVIR.ZIP	All Mac viruses
MSDOSVIR.ZIP	All MSDOS viruses
MVSVIR.ZIP	(=MVSVIR.793 PKzipped)
UNIXVIR.ZIP	(=UNIXVIR.793 PKzipped)

Virus Test Center's FTP site:
ftp.informatik.uni-hamburg.de
Address: 134.100.4.42
login anonymous;
password: your-email-address;
directory: pub/virus/texts/catalog

Any assistance and helpful critical remarks are appreciated.

Klaus Brunnstein, University of Hamburg, Faculty for Informatics
Virus Test Center, 18 Aug 1993 <brunnstein@rz.informatik.uni-hamburg.d400.de>

InfoWar announcement

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
18 Aug 93 06:31:20 EDT

INFOWARFARE '93: 1st NCSA Conference in Canada
15 September 1993, Meridien Hotel, Montreal, Quebec

------------------------------FRENCH IN AM----------------------------

08:45-09:15 Introduction, probleme de la securite des reseaux (NCSA,MK)
09:15-09:45 Les lecons du desastre World Trade Center
(Samson Belair Deloitte Touche Ross)
09:45-10:30 Video et cafe
10:30-11:00 Desastres legaux
(Bourse de Montreal)
11:00-11:15 Fraude a distance: teleraude et reseaux (MK)
11:15-12:00 Table ronde: Mesures contre la fraude telephonique
(BELL, CANTEL, NORTHERN TELECOM)

-----------------------------ENGLISH IN PM----------------------------

12:00-13:15 --lunch for all-day attendees-- [ROYAL BANK: ATM fraud]
12:30-13:15 Registration for PM only
13:15-14:30 Information Warfare (Winn Schwartau)
14:30-15:15 Panel discussion: IW today (DND, RCMP, MoJ, SG, HQ, GSC)
15:15-15:30 Coffee and videos
15:30-16:15 Panel: Convincing upper mgmt (ASM,ASIMM,AVIMM,ISSA,CAAST)
16:15-16:30 Closing remarks (NCSA)

Costs:

AM or PM only	$105
Lunch only	$ 60
All day incl lunch	$225

Members of the NCSA, ASM, ASIMM, AVIMM, ISSA: 10% discount
For more info: phone 514-931-6187; fax 514-931-0878; email 75300,3232.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn
Jinbu, P.O. Box 509 Westmount, Montreal, Quebec H3Z 2T6 CANADA (514) 931-6187

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 86

Monday 23 August 1993

Contents

Everyone gets a 'A' for Welsh exam

Richard Clayton <richard@locomotive.com>
Mon, 23 Aug 93 17:32:02 GMT

>From the 'The Guardian' (UK National paper) 23 Aug 1993

Exam blunder

A computer blunder was blamed yesterday for wrongly awarding A grades
to all 84 students who sat a Welsh Language exam. Corrected results
with apologies were sent out by the Welsh Joint Education Committee
after the error was discovered.

[[
  I assume these would be 'A Level' exams for 18 year olds because
  these results came out last week. Grade A is the highest level of
  pass. They are vital for University entrance, and the papers have
  been full of stories about the necessity to get good grades in order
  to get on a course this year because of cutbacks. There must be 84
  rather worried kids out there whose plans may have to be changed!
]]

Richard Clayton, Locomotive Software   tel: +44 306 740606
Dorking Business Park, DORKING, Surrey, UK. RH4 1YL   fax: +44 306 885529

Medicare checks for $0.01

Bear Giles <bear@eagle.fsl.noaa.gov>
Mon, 23 Aug 93 17:06:10 GMT

The 23 August issue of the _Rocky Mountain News_ (Denver) reports that numerous people (>100) have received Medicare reimbursement checks for $0.01.

No, it was not a design error where no lower limit on checks was defined.

It seems that Blue Cross and Blue Shield, Medicare provider for Colorado, recently changed software packages and the previous version had used a sum of "$0.01" to indicate that claims should be sent to review. The new software doesn't use "in-band" signaling and simply cut checks for the apparent amount.

At least they used a *small* amount to use as signals. Imagine the consequences of choosing a large amount. Say, $9,999,999.99.

Bear Giles bear@fsl.noaa.gov

E-mail privacy

"Mich Kabay / JINBU Corp." <75300.3232@compuserve.com>
07 Aug 93 09:04:09 EDT

From UPI (United Press International) newswire (08/06 1259 Virginia News Briefs):

  City employee booted for snooping
  NEWPORT NEWS, Va. (UPI) -- A computer programmer employed by Newport
  News was fired for snooping on electronic mail between colleagues.

The brief note says that the fired computer programmer admits having printed electronic mail between her colleagues, including "backbiting comments about coworkers ... [and]... sexually explicit love notes."

She was fired for invasion of privacy and gross misconduct.

Moral: (user version) email is no more private than snail mail. Act accordingly.

Moral: (administrator version) email is as private as snail mail. Act
accordingly.

Michel E. Kabay, Ph.D., Director of Education, National Computer Security Assn

Re: Child-Prodigy -- clarification

Ed Ravin <elr@wp.prodigy.com>
Mon, 23 Aug 1993 16:54:03 -0400

In RISKS-14.85, harrison@cs.ubc.ca writes:

> As a supposed joke, a 14-year-old Seattle-area girl sent a Prodigy message
> to her boyfriend in New Jersey containing a phony death threat ...
> Known for its monitoring of messages, Prodigy alerted the police ...

It should be pointed out that the "monitored message" that contained the phony death threat was NOT a person-to-person email message on Prodigy, but a public bulletin board post. Although Prodigy has a well-deserved reputation for controlling content on their bulletin boards, they do not monitor or interfere with private email. Federal law (ECPA 1986) also prohibits monitoring of email, and all responsible online services providers (including Prodigy :-) abide by the law.

The occasional inability of police departments to distinguish between a joke and an actual threat is well-known -- one famous example is the Secret Services' assertion that Steve Jackson's GURPS Cyberpunk fantasy roleplaying game was really a "handbook for computer crime". One wonders what will happen if the police ever start reading bulletin boards like the average unmoderated Usenet newsgroup -- "Um, yes Officer, I know I posted on alt.flame.computers that all MS-DOS users deserved to die, but, er, I was only kidding around..."

Disclaimer: I work for Prodigy as a telecommunications programmer, and these are my opinions only, not those of my employer.

Ed Ravin, Prodigy Services Company, 445 Hamilton Avenue, White Plains NY 10601
elr@wp.prodigy.com   eravin@panix.com   +1 914 993 4737

Re: Child-Prodigy or Prodigy-Child? 14-year-old triggers alarms

Jeffrey I. Schiller <jis@MIT.EDU>
Sun, 22 Aug 93 16:26:18 -800

This note raises many very interesting issues. How did Prodigy know about the threat? Did the recipient (the boyfriend) report the message to them, or am I to read this message to indicate that Prodigy is monitoring personal mail between individuals? Let's assume so...

It's a scary world we are entering if our personal communications are being monitored and judged by the "authorities".

It's even worse when these "authorities" can misunderstand our words and make us pay for their trouble! Talk about chilling free speech!

At MIT I supervise the campus computer network, the MIT portion of the Internet. We have an internal policy that we do *not* monitor messages between individuals. We, however, state that our staff *may* inadvertently encounter personal mail due to our maintenance activities (more then likely because the mail system barfs and the message is delivered to the dead letter bin for manual routing).

Consistent with the ECPA of 1986, if we come across a message that indicates that something illegal is going on, we will notify law enforcement. However whatever action we or law enforcement takes is at our mutual risk if there is in fact no crime.

I can easily envision a situation where we uncover a message that in part reads:

"Tomorrow we will assassinate the leader of [insert your favorite country here]."

We will no doubt notify the appropriate authorities. However, it may turn out that the message had to do with a role playing game where the actors were playing agents of various countries (such games do exist). In this context the above message would be quite innocent. However some significant resources may be expended (read: money spent) before this is determined.

Who Pays?

Does it really make sense to have the innocent message originator pay? That is what it sounds like Prodigy et al. believe!

Big Brother is watching us... through our computers!

-Jeff

P.S. The scariest thing about services like Prodigy monitoring the mail is that People seem to tolerate it!!!

AT&T Security Authenticators

<thomp962@armstrong.edu>
Mon, 23 Aug 1993 09:11:28 -0400 (EDT)

I agree that AT&T is very willing to use alternate authenticators, but their security overall for Universal Card (MasterCard & Calling Card in one) is poor at best. To defend this assertion, I present the case of my new Universal Card, which, after delivery to a neighbor of mine who was required to eliminate dumping process water on my law, didn't arrive at all. No charges mind you, but AT&T did discuss the account with my neighbor, who phoned up and chatted about my credit line, cash machine PIN number, my age (he claimed I wasn't out of high school...), and best of all, the fact that my car had been repossessed last week (funny, I thought I paid cash for it). Anyway, AT&T's response was to pull three credit bureaus in one day, send me a new card, and not inform me of these little chats. I only found out when I wanted to get a new card air-expressed after I dry-cleaned mine.

Re: Remotely accessible answering machines (Shimomura, RISKS-14.85)

Mark A Biggar <mab@wdl.loral.com>
Mon, 23 Aug 93 14:56:18 PDT

This type of answering machine can become a physical security problem as well. My sister lives in a so called "high security" apartment building. To gain entry to visit someone, you enter their apartment number on a panel at the front door, the system then places a phone call to that apartment and provides a mic and speaker so you can talk to the person you want to visit. If they want to let you into the building, all they have to do is punch a code on their phone (#9 if I remember right). Now, my sister also has one of these smart answering machines, which of course is what answers if no-one is home. My sister was very startled when I showed her that if I knew the access code to her answering machine, I could program it to playback the signal to let me in the front door. Even a simpler machine with just remote playback can be spoofed this way. All you need is a pocket tape machine with a recording of the #9 tones, call the machine once to recorde the tones and call it a second time to play the tones back.

