Internet of Things

Lecture 11

Security and Privacy 1

Surveillance and behavioural patterns

Michael Engel

Surveillance in the IoT

Challenge:

Using the IoT on personal devices, we open up opportunities for surveillance of IoT users through the use of single and fusioned sensor data.

Questions:

- Can we enable (some level of) anonymity when using IoT applications?
- What is the tradeoff between functionality and privacy?
- Which unexpected privacy invasions are in use in IoT devices?

Back to Mark Weiser…

"The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used ... and what are the consequences of any given action." [1]

With (deeply) embedded devices such as IoT nodes and smartphones, users have no control over how their data is processed and distributes

Even experienced users have little chance to gain more insight, since the source code for most IoT appliances is not available

IoT Privacy Issues [4]

- **Too Much Data:** The sheer amount of data that IoT devices can generate is staggering. A Federal Trade Commission report entitled “Internet of Things: Privacy & Security in a Connected World” found that **fewer than 10,000 households can generate 150 million discrete data points every day.** This creates more entry points for hackers and leaves sensitive information vulnerable.
- **Unwanted Public Profile:** You’ve undoubtedly agreed to terms of service at some point, but have you ever actually read through an entire document? The aforementioned FTC report found that **companies could use collected data that consumers willingly offer to make employment decisions**. For example, an insurance company might gather information from you about your driving habits through a connected car when calculating your insurance rate. The same could occur for health or life insurance thanks to fitness trackers.
- **Eavesdropping:** Manufacturers or hackers could actually use a connected device to **virtually invade a person’s home**. German researchers accomplished this by intercepting unencrypted data from a smart meter device to determine what television show someone was watching at that moment.
- **Consumer Confidence:** Each of these problems could put a dent in consumers’ desire to purchase connected products, which would prevent the IoT from fulfilling its true potential.

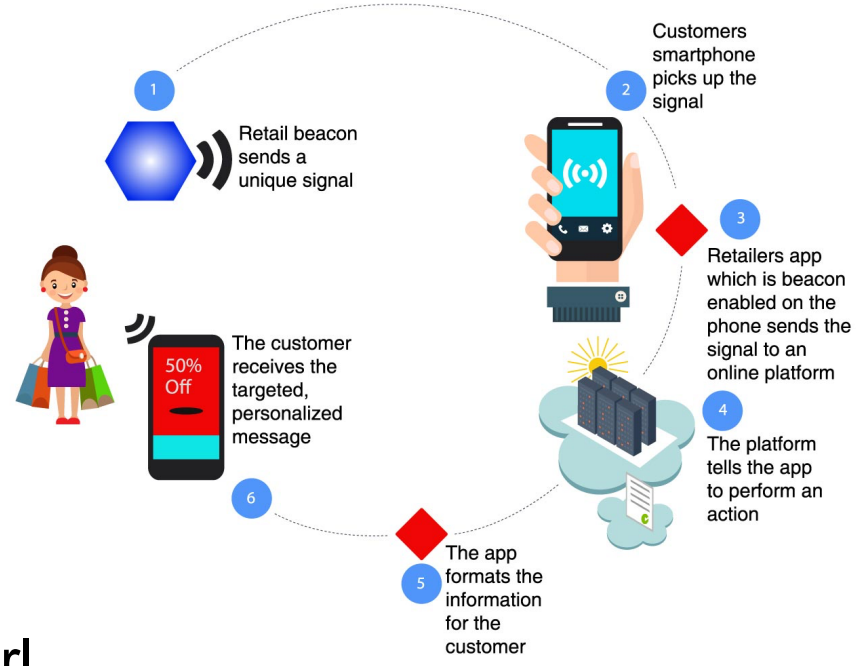
Surveillance example 1

- Fitness trackers collect very sensitive data about your health
- e.g. data collected by a FitBit tracker [20]:
  - steps you take, your distance traveled, calories burned, weight, heart rate, sleep stages, active minutes, and location
- If health insurance companies can access this data, there is an *information asymmetry* to the disadvantage of the user
  - Insurance companies can adjust rates or deny coverage based on current and previous behavior of the customer
  - Insurance companies already provide "free" health trackers

- Similar effects exist for car insurance
  - Tracker observes speed, braking, distance covered etc.

