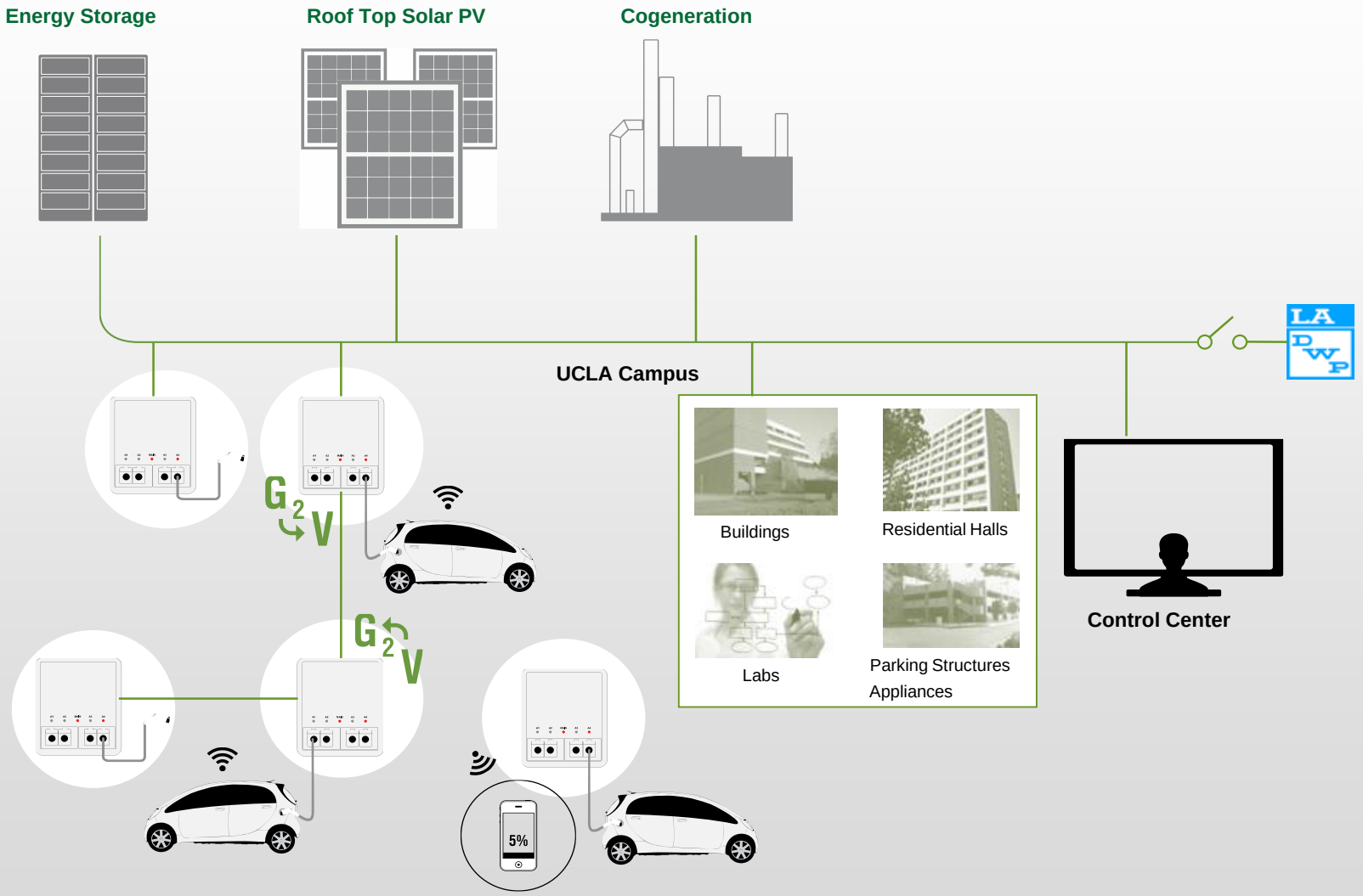
UC-Lab Center for Electricity Distribution Cybersecurity

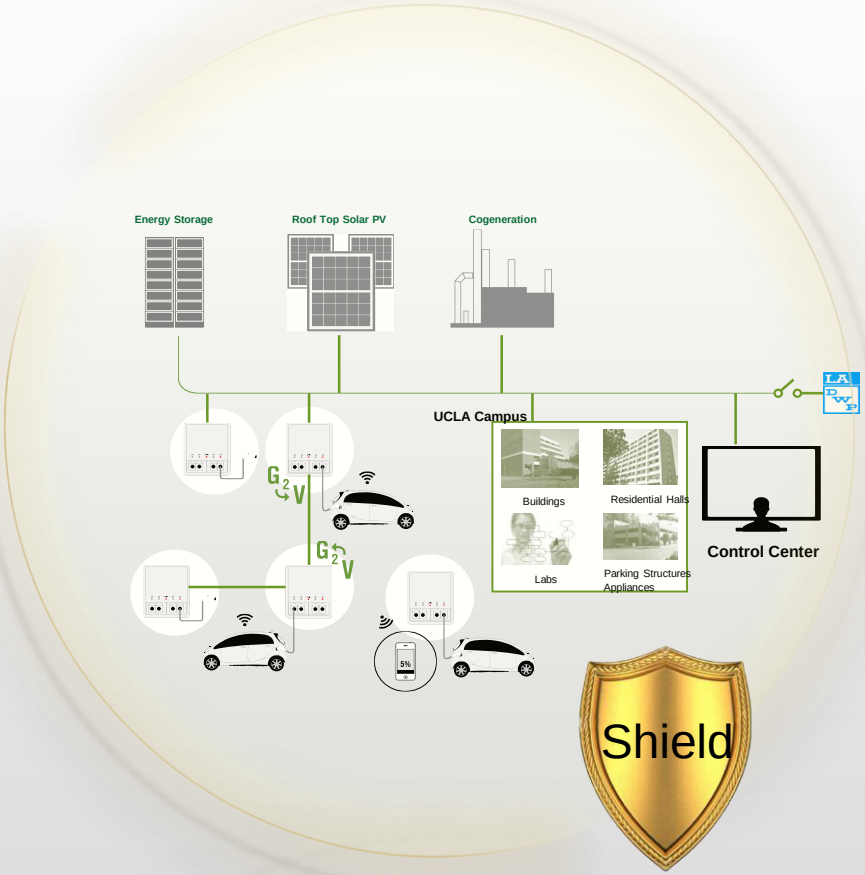
Privacy, Cyber-Physical
Device Compromise, Vulnerability,
Attack Surface, Risk -
Analysis, Assessment, Characterization
and Impact

UCLA Smart Grid Energy Research Center

UCLA Microgrid – Increase in DERs: solar, EV, BESS



Background: Importance of Cybersecurity



- The evolving cyber-threats potential to [1]
  - jeopardize microgrid/DER operations
  - violate customer privacy.
- Vulnerabilities analysis and risk assessment can help
  - Understand weaknesses of the cyber-physical system [1]
    - By Highlighting the areas of highest risk and prioritizing remediation effort accordingly.
    - Categories of the failure scenarios:
      - Electric Transportation (ET): 16 scenarios
      - Demand Response (DR): 7 scenarios
  - Prevent potential cyberattacks and thus harden the microgrid [2]
    - Systematically manage and reduce the attack surface by allocating security resources to where they are most needed.

References:

1. EPRI (2018). Grid Resiliency. [Online] https://www.epri.com/#/pages/sa/grid_resiliency?lang=en
2. Clark-Ginsberg, A. (2016). What's the Difference between Reliability and Resilience?. [online] https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_MAR_16/reliability%20and%20resilience%20pdf.pdf

Privacy Issue - Data Breach on the Internet Statistics – between 2013 and July 2018[3]

Data records lost or stolen since 2013:

9,727,967,988

Without a robust vulnerability management plan in place, attacker can exploit this weakness, move laterally across the system network and steal personal information, such as charging location, payment method and energy consumption data.

Data records are lost or stolen with the following frequency:

Every Day	Every Hour	Every Minute	Every Second
4,775,635	198,985	3,316	55
Records	Records	Records	Records

References: [3] Breach Level Index. [Online] https://breachlevelindex.com

Impact of Cyber-Physical Device Compromise

Attack \ Consequence	Cyber	Physical
Cyber	OpenSSL heartbleed bug - Eavesdropping of private information	Stuxnet, WannaCry virus
Physical	Meter bypassing	Instability due to physical destructions

[4]

➔ **Classification of the impacts:**

➢ *Cyber-Cyber (CC); Cyber-Physical (CP); Physical-Cyber (PC); and Physical-Physical (PP)*

➢ **Types of concerns [5]:**

- Denial of Service
- Intrusion / Insider
- Password compromised
- Equipment affected
- ARP Spoofing
- Eavesdropping
- Network compromised
- Man in the middle attack
- Phishing
- Trojan

➢ **An unfair advantage for hackers!!!**
Hackers can choose the time and place of battle and attack only a single weak point of the system.

Example: A variant of WannaCry virus strikes semiconductor manufacturer TSMC causing assembly line shut down on 8/3/2018. It will result in 3% quarterly revenue reduction [14].

"TSMC has been attacked by viruses before, but this is the first time a virus attack has affected our production lines." - TSMC

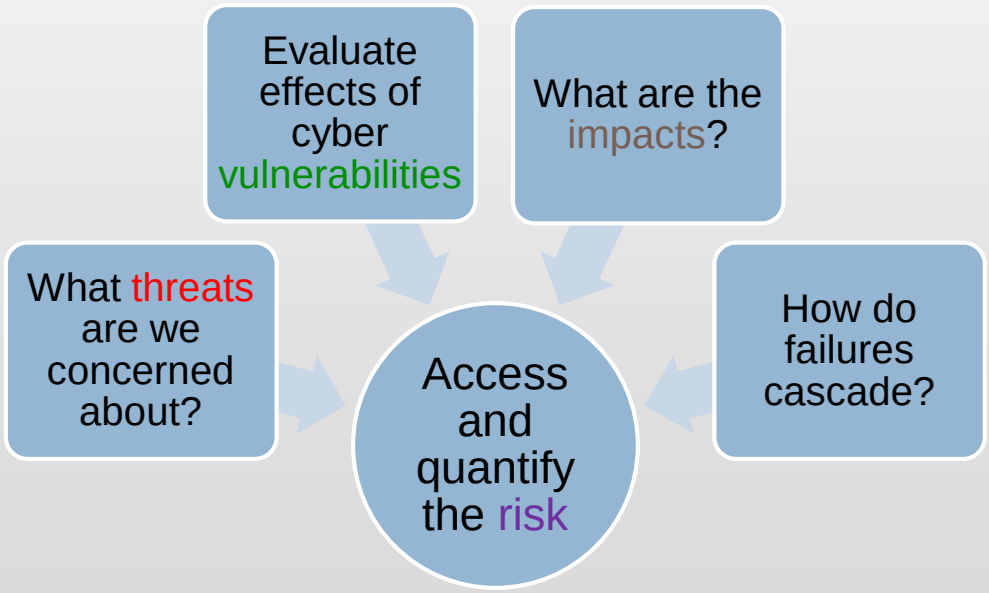
Reference:

4. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195-209.
5. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys and Tutorials*, *19*(1), 446-464.
14. The Hacker News: "TSMC Chip Maker Blames WannaCry Malware for Production Halt". August 6, 2018.

Vulnerability and Risk (1.2 and 1.3)

Definition: A “vulnerability” is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. -NISTIR [6]

Generic model of Risk[6] :



- Ranking the risk to prioritize the remediation efforts for each failure scenario considering [7]:
  - ✓ the impacts of cyberattacks,
  - ✓ effects on the likelihood and opportunity, and
  - ✓ the costs of the attacks.

$$Risk = \frac{Impact\ of\ attack}{Cost\ of\ attack}$$

Reference:

6. NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010
7. National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

UCLA Testbed and Tools

- WINSmartEV™
  - WINSmartEV™ is a smart, grid friendly, garage-friendly and user friendly research platform being developed in UCLA that allows plug-in devices or EVSmartPlugs™ to perform remote monitoring and control of EV charging through a smart communications network called WINSmartGrid™.

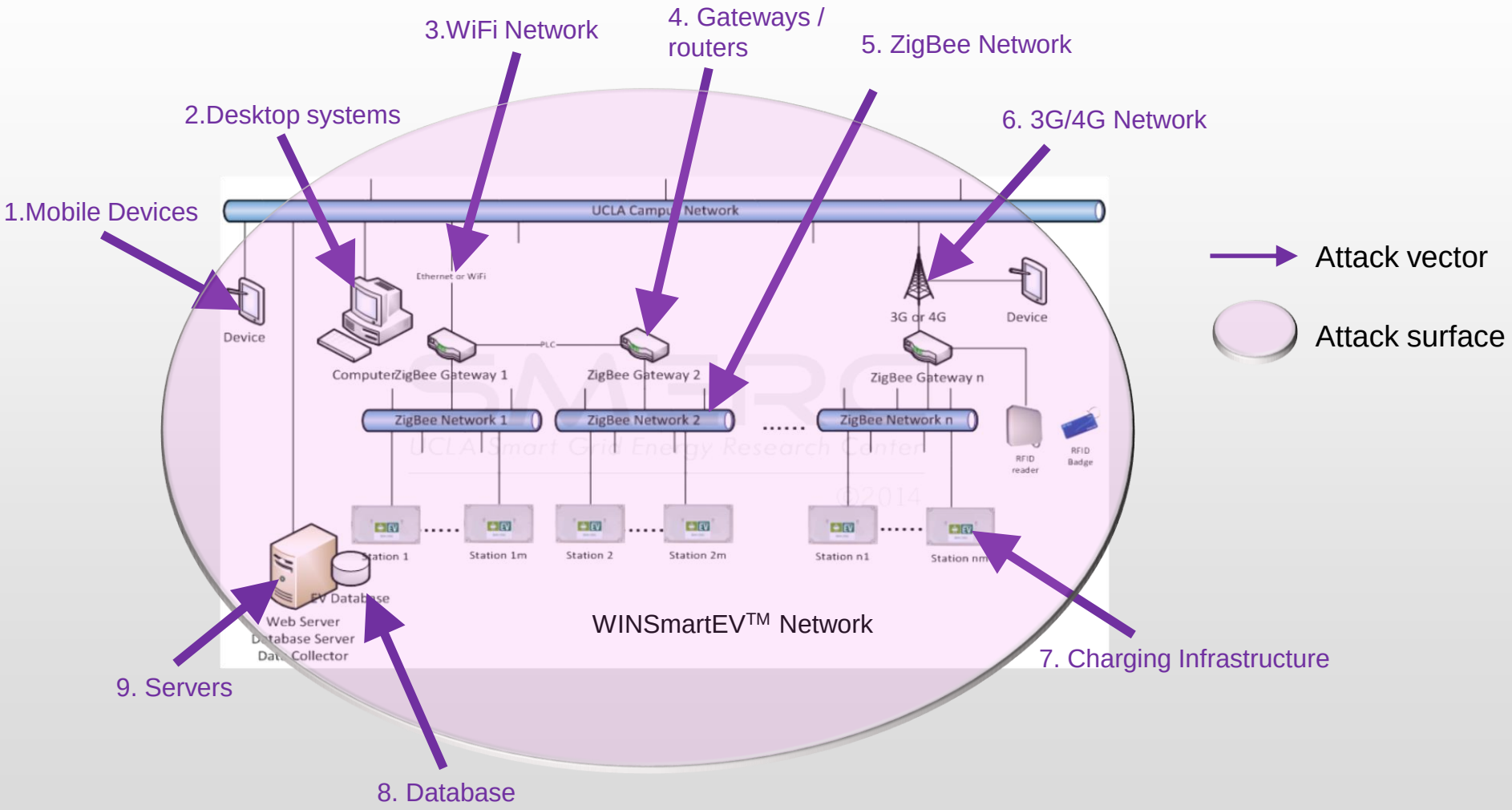
- Resource Centric Security (RCSec)[15]
  - The RCSec platform at UCLA SMERC will be utilized to prototype and test standard cybersecurity as well as physics-aware cybersecurity strategies on various electricity distribution system devices.