Mark Biggar mab@wdl.loral.com

worrying about online education

Steve Talbott <stevet@ora.com>
Thu, 12 Aug 1993 17:31:09 GMT

I am cross-posting the following essay (1670 words) from the Consortium for School Networking discussion list. In this way I hope to find out whether the readership of comp.risks is at all interested in the more "hidden" issues posed by computers and network technology. By this I mean not so much questions of privacy, physical health, computer error, and so on, as those relating to the more subtle and intimate interrelationships between ourselves and the patterns of intelligence we have been embodying in our machines.

I'm also curious whether there's any possibility for a discussion of these issues that does not degenerate into the worthless shouting matches so common in the "philosophy" groups. The sobriety of comp.risks gives one hope.

I'll welcome all critical response. (Feel free to say "not interested" as well.) Many thanks for your attention.

(I am not an educator, although I home-taught two of my children for a few years. I have worked in the software and technical writing field for some

12 years, and am currently an editor at O'Reilly and Associates. We publish books related to computers--including the immensely popular Whole Internet User's Guide and Catalog. This essay is one of a collection of short, Internet-related pieces I am currently working on.)

Steve Talbott
stevet@ora.com

##

##

Net-based Learning Communities

Entering a classroom, the sixth-grade girl sits down at her terminal and composes an email message to her "net pal" in India. The two of them are comparing notes about efforts to save endangered species in their separate localities, as part of a class project. (During the afternoon, a reply comes back.) In later years, these children may even chance to meet, and their email exchanges will have prepared them to accept each other on equal terms, rather than to be put off by cultural barriers.

An attractive picture? Very much so. This sort of thing is one of the bright promises of the net. Personally, however, I doubt we will see its broad realization any time soon. Why? Because the promise is being overwhelmed by sentimentality, uncritical futurism, and the worship of technology. We're seeing an unhealthy romanticization of the net.

Allow me a brief flanking movement here. It's now routine for social critics to bemoan the artificial, fantasy-laden, overstimulating (yet passive) environments in which our children grow up. I'm not sure the bemoaning helps any, but I believe the concerns are largely justified. The problem is that they too rarely strike through to the heart of the matter. For if the child must fill up his existence with "virtual" realities and artificial stimulation, is it not because we have systematically deprived him--not to mention ourselves--of the real world?

Link together in your mind a few simple facts, many of them commonplaces:

Schools have become ghettos for the young. Perhaps for the first time in history, our century has seen children strictly cut off from meaningful connection to the world of adult work. That work is hidden away behind the walls of the industrial park. Likewise, all the once-local functions of government have become distant, invisible abstractions, wholly disconnected from what the child observes going on around him. As to the evening news, it concerns events that he must find hard to distinguish from last night's movie. (And when he grows up and hears the screaming on the city street, will he know to do anything but *watch*?) The ubiquitous television serves in addition to cut him off from meaningful interaction with his own family. Even the eternal necessities have become invisible; sickness and death are but the rumors of a sanitized mystery enacted behind closed doors in the hospital--grandmother will not utter her last groans and die untidily on the couch in the living room. And perhaps most importantly (but this we do not pay attention to), the science he encounters at school is increasingly a science of abstractions -- forces and vectors, atoms and equations. And so he is deprived also of his living connection to trees, rain, and stars. The world recedes behind a screen, a veil of unreality.

I do not pine for the particular forms of a lost past. The question, rather, is how to replace what needs replacing, and with what. As things stand, the picture cited above leads to to a crushing conclusion, first elaborated so far as I know by the Dutch psychologist, Jan Hendrik van den Berg, at mid-century. Can we rightly complain, van den Berg asked, when the child grows up and somehow fails to "adjust"? Adjust to what? Nothing is there--everything is abstract, distant, invisible! And so the modern conclusion of the matter seems inevitable: we force the child to live within an inner fantasyland, cut off from the nurturing, reassuring matrix of visible, tangible, accessible structures and authorities that once constituted "community." No wonder the surreal world of the video game is his natural habitat. Nor will it do any good to trash the video games, if we find no way to replace them with real-world involvement.

To turn such a child over to the net for learning purposes is not a simple and automatic good. Can we structure the bewildering, abstract, game-like maze of possibilities into healthy learning experiences, appropriate to the child's age? Or will he be much more inclined to find here simply a yet more glorious video game landscape?

The "interface" between the young girl and her net pal is undeniably thin, one-dimensional, remote. As valuable as it may nevertheless be, it is not the missing key for redeeming the learning community. Even as a tool for promoting global understanding, it scarcely counts beside the much more fundamental--and deeply threatened--sources of social understanding. The girl, of course, will learn whatever she does of friendship from peers who sweat, bleed, taunt, curse, tantalize, steal, console, and so on. If I need to find out whether she will become a good world citizen, don't show me a file of her email correspondence. Just let me observe her behavior on the playground for a few minutes. (This assumes, of course, that she spends her class breaks on the playground, not at her terminal playing video games.) Unfortunately, the assessment is not likely to turn out positive so long as the schoolyard is hermetically isolated from any surrounding, multi-dimensioned community. And to see the net as an easy remedy for *this* kind of isolation is, at best, simplistic.

The danger of the net, then, is the very opposite of the romantic picture: it invites further de-emphasis of the single, most important learning community--the one consisting of people who are fully present--in favor of a continuing retreat into communal abstractions -- in particular, retreat into a community of others whose odor, unpleasant habits, physical and spiritual needs, and even whose challenging ideas, a student doesn't have to reckon with in quite the same way his neighbor demands.

The most bothersome thing here is our tendency to leap rather too easily from raw technology, or from simple images of its use, to far-reaching conclusions about extraordinary complex sociological issues. There is, after all, one absolutely unavoidable fact: technologies for "bringing people together" do not necessarily *bring people together*.

Before the news media went gaga about the information superhighway, there were asphalt superhighways. Didn't these bring us all closer together? In many ways they certainly did. The whole transportation revolution was no puny thing, even beside the computer revolution. It re-made society. We now brush up against each other in ways unimaginable in earlier eras. Few of us would want to give up all the new possibilities. But, still, the uncomfortable question remains: is that the spirit of "community" I feel as I peer over the edge of the superhighway at the dilapidated tenements below? And when I turn to the net for my commuting, will I lose even the view from the asphalt?

Actually, the rhetorical question is unnecessary. For the answer, in my case, is already given: I telecommute from my suburban basement, and rarely have occasion to venture very far out. I blame no one else--nor any technology--for this; the choices are my own. But one still needs to ask: how will technology play into the kinds of choices society (that is, we) are already tending to make? *Here* is the sort of question we should be asking when we gaze into the future. Some technologies naturally tend to support our virtues, while others give play most easily to our vices. I am dumbfounded that so many fail to see how the spreading computer technologies--in education as in many other arenas--not only offer distinct hopes but also tempt us with seductive overtures at a most vulnerable moment. It would be much easier to welcome the truly exciting things computers promise us, if one didn't see so many eyes firmly closed to already existing tendencies.

Perhaps my single greatest fear about the growing interest in networked learning communities is the fear that we will further undermine the human teacher. The most critical element in the classroom is the immediate presence and vision of the teacher, his ability to inspire, his devotion to truth and reverence for beauty, his moral dignity--all of which the child observes and absorbs in a way impossible through electronic correspondence. Combine this with the excitement of a discovery shared among peers in the presence of the actual phenomena occasioning the discovery (a worm transforming itself into a butterfly, a lightning bolt in a jar), and you have the priceless matrix of human growth and learning.

The email exchange between the young girl and her Indian counterpart, added to *such* an environment, could be a fine thing. (Actually, it is happening already, here and there.) But let's keep our balance. Surely the problems in modern education stem much more from the rarity of the aforementioned classroom milieu than from lack of student access to such net "resources" as overseas pen pals.

Many people in our society are extremely upset--justifiably so, in my opinion--with the current educational system. That gives some hope. But a dramatic and ill-advised movement toward online education may well be the one smoke screen fully capable of preventing an aroused public's focus upon the issues that really count.

Yes, the student will have to acquire net skills, just as he had to learn about word processors and the organization of reference materials in the

library. But this is not a new model of learning. The most evident new
model--not a very desirable one--lies still half-understood in the net's
undoubted potential for dispersing energies, distracting attention, reducing
education to entertainment, and--above all else--leading the
television-adapted student ever further from human community toward a world of
fantasies and abstractions, a world too artificially plastic and manipulable,
a world desperately removed from those concrete contexts where he might have
forged a sturdy, enduring character.

Let's give our teachers a realistic sense for the possibilities and the
challenges of the net, so they can soberly assess how it might further this or
that teaching goal. Let's *not* subject them to a tidal wave of blind,
coercive enthusiasm that adds up to the message: "connect as soon as possible,
or be left behind."

Stephen L. Talbott

NCSC 16 Announcement for RISKS

<Reiner@DOCKMASTER.NCSC.MIL>
Thu, 19 Aug 93 12:32 EDT

16TH NATIONAL COMPUTER SECURITY CONFERENCE
Dates: 20-23 September 1993
Location: Baltimore Convention Center Baltimore, Maryland
Registration fee: $275

The National Computer Security Center and the National Institute of Standards
and Technology will present the 16th National Computer Security Conference
from 20-23 September at the Baltimore Convention Center.

This year's three and one-half day program features tracks in : Research &
Development; System Implementation; Management & Administration; Criteria &
Evaluation; Tutorials & Other Presentations.

aA summary of the technical program follows. To obtain more information about
the technical program send a message to

NCS_Conference at DOCKMASTER.NCSC.MIL or
call the NCSC on 410-859-4371.