Surveillance example 2

- Customer tracking in stores is prevalent [8]
  - Combination of Beacons, custom mobile apps, and Bluetooth Low Energy (BLE) appliances
- Beacons in stores detect proximity of a specific customer
- Displays in stores use information (→ big data) about the customer's purchasing behavior to display personalized ads
- Significant **privacy invasion**: "Target Figured Out A Teen Girl Was Pregnant Before Her Father Did" [17]



Surveillance example 3 – AirTag

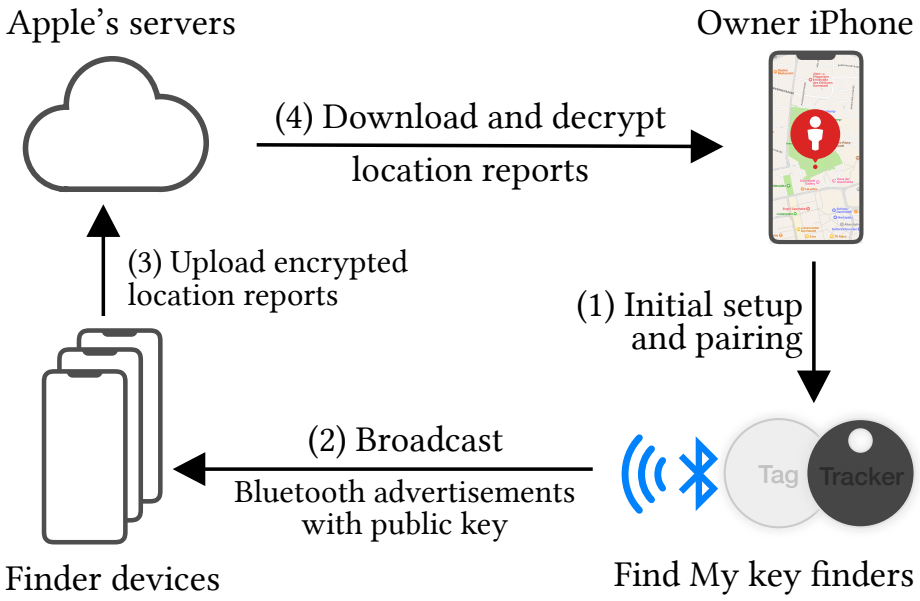
- *"AirTag is a super easy way to keep track of your stuff. Attach one to your keys. Put another in your backpack. And just like that, they're on your radar in the Find My app, where you can also track down your Apple devices and keep up with friends and family."* [Apple product desciption]
- A $29 mobile, battery-powered device you can attach to your things, pets, …
- Allows tracking via Bluetooth LE without long-range wireless technology
  - …as long as there are iPhones around which forward tracking info to iCloud
  - Other tracking devices exist, but their efficiency depends on the ubiquity of devices to connect to that provide long-range communication
- **What are the privacy implications of AirTag?**

Apple AirTag Tracker
CC BY-SA 4.0 by KKPCW

Surveillance example 3 – AirTag "FindMy" net

How can AirTags communicate? [10]

- AirTags can connect to nearby iPhones using BT LE
  - …to **any iPhone**, not just your own!
- AirTag sends Bluetooth advertisement packets received by all iPhones in radio range
- Receiving iPhone forwards encrypted location report to Apple's iCloud service
  - Encrypted, so iPhone user does not gain access to location data
- AirTag owner can locate AirTags paired to their phone using the "FindMe" cloud service

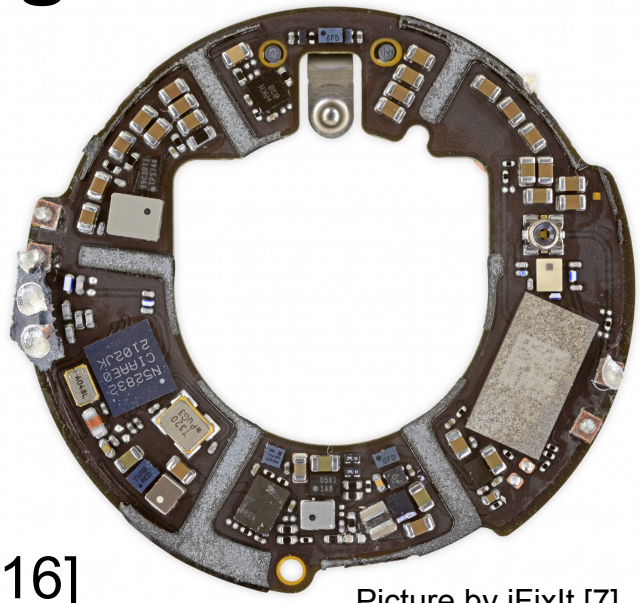


Apple's FindMy network, simplified (from [10]

Surveillance example 3 – AirTag internals

What's inside an AirTag? [7]

- Sensors and actuators
  - 3-axis accelerometer
  - voice coil solder points for speaker



Picture by iFixIt [7]