- UCLA CrowdZen Project [16][17]
  - CrowdZen is a research project whose goal is to provide real-time preserving open data to help transform UCLA into a data driven and smart campus. This technology will be used to test the privacy aspect of cybersecurity.

Reference:

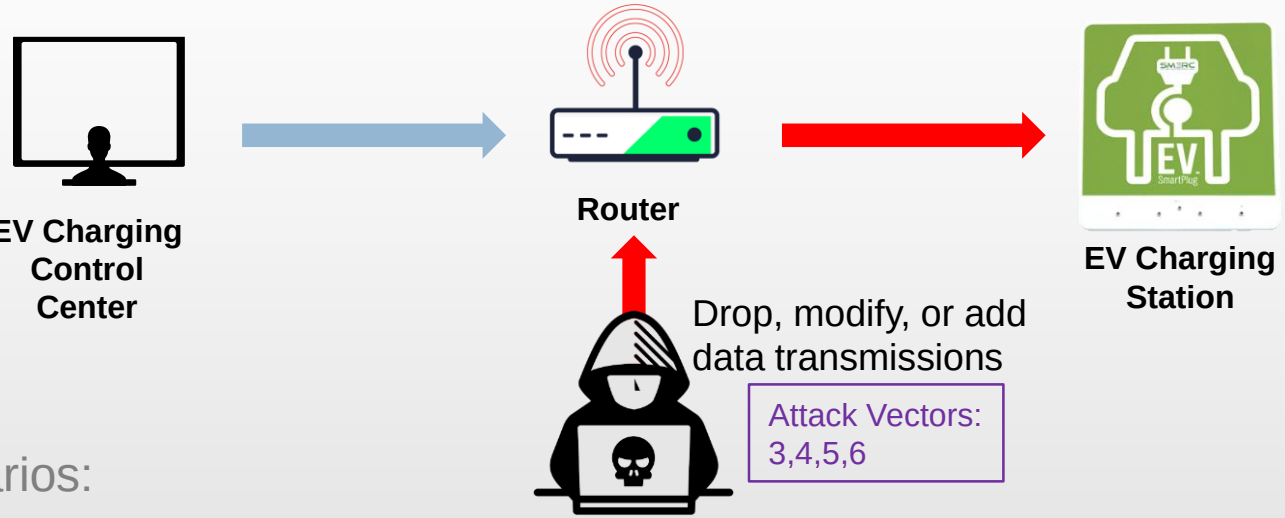
15. Lee, E. K., Gadh, R., & Gerla, M. (2012, November). Resource centric security to protect customer energy information in the smart grid. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on* (pp. 336-341).
16. Daily Burin: New Dining Services online feature optimizes meal-time efficiency. May 25, 2017
17. The privacy Point: Announcing CrowdZen. May 23, 2017.

Attack Surface of UCLA WINSmartEV™ Network



Potential Cyber-Attack Capabilities - Man in the Middle Attack

- A man-in-the-middle (MITM) attack is an attack where the attacker secretly replays and possibly alters the communication between two parties[8][9].



- Scenarios:
  - ET2 - Simultaneous Fast Charges cause Transformer Overload
  - ET5 - Compromised Protocol Translation Module Enables Control of EVs
  - ET6 - EVSE Connects Wirelessly to Wrong Meter and Compromises Billing
  - ET15 - Malware Causes Discharge of EV to the Grid
  - ET16 - An EV is Exploited to Threaten Transformer or Substation
  - DR3 - Messages are Modified or Spoofed on DRAS Communications Channel

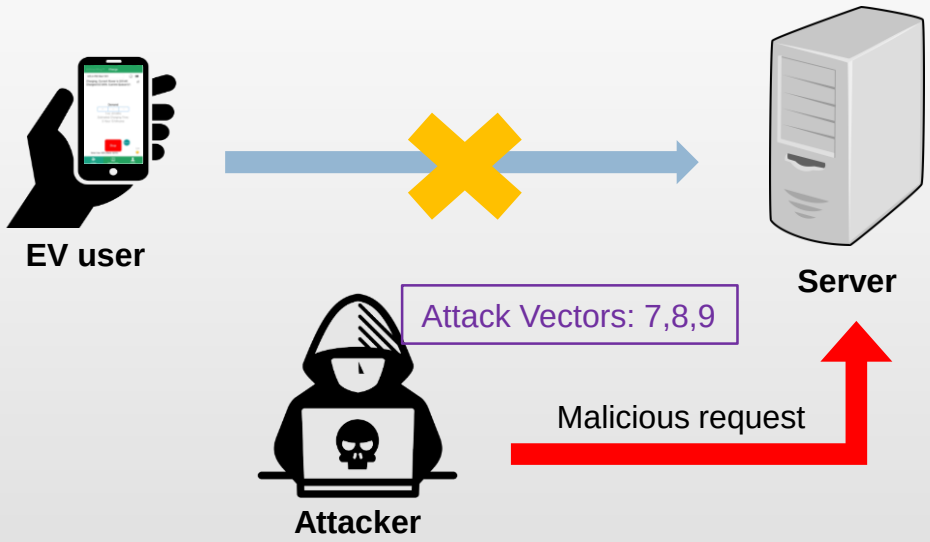
Reference:

8. Rahim, R. (2017). Man-in-the-middle-attack prevention using interlock protocol method. *ARPN J. Eng. Appl. Sci*, *12*(22), 6483-6487.
9. Carter, C., Cordeiro, P. G., Onunkwo, I., & Johnson, J. T. (2018). *Cyber Assessment of Distributed Energy Resources*(No. SAND2018-0281C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Potential Cyber-Attack Capabilities - Denial of Service Attack

- A denial of service (DoS) attack occurs when an attacker takes action intending to overload and flood the network, so that a network service is unavailable to its intended users[9][10]. There is an advanced DoS which called distributed DoS (DDoS).*

  * While The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.



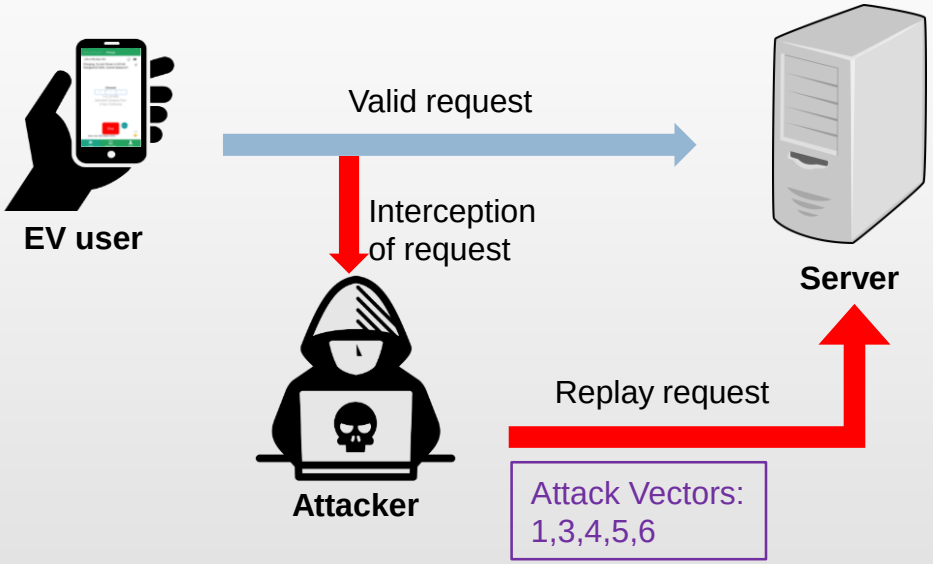
- Scenarios:
  - ET12 - Unavailable Communication Blocks Customer Use of EV Preferential Rate
  - ET14 - EV Charging Process Slowed by Validation Delay of EV Registration ID
  - DR1 - Blocked DR Messages Result in Increased Prices or Outages

Reference:

9. Carter, C., Cordeiro, P. G., Onunkwo, I., & Johnson, J. T. (2018). *Cyber Assessment of Distributed Energy Resources*(No. SAND2018-0281C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
10. Qin, J., Li, M., Shi, L., & Yu, X. (2017). Optimal Denial-of-Service Attack Scheduling with Energy Constraint Over Packet-dropping Networks. *IEEE Transactions on Automatic Control*.

Potential Cyber-Attack Capabilities - Packet Replay Attack

- A packet replay attack occurs when an attacker maliciously captures and repeats, or delays, valid data transmissions[5][9].



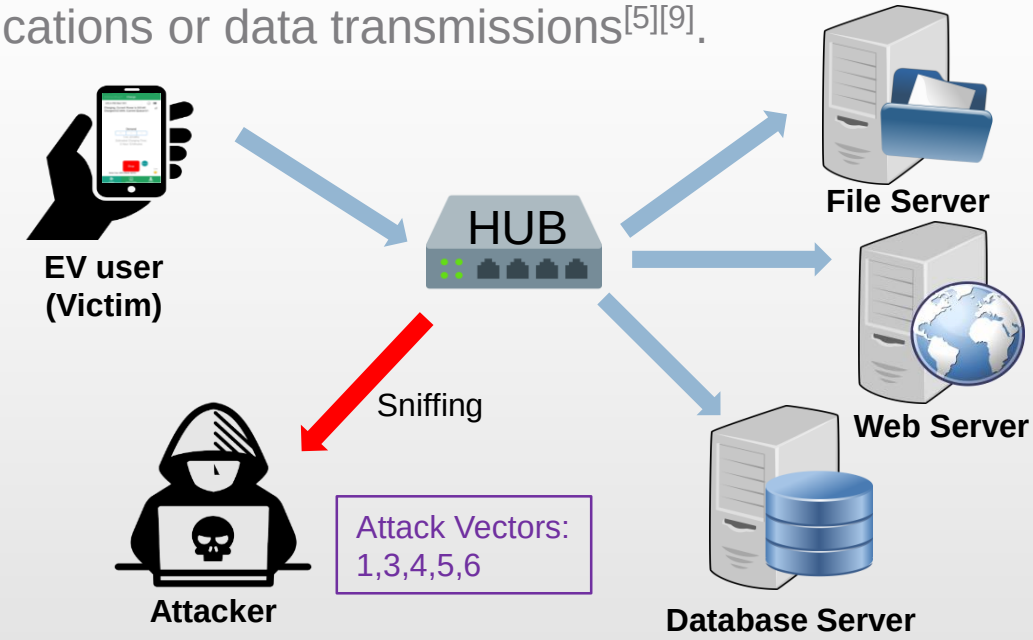
- Scenarios:
  - ET14 - EV Charging Process Slowed by Validation Delay of EV Registration ID
  - DR3 - Messages are Modified or Spoofed on DRAS Communications Channel

Reference:

5. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys and Tutorials*, *19*(1), 446-464.
9. Carter, C., Cordeiro, P. G., Onunkwo, I., & Johnson, J. T. (2018). *Cyber Assessment of Distributed Energy Resources*(No. SAND2018-0281C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Potential Cyber-Attack Capabilities - Eavesdropping Attack

- An Eavesdropping occurs when an attacker reconnoiters and intercepts private communications or data transmissions[5][9].



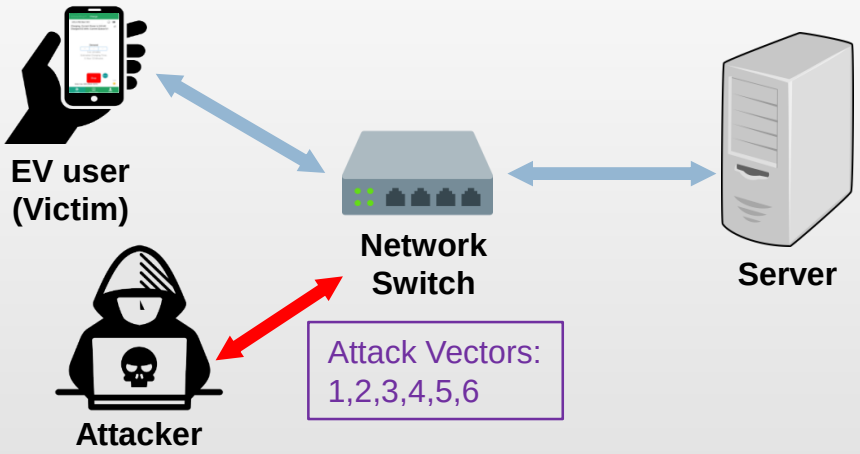
- Scenarios:
  - ET4 - EV Charging Locations Disclosed via Utility Database
  - ET7 - Private Information Disclosed in Transit between EV and EVSE
  - ET9 - EV Registration ID Stolen to Obtain Preferential Rate
  - ET10 - High Priority EV Registration Identity Misused to Obtain Faster Charging
  - DR2 - Private Information is Publicly Disclosed on DRAS Communications Channel

Reference:

5. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys and Tutorials*, *19*(1), 446-464.
9. Carter, C., Cordeiro, P. G., Onunkwo, I., & Johnson, J. T. (2018). *Cyber Assessment of Distributed Energy Resources*(No. SAND2018-0281C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Potential Cyber-Attack Capabilities – ARP Spoofing

- Address Resolution Protocol (ARP) spoofing attack occurs when an attacker sends falsified ARP message over a local area network, resulting in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Therefore, the attacker will be able to receive any data that is intended for that IP address[10].

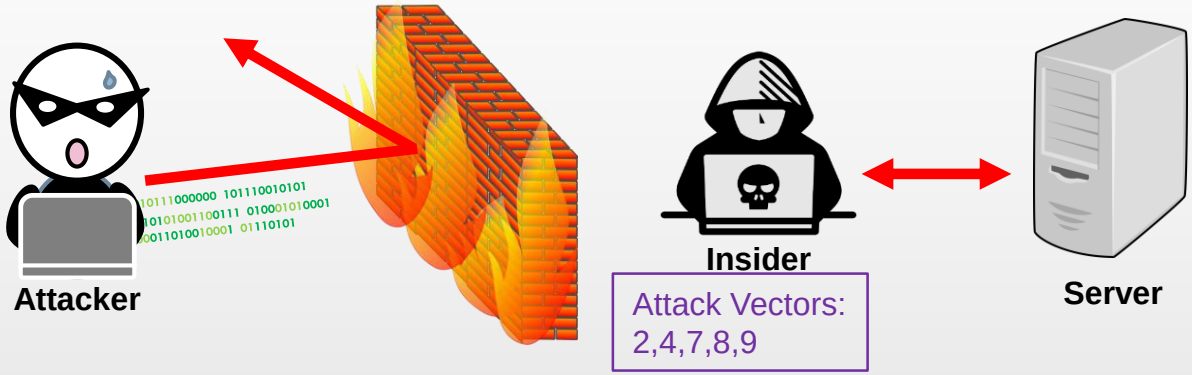


- Scenarios:
  - ET4 - EV Charging Locations Disclosed via Utility Database
  - ET7 - Private Information Disclosed in Transit between EV and EVSE
  - ET9 - EV Registration ID Stolen to Obtain Preferential Rate
  - ET10 - High Priority EV Registration Identity Misused to Obtain Faster Charging
  - ET13 - Invalidated EV Registration ID Blocks Customer use of Preferential Rate
  - DR4 - Improper DRAS Configuration Causes Inappropriate DR Messages

Reference: [10] Bijral, R., Gupta, A., & Sharma, L. S. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. *International Journal of Advanced Research in Computer Science*, *8*(5).