To obtain a registration form, call the Conference Registrar at
301-975-2775 or send a message to NCS_Conference at DOCKMASTER.NCSC.MIL

TECHNICAL PROGRAM SUMMARY:

R&D TRACK

PANELS - Strategies for Integrating Evaluated Products
Chair: J. Williams, MITRE
- Multilevel Information System Security Initiative
Chair: G. Secrest, NSA
- Trusted Applications

```
              Chair: J. Cugini, NIST
          - Best of the New Security Paradigms Workshop II
              Chair: H. Hosmer, Data Security Inc.
          - Enterprise Security Solutions
              Chair: P. Lambert, Motorola

   PAPER SESSIONS - Honesty Mechanisms
                      Chair: E. Boebert, SCTC
                  - Database Research
                      Chair: M. Schaefer, CTA
                  - Access Control
                      Chair: P. Neumann, SRI

  SYSTEM IMPLEMENTATION TRACK

    Panels: - Perspectives on MLS System Solution Acquisition
              Chair: J. Sachs, ARCA
            - Network Management -- The Harder Problem
              Chair: R. Henning, Harris Corp.
            -  Application of INFOSEC Products on WANs
              Chair: J. Capell, Lockheed
            - Security for the Securities Industry
              Chair: S. Meglathery, NYSE

   Paper Sessions:  - Access Control Topics
                      Chair: D. Balenson, TIS
                    - Network Risks & Responses
                      Chair: B. Burnham, NSA
                    - Software Engineering
                      Chair: V. Gibson, Grumman
                    - System Engineering with OTS Products
                      Chair: M. Tinto, NSA
                    - Network Implementation
                      Chair: F. Mayer, Aerospace Corp

  MANAGEMENT & ADMINISTRATION TRACK

   PANELS - Virus Attacks & Counterattacks: Real World Experiences
              Chair: J. Litchko, TIS
          - Terror at the World Trade Center
              Chair: S. Meglathery, NYSE
          - Contingency Planning in the 90s
              Chair: I. Gilbert-Perry, NIST
          - On a Better Understanding of Risk Management Techniques
              Chair: S. Katzke, NIST
          - Security Awareness, Training & Professionalization
              Chair: D. Gilbert, NIST
          - Accreditor's Perspective - How Much is Enough?
              Chair: J. Litchko, TIS
          - Security & Auditability of Electronic Voting Systems
              Chair: R. Mercuri, U. of Penn.
          - Protection of Intellectual Property
              Chair: G. Lang, Harrison Ave. Corp.
          - The Privacy Impact pof technology in the 90s
```

Chair: W. Madsen, CSC
- Electronic Crime Prevention & Investigation
Chair: R. Lau, NSA

PAPER SESSION - Managing & Promoting INFOSEC Programs
Chair: D. Parker, SRI

TUTORIALS & PRESENTATIONS TRACK

Tutorials: - Threats & Security Overview
A. Liddle, IRMC
- Trusted Systems Concepts
C. Abzug, IRMC
- Trusted Networks
R. Bauer, E. Schultz, ARCA
- Trusted Databases
G. Smith, W. Wilson, ARCA
- Trusted Integration & System Certification
J. Sachs, ARCA

Panel Presentations: - CLIPPER Chip
Chair: L. McNulty, NIST
- Getting Your Work Published
Chair: J. Holleran, NSA
- INFOSEC Standards: The DISA Process
Chair: W. Smith, DISA
- Security Requirements for Cryptographic
Modules; Chair: L. Carnahan, NIST

CRITERIA & EVALUATION TRACK

Presentations: - Introduction to the Federal Criteria
G. Troy, NIST; D. Campbell, NSA
- Federal Criteria: Protection Profile Development
J. Cugini, NIST; M. DelVilbiss, NSA
- Federal Criteria: Registration of Protection Profiles
D. Ferraiool, NIST; L. Ambuel, NSA

Panels - Federal Criteria: Protection Profiles for the 90s
Chair: R. Dobry, NSA
- Federal Criteria: Vetting & Registration of Protection Profiles
Chair: L Ambuel, NSA
- Evaluation Paradigms: Update on TPEP and TTAP
Chair: S Nardone, NSA
- European National Evaluation Schemes
Chair: E. Flahavin, NIST
- The European Evaluation Process
Chair: P. Toth, NIST
- International Harmonization I
Chair: Y. Klein, SCSSI, France
- Goals & Progress Toward the Common Criteria
Chair: G. Troy, NIST
- Federal Criteria User Forum

Chair: C. Wichers NSA

Plenary: "Information System Security Strategies for the Future"
Chair: Stephen Walker
Panel: James P. Anderson
Dr. Willis Ware
Dr. Roger Schell

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 87

Wednesday 25 August 1993

Contents

Mars Observer

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 26 Aug 93 9:48:10 PDT

I've been holding off on running anything on the Mars Observer, hoping for either a miraculous recovery or further details on what actually happened. In this case, no news is bad news; hopes for restoring communications with the $1B spaceprobe are dwindling rapidly, and details on what happened may never be known. Communications were interrupted at 6 p.m. on Saturday, August 21, just after the Observer had pressurized its propulsion-system fuel tanks, preparatory to the rocket firings that would slow it down and allow it to be captured by Martian gravity --- placing it in orbit around Mars. The subsequent request to switch on its antenna received no response. Up until that point the mission had been relatively trouble free --- except that on two occasions the spacecraft's instructions had to be revised to overcome temporary problems. Even if command communications from the ground failed, the mission had been programmed to attain orbit anyway, if a few assumptions were satisfied --- such as that the backup programs worked and the antenna was functioning properly,

On Monday (August 23), Glenn Cunningham, project manager at the Jet Propulsion Laboratory speculated on several possible scenarios that might have caused the failure: the Observer's onboard clock may have stopped; the radio could have overheated; its antenna could have gone askew. On Wednesday, John Pike of the Federation of American Scientists noted that, because the disruption of communications coincided with the precise moment that the spacecraft was programmed to pressurize its helium tank (which in turn pressurizes the hydrazine-oxygen fuel system), the increased pressure might have caused a leak in one of the helium lines or a *virtual explosion*. He added that if the leak were pinhole-sized, the spacecraft would now be spinning. If it were larger, the spacecraft would be completely out of control. Cunningham disclosed that, while the spacecraft was being built, a slow leak had been discovered in the original helium tank. which was replaced. Meanwhile, silence persists.

The $1.4B Galileo spacecraft en route to Jupiter is also experiencing difficulties. Its main antenna jammed, and it can transmit only very slowly with its low-gain antenna. It is supposed to photograph an asteroid named Ida, beginning on Saturday. [Gilbert and Sullivan wrote on operetta on that subject about one hundred years ago -- Prints Is Ida.]

These problems come on the heels of the continued launch delays on the latest Discovery mission, a weather satellite that died in orbit last week after an electronic malfunction, and the Navy communications satellite that was launched into an unusable orbit from Vandenburg last March ($138M). Shuttle launches are seriously delayed, which is likely to affect the planned space walk to repair the Hubble Telescope, currently scheduled for December.

[This summary report is based on articles in the *San Francisco Chronicle*, August 23 by John Noble Wilford of *The New York Times*, August 24 from the *Los Angeles Times*, and August 25-26 by David Perlman, Chronicle Science Editor.]

Chronicle of a bug foretold

Paul Eggert <eggert@twinsun.com>
25 Aug 1993 20:05:14 -0700

I've often wanted something like a National Weather Service for software failures -- an early warning system that would let us know a few days or hours before trouble strikes. Well, sometimes daydreams can become true, at least in special domains. Here are two forecasts:

On August 28, 1993, at 2 AM local time, workstations and PCs in Israel

> that are running Sun's Solaris 2.2 will suddenly lose an hour.
>
> On October 24, 1993, at 2 AM local time, Solaris 2.2 workstations and
> PCs in the British Isles will _not_ lose an hour. Unfortunately,
> everyone else there will be turning back their clocks that morning.

These failures will occur because of errors in Solaris 2.2's time zone tables, which seem to stem from a configuration management problem. When going from Solaris 1 to Solaris 2, Sun's software developers somehow reverted to an early 1989 version of Arthur David Olson's public domain time zone tables, thus discarding all time zone changes due to laws passed by parliaments since then. Given the AT&T/Sun proprietary notices that are plastered over the Solaris 2 tables, I would guess that AT&T bears some blame for this bug and that other SVR4 Unix hosts may have similar problems.

If you're technically inclined and have a Solaris 2 host handy, you can confirm the bug by running the command `/usr/sbin/zdump -v Israel | grep 1993' (similarly for `GB-Eire'). To fix the bug, apply the `zic' command to Olson's latest tables, which you can FTP from elsie.nci.nih.gov:pub/tzdata93d.tar.Z.

> [I wonder what happened in Kwajalein, where there was NO Friday, August 20, 1993. Thursday night at midnight Kwajalein switched sides with respect to the International Date Line, to rejoin its fellow islands, going from 11:59 p.m. Thursday to 12:00 m. Saturday in a blink. Are there any RISKS readers out there who have anything to report? PGN]

Quote for the Day

Brinton Cooper <abc@ARL.ARMY.MIL>
Wed, 25 Aug 93 20:11:10 EDT

...out of context, of course.

>From "Computer Organization and Design--the Hardware Interface" by David Patterson and John Hennessy:

> "...minimizing the logic is both complex and error-prone
> and, thus, is better left to a program."

_Brint

RISKS of elaborating on exploitation of known RISKS

David P. Reed <reed@interval.com>
Tue, 24 Aug 93 09:45:29 PDT

The posting on RISKS or any other mailing list of novel ways to exploit defects in systems to commit crimes is itself a RISK of the technology that makes RISKS possible. The inclusion of "smart answering machine" hacks as a new subtopic is a little disturbing to me personally. In the early '70's I devoted a reasonable amount of time to "tiger team" activities (sponsored by

ARPA) to learn how secure typical computer systems were (TENEX, Unix, and Multics, e.g.).

As such, I had a lot of time to think about what to do with what I learned. I offer the following suggested social ethic around mitigating the risk-amplification RISK associated with publishing RISKS, while preserving the benefit of identifying risks.

There is a big difference between discovering and publishing a generic weakness such as "programming a smart answering machine with weak security to carry out tasks on your behalf", and the second level of inventing the cleverest or most profitable scenario for use, and publishing a detailed cookbook approach to using the weakness for committing various crimes. This doesn't illuminate the weakness further, unless you posit that your audience is stupid. RISKS readers are not.

A reasonable rule, then, is to identify and publish broad categorizations of weaknesses, but it probably amplifies the risk for all of us to then broadcast to everyone the cleverest exploitations of those risks you can think of.

I carry to my grave some wonderfully clever ways to make myself rich, destroy my enemies, and earn the perverse fame and glory associated with destructive or prankish hacking. But my conscience would hurt if others were hurt by my dissemination of these ideas.