- Electronics
  - U1 ultra-wideband transceiver chip [10,16]
    - Allows communication with other U1 chips in iPhones
  - Nordic Semiconductor nRF52832
    BT LE SoC w/NFC controller
  - Audio amplifier
  - Battery and power regulators

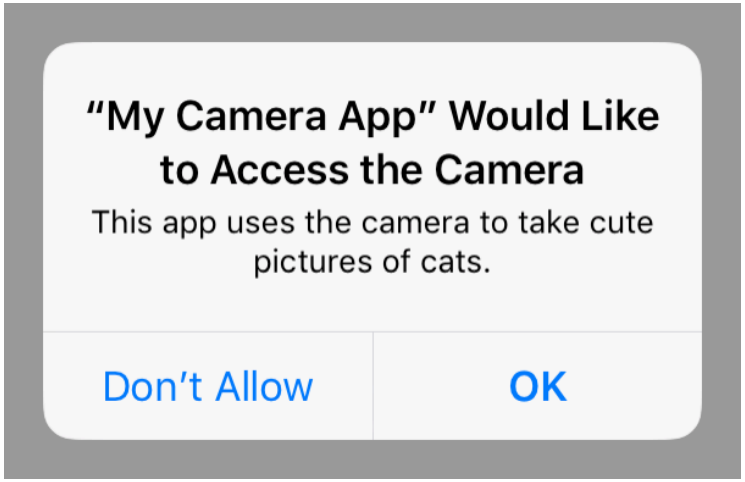
Surveillance example 3 – AirTag

Problem: using AirTag enables you to ***track (stalk) other people and/ or their property!*** [12,13]

- To prevent malicious use, an iPhone will…
  - alert its user if an AirTag not registered to their iCloud account seems to be following them
  - additionally, an AirTag separated from its owner for an extended period of time will play a sound when moved to draw attention to it
- **Are these privacy measures sufficient?**
  - "currently, users will receive an alert at a random period between eight and 24 hours once an unknown AirTag has been detected traveling with them" [14]
  - What if you don't have an iPhone (but e.g. Android)? [9]
  - What if the hardware is manipulated not to alert? [15]
  - Can other, malicious devices utilize Apple's "FindMy" network? [10]

When "off" does not mean "off"

- Can you trust your device?
  - Mobile phones have sensors like cameras, microphones, GPS sensors, acceleration sensors…
  - How can you know the device sensor is really switched off?
  - How can you ensure only specific apps access the sensors?
- Access to sensors + device data
  - Address and call data, browsing history, IP address, …
- **Solution?** Hardware kill switches
- e.g. Purism Librem 5 phone switches:
  - Cellular Modem
  - Wireless & Bluetooth
  - Camera & Microphone

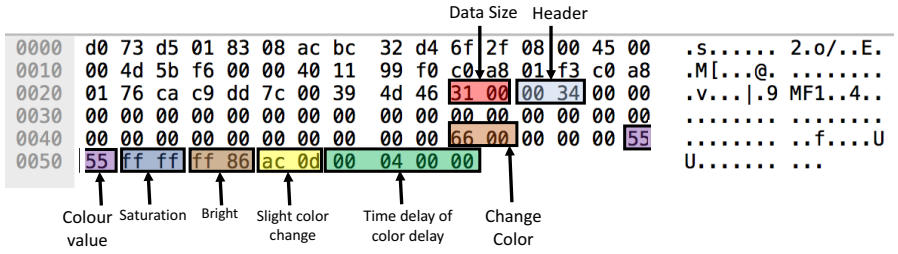


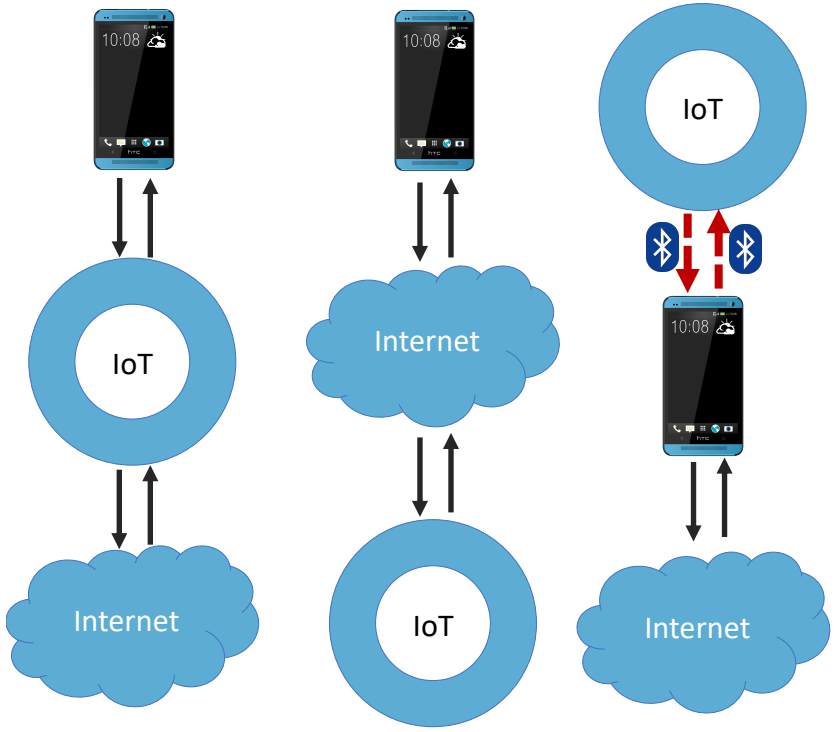
When "off" does not mean "off"