Potential Cyber-Attack Capabilities – Insider Attack

- While an attacker tries to break into a network, an insider is just in as much danger on the inside of the firewall as from the outside. An insider can be employees, contractors or an insider from outside[5].



- Scenarios:
  - ET1 - Custom Malware causes EV Overcharge and Explosion
  - ET2 - Simultaneous Fast Charges cause Transformer Overload
  - ET3 - Virus Propagated between EVs and EV Service Equipment (EVSE)
  - ET6 - EVSE Connects Wirelessly to Wrong Meter and Compromises Billing
  - ET15 - Malware Causes Discharge of EV to the Grid
  - ET16 - An EV is Exploited to Threaten Transformer or Substation
  - DR5 - Non-specific Malware Compromises DRAS or Customer DR System
  - DR6 - Custom Malware Compromises DRAS

Reference:

5. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys and Tutorials*, *19*(1), 446-464.

Risk Assessment [7]

- Risk : **Impact/cost** ratio of the failure scenarios

  - Categories of the failure scenarios:
    - Electric Transportation (ET): 16 scenarios
    - Demand Response (DR): 7 scenarios

- Ranking of the risk:
  - To highlight the areas of highest risk and prioritize remediation effort
  - This approach had been used successfully by a NESCOR member company in the past to rank intentional attacks.
  - **Impact**: the “impact” and “effects on likelihood and opportunity” scores are combined in to a **Impact score**.
  - **Cost**: Cost to the adversary (attacker)

Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Risk Assessment - Scales for the Ranking [7]

- **Impact score**
  - Assign a score of 0, 1, 3, or 9, to represent the impact of the failure scenario, as it ranges from minor to significant.
  - Example:
    - 0: one customer out of power for 15 minutes, petty cash expenses,
    - 1: small generation plant off-line,
    - 3: 20% of customers experience defect from smart meter deployment,
    - 9: large transformer destroyed and major city out of power for a week.
- **Cost score**
  - Assign a score of 0.1, 1, 3 or 9, to represent the cost and difficulty to the threat agent to carry out the failure scenario, from low to high.
  - Example:
    - 0.1: It is easy to trigger the failure scenario, almost no cost,
    - 1: a bit of expertise and planning needed, such as capture keys off unencrypted smart meter bus
    - 3: serious expertise and planning needed to carry out scenario,
    - 9: probably needs nation-state resources to carry out scenario (e.g., Stuxnet)

Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Rankings for Failure Scenarios

I: Impact; C: Cost; R: Ratio

Class: Classification of the impact

Scenarios	Description	I	C	R	Ranking	Class
ET1	Custom Malware causes EV Overcharge and Explosion	3	9	0.33	Negligible	CP
ET2	Simultaneous Fast Charges cause Transformer Overload	1	9	0.11	Negligible	CP
ET3	Virus Propagated between EVs and EV Service Equipment (EVSE)	9	3	3.00	Low	CP
ET4	EV Charging Locations Disclosed via Utility Database (violating customer privacy)	1	1	1.00	Low	CC
ET5	Compromised Protocol Translation Module Enables Control of EVs	3	3	1.00	Low	CP
ET6	EVSE Connects Wirelessly to Wrong Meter and Compromises Billing	3	3	1.00	Low	CC
ET7	Private Information Disclosed in Transit between EV and EVSE (violating customer privacy)	3	3	1.00	Low	CC
ET8	Customer Misuses their EV Registration ID to Obtain Preferential Rate	0	0.1	0.00	Negligible	CC
ET9	EV Registration ID Stolen to Obtain Preferential Rate	0	0.1	0.00	Negligible	CC
ET10	High Priority EV Registration Identity Misused to Obtain Faster Charging	0	1	0.00	Negligible	CC
ET11	All EV Registration IDs Stolen from Utility	3	0.1	30.00	High	CC
ET12	Unavailable Communication Blocks Customer Use of EV Preferential Rate	1	3	0.33	Negligible	CC
ET13	Invalidated EV Registration ID Blocks Customer use of Preferential Rate	1	3	0.33	Negligible	CC
ET14	EV Charging Process Slowed by Validation Delay of EV Registration ID	1	3	0.33	Negligible	CC
ET15	Malware Causes Discharge of EV to the Grid	3	0.1	30.00	High	CP
ET16	An EV is Exploited to Threaten Transformer or Substation	9	9	1.00	Low	CP
DR1	Blocked DR Messages Result in Increased Prices or Outages	9	0.1	90.00	High	CP/CC
DR2	Private Information is Publicly Disclosed on DRAS Communications Channel (violating customer privacy)	1	3	0.33	Negligible	CC
DR3	Messages are Modified or Spoofed on DRAS Communications Channel	9	1	9.00	Moderate	CP/CC
DR4	Improper DRAS Configuration Causes Inappropriate DR Messages	9	1	9.00	Moderate	CP/CC
DR5	Non-specific Malware Compromises DRAS or Customer DR System	9	1	9.00	Moderate	CP/CC
DR6	Custom Malware Compromises DRAS	9	1	9.00	Moderate	CP/CC
DR7	Custom Malware Compromises DR system	9	1	9.00	Moderate	CP/CC

Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 1

I:3, C:9, R:0.33, Class: CP

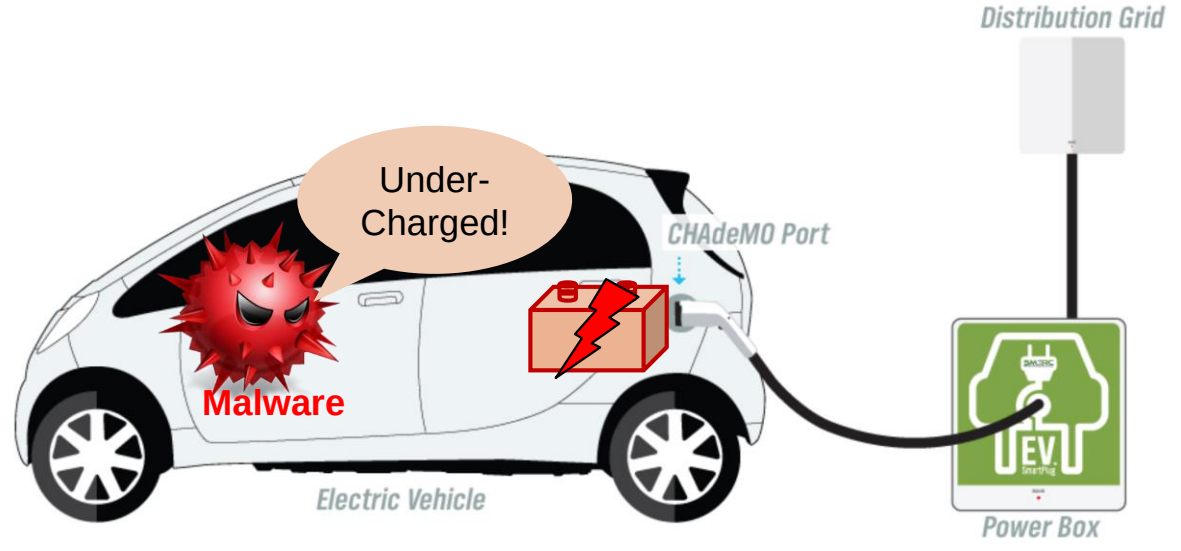
➢ Custom Malware causes EV Overcharge and Explosion

Relevant Vulnerabilities:

- Design, implementation, or maintenance permits system to enter a hazardous state by overcharging or draining the battery beyond limits,
- System permits unauthorized changes to EV firmware using easily accessible interfaces,
- System permits unauthorized changes to EV firmware.

Impact:

- Possible loss of life and property damage,
- A tragic accident can lead to a loss of public confidence.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 2

I:1, C:9, R:0.11, Class: CP

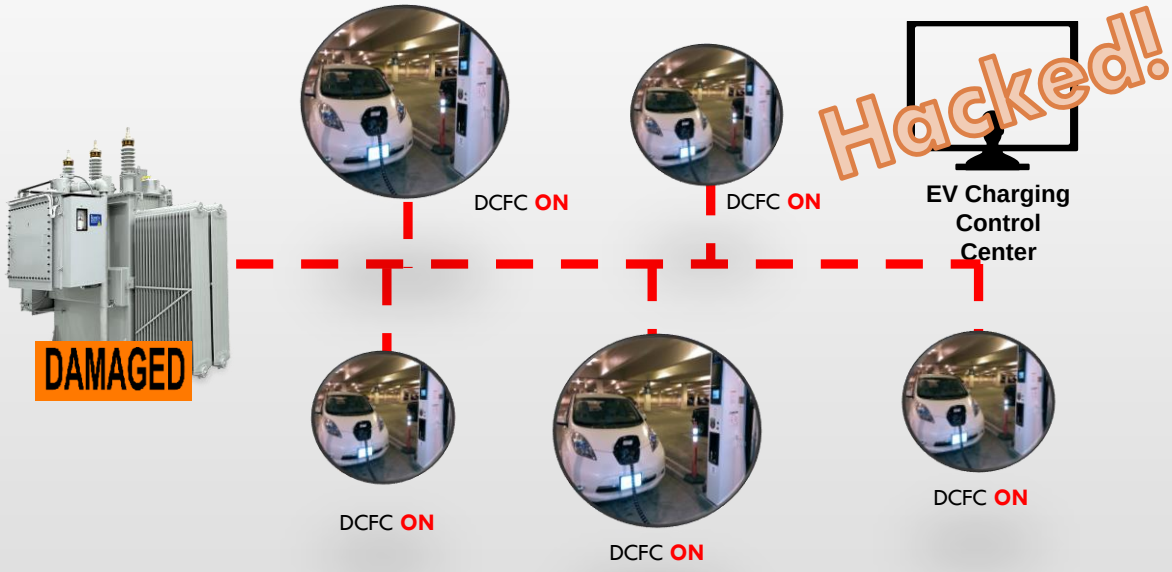
- Simultaneous Fast Charges cause Transformer Overload

Relevant Vulnerabilities:

- System permits unauthorized changes to the fast-charging station management system software and configuration,
- Design, implementation, or maintenance permits system to enter a hazardous state by letting circuits become overloaded in the distribution transformer.

Impact:

- Power outage to EVs and the charging station,
- Damage to the distribution transformer.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 3

I:9, C:3, R:3.00, Class: CP

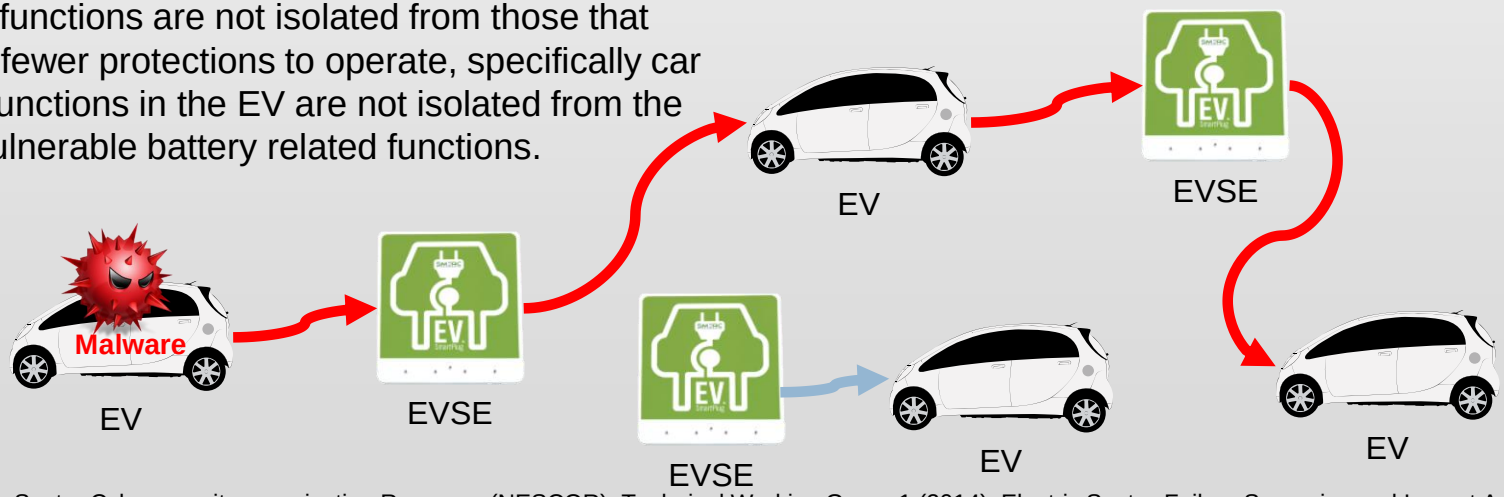
- Virus Propagated between EVs and EV Service Equipment (EVSE)

Relevant Vulnerabilities:

- System permits installation of malware in an EV, at the EV factory and maintenance center,
- System permits installation of malware in the public charging station system,
- Critical communication paths are not isolated from communication paths that require fewer protections to operate, specifically, EV charging and conventional data transmission during charging,
- System permits installation of malware in the public charging station system or EV being charged, during charging,
- Critical functions are not isolated from those that require fewer protections to operate, specifically car safety functions in the EV are not isolated from the more vulnerable battery related functions.

Impact:

- For affected EVs, range from minor nuisances to major safety problems which could cause loss of life,
- For affected EVSE's, potential for arbitrary malfunctions and revenue loss due to shutting down charging stations for troubleshooting,
- Negative publicity concerning EVs,
- Litigation for owner of charging station.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 4

I:1, C:1, R:1.00, Class: CC

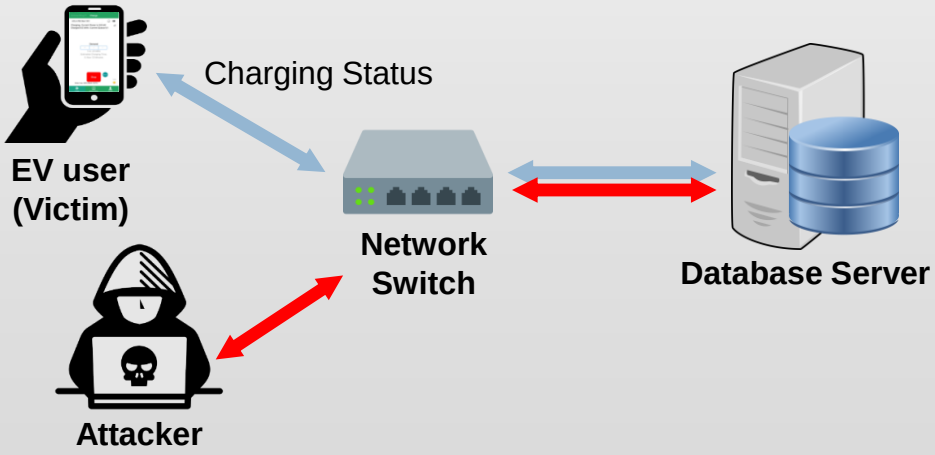
➢ EV Charging Locations Disclosed via Utility Database

Relevant Vulnerabilities:

- Unnecessary access is permitted to the database in the firewall protecting the EV database server,
- System relies on credentials that are easy to obtain for access to the EV database server,
- Unnecessary access is permitted to the database in the database server.