Re: RISKS of elaborating on exploitation of known RISKS

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 26 Aug 93 10:34:12 PDT

David Reed discusses a very sticky wicket that has been discussed repeatedly in RISKS. The biggest problem with not having the flaws publically discussed is that supposedly unknown flaws tend NEVER to get fixed. The general compromise strategy seems to be to inform people who might actually do something about discovered flaws, and then if those folks do nothing, let the flaws be known.

There is a pervasive need for knowledge that particular schemes are intrinsically unsafe/unreliable/unsecure. Many people are living with blinders on, as is evidenced by the recurrence of the same types of problems, over and over. Almost every remotely controllable answering-machine system is vulnerable today. Cellular phones are intrinsically vulnerable today. How many installations run with the sendmail debug option enabled? How many .rhosts files permit file systems to be accessible remotely? Does anyone care?

Cisco routers

Al Whaley <Al.Whaley@sunnyside.com>
Wed, 25 Aug 1993 12:56:54 -0700 (PDT)

Rumors abound that Cisco routers have a back door; that is when a TCP port is disabled, it can still be accessed from Cisco's IP number.

I have personally verified this with the sendmail port.

Al Whaley   al@sunnyside.com   +1-415 322-5411(Tel), -6481 (Fax)
Sunnyside Computing, Inc., PO Box 60, Palo Alto, CA 94302

[Private trapdoors for developers and maintenance folks are remarkably common, and in many other cases represent more serious risks than this one. WarGames was not pulling your leg. PGN]

[***** NOTE ADDED ON 2 SEP 1993 TO THE ARCHIVE COPY: Subsequent discussion has indicated that the above noted rumours are UNFOUNDED. PLEASE SEE RISKS-15.01 FOR CLARIFICATION. PGN *****]

Phone Number Gridlock Looms

Sanford Sherizen <0003965782@mcimail.com>
Wed, 25 Aug 93 12:31 GMT

A *Los Angeles Times* article by Jube Shiver Jr. printed in the Sunday *New Hampshire News* (Aug. 22, 1993) states that Bellcore will phase out oversight of number allocation in the next 12-18 months. Bellcore's decision will affect the rate at which new communication technologies can be put into service and the complex task of allocating numbers will have to be administered by some other organization.

Number allocation includes areas codes, five-digit long distance carrier identification codes, some local phone numbers and codes for toll-free and 900-prefix information services.

According to the article, Bellcore was abandoning this free role in response to what its president called unfounded complaints by its rivals that it might discriminate in favor of its owners in the distribution of new phone numbers.

This change occurs at a time when federal regulators are preparing to authorized the first of a host of new communications services. Bellcore's announcement followed a surprise FCC decision earlier this month to halt the company's planned assignment of 500 service-access codes to personal communications services (PCS). The FCC cited industry concern that several of Bellcore's owners were among those vying for the new codes.

Sanford Sherizen, Data Security Systems, Natick, MA

Digital markets

Phil Agre <pagre@weber.ucsd.edu>
Wed, 25 Aug 1993 17:11:21 -0700

The following article provides an exceptionally clear account of computerized high finance centered on so-called "derivative products". These are (among other things) ways of buying and selling debt streams with given properties. For example, a company in need of short-term cash might exchange a bundle of 30-year home mortgages (which provide money with high reliability but at low rates of return and over a long period) in favor of a bundle of junk bonds (which provide money with lower reliability but at higher rates of return and on a variety of schedules).

Robert Lenzner and William Heuslein, How derivatives are transforming Wall Street, Forbes 151(7), 29 March 1993, pages 62-72.

This is Forbes, though, so the critical perspective is pretty much missing. For that you might turn to a new book by a New York Times reporter:

Joel Kurtzman, The Death of Money, New York: Simon and Schuster, 1993.

This is a wide-eyed account of how the truly gigantic international flows of cash, greatly facilitated by computers and telecommunications, are changing economic institutions and theories. For example, he interviews mathematicians and physicists who engage in high-powered zaitech (financial engineering) for Wall Street companies.

I'm not entirely comfortable with the book. I don't think it's successful in its argument that a radical change in the very nature of money is making neoclassical economics obsolete. (Neoclassical economics may be obsolete anyway, of course, but that's another topic.) For example, he places an awful lot of weight on the end of the gold standard. And regular economists will argue that most fancy zaitech is just arbitrage, which (they say) simply makes markets function more efficiently.

His main arguments for a computer-based risk to society are based on observations about market volatility and a critique of "speculation". On the topic of market volatility, you'll have to read his argument about the 1987 stock market crash and see for yourself. And he really doesn't give us enough information to form any very novel opinions on the common view that rapid, quantitative investment decisions, by focusing on short-term fluctuations, ignore and thus undermine market "fundamentals". Nonetheless, I do recommend the book as an introduction to the people and numbers. He also cites some of the more technical literature.

On a related topic, I cannot recommend highly enough the following book:

Stanley M. Davis, Future Perfect, Reading, MA: Addison-Wesley, 1987.

Davis is a management consultant who sees an amazing future in which computer and telecommunications technology, among other things, changes the nature of many products and markets through dramatically more rapid and specific responses to changing customer needs.

The book is hard going and downright weird in places, but it's full of remarkable speculations. For example, he suggests that businesses try as much as possible to separate the "material" and "information" dimensions of a product, combining them as close to the customer as possible. The idea is that information (a) can be moved much faster than physical materials and

(b) is much more amenable to rapid and highly specific customization, and so therefore should be processed in a centralized way, whereas physical materials should be distributed as widely as possible to minimize delivery times.

What does this mean in practice? You'll have to hire a management consultant to help you figure that out.

Phil Agre, UCSD

Re: Everyone gets a 'A' for Welsh exam

<lhe@sics.se>
Tue, 24 Aug 93 09:29:01 +0200

A similar thing happened in Sweden last week. Due to a programming errors, some positions for studying to dentists in Gothenburg were given to applicants with the poorest grades!

According to Swedish law, a formal decision to enroll someone in a university program can't be revoked so the University of Gothenburg has no choice but to accept these students.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263
S-164 28 KISTA, SWEDEN lhe@sics.se +46 8 752 15 09 Fax: +46 8 751 72 30

InfoTech Security and Control, Conference Report

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.d400.de>
Mon, 23 Aug 1993 18:52:59 +0200

Report on an International IFIP Working Conference on
"Security and Control of Information Technology"
(Stockholm-St.Petersburg August 12-17,1993)

From: Klaus Brunnstein, University of Hamburg (August 21, 1993)

Under the auspices of the International Federation for Information Processing (IFIP) WG 9.6 "IT Misuse and the Law" (chairman: R.Sizer/UK), an International Working Conference on "Security and Control of IT in Society" was held on a ship plying between Stockholm and St.Petersburg, prepared by University of Stockholm (Ann Marie Bodor, Louise Yngstroem). Attended by about 60 active participants, this event included one day in St. Petersburg's Russian Academy of Science's Steklov Mathematical Institute, packed with information on the status of IT Security and Legislation in Russia, prepared by Eldar Musaev (St. Petersburg) and Simone Fischer-Huebner (Hamburg).

Following the dominant professional interests of participants, almost equally divided into technical and legal aspects, the program onboard the ship was dominated by often rather controversial discussions about legal versus technical aspects. This biased approach was even stimulated by an introductory panel discussing the thesis that "Law cannot help to Control IT Security", intending to argue in traditional (Oxfordian) debate style about pro's and contra's of legal IT regulations. Though well-intended, this debate may have set an unhappy start of an otherwise stimulating event (the thesis was rejected in a voting process with majority).

The onboard program's first part was devoted to legal aspects, esp. dealing with privacy. Here, a paper presented by Norwegian anthropologist Rolf Lunheim in cooperation with computer scientist Gottorm Sindre gave several examples that privacy is rather inconsistently understood in different cultures. Such different views even between Western participants became evident in the presentations of some leading privacy and law experts, which used the term in their resp. cultural understanding. Here, Bieke Spruyt and Bart de Schutter (University of Brussels) discussed whether an International Law on Security of Information Systems is emerging; they saw needs for such standardisation and pointed to few emerging building stones of future regulations, such as the OECD guidelines, which were presented in good detail later by Richard Hackworth (Berkhemstead), UK member of the OECD expert panel which developed these guidelines.

Within the legal stream, Margaret Jackson (Royal Melbourne Institute of Technology) contributed significant details in describing the status of Australian IT-related legislation, including such diverse areas as intellectual property protection, civil and criminal law. She also described proactive contributions by Australian courts and commissions. Moreover, she gave interesting details about developments in selected countries in the Asia-Pacific region (e.g. Korea) in related legal fields.

Completing the critical survey of state-of-law, Lawrence F. Young (University of Cincinnati, Ohio) presented his analysis of "Utopians, Cyberpunks, Players, and others Criminals: Deterrence and the Law" with special emphasis on the contemporary US situation. After describing shortcomings of US federal and state laws, he analysed diverse forms of computer crimes, including violations of privacy and intellectual property, interruption and theft of services, larceny, espionage etc. He concluded that even recent US laws need serious revision, including extension in scope and more uniform formulations to make them comparable and applicable over US federal states' boundaries.

In some contrast with the analysis concentrating on the legal situation, Ruud Ketelaar (Amsterdam) and Simone Fischer-Huebner (University Hamburg) addressed both legal and technical aspects by arguing that some IT security mechanisms (e.g. collecting audit trails) further invade privacy and protection of personal data, thus even enlarging the legal problems. Besides some rather controversial discussion whether the term "confidentiality" as used in IT security discussions may be understood as somehow equivalent to "privacy" in legal fields, Ketelaar's and Fischer-Huebner's contribution were the only ones to transgress the evident gap between lawyers and technicians.

The "Russian Day" held Saturday on solid ground in St. Peterburg unvealed surprising insights into implications which the recent dramatic political changes (known as "perestroyka") produce in Russian society, esp. such ones related to IT Security. In his introduction into "IT versus Security in Russia", Eldar Musaev (Steklov Mathematical Institute, Russian Academy of Sciences, St.Petersburg) presented examples of major incidents in Russia in recent years. Probably the most shocking one was the theft of a computer including a database of Chernobyl victims and related statistics; as no backup was done due to lack of magnetic media, this database was definitely lost. Until now, it is unclear whether the thieves were merely interested in the computer (which is the likely assumption) or were interested in the database.