- Trend towards "smart" devices, e.g. Smart TVs
  - Devices contain significant computing power, equivalent to a modern smartphone or tablet
- Connection to WiFi required, e.g. for firmware updates
  - Some Smart TVs don’t start without internet connectivity
  - Some also *actively seek* open WiFi networks
- Smart TVs are capable of collecting audio, video and TV usage data [19] in order to harvest user data, e.g. to display ads
  - Voice activation and microphones
  - Picture content analyses
- "Dumb" TVs which only display a picture via HDMI are hard to find today
  - Price of Smart TVs subsidized by surveillancy features

Side channels

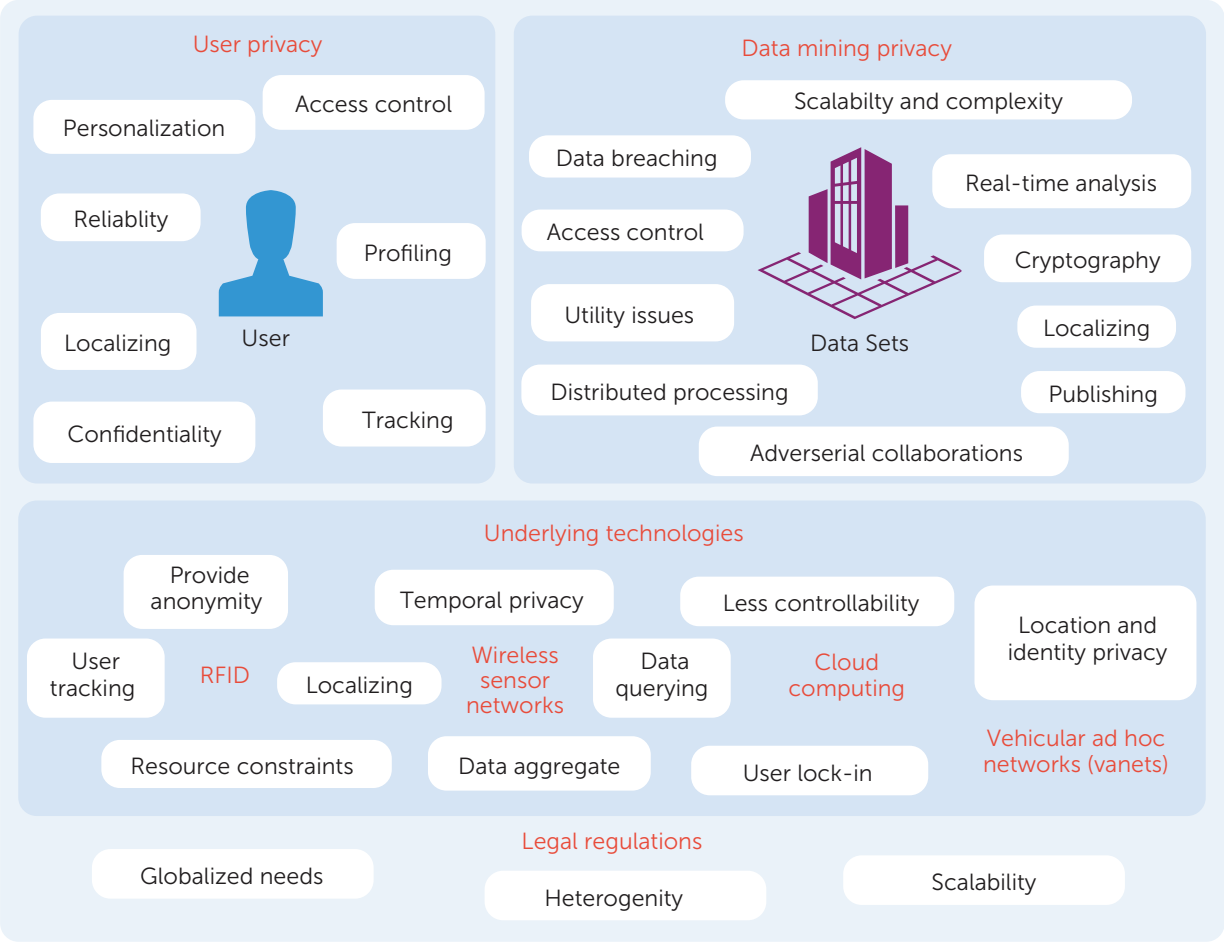
- Privacy of users can be compromised not only by directly reading data, but also by analyzing metadata ("side channels")
  - e.g. network traffic patterns [18]
- Example: smart light bulbs
  - Each light bulb has its own device address, transferred unencrypted
  - Even if payload is encrypted (see figure below), transmission of packets with device address indicates events, such as turning on/off the lightbulb
  - Possible to deduce e,g, room occupation from traffic pattern