Impact:

- Privacy violation for customers,
- Potential cost to the utility because of privacy lawsuits by customers,
- Potential legal action by government or regulatory agencies against the utility if applicable privacy laws are violated,
- Decrease in usage of utility charging stations and public relations issue for the utility.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 5

I:3, C:3, R:1.00, Class: CP

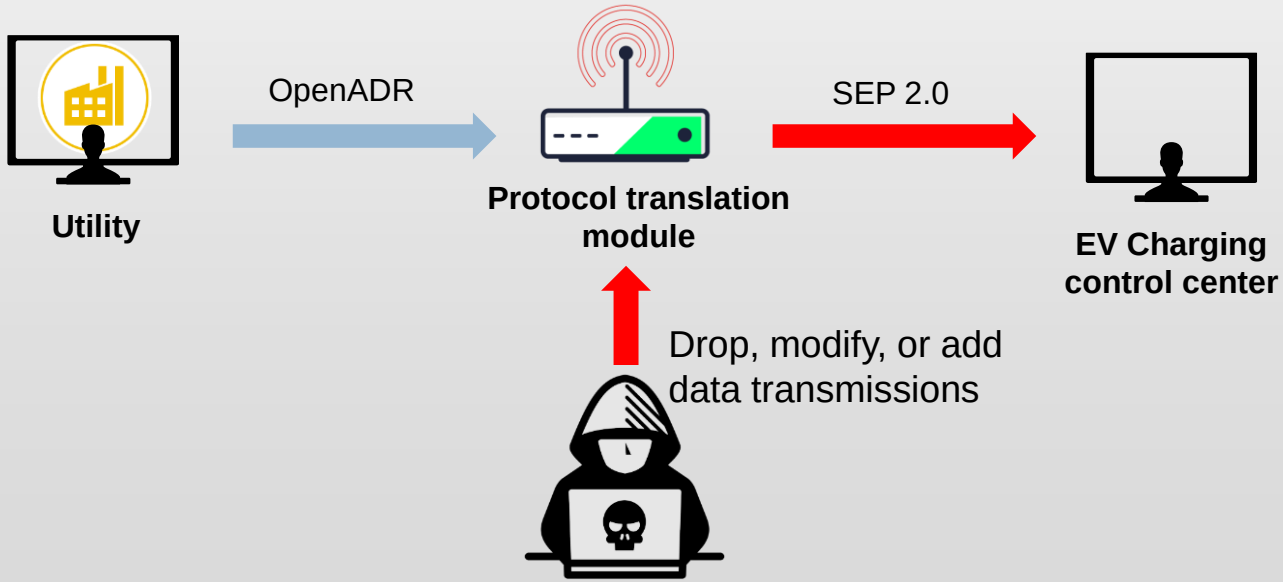
- Compromised Protocol Translation Module Enables Control of EVs

Relevant Vulnerabilities:

- System permits unauthorized changes to code in the protocol translation module.

Impact:

- Potential for turning charging on or off for a large number of vehicles within a short time period,
- Inconvenience to customers,
- Cost of customer service situations,
- Potential to overpower and damage transformer in a neighborhood.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 6

I:3, C:3, R:1.00, Class: CC

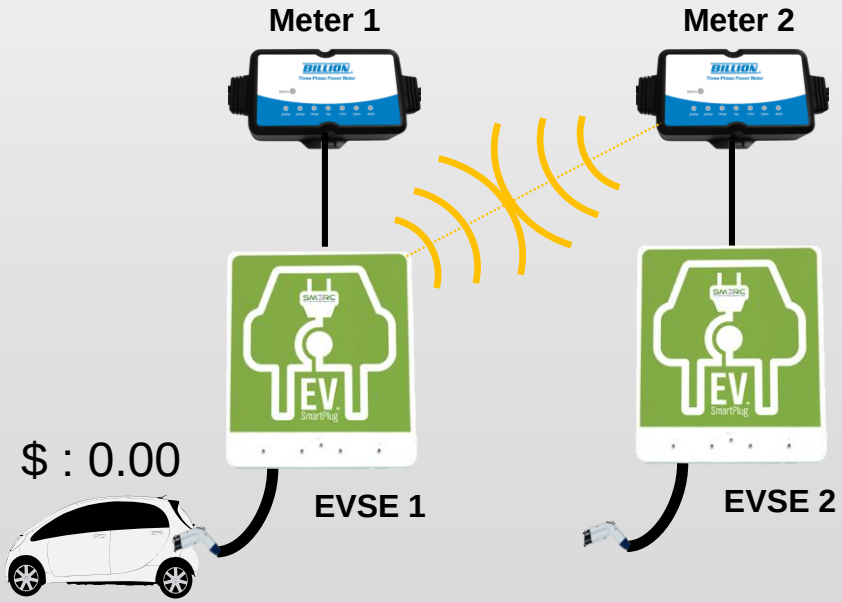
➢ EVSE Connects Wirelessly to Wrong Meter and Compromises Billing

Relevant Vulnerabilities:

- Inadequate binding of meter with energy users authorized to charge to that meter,
- Users lack visibility that unauthorized changes were made in the association between an EVSE and its smart meter.

Impact:

- Cost of billing disputes that could be raised by any customer,
- Delay or loss of payment to the utility,
- Likely cost to upgrade or replace the smart meter and/or EVSE.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 7

I:3, C:3, R:1.00, Class: CC

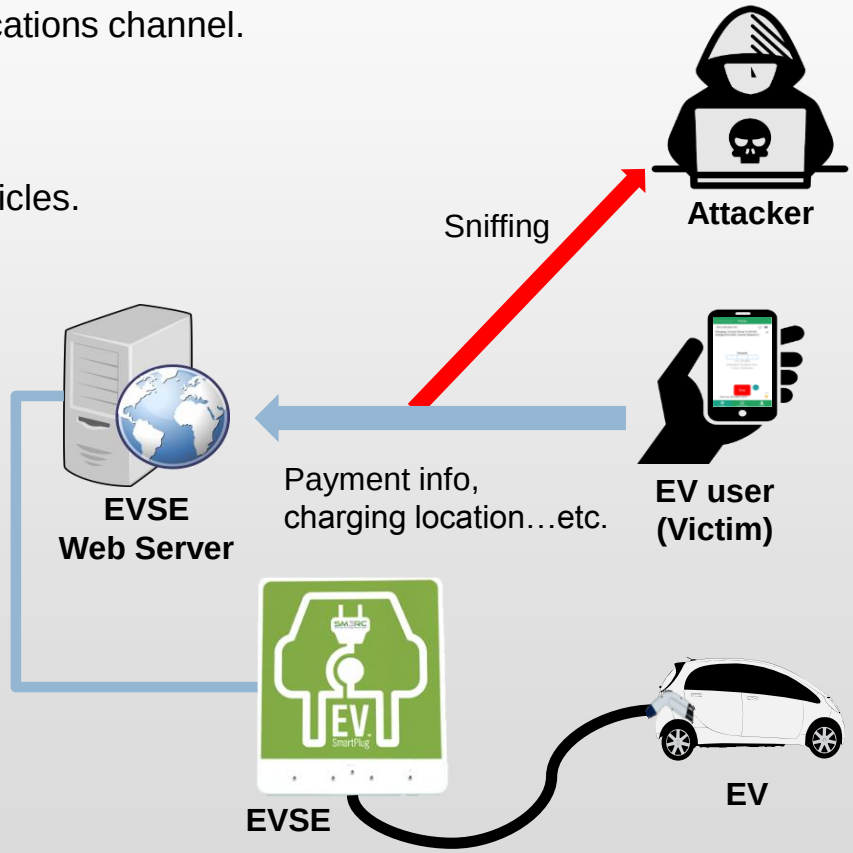
➢ Private Information Disclosed in Transit between EV and EVSE

Relevant Vulnerabilities:

- System makes private data accessible to unauthorized individuals in the EV/EVSE communications channel.

Impact:

- Loss of customer privacy,
- Decreased acceptance of electric vehicles.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 8

I:0, C:0.1, R:0.00, Class: CC

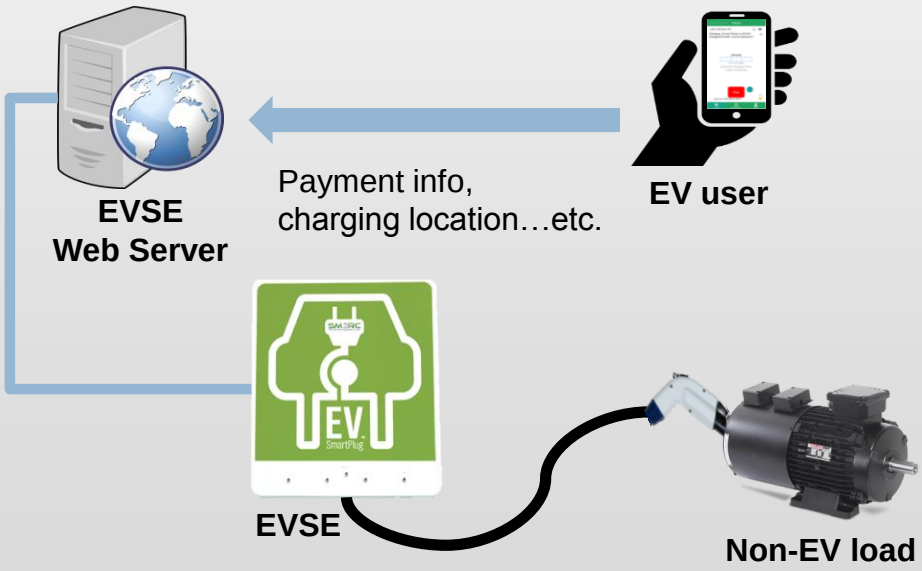
➢ Customer Misuses their EV Registration ID to Obtain Preferential Rate

Relevant Vulnerabilities:

- System permits device identifier to be misused to charge non-EV items when charging takes place based upon an EV registration identifier.

Impact:

- Loss of revenue to a utility,
- The non-EV load may draw too much current and blow the fuse of the EVSE or
- trip the local circuit breaker.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 9

I:0, C:0.1, R:0.00, Class: CC

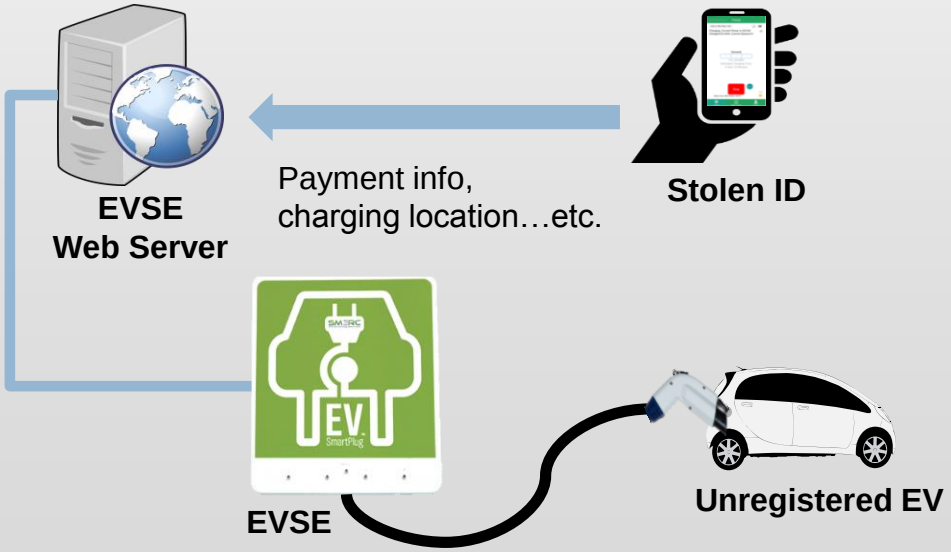
➢ EV Registration ID Stolen to Obtain Preferential Rate

Relevant Vulnerabilities:

- System permits device identifier to be misused to masquerade as valid customer whose EV is being charged when charging takes place based upon the identifier.

Impact:

- Illegitimate charges billed to legitimate owner of the EV registration ID,
- Cost of associated customer service situation for this owner,
- Likely loss of revenue by the utility.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 10

I:0, C:1, R:0.00, Class: CC

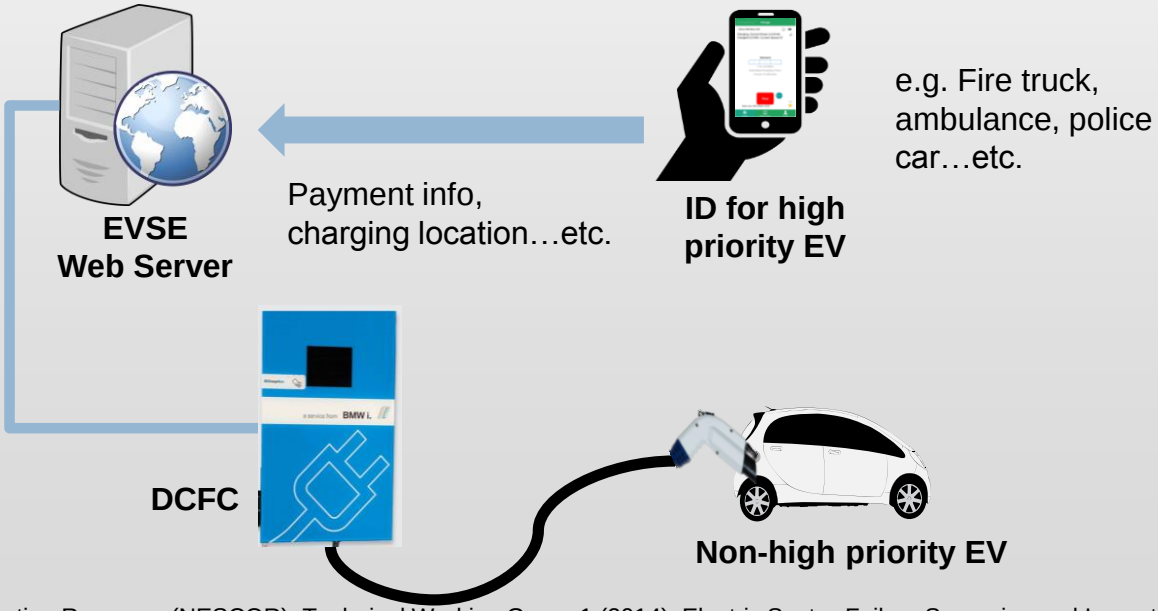
- High Priority EV Registration Identity Misused to Obtain Faster Charging

Relevant Vulnerabilities:

- System permits device identifier to be misused to masquerade as a high priority EV that is being charged.