Most interesting contributions concerned the constructive approaches to improve technical and legal instruments for preventing or fighting IT misuse. Here, Yuri Andreevich Timofeef, chairman of Russia's National Subcommittee (127) on methods and means of information protection, reported about the systematic approach which is undertaken by several cooperating institutions to establish a basic concept (including definition of terms) as well as national IT security criteria for both IT products and systems, for government, commercial and private applications. These "Russian IT Security Evaluation Criteria" published in late 1992 (in Russian) in 5 volumes adapt other criteria (esp. US-TCSEC and Europe-ITSEC) to Russia's national needs. Related to this developments of concepts, a Russian IT security industry (with yet more than 50 enterprises in Moscow) has yet developed as experts from former military IT security fields are seeking for commercial jobs, and with several new products and ideas, accompanied by a National conference and a new Russian Journal on IT Security.

Closely related to Russian IT Security concepts as well as to the present development of a new constitution including principles on both the right for information and the right for private life and private mail, Andrey Petrovich Kurilo (Moscow), head of department of information technologies security branch in the State Technical Commission of Russia described the structure of the emerging Russian IT related legislation. Here, the Russian Draft InfoSEC Act aims at covering almost all fields, including:

1) Administrative and Physical Protection,
2) Protection against unauthorized access to information
   in single systems (somehow comparable to COMPSEC),
3) Protection of information and availability in networks
   (comparable to COMSEC),
4) Protection of Electronic Document Interchange, including
   regulation of digital signatures,
5) Protection from compromising secrecy by detection of
   signals and electromagnetic radiation (TEMPEST-like),
6) Protection from malicious software (viruses etc), and
7) Protection against threats to Intellectual Property,
   illegal copying etc.

In the legislation process, several "secrets" shall be legally protected (addressing operations of state and military, commerce, banks, as well as concerning personal data, microcircuits and digital signatures). Here, appropriate criminal, civil and labour laws are being developed.

As examples of Russian ITSEC legal approaches, a paper on "Legal aspects of digital signature standardisation" was presented by Viktor V. Markelov (Federal Agency of Government Communication and Information, Moscow), which was later nicely complemented by a survey about work, problems and developments in Germany by Kathrin Dippel (Darmstadt/Germany). Moreover, an example of a new Russian product was the description of an AntiVirus product (AIDSTEST), which was said to protect the user against over 95% of present and future viruses. Mixed in between the Russian papers to exchange also information from West to East, overviews of Western developments presented OECD Guidelines (Hackworth), US Federal Criteria (Abrams) and IT Security Policies (White).

Back onboard, the last day centered on technical discussions concerning IT security classification, education and esp. problems of electronic signatures. This was somehow "interrupted" by Larry Young's contribution and by an overview of IFIP's present activities in formulating a "Framework for Codes of Ethics and Professional Conduct", presented by Conference Chairman Richard Sizer (UK).

An overview of "Recent Development in IT Security Evaluation" was presented by Kai Rannenberg (Freiburg/Germany), who overviewed and compared approaches from Orange Book to Europe's IT Security Evaluation Criteria (ITSEC), the Canadian approach (CTCPEC) and the recent US Federal Criteria (FC-ITS) with concepts discussed in ISO working groups. While Rannenberg suggests "facets of security and services" as new ordering scheme, Marshall Abrams (MITRE, McLean/Virginia) in his distinguished way described a "Symbiosis among IT Security Standards, Policies, and Criteria" where he presented both progresses and demands for research in miscellaneous fields. He esp. mentioned "assurance" as ill-understood, and he suggested that multiple policy models be analysed to select the most adequate one for an economic or governmental organisation's demand. Both presentations reviewed the IT Security with critical view towards shortcomings in the technical concepts but the papers as well as related discussions did not explicitly analyse basic paradigms inherent in InfoSEC concepts nor did they describe implied social risks.

One of Marshall Abram's conclusions about IT security policies was that "If security is everybody's obligation, it is nobody's obligation". This seemed to be in contradiction with a position which Peter White, security consultant from Ipswich/UK presented in his paper on "Preparing System Security Policies". Based on a formal framework, he described results of a survey about evaluations of experienced threats and countermeasures against theft, infiltration and loss of confidence. To enforce general System Security Policies in organisations, every persons must behave according to her/his responsibility, rather than projecting security demands on "secure and safe" systems including security managers.

In two final workshops, potential impact of the OECD Guidelines (chaired by Richard Hackworth) and relations between legal paradigms and InfoSEC (chaired by Peter White) were discussed. With some suggestions for future work and some clarification of terms which before may have been differently understood, the conference at this stage may have overcome some gaps in understanding between the InfoSEC and the Law parties as observed before. Apart from the rather general notion that both Law and InfoSEC act within society and affect it, it remained open what the specific social implications of InfoSEC might be which the parent committee IFIP TC-9 "Relationship between Computers and Society" is concerned with.

Summarizing and assessing the value of this event, two essential steps were taken which may produce future insights. First, the start of an information exchange between Russia and other countries alone was worth the trip to St. Petersburg. Second, besides many interesting contributions, the onboard conference may be regarded as an initial step in bridging the evident gap between ITSEC professionals, law experts and other fields (like sociology and anthropology) presently less active. In this sense, the Conference Proceedings (to be published by Elsevier/North Holland in fall 1993) will surely form an interesting basis for future work.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 88

Wednesday 25 August 1993

Contents

Re: Mars Observer (Neumann, RISKS-14.87)

Lee Mellinger <leem@tsunami.Jpl.Nasa.Gov>
Thu, 26 Aug 1993 20:29:45 GMT

Just a few comments. I'm on the Mars Observer project, and some of the information published in public sources has been somewhat misleading or incorrect. First, the spacecraft did not cost $1B, is was about $300M, the Titan booster was about $500M and ground systems and ops about $200M. In NASA's new way of doing business all costs are lumped together, so to make a fair comparison to other projects, you must understand that the costs quoted in the past did not cover the launch and sometimes not the ground system. Second, the communications with the spacecraft were not "disrupted" [actually David Perlman in the Chron said Pike noted that Mission Control engineers at JPL had ``lost contact with the Mars Observer'' --- PGN] as John Pike has said, nor "interrupted", they were intentionally turned-off. The transmitter

beam voltage was shut down to protect the filament when the fuel and oxidizer
pyro valves were blown to pressurize the tanks. The beam voltage was supposed
to be turned back on after the tank pressurization event by the command
sequence stored in the SCP, the spacecraft control processor. We do not konw
what happened after the beam-off was executed because the downlink was not
seen again, and that is all we know for sure.

We have been commanding a series of events, presuming that certain scenarios
have occurred. None has been successful as far as we know. We continue to
send commands because the Command Detector Unit is connected to the Low
Gain Antennas and do not require precise pointing by the spacecraft to
achieve command reception.

We do not know that whatever happened, happened when the pyro valves were fired
because that did not occur until sometime after the beam voltage was turned
off. There was a time interval to allow sufficient cooling of the filament.

We are at this moment waiting for the expiration of the the secondary
command loss timer, which will reconfigure the spacecraft telecom to 10bps
and the Low Gain Antennas for downlink. That will occur (assuming that
no commands have be accepted since last Friday) at 93/238-21:56:35 UTC,
that is today, the 27th at 14:56:35 PDT.

Lee F. Mellinger, Caltech/Jet Propulsion Laboratory - NASA, 4800 Oak Grove Dr.
Pasadena, CA 91109 818/354-1163 leem@jpl-devvax.JPL.NASA.GOV

Re: Mars Observer (RISKS-14.87)

Michael Stern <stern@deshaw.com>
Thu, 26 Aug 1993 17:15:33 -0400

Unfortunately I can not provide the names of my sources for this material,
as it would not be fair to them. Treat anonymous sources with appropriate
skepticism; I think you'll find this an interesting tidbit nonetheless.

Apparently the tank pressurization system on the Observer was tested
exactly once, and it "blew up." Whether this phrase is meant to imply
an explosion or merely a bad leak is an exercise left to the reader.

NASA had one spare tank.

Result: the Observer was launched with the second tank, with no further
testing or development.

/stern

Re: RISKS of elaborating on exploitation of known RISKS

Bob Brown <bbrown@gmcf.org>

Thu, 26 Aug 93 15:52:58 EDT

The issue raised by David P. Reed is indeed sticky, and I agree with the moderator that the first step upon identifying a risk is to bring it to the attention of someone who can do something about it.

In some cases that someone chooses, for whatever reason, to do nothing. In other cases, there *is* no someone. Smart answering machines are as good an example as I can think of. Publishing a "generic" warning doesn't give one (er, at least not *this* one) enough information to realize that DTMF tones can be recorded on the answering machine, then played back into the phone network.

Somewhat reluctantly I find I have to disagree with Reed. Publishing specific details of RISKS does create the risk that someone will exploit those details. *However*, trying to express risks generically doesn't do much to keep bad guys from exploring and exploiting the RISKS. The bad guys will take time to think about the generic risks, searching for areas to exploit. The good guys (that's us) will probably *not* take time to ponder the generic risks, but we probably will respond to a report of a specific threat.

Re: RISKS of elaborating on ... known RISKS (Reed, RISKS-14.87)

Douglas W. Jones <jones@pyrite.cs.uiowa.edu>
Thu, 26 Aug 93 13:47:21 CDT

... discussed... Not only in RISKS! Consider the following essay, quoted from Charles Tomlinson's Rudimentary Treatise on the Construction of Locks, published about 150 years ago. (This quote has been bouncing around the net for a while, but it bears repeating.) These issues have been hashed over for a long time!
          Doug Jones jones@cs.uiowa.edu

> A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and already know much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lockpicking long before locksmiths discussed it among themselves, as they have lately done. If a lock -- let it have been made in whatever country, or by whatever maker -- is not so inviolable as it has hitherto been deemed to be, surely it is in the interest of *honest* persons to know this fact, because the *dishonest* are tolerably certain to be the first to apply the knowledge practically; and the spread of knowledge is necessary to give fair play to those who might suffer by ignorance. It cannot be too earnestly urged, that an acquaintance with real facts will, in the end, be better for all parties.