Privacy challenges and technologies overview

- We can only present a small part of the problem landscape [2]



Conclusion

- Privacy in the IoT is hard to ensure – "data is the new oil"

- Devices can spy on you and others
  - Sometimes without you recognizing
  - Useful functionality can be abused for privacy invasion

- Companies and states are interested in your data
  - Behavioral control (health insurance), ad delivery, …
  - Also: Constraint of free speech

- Hard to escape ubiquitous surveillance
  - Devices collect and send data without user consent
  - Few devices provide hardware off switches for sensors

References

[1] M. Weiser et al., *The Origins of Ubiquitous Computing Research at PARC in the Late 1980s*, IBM Syst. J., vol. 38, no. 4, 1999, pp. 693–696

[2] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov and A. V. Vasilakos, *The Quest for Privacy in the Internet of Things*, in IEEE Cloud Computing, vol. 3, no. 2, pp. 36-45, Mar.-Apr. 2016, doi: 10.1109/MCC.2016.28

[3] L. Babun, Z. Celik, P. McDaniel and A. Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*. Proceedings on Privacy Enhancing Technologies,2021(1), 145-166

[4] R. Chow, *The Last Mile for IoT Privacy*, in IEEE Security & Privacy, vol. 15, no. 06, pp. 73-76, 2017

[5] Insider Intelligence, *The security and privacy issues that come with the Internet of Things*, https://www.insiderintelligence.com/insights/iot-security-privacy/

[6] Lau, Josephine, Benjamin Zimmerman, and Florian Schaub. *Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers*, Proc. ACM conf. on Human-Computer Interaction (2018): 1-31.

[7] Sam Goldheart, *AirTag Teardown: Yeah, This Tracks*, iFixIt 2021, https://www.ifixit.com/News/50145/airtag-teardown-part-one-yeah-this-tracks

[8] https://smartstores.com/smart-stores-and-beacon-tracking/

[9] Heinrich, Alexander, Niklas Bittner, and Matthias Hollick. "AirGuard--Protecting Android Users From Stalking Attacks By Apple Find My Devices." arXiv preprint arXiv:2202.11813 (2022)

[10] Mayberry, Travis, et al. "Who Tracks the Trackers? Circumventing Apple's Anti-Tracking Alerts in the Find My Network." Proceedings of the 20th Workshop on Privacy in the Electronic Society. 2021

[11] https://www.pocket-lint.com/phones/news/apple/149336-how-apple-s-u1-chip-adds-amazing-new-capabilities-to-the-iphone

[12] https://www.npr.org/2022/02/18/1080944193/apple-airtags-theft-stalking-privacy-tech?t=1650638324106

[13] https://www.bbc.com/news/technology-60004257

[14] https://www.theverge.com/2022/2/10/22927374/apple-airtag-safety-update-stalking

[15] https://embracethered.com/blog/posts/2021/airtag-hacks/

[16] J. Classen, A. Heinrich, *Wibbly Wobbly, Timey Wimey – What's Really Inside Apple's U1 Chip*, BlackHat USA 2021

[17] https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[18] Arunan Sivanathan, *IoT Behavioral Monitoring via Network Traffic Analysis*, Dissertation, UNSW 2019

[19] Marco Ghiglieri, *Smart TV privacy risks and protection measures*, Dissertation, TU Darmstadt 2017

[20] Etye Steinberg, Run for Your Life: The Ethics of Behavioral Tracking in Insurance, Journal of Business Ethics. Jun 2021

[21] https://www.fitbit.com/global/us/legal/privacy-summary