Impact:

- Possibility for slower charging of high priority or other normal priority vehicles.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 11

I:3, C:0.1, R:30.00, Class: CC

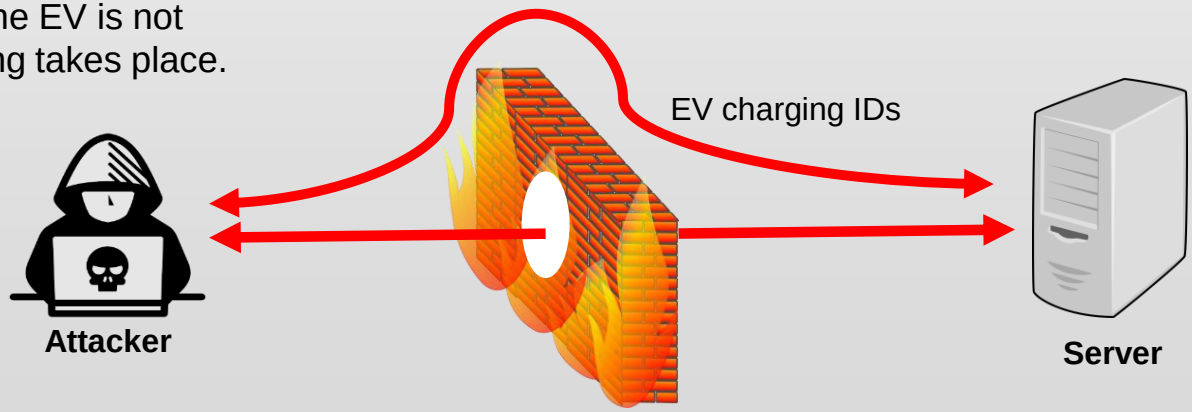
➢ All EV Registration IDs Stolen from Utility

Relevant Vulnerabilities:

- Unnecessary network access is permitted for utility networks or databases that store or transmit registration identities,
- Unnecessary access is permitted to the database that stores registration identities,
- System makes private data accessible to unauthorized individuals in the storage of registration identities,
- System permits device identifier to be misused to masquerade as a trustworthy transaction. The ID could be misused by another person if the user's identity is not verified at the point of use. It can be misused for another EV if the EV is not authenticated when charging takes place.

Impact:

- Cost of reissuing identities and verifying receipt of new identities so that stolen ones can be cancelled,
- Loss of revenue while any stolen identities remain valid,
- Inconvenience to customers,
- Cost of handling customer service situations.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 12

I:1, C:3, R:0.33, Class: CC

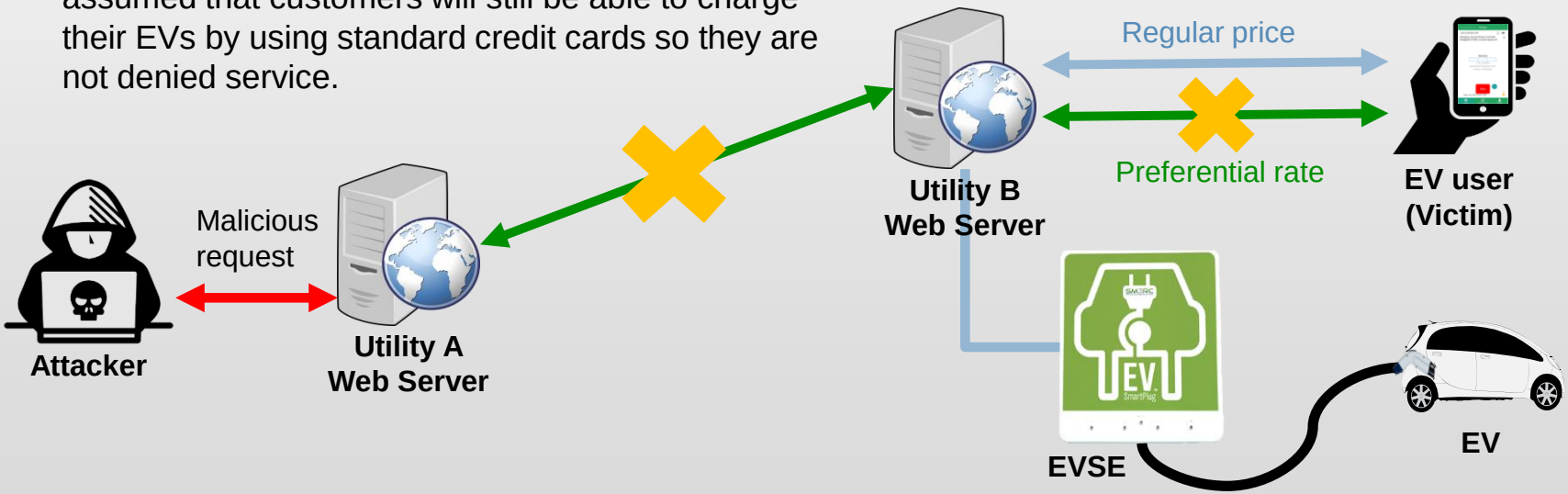
➢ Unavailable Communication Blocks Customer Use of EV Preferential Rate

Relevant Vulnerabilities:

- Critical components exhibit single point of failure such as communication paths or databases used to verify registration identities between utilities.

Impact:

- Customer inconvenience,
- Cost of customer service situation handling complaints and coordinating refunds with servicing utility. It is assumed that customers will still be able to charge their EVs by using standard credit cards so they are not denied service.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

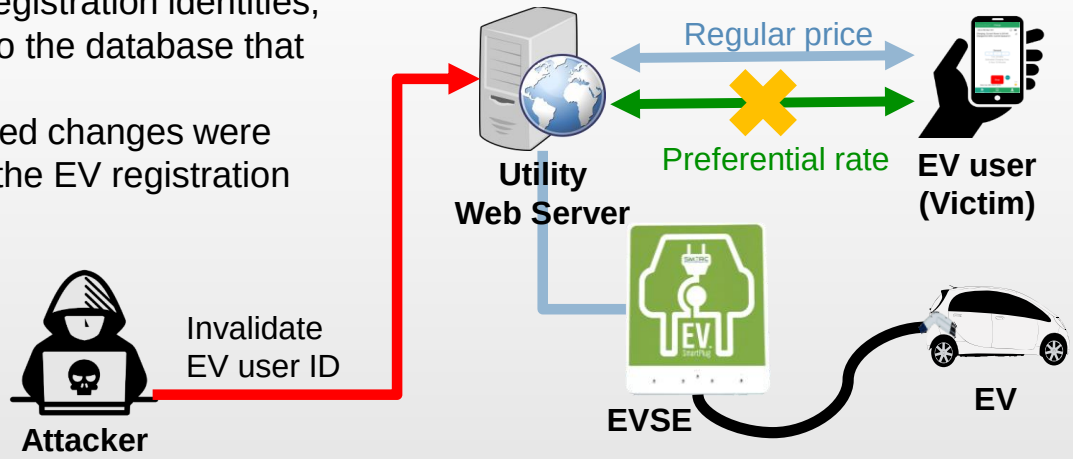
Electric Transportation (ET) – Scenario 13

I:1, C:3, R:0.33, Class: CC

➢ Invalidated EV Registration ID Blocks Customer use of Preferential Rate

Relevant Vulnerabilities:

- Unnecessary network access is permitted to utility networks or databases that store registration identities,
- Unnecessary access is permitted to the database that stores registration identities,
- Users lack visibility that unauthorized changes were made via transactions that impact the EV registration ID database.



Impact:

- Serious inconvenience and embarrassment to customers in any situation where credit cards or other billing methods using the regular electricity rate are not available. One example is a visitor to any non-retail location where the party responsible for the electricity account for the facility visited is not expected to pay the visitor's bills (such as a contractor travelling to a job site or a professor's visit to a colleague),
- Cost of customer service situations to handle complaints and to coordinate refunds with other utilities. This assumes that in a retail situation the customer will still be able to charge their EV by using standard credit cards so they are not denied service. Also assumed is that when at home, the customer would be billed at the standard rate if their registration identify was invalid.

Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 14

I:1, C:3, R:0.33, Class: CC

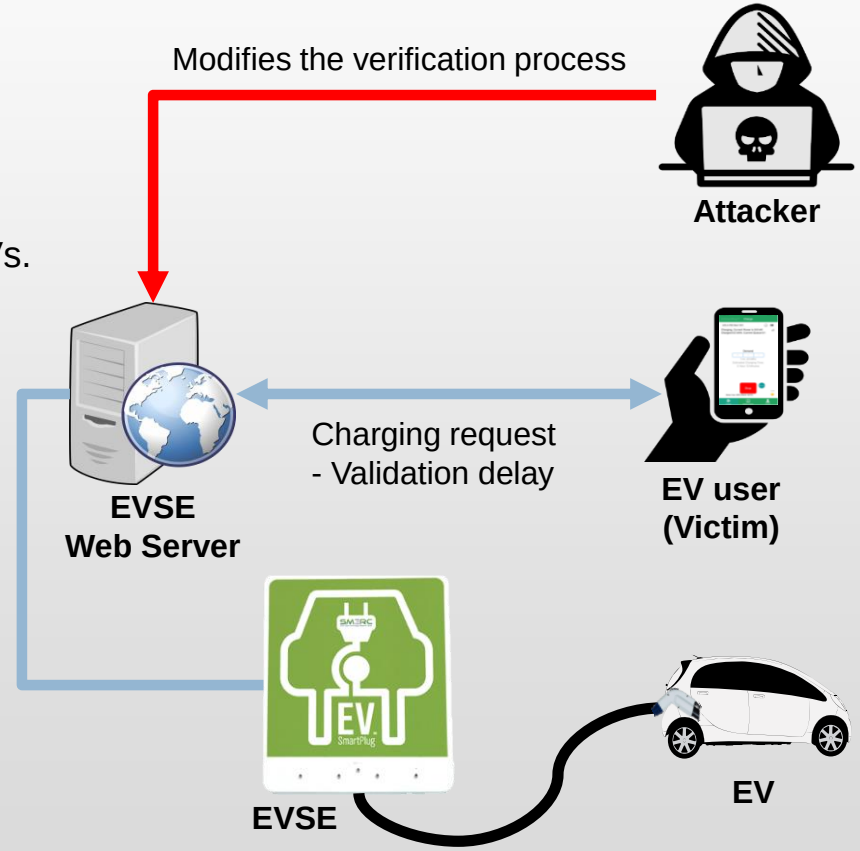
➢ EV Charging Process Slowed by Validation Delay of EV Registration ID

Relevant Vulnerabilities:

- System permits unauthorized changes to software.

Impact:

- Inconvenience to customers,
- Cost of handling customer complaints,
- Cost of troubleshooting problem,
- Embarrassment to the utility,
- Creates poor perception of the usability of EVs.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 15

I:3, C:0.1, R:30.00, Class: CP

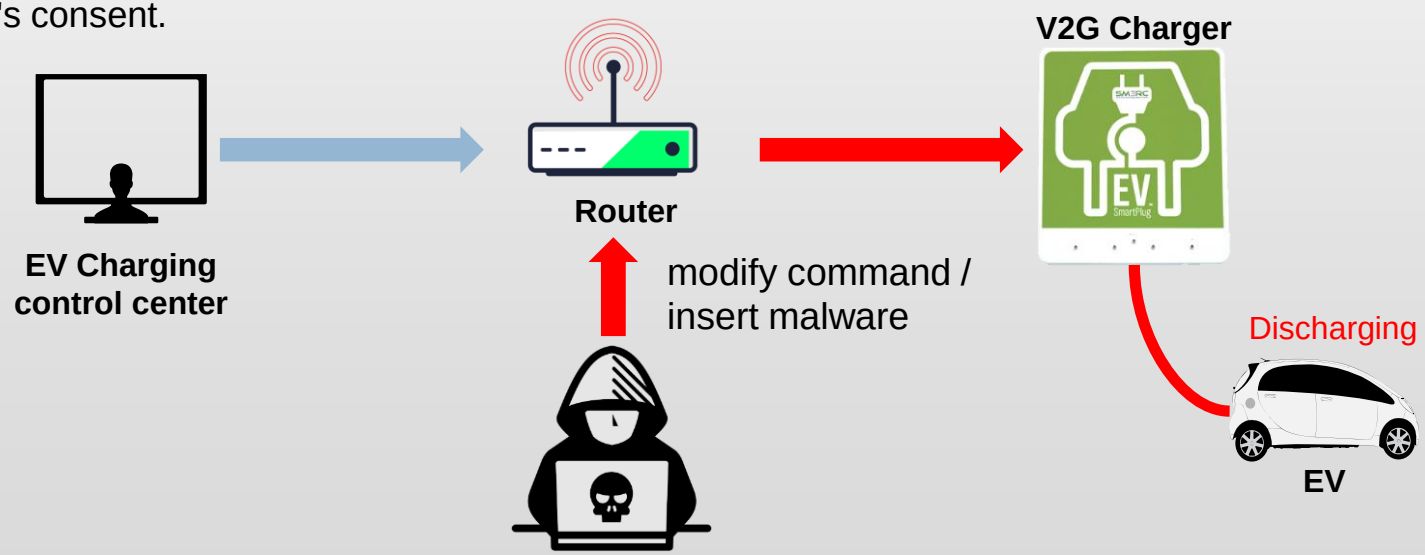
➢ Malware Causes Discharge of EV to the Grid

Relevant Vulnerabilities:

- System permits unauthorized changes to code in the charging station management system and protocol translation module,
- Design, implementation, or maintenance permits system to enter a hazardous state by overloading of the distribution transformer if many EVs are discharged,
- System takes action before confirming changes with user causing EVs to be discharged without owner's consent.

Impact:

- Critical damage to electric vehicles,
- Inconvenience to customers,
- Cost of customer service situations,
- Violation of customer contracts and loss of customer confidence,
- A sudden, large amount of electricity from EVs could damage a transformer in a neighborhood.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Electric Transportation (ET) – Scenario 16

I:9, C:9, R:1.00, Class: CP

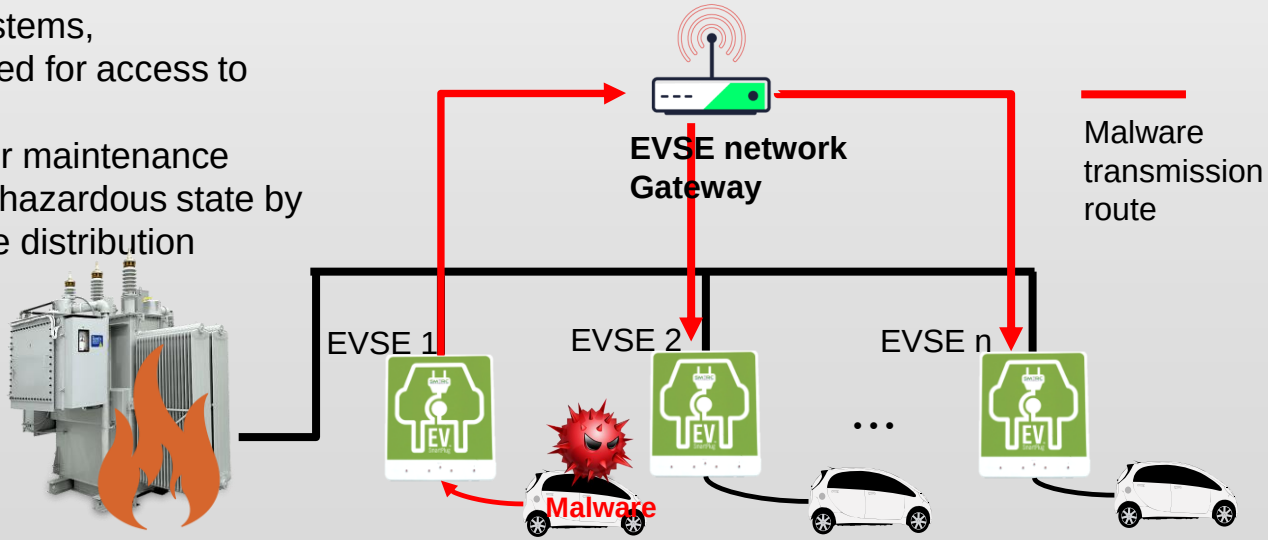
➢ An EV is Exploited to Threaten Transformer or Substation

Relevant Vulnerabilities:

- System permits installation of malware in the EVSE during charging between the EV and the EVSE,
- System permits installation of malware due to the malware spreading between EVSEs on the network hosting the EVSEs for the charging station,
- System permits unauthorized changes to the in-vehicle system,
- System permits installation of malware in public charging station systems,
- Shared credentials are used for access to nearby EVSEs,
- Design, implementation, or maintenance permits system to enter a hazardous state by allowing overloading of the distribution transformer.