Some time ago, when the reading public was alarmed at being told how
London milk is adulterated, timid persons deprecated the exposure, on
the plea that it would give instructions in the art of adulterating milk;
a vain fear -- milkmen knew all about it before, whether they practised
it or not; and the exposure only taught purchasers the necessity of a
little scrutiny and caution, leaving them to obey this necessity or not,
as they pleased.

... The unscrupulous have the command of much of this kind of knowledge
without our aid; and there is moral and commercial justice in placing
on their guard those who might possibly suffer therefrom. We employ
these stray expressions concerning adulteration, debasement, roguery,
and so forth, simply as a mode of illustrating a principle -- the
advantage of publicity. In respect to lock-making, there can scarcely
be such a thing as dishonesty of intention: the inventor produces a lock
which he honestly thinks will possess such and such qualities; and he
declares his belief to the world. If others differ from him in opinion
concerning those qualities, it is open to them to say so; and the
discussion, truthfully conducted, must lead to public advantage: the
discussion stimulates curiosity, and curiosity stimulates invention.
Nothing but a partial and limited view of the question could lead to the
opinion that harm can result: if there be harm, it will be much more
than counterbalanced by good.

Telephone verification (Re: Grodberg, RISKS-14.85)

not Swift, not Suiss, Swiss!)
Thu, 26 Aug 93 14:36:04 -0400

I'd like to comment on my experience with Citibank on this.

About a year ago, I called to confirm receipt of a new card. For verification, the representative on the other end asked for my zip code (which, if someone had intercepted this card in the mail, or found it in my wallet, would be easily known), then for my mother's maiden name.

Trained by RISKS reading to look for security holes when giving out personal information, I asked, "Do _you_ know my mother's maiden name?"

"No." (Imagine the implications if she'd said "Yes"!)

"So I could tell you anything, couldn't I?"

"Yes, but we'll use that next time you call as verification."

"But, if I weren't the person who was supposed to have this card, I could tell you anything, and have the use of this card."

"Um, yes. Hmmm..."

To her credit, the rep seemed to understand the problem once it was pointed out, and promised to bring it up "at the next meeting".

A few months ago, when I had to repeat the procedure, the rep asked for my SSN (he was willing to accept a subset of the digits when I expressed reluctance), then for the maiden name, which will be used for future verification. (I suppose I should have asked if he already knew my SSN or not...)

Of course, this means that my mother's father's last name has now become information I have to regard as "confidential".

Citibank gives out an ATM PIN with it's cards. Why in the world they don't use that as telephone authentication (after some intial check like the SSN to confirm the right person got the card and the PIN), I have no idea. Wouldn't it be easier to use information I already keep secure, rather than ask me to keep other information - which, prior to this, I might have given out with a thought - secure?

On a side note: preparing this post made me realize that, although I haven't thought about it in years, keeping my Social Security card in my wallet probably isn't the best of ideas.

Tom Swiss/tms@cs.umd.edu

Re: Digital Markets (Agre, RISKS-14.87)

A. Padgett Peterson <padgett@tccslr.dnet.mmc.com>
Thu, 26 Aug 93 14:46:09 -0400

>What does this mean in practice? You'll have to hire a management consultant
>to help you figure that out.

In the computer world we have been seeing this for some time: buy software (really the documentation) once, and everything thereafter is electronic. One of the first was "Using MS-DOS Kermit" from Digital Press. The software is "free", however since the on-line documentation is now minimal (last full copy I have is dated 1989), the book is a near necessity, only the updates come with the software when you FTP it (ver 3.13 now). Of course we are now getting to the point where you need to buy the second edition also to stay current 8*(.

Another example is the use by some manufacturers of "Flash ROMs", while this is supposed to be an aid to updating, it looks more like an excuse for slip-shod engineering (we had several from a well-known manufacturer who shall remain nameless but is famous for selling high priced monitors as "15 inch" that have 13.8 inch (diagonal) viewing surfaces that would not recognize a "three finger salute" until the ROM was updated...).

In the same token, Compuserve seems to be becoming the center for software updates & "slipstreams" for problems that should never have occurred. (For me, US Sprint & a Supra 14.4 modem (plugs) make direct connections to the mfr - those that do not have FTP sites that is - cheaper than the Compuserve hourly charges for anything interesting).

Once upon a time, software was difficult to update so manufacturers, those that expected to stay in business, took pains to test software before releasing it. DOS 3.3 lasted from 1987 to 1991 (admittedly partly because DOS 4.x didn't work). Today the world seems to be one long beta test.

What we might expect in the future is "upgradable" hardware. Want to toast bagels in your four-slice pop-up ? Dial 1-900-4NOBURN and connect to the serial port. Your washing machine doesn't do the newest fabrics properly ? 1-900-NEWDUDS. Automotive recalls do not require stopping at the dealer, just an ISDN connection. Latest & greatest or just an invitation to do away with quality control ? You decide.

Padgett

Re: Child-Prodigy or Prodigy-Child? (Schiller, RISKS-14.86)

<Bob_Frankston@frankston.com>
Thu, 26 Aug 1993 15:23 -0400

Jeff writes; "At MIT I supervise the campus computer network, the MIT portion of the Internet. We have an internal policy that we do *not* monitor messages between individuals. We, however, state that our staff *may* inadvertently encounter personal mail due to our maintenance activities (more then likely because the mail system barfs and the message is delivered to the dead letter bin for manual routing)."

In my own gateway implementation, I purposely suppress the body of messages that get reported to the administrator. Systems designers need not only refrain from invading privacy but proactively avoid inadvertent disclosures. Perhaps one should go so far as to simple scrambling of email messages stored on disk simply to avoid inadvertent display when looking at system logs or dumps.

First Class mail tends to be sent in envelopes. Those who send post cards are accepting the risks of disclosure.

911 & Call Privacy *67 problems (US West) [David Kovanen]

Richard Jensen <rjensen@mimir.persistence.com>
Thu, 26 Aug 93 11:43:23 PDT

I've forwarded this by request of David Kovanen [kovanen@first.com].

Richard Jensen, Persistence Software, Inc., rjensen@persistence.com

----- Begin Included Message -----

Date: Wed, 25 Aug 1993 20:07:25 PDT
From: uunet!First.Com!Kovanen (David Kovanen)
To: wizard@moz.hookup.net

Subject: 911 & Call Privacy *67

I recently ran into an embarrassing problem that was created by my local telephone company (US West.) The problem involved the new "Caller ID" feature and my local police @ 911.

In anticipation of the introduction of Caller ID here in Washington state I began to insert *67 before all telephone numbers in my computer dialing directory. After all, I didn't want people calling me back on my data line.

Everything worked fine up until February 1993. At that time US West began to install a new and "improved" version of the call blocking software. This "improved" version resulted in several calls from my computer to 911:

Previously, a computer could dial *67 and immediately dial the desired telephone number without waiting for a second dialtone. (As can still be done with *70 to block Call Waiting.)

The "improved" Central Office software now *REQUIRES* that the dialing device wait for a second dialtone and the C.O. ignores all dialed digits for approximately 1/2 second after the code has been dialed. There is no technical reason for this to be done, other than the fact that US West dislikes being forced by the Utilities Commission to offer Caller ID blocking.

Here is the problem: I was calling a local telephone number, 572-5911 as follows: "ATDT*675725911". The four digits after the *67 (572-5) were suddenly ignored and the call promptly went to 911! It took several tries until I realized what happened.

It is important to note that the operation of most of the central Office codes still do not insert this mandatory pause, including *67 prior to February 1993.

There is one other problem with Call Vlocking that people with laptops should be aware of: *67 CAN NOT be dialed from a line that has blocking enabled for all calls. Thus, if you use your laptop on some lines with blocking and some without, you must keep two entries in your directory. This is a pain! It should be possible to dial *67 on a Blocked line to confirm that the call will be blocked.

Incidentally, the problem with calls to 911 is equally true with any phone that has a redial feature: The redial feature will generally not store a pause after *67 and so the redial is effectively disabled (inoperable) for calls that you wish to block Caller ID on.

This entire situation was brought to the attention of US West in March of 1993 and they responded that Caller ID would not be available until August 1993 so why was I complaining. It is now August and their response is: So don't use Call Blocking on your computer. As for my redial button: They say don't use it--buy their $3/Month "Continuous Redial". (Which incidentally is not like the PBX Automatic Callback feature--it only "looks" at a busy number about once every 45 seconds!)

David J. Kovanen Kovanen@First.Com ... (206) 925-1000

10 Caledonia Summit NE, Browns Point, Washington, U.S.A. 98422-1620

More Gripen Griping

Dr Peter B Ladkin <pbl@compsci.stirling.ac.uk>
26 Aug 93 20:30:00 BST (Thu)

Flight International, 24-31 August 1993, p5, `Report Challenges Gripen
Controls' by David Learmount.

Saab says that it was aware of the fly-by-wire (FBW) system software inadequacy which caused the crash of its [..] Gripen [...] on 8th August [...]. The "software limitation" had been reported by one of the company's programme test pilots, but was believed to be at a corner of the flight envelope unlikely to be used. Saab says that the corrections [....were....] set for October, but may be delayed.

The Swedish Accident Investigation Board's preliminary report says: "The accident was caused by the flight-control system's high amplification of stick commands in combination with large, rapid stick movements by the pilot. This led to the stability margins being exceeded and the aircraft entering a stall."

A contributory factor, says the report, was the "late display" of the angle-of-attack warning, "...which gave the pilot too little time to react".

The report, based on flight-data-recorder information, says that Saab test pilot Lars Radestrom had flown a left-hand turn at 154kt [..] with 65 [degree] bank, at 2g, with a high 21 [degree] angle of attack.

Radestrom attempted to roll sharply out of the turn by applying full-right aileron and, simultaneously, a sharp pitch down. Instead of stopping at wings level, as intended, the aircraft continued to roll to 20 [degrees] right bank. The pilot reacted to the bank by a full control column movement to the left, still with pitch down.

At this point, the software started to produce control over-reaction, and the pilot started compensating with three of four more full-deflection control-column cycles. Radestrom felt that he had lost control and ejected.

As the aircraft then entered a steep descent, it appeared to have recovered to stable flight. "The aircraft's control system includes a recovery mode. We have observed that this mode has operated in the intended manner," says Saab, while admitting that there was not enough height for recovery.

[End quote]

The last paragraph paragraph is particularly .... interesting. Maybe someone should be collecting examples of airplane-industry double-speak. It seems to surface when fly-by-wire systems are involved, or is it just my impression? I don't recall anyone from Boeing saying "the safety bolts on ..... functioned to specification" when El Al crashed into the apartment building in Amsterdam last year, or someone from MD saying `the slat controls worked as intended' when China Airlines killed 2 people and injured the rest with an inadvertent slat deployment on an MD11 at cruise over the Aleutians earlier this year.

Peter Ladkin

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 14: Issue 89

Friday 27 August 1993

Contents

Re: The Mars Observer

Theodore M.P. Lee) <Sandy Murphy <sandy@TIS.COM> (via tmplee@tis.com>
Fri, 27 Aug 1993 11:32:36 -0600

>From sci.space.news Fri Aug 27 11:32:16 1993

```
>Newsgroups: sci.space.news
>From: baalke@kelvin.Jpl.Nasa.Gov (Ron Baalke)
>Subject: Mars Observer Update #2 - 08/26/93
>To: sci-space-news@uunet.uu.net
>Followup-To: sci.space

>Forwarded from:
>PUBLIC INFORMATION OFFICE
>JET PROPULSION LABORATORY
>CALIFORNIA INSTITUTE OF TECHNOLOGY
>NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
>PASADENA, CALIF. 91109.  (818) 354-5011
>
>                MARS OBSERVER MISSION STATUS
>                      August 26, 1993
>               2:30 p.m. Pacific Daylight Time
>
>     Communications with the Mars Observer spacecraft have not yet
>been restored, one and a half days past its planned insertion into
>orbit around Mars.
>
>     Mission controllers at JPL continued through the night and
>morning with efforts to re-establish the necessary radio link with
>the spacecraft by cycling the various elements of the
>communications system.
>
>     At 2:37 p.m. Pacific Daylight Time today, the continued
>execution of the command loss timer subroutine will try to position
>the spacecraft for optimum pointing and will switch antennas to try
>to restore communications.
>
>     Project officials still do not believe that the propulsion
>tanks leaked or exploded at the time of their pressurization. The
>pressure in the tanks at launch was 285 pounds per square inch
>absolute (psia).  As propellants were used during the three
>trajectory correction maneuvers, the pressure was reduced to about
>167 psia. Pressurizing the tanks would have raised the pressure to
>264 psia. Any greater pressure would require a failure of both of
>the in-series pressure regulators. The burst pressure specification
>of the tanks is 465 psia and actual test data ruptured tanks at 678
>psia.  Flow restrictions limit the rate at which the pressure can
>increase.  Analysis indicates that the probability that the
>pressure in the tanks would increase to the burst level within the
>9 minutes that the radio transmitter was off is less than 0.1%.
>
>     Project officials are systematically evaluating the most
>probable sources of the cause of the spacecraft's failure to
>communicate.
>
>     One such source which has been receiving considerable
>attention is the potential failure of the spacecraft's central
>clock, whose official name is the "redundant crystal oscillator,"
>or RXO for short.  Proper operation of this device is required for
>operation of the spacecraft's central computers, which sequence the
```

```
>events on the spacecraft.
>
>    The first hypothesis for the lack of communications pointed
>to the failure of the central computer to turn the transmitter back
>on.  Failure of the central clock would prevent the central
>computer from doing its job.  After sending commands to turn on the
>transmitter, switching to the backup clock was the next action
>taken by mission controllers.
>
>    The central clock has been the focus of investigation because
>it contains transistors which have failed in other spacecraft
>applications using this type of clock.
>
>    The launch of the NOAA-I spacecraft was delayed at the end of
>June 1993 when it was discovered that its RXO had failed.  A
>subsequent investigation revealed that the RXO failure was caused
>by the failure of a 2N3421 transistor.  Two of these transistors
>are used in each of the redundant halves of the RXO.  Transistors
>from the same manufacturing lot as those in the NOAA-I RXO are
>installed in the Mars Observer RXO, making the reliability of Mars
>Observer's RXO suspect.
>
>    The transistors fail when a weld between a gold-plated post
>and an aluminum wire breaks.
>
>    This potential problem was discovered when Mars Observer was
>only 55 days away from Mars after the spacecraft had been in flight
>for over nine months.  Because of the way that these transistors
>are used in the RXO, Mars Observer would be susceptible to losing
>its central clock function if one particular transistor in each
>half of the RXO failed.
>
>    There is no alternative source of the central clock function
>in Mars Observer, and should the loss of this function occur, it
>would be a non-recoverable situation.
>
>    The RXO, on its primary side, was working perfectly
>immediately before the pressurization activity.  The last time the
>backup side of the RXO was tested was in a launch GO/NO-GO test on
>launch day, when it was also found to be working perfectly.
>
>    Project officials were not, at first, concerned about the
>NOAA-I RXO failure because it would take a failure of two of these
>transistors to cause the loss of the central clock function.  The
>spacecraft is not designed to automatically protect itself against
>more than a single failure in any piece of hardware.
>
>    The restoring of the spacecraft's transmitter and the
>spacecraft's failure to act on ground commands could be tied to the
>loss of the central clock function.  Project officials now surmise
>that one explanation for the loss of communications could result
>from the failure of the crucial transistor in each half of the RXO,
>or its failure to autonomously switch to the backup side.  Then
```

>there would be no central timing function. This failure could have
>been induced by the shock of the pressurant valves operating during
>the propulsion tank pressurization event on Aug. 21, after which
>communications were not restored.

>[Ron Baalke, Jet Propulsion Lab, M/S 525-3684 Telos
>Pasadena, CA 91109 baalke@kelvin.jpl.nasa.gov]

Re: More Gripen Griping

Mary Shafer <shafer@ferhino.dfrf.nasa.gov>
Thu, 26 Aug 93 15:40:49 PDT

As far as I can tell, the real problem was control-surface rate limiting. Cf. the YF-22 crash and the Space Shuttle ALT-5 multi-axis PIO.

I've flown a rate-limited configuration in a variable-stability Learjet and it looked a lot the same, just before the safety trips gave the plane back to the safety pilot.

I've read the articles in AvLeak and Flight International and looked at the video a couple of times. My branch chief and some USAF handling qualities guys are going to Sweden the end of next week, too. Not controls engineers, handling qualities engineers.

Mary Shafer, Dryden Flight Research Facility

Be careful with your test cases!

<Kenneth.Wood@prg.ox.ac.uk>
Fri, 27 Aug 93 16:55:35 BST

The Feedback section of the latest New Scientist relates the following Computer Weekly story about an unfortunate programmer at an unnamed bank. Apparently, the bank wanted to target its wealthiest customers with a mailshot promoting various new services and the programmer in question wrote a program to select the 2000 wealthiest customers from the bank's records and to generate an appropriate letter for each. In the process of testing the program, he made use of a fictitious customer named Rich Bastard.

Unfortunately, as you may already have guessed, something went amiss and every single one of the bank's 2000 prize customers received a letter which began "Dear Rich Bastard, ..."

The risks involved? Well, for one thing, the hapless programmer lost his job over the incident. More generally, I suppose it's just another example of the way in which the complex interactions amongst program development, testing, and maintenance can produce unpredicted and undesirable consequences. The latter analysis is, of course, rather generous to the programmer.

Re: Quote for the Day (Cooper, RISKS 14.87)

"Wes Plouff, LKG2-2/Y10, DTN 226-6780" <plouff@levers.enet.dec.com>
Thu, 26 Aug 93 18:23:39 PDT

Brinton Cooper quotes out of context, incidentally from a book whose subtitle reads "the Hardware/Software Interface," a line he probably intends as a subject for meditation. Saying "...minimizing the logic is both complex and error-prone and, thus, is better left to a program," has ironic overtones in this forum. But I'd bet a cup of coffee that, taken in context, it's sound engineering advice.

The workstations and PCs we use to read RISKS all contain semi-custom and sometimes programmable logic chips. Reduction of the Boolean logic equations, that is, minimization of AND-OR logic terms, directly influences the size of the chips and thus their cost. Reducing large Boolean equations by hand _is_ complex and error-prone, just like programming large systems in assembly language would be. Thus it's a safe bet that the book's authors are advocating the use of design automation tools for real-world digital logic design.

Chip designers would argue, justifiably, that today's automated tools decrease both design time and design risk. The RISK Cooper illustrates is in mistaking a practical viewpoint for complacency.

Wes Plouff Digital Equipment Corp, Littleton, Mass.

dial 1 first

Fredrick B. Cohen <fc@Jupiter.SAIC.Com>
Fri, 27 Aug 93 04:56:12 PDT

Until recently, I had the good fortune of living in a telephone exchange without this problem, but I had heard about it from others and just couldn't believe it was so.

Why do I have to dial 1 before some numbers and not before others? The computer at the phone company politely tells me to dial 1 first, or to not dial 1 first depending on where the call is made to, but this is little comfort for my autodialer making a series of several thousand calls to send out FAXes. If they can tell me to add 1 or not, why can't they just add it or not for me?

The Cisco router problem is particularly important because so many people use this router to secure their network into isolated partitions.

[*** Some correspondence from Cisco doubts that this vulnerability exists, and indicates that there is certainly NO INTENTIONAL TRAPDOOR. An official response follows. PGN ***]

The risks of not receiving risks and risks not finding out about it may be more severe than the risks of sending out risks for all to see. My computer mail address was recently cut off, and apparently, every piece of mail sent to me was not forwarded, and not reported as undelivered! I must have missed a lot of risks that I am now vulnerable to and don't know about! Then there is the question of who got those mailings I missed. Is there a forger out there claiming to be me? Or am I the forger claiming to be him? The finger command has a few minor problems worthy of note. One is that it tells you if my mail has been removed from the mail queue, but not if I really read it. Another is pointed out if you finger me at this mailing address. Something about the plan containing false and misleading information.
FC

Re: Cisco backdoor?