Impact:

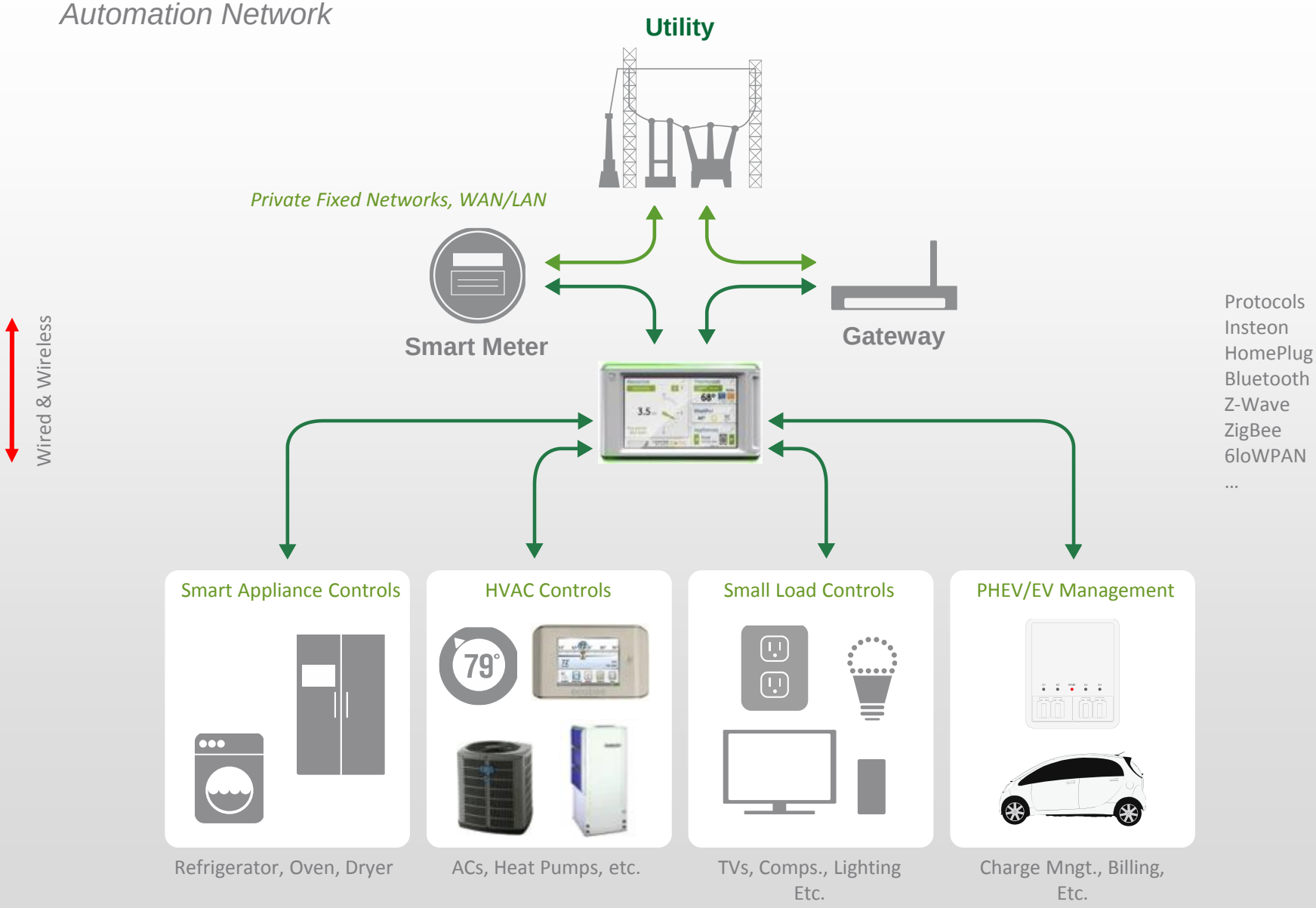
- Potential to overpower and damage transformer in a neighborhood,
- Temporarily loss of capability for charging station to service customers,
- Potential damage to electric vehicles,
- Revenue loss of the owner of the charging stations due to their damage,
- Violation of customer contracts and loss of customer confidence.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response

Automation Network



Demand Response (DR) – Scenario 1

I:9, C:0.1, R:90.00, Class: CP/CC

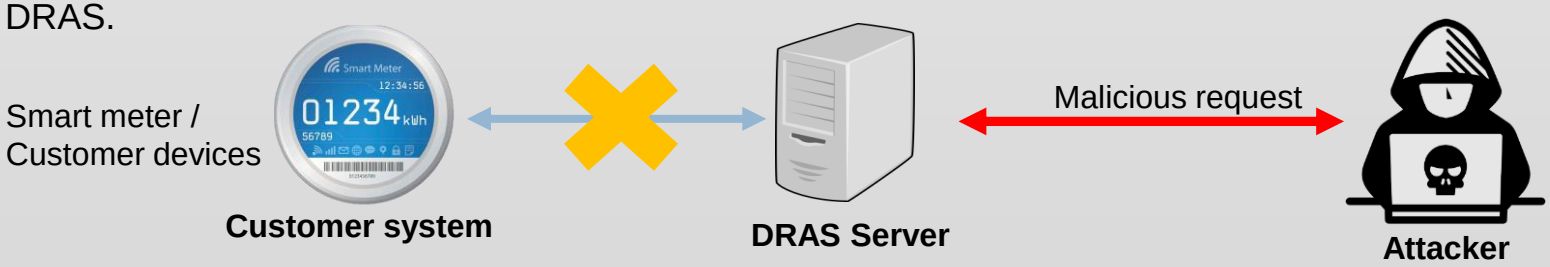
➢ Blocked DR Messages Result in Increased Prices or Outages

Relevant Vulnerabilities:

- Physical access may be obtained by unauthorized individuals to communications channel components,
- Unnecessary access is permitted to the communications channel,
- Publicly accessible and/or third party controlled links used in DRAS/customer communication channels,
- System relies on communications that are easy to jam in wireless DRAS/customer communications channels,
- System permits unauthorized changes to the messaging interface components of the DRAS,
- System permits unauthorized changes to the messaging components of the customer systems,
- Users lack visibility of threat activity specifically unusual traffic load on the communications channel from the DRAS to customer systems or interactions with channel components not originated by the DRAS.

Impact:

- The effects would be correlated to the extent of blockage:
  - If the blockage is local, the impact may be limited to increased energy charges to consumers,
  - Blockage of DR messages on a larger scale, particularly messages to large industrial customers, may cause outages at a local or regional level if demand is too great and increased energy costs to customers over a larger area,
- In sell-back or brokerage scenarios, the blockage of DR signals may result in increased prices for electricity for the utility company and be instrumented for considerable financial gain for parties selling electricity back to the utility company.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 2

I:1, C:3, R:0.33, Class: CC

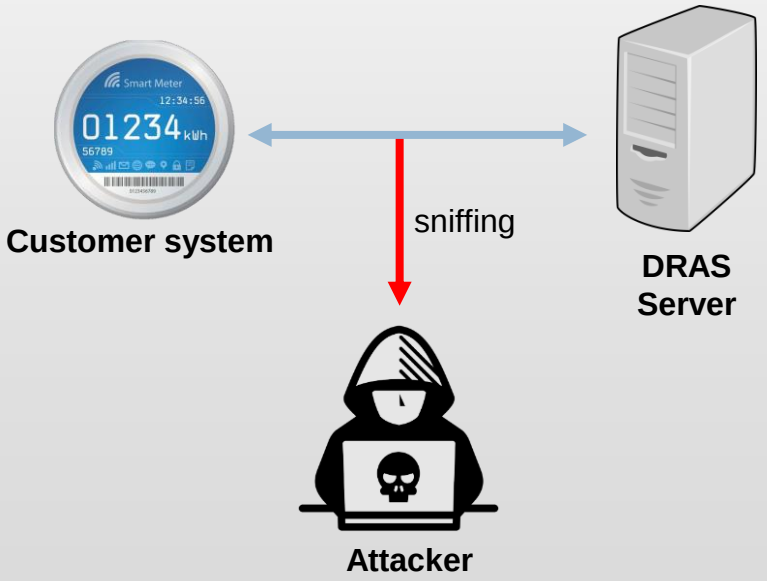
➢ Private Information is Publicly Disclosed on DRAS Communications Channel

Relevant Vulnerabilities:

- Physical access may be obtained by unauthorized individuals to communications channel components,
- Unnecessary access is permitted to the communications channel,
- Publicly accessible and/or third party controlled links used in DRAS/customer communications channels,
- Encryption keys are shared by multiple computers on the DRAS network,
- System makes messages accessible to unauthorized individuals (easy to tap) in wired/wireless communications channels in the DRAS network,
- Users lack visibility of threat activity specifically the presence of unknown entities creating traffic on the DRAS/customer communication channel.

Impact:

- Malicious eavesdropping can reveal private information that may be made public. This violates customer privacy,
- Potential for lawsuits and fines against the utility,
- Loss of public confidence in the utility and the DR program, resulting in resistance to both.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 3

I:9, C:1, R:9.00, Class: CP/CC

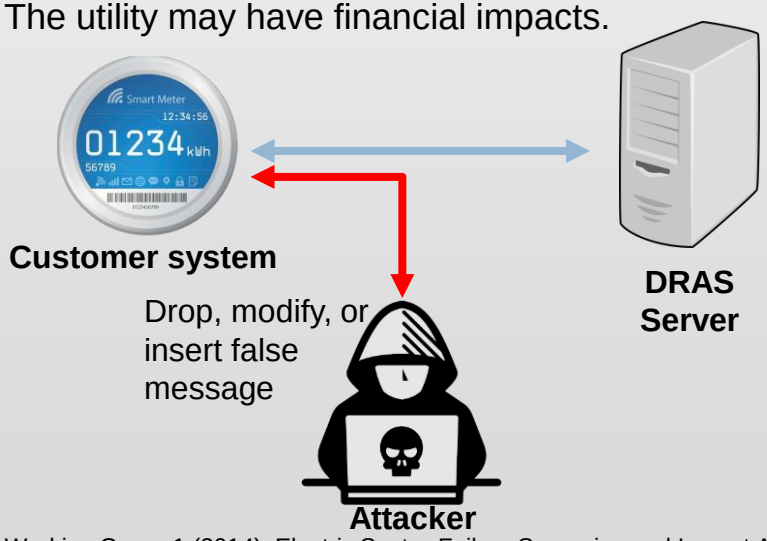
➢ Messages are Modified or Spoofed on DRAS Communications Channel

Relevant Vulnerabilities:

- System permits messages to be modified by unauthorized individuals between the DRAS and customer DR component,
- Message modified by an adversary is either difficult or infeasible to distinguish from a valid message between the DRAS and customer DR component,
- Physical access may be obtained by unauthorized individuals to communications channel components,
- Unnecessary access is permitted to the communications channel,
- Publicly accessible and/or third party controlled links used,
- Users lack visibility of threat activity specifically the presence of unknown entities with access to the DRAS/customer communication channel.

Impact:

- A false message may request the DRAS to reduce power supply or to trigger an inappropriate DR event,
- A false message may deliver information indicating cheaper prices to consumers, which encourages them to increase power consumption during on-peak periods,
- Possible service impacts on various (possibly quite large) scales,
- Potential power loss,
- The utility may have financial impacts.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 4

I:9, C:1, R:9.00, Class: CP/CC

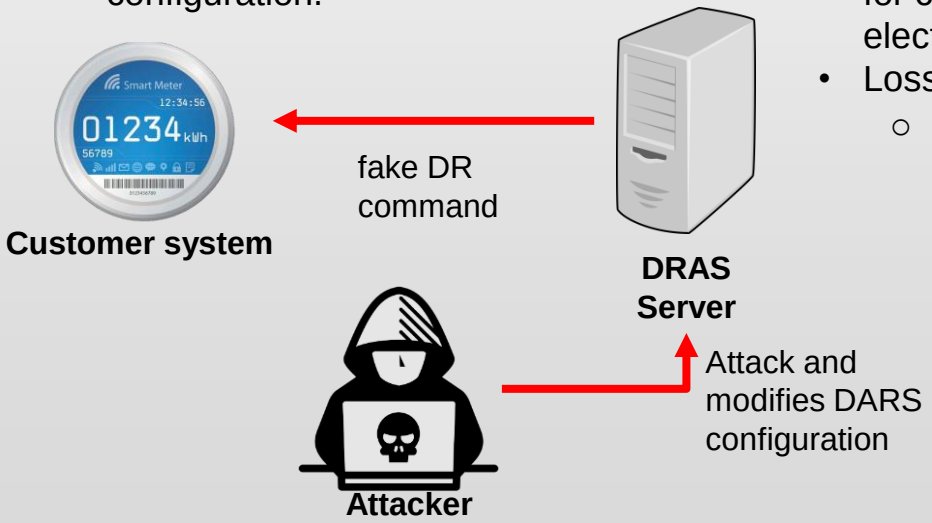
➢ Improper DRAS Configuration Causes Inappropriate DR Messages

Relevant Vulnerabilities:

- System permits unauthorized changes to DRAS configuration,
- Users lack visibility that unauthorized changes were made in the DRAS configuration,
- Unnecessary network access is permitted to the network on which the DRAS resides,
- System relies on credentials that are easy to obtain for access to the DRAS configuration.

Impact:

- A false message may deliver information indicating lower prices to consumers, which encourages them to increase power consumption during on-peak periods,
- Damage to the smart grid infrastructure with possible service impacts from small to large scale,
- Potential power loss,
- The utility may have financial impacts,
- In sell-back or brokerage scenarios, withholding of DR signals at the source DRAS may result in increased prices for electricity to the utility and be instrumented for considerable financial gain for parties selling electricity back to the utility company,
- Loss of public confidence in utility and DR program,
  - The customer, receiving an unintended DR message, may reduce power consumption without seeing any benefit applied in their bill.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 5

I:9, C:1, R:9.00, Class: CP/CC

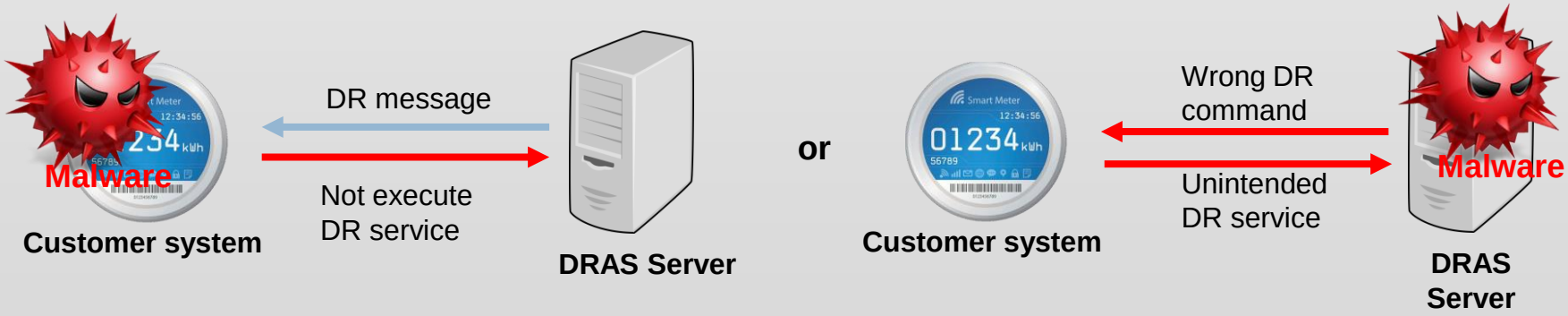
➢ Non-specific Malware Compromises DRAS or Customer DR System

Relevant Vulnerabilities:

- Software patches are not checked regularly to ensure that they are current,
- The list of signatures used for detection of attacks is no longer current,
- Unnecessary system services are configured to run on un-blocked or
- Unnecessary opened ports,
- Remote access may be obtained by unauthorized individuals to the customer system from remote networks,
- Physical access may be obtained by unauthorized individuals to the DRAS (e.g., to use a Universal Serial Bus (USB) device).

Impact:

- Unstable power balance at the utility due to failure to communicate or execute reduction of power demand during on-peak periods, possibly resulting in loss of power for some customers,
- Potential revenue loss due to failure to communicate or execute a return to non-peak conditions in which customers may increase usage,
- Capture and exfiltration of sensitive DR information would violate customer privacy,
- Loss of public confidence in the utility and DR program.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 6

I:9, C:1, R:9.00, Class: CP/CC

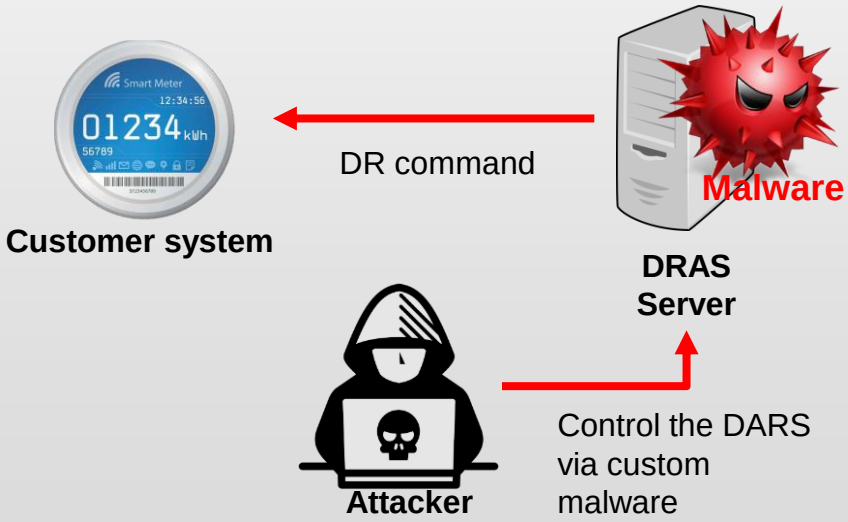
- Custom Malware Compromises DRAS

Relevant Vulnerabilities:

- System permits unauthorized changes to software in the DRAS,
- Users lack visibility that unauthorized changes were made to the DRAS software,
- Unnecessary system services are configured to run on un-blocked or unnecessary open ports,
- Unnecessary network access is permitted to the network on which the DRAS resides.

Impact:

- Addition of extra load at peak times and reduction of load at non-peak times could result in power outages and physical power system damage,
- Loss of public confidence in the utility and DR program.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Demand Response (DR) – Scenario 7

I:9, C:1, R:9.00, Class: CP/CC

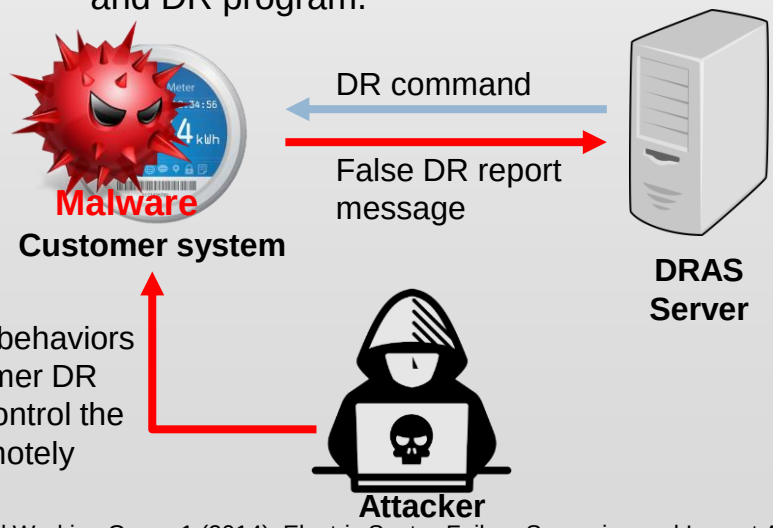
➢ Custom Malware Compromises DR system

Relevant Vulnerabilities:

- Software patches are not checked regularly to ensure that they are current resulting in vulnerabilities that support the injection of custom malware,
- The list of signatures used for detection of attacks is no longer current resulting in vulnerabilities that support the injection of custom malware,
- Unnecessary system services are configured to run on un-blocked or unnecessary open ports,
- Unnecessary access is permitted to system functions in the customer DR program,
- System assumes data inputs and resulting calculations are accurate in customer energy usage,
- System permits unauthorized changes to software in the customer DR system,
- Users lack visibility that unauthorized changes were made to the customer DR software.

Impact:

- Incorrect estimation of the total energy reduction before/during/after the DR event period, which can lead to the failure of the DR program,
- Potential power outages for the grid operator,
- The utility may have financial impacts - it computes customer incentives based on customer energy usage information,
- Loss of public confidence in the utility and DR program.



Reference: [7] National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.

Year 2 (1.2 and 1.3):

- Privacy
  - Potential privacy issues are identified within the system
  - Further analysis and research in protecting customer's privacy is needed.
- Cyber-Physical Device Compromise
  - The impacts of Cyber-Physical Device Compromise are analyzed and classified.
  - Further measurement of the impacts subject to the EV and demand respond network via pilot study.
- Vulnerability
  - Potential vulnerabilities are identified within the system
  - Refine quantifying the vulnerabilities for the risk assessment.
- Attack Surface
  - Attack Surface is identified within the system
  - Finalize the framework for cyber attack simulation to test the known attack vectors and uncover the other potential attack vectors.
- Risk
  - Risk assessment is conducted and the priority of the remediation efforts are identified as a rough preliminary evaluation.
  - Conduct a simulated cyber attack and evaluate the impact and cost scores based on the simulated attacker's report.

Simulation and Pilot Study in UCLA Microgrid (Year 2)

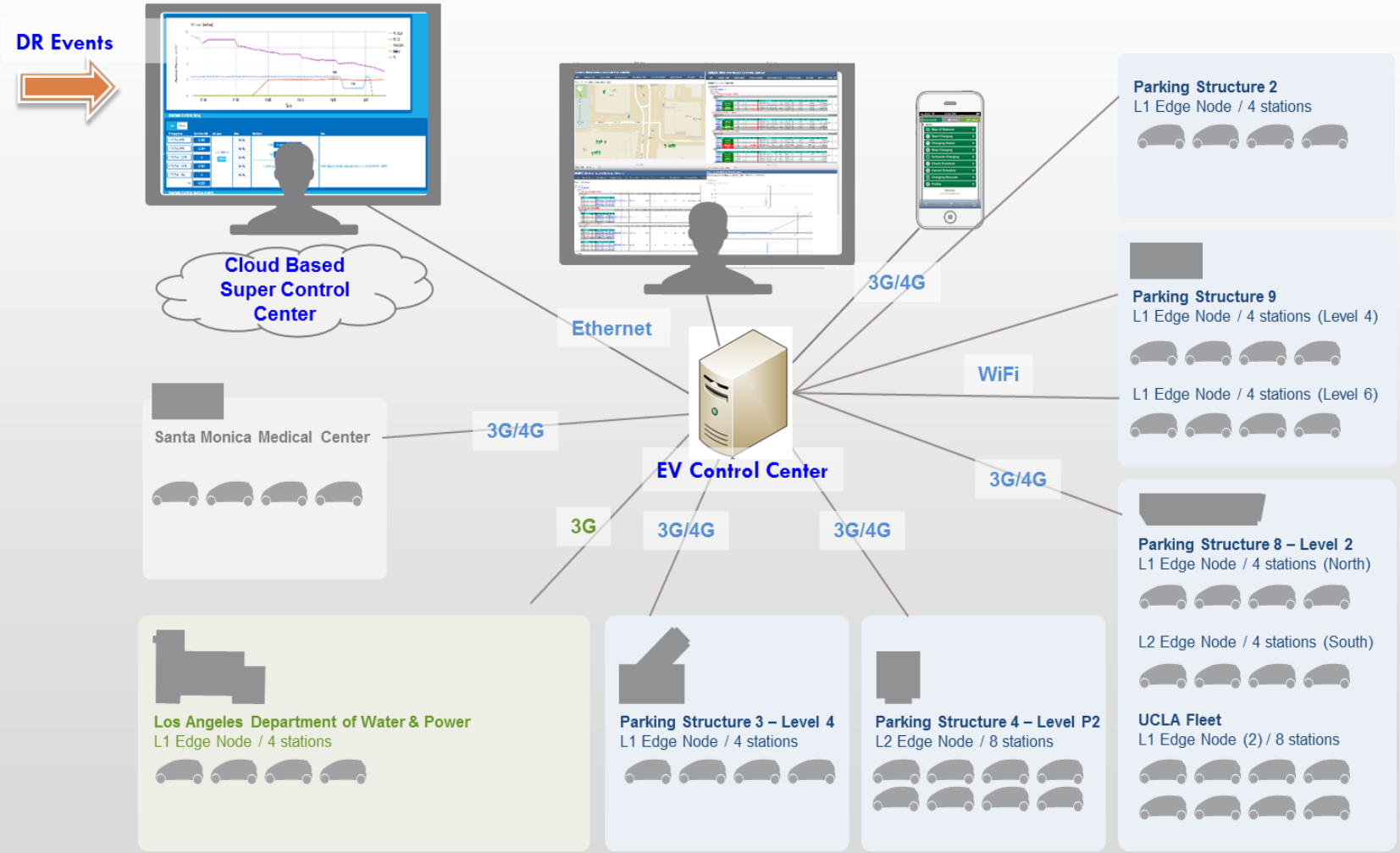
- Conduct a cyberattack simulation
  - Cyber-attack modeling and simulation for cyber-physical system [11] [12]
  - Investigate commercial products for cyber-attack simulation such as “Skybox security”- attack simulation or “Cymulate” –breach and attack simulation and vulnerability testing
- Setup a framework for cyber-attack pilot testing within UCLA WINSmartEV™ network (penetration testing, aka pen-testing).
  - Provide pen-testing tools for testers to test out the network on the real infrastructure, including the smart charging app.
    - Investigate pen-testing tools such as **Metasploit, Burpsuite or Sqlmap**[13]
  - Work with local distribution utilities, SCE and LADWP, that serve on SMERC advisory board to understand and measure the impact of the cyberattacks.
- Conduct research and come up with mitigation solution based on the pilot testing result to reduce attack surface.

Reference:

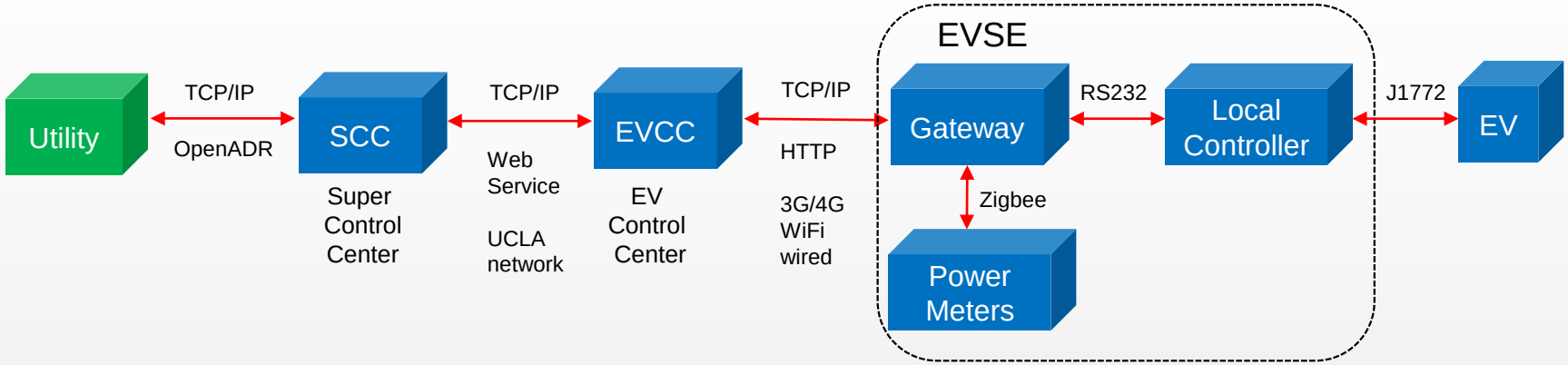
11. Sadi, M. A. H., Ali, M. H., Dasgupta, D., & Abercrombie, R. K. (2015, April). OPNET/simulink based testbed for disturbance detection in the smart grid. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (p. 17). ACM.
12. Potteiger, B., Emfinger, W., Neema, H., Koutosukos, X., Tang, C., & Stouffer, K. (2017, September). Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed. In Resilience Week (RWS), 2017(pp. 177-183). IEEE.
13. 37 Most Powerful Penetration Testing Tools (Security Testing Tools) [online] https://www.softwaretestinghelp.com/penetration-testing-tools/