Paul Traina <pst@cisco.com>
Fri, 27 Aug 1993 11:15:23 -0700

There are no known bugs in any software providing access-control-list functionality in any current cisco software. There has only been one very obscure bug that could cause a security problem in the history of our product, and we immediately fixed this problem, published an immediate workaround, and informed CERT of this problem. We have never, and will never implement any sort of trapdoor or backdoor functionality which would allow bypassing of ordinary security systems.

Paul Traina, cisco Systems

[***** NOTE ADDED ON 2 SEP 1993 TO THE ARCHIVE COPY:
PLEASE SEE RISKS-15.01 FOR FURTHER CLARIFICATION. PGN *****]

sendmail debug option? RISK or friend?

Eric Allman <eric@CS.Berkeley.EDU>
Fri, 27 Aug 1993 11:17:09 -0700

In RISKS-14.87, PGN repeats the oft cited claim that the sendmail debug option opens a security hole. Although it is true that earlier versions of sendmail did allow debugging to enable mail to arbitrary addresses (including programs), this hole should be well plugged by now.

Conversely, encouraging people to disable all debugging options may itself cause problems. Many of the debug flags are exteremely useful when installing and debugging config files. Scaring people into turning off all debugging is not productive.

By the way, despite many claims to the contrary, the security hole used by RTM was not an intentional back door -- it was a bug, plain and simple, as I've published in the past (for example, see the C Advisor column in UNIX Review 7, 1 (January 1989)).

Eric Allman <eric@CS.Berkeley.EDU>

[Eric, Thanks for the clarification. BTW, are you convinced that EVERYONE is using the unbuggy version? I know some systems that do not get upgraded very often --- if ever! PGN]

Re: RISKS of elaborating on exploitation of known RISKS

<jhudson@legent.com>
Fri, 27 Aug 93 11:58:02 EDT

PGN's reply on this subject ended with

> Does anyone care?

I've noticed that most people tend to focus their energies on whatever "fire" happens to be blazing in front of them. I often go to a sysadmin with a clear description of some hole in security (or procedures, or ...), only to be told "I'll get to it when I can" (which means "never"). The only time that the problem gets their attention is when an actual breach (or failure) occurs, and peoples' work is lost. I can sometimes feel like taking Robert Morris' approach and breaking something just so that it will get the attention it deserves.

The preceding symptom is certainly not limited to computer systems. Here in Massachusetts, there has been a rash of "child fallen out the upper-story window" incidents this summer. The cause of the problem is children playing in an upper-story room with an open window and only the screen for protection. Now that 3 children have died and 13 more spent time in hospitals, local organizations are distributing safety bars for windows.

I fear that the answer to Peter's question is "No, no-one cares, until someone gets hurt."

Jim Hudson <JHudson@legent.com>

Call Privacy *67 faults

Ed Ravin <elr@wp.prodigy.com>
Thu, 26 Aug 1993 21:54:50 -0400

In New York, NY Telephone has managed to really screw up *67 caller ID blocking -- a phone line defaults to "send caller number" mode, and dialing *67 prevents the calling number from being displayed on the other side. If you tell the phone company that you want your line to default to NOT send the calling number, they give you "all call restrict" and you are supposed to dial *67 if you WANT your number to be displayed on the other side.

Naturally, there's no way to tell which way a phone line defaults to -- except for the reminder stickers that NY Tel sends you to stick on your phone. So if you're using an unfamiliar phone, just what *67 will do is undeterminate. My suspicion is that NY Tel did this to discourage people from trying to suppress Caller ID, since they want the service to be as universal as possible. My suspicions are furthered by the fact that when I installed a new line, they didn't ask me whether I wanted to default to outgoing caller ID blocking or not...

Re: ... Call Privacy *67 problems (Kovanen, RISKS-14.88)

Stuart Moore <smoore@itd.nrl.navy.mil>
Fri, 27 Aug 93 10:36:55 EDT

Perhaps the most annoying feature of the *67 call blocking services is that they do *NOT* block your phone number for companies that purchase commercial "caller ID" services (Automatic Number Identification) from their common carrier. For example, when you call a catalog retailer's 800 number using the *67 number, the retailer is still able to capture your phone number and add it to their data base. The *67 service only blocks your number for people who have the residential Caller ID service. The RBOCs that offer *67 call blocking services do not seem to mention this distinction. As a result, many callers are tricked into thinking that their privacy is protected through *67 when, in many cases, it is not.

Stuart C. Moore

Re: Electronic Education (Talbott, RISKS-14.86)

Shyamal Jajodia <SHYAM@mitvmc.mit.edu>
Tue, 24 Aug 93 14:28:10 EDT

Before we go overboard with this abstraction replacing reality idea, consider that books which we have been reading for much longer than we have had computers or television are also abstractions. Audio Visual media may be a great improvement on text but they cannot become reality. Otherwise we would not go to ball games, and foreign countries, join demonstrations and meet people for lunch. As in the case of any successful abstraction people's appetite for reality is increased not diminished by the taste they get on the television or computer screen. This actually goes back to the old debate in artificial intelligence - "Can a computer become sentient?" The true question there was not whether a computer can or not but "What is sentience?" In the same way before we ask whether virtual reality can replace reality, we must first ask what is it that we call reality.

Use of PIN as authenticator to humans (Swiss, RISKS-14.88)

<horning@src.dec.com>
Thu, 26 Aug 93 16:34:45 -0700

> Citibank gives out an ATM PIN with it's cards. Why in the world they don't use that as telephone authentication..., I have no idea.

I do.

My bank has an explicit policy that bank employees are not to be told PINs--PINs are only to be keyed into machines (which presumably encrypt them before transmission). If a dishonest person who found your wallet could do damage with your authenticator, imagine the damage that could be done by a dishonest "inside person."

Jim H.

Re: Telephone verification

Joe Konstan <konstan@cs.umn.edu>
Thu, 26 Aug 1993 18:11:59 -0500

Tom Swift asks (in RISKS-14.88) about the common practice of asking for and using a separate password (Mother's maiden name) for bank accounts rather than using the already secret PIN.

I think Banks have the right idea here, though they often implement it poorly. There are several good reasons for not using the PIN as a telephone verification password.

1. Most banks don't give PIN access to phone clerks since the PIN poses the most direct security risk (they must allow account numbers to be identified and PIN+acct+card writer == ca$h).

2. Many smaller banks and credit unions can't change the PIN without reissuing the card or account. While their PIN system may be crippled, it is certainly wise not to risk compromising it over the phone.

3. A pin is too easy to overhear over the phone.

4. What happens when you lose (forget) your PIN? You need some way of calling to have a new one assigned.

Mother's maiden name isn't ideal, but almost every bank is open about the fact that they'll take any pronounceable password. Accordingly, you can make up a good mother's maiden name and have extra security.

American Express handles things somewhat differently. Usually they ask a simple question like "is anyone else on the card with you?" or "how many additional cardholders are on the account?" but they tend to ask more detailed questions when you are talking major action (as opposed to simple queries). Among the more interesting questions are ones that ask you to describe recent transactions (once I was asked for the last meal I charged on the card) which, seem like good general authentication questions that would only be troublesome if the card were already stolen and used successfully.

Joe Konstan

Call for Papers: IEEE Computer Security Foundations Workshop VII

Li Gong <gong@csl.sri.com>
Thu, 26 Aug 1993 16:03:16 -0700

CALL FOR PAPERS
IEEE COMPUTER SECURITY FOUNDATIONS WORKSHOP VII
June 14-16, 1994
Franconia, New Hampshire
Sponsored by the IEEE Computer Society

The purpose of this workshop is to bring together researchers in computer science to examine foundational issues in computer security. We are interested both in papers that describe new results in the theories of computer security and in papers, panels, and working group exercises that explore open questions and raise fundamental concerns about current theories of security. Possible topics include, but are not limited to:

access control
authentication
covert channels
data and system integrity
database security
distributed systems security
formal methods for security
information flow
secure protocols
security models

We are also interested in examining the interactions and trade-offs between computer security requirements and other system requirements such as availability, dependability, and real-time, and in exploring foundational security issues in emerging areas such as ubiquitous computing, multimedia, and computer supported cooperative work. The proceedings are published by the IEEE Computer Society and will be available at the workshop. Selected papers will be invited for publication in the Journal of Computer Security.

Instructions for Participants: Workshop attendance will be by invitation only and limited to thirty-five participants. Prospective participants should send five copies of a paper (limit 7500 words), proposal for panel discussion or working group exercise to Li Gong, Program Chair, at the address below. Please provide E-mail addresses and telephone numbers (voice and fax) for all authors and clearly identify the contact author.

IMPORTANT DATES: Author's submission: February 10, 1994
Notification of acceptance: March 11, 1994
Camera-ready final papers: April 11, 1994

Program Committee

Simon Foley,	Univ. Col., Cork, Ireland
Virgil Gligor,	U of Maryland, USA
Simon Lam,	U of Texas, Austin, USA
Stewart Lee,	U of Toronto, Canada
John McLean,	Naval Research Lab, USA
Catherine Meadows,	Naval Research Lab, USA

Michael Merritt,	AT&T Bell Labs, USA
Jose Meseguer,	SRI International, USA
Jonathan Millen,	MITRE, USA
Chris Mitchell,	U of London, RHNBC, UK
Robert Morris,	DoD, USA
Ravi Sandhu,	George Mason U, USA

For further information contact:

General Chair	Program Chair	Publications Chair
Ravi S. Sandhu	Li Gong	Joshua Guttman
ISSE Department	SRI International	The MITRE Corporation
George Mason University	Computer Science Lab	Burlington Road
Fairfax, VA 22030-4444	333 Ravenswood Avenue	Bedford, MA 01730
+1 703-993-1659	Menlo Park, CA 94025	+1 617-271-2654
sandhu@sitevax.gmu.edu	+1 415-859-3232	guttman@linus.mitre.org
	gong@csl.sri.com	

Search RISKS using swish-e

Report problems with the web pages to the maintainer