Testbed - UCLA SMERC EV Charging Network Infrastructure

Super Control Center v.s. EV Control Center Infrastructure

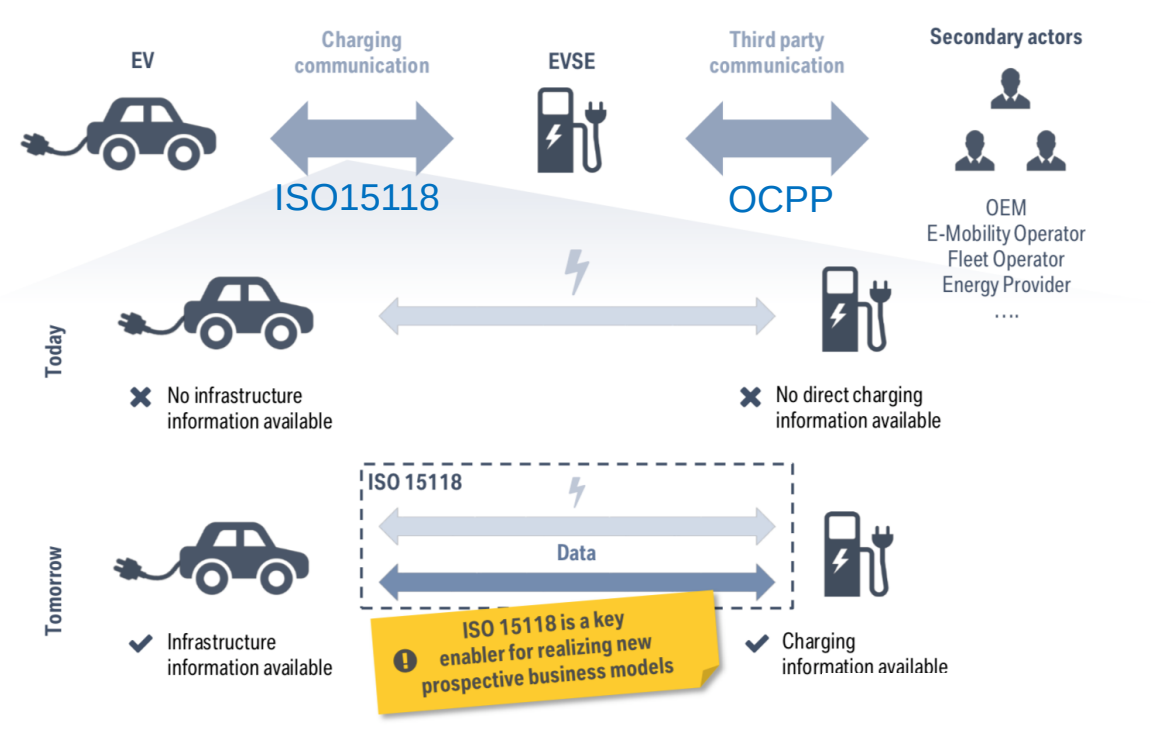


Protocols used in UCLA SMERC EV Charging Network Testbed



- Attacker Skillset Categorization
  - TCP/IP – OpenADR, Web service, HTTP, Zigbee – **CS** background
  - Controller - RS232, J1772 – **EE** background
- Risk Assessment
  - Present UCLA SMERC EV Charging network to CS and EE students in UCLA
  - Interviews and questionnaires will be used to collect impact and cost scores
- Attack Test Design
  - Implement attack simulation platform to issue attacks at various vulnerable layers at random or specific time and intervals

- EV charging protocols
  - ISO 15118 [21]
    - Communication between EVSE and EV
    - Standard that defines a vehicle to grid (V2G) communication interface for bi-directional charging/discharging of EVs.

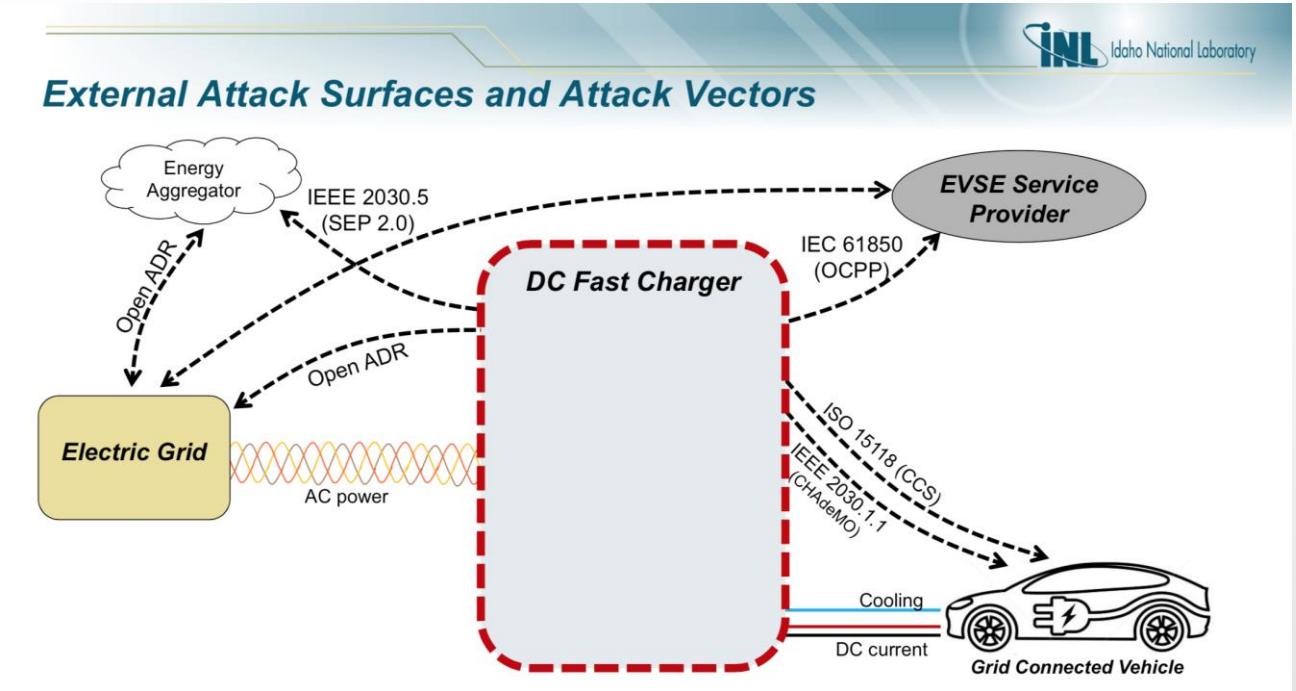


- Charging details (such as SOC)
- Payment / Billing
- AC/DC charging control
- Inductive charging control
- Reverse power flow (V2G)
- Optimized load management

Reference:

21. ISO15118 Standardization and Rollout [Online] https://assets.vector.com/cms/content/events/2017/EMOB17/Vector_EMOB_2017_Michael_Schwaiger.pdf

Year 2



[19]

Scenarios subject to DCFC charger and the ISO 15118 protocol

ET1. Custom Malware causes EV Overcharge and Explosion
ET2. Simultaneous Fast Charges cause Transformer Overload
ET3. Virus Propagated between EVs and EV Service Equipment (EVSE)
ET5. Compromised Protocol Translation Module Enables Control of EVs
ET10. High Priority EV Registration Identity Misused to Obtain Faster Charging
ET15. Malware Causes Discharge of EV to the Grid

Reference:
19. Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid [Online] https://avt.inl.gov/sites/default/files/pdf/presentations/INLCyberSecurityDCFC.pdf

Risk Assessment update (Year 2)

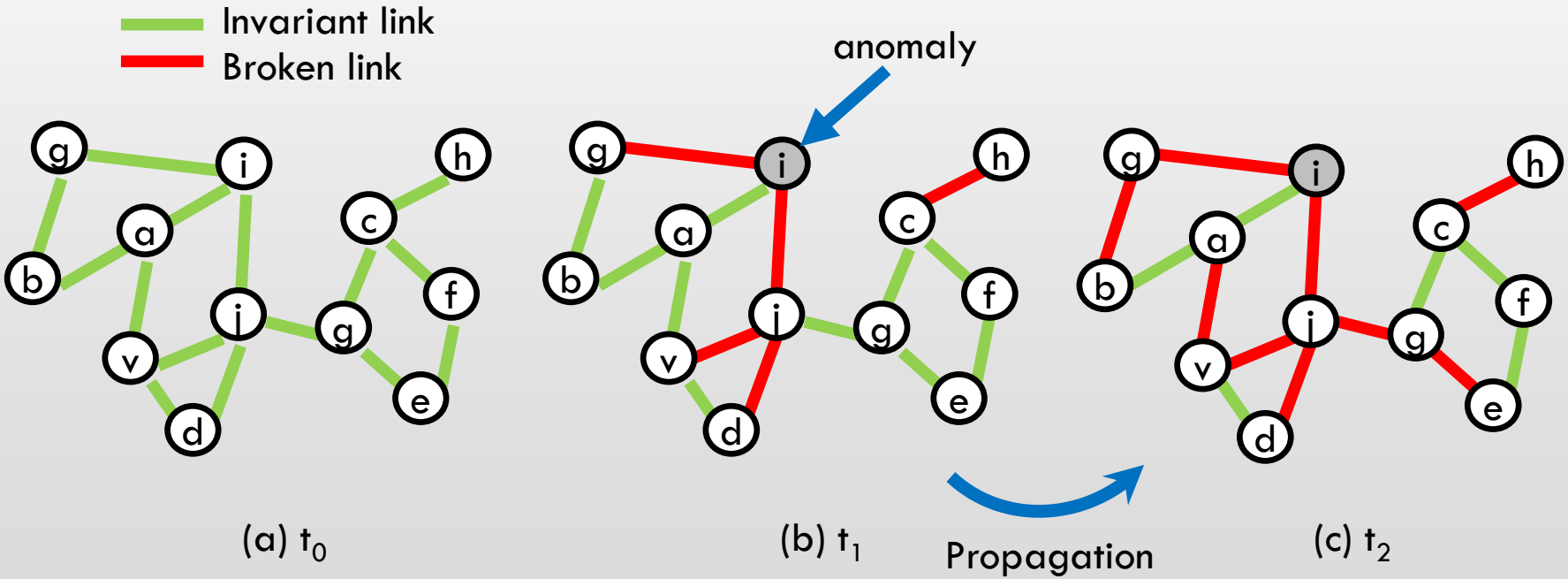
$$Risk = \frac{Impact\ of\ attack}{Cost\ of\ attack}$$

- Impact score:
  - In addition to the EVSE owner, have grid operator to evaluate the impact score, then average the scores
    - Assign a score of 0, 1, 3, or 9, to represent the impact of the failure scenario, as it ranges from minor to significant.
- Cost score (Cost to the attacker):
  - Conduct a survey to quantify the cost for the risk assessment then average the scores.
    - Assign a score of 0.1, 1, 3 or 9, to represent the cost and difficulty to the threat agent to carry out the failure scenario.
- Initially using the "average" for the scores, will do research on a composite score.

➔**Ranking the risk:** To highlight the areas of highest risk and prioritize remediation effort

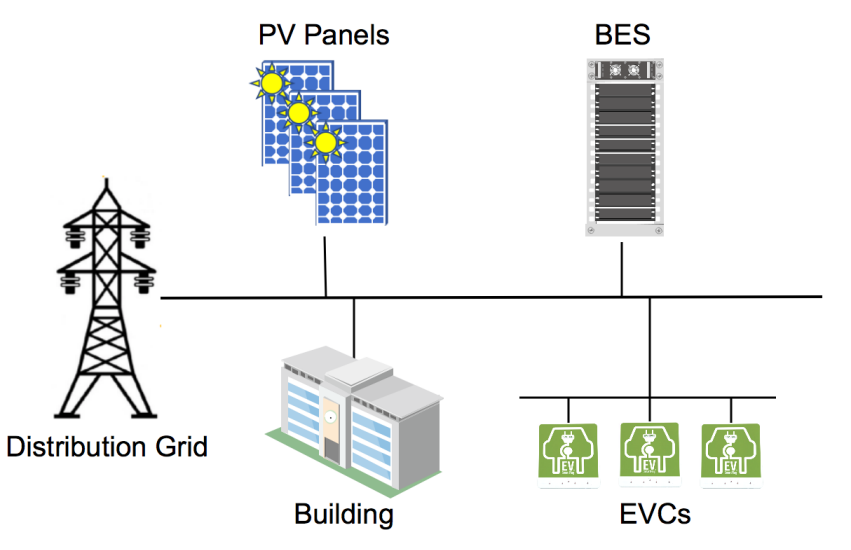
- Conference paper – accepted February 2019, IEEE ITEC 2019
  - **Title**: Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats
  - Based on the UCLA microgrid
    - EV charging system vulnerability analysis and the risk assessment
  - The impact of the potential cyber attacks
    - Case study of each electric transportation (ET) failure scenario

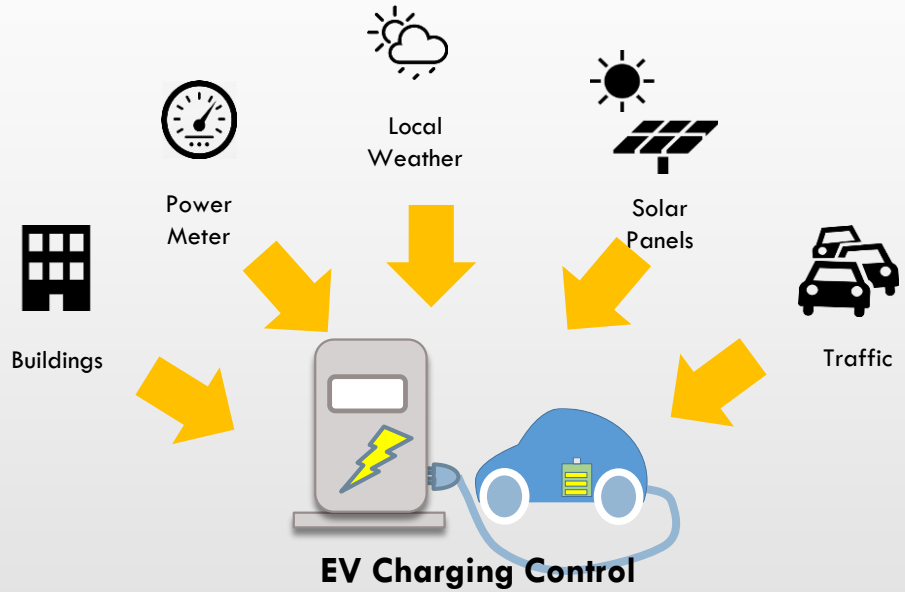
- **Physical-aware and Contextualized Attack Detection (2.2)**
  - Develop an Invariant network diffusion-based framework[22]
  - Identify significant causal anomalies
  - Model the fault propagation and rank the causal anomalies



Reference:
22. W. Cheng, K. Zhang, H. Chen, G. Jiang, Z. Chen and W. Wang, "Ranking Causal Anomalies via Temporal and Dynamical Analysis on Vanishing Correlations," ACM Transactions on Knowledge Discovery from Data (TKDD), p. 11(4): p. 40, 2017.

Invariant EV Charging Network





- Objectives for EV charging scheduling
  - Reduce cost
  - Reduce load variation
  - Optimal use of solar power
- Data Analytics
  - Inputs that effect the EV charging network
  - The correlation among multiple sources of geospatial time-series data

- DCFC Impact Simulation
  - High power – up to 350kW
  - Assuming a DCFC controller is compromised, what will be the impacts of unregulated DCFC to a microgrid?
  - Study the DCFC impact to the UCLA microgrid by RTDS simulation
  - Response of the DCFC: Full power to standby power, and the reverse
    - Power quality changes, including voltage variation, power factor, and current total harmonic distortion (THD)
    - Unwanted operation of the grid protection action – potentially disconnecting a feeder from the grid
    - Disturbance of the EV charging scheduling – increase the charging cost and lead to more variation in electricity load

Princeton Power V2G charger

RTDS

EV charging v.s. Solar generation [23]

Smart Charging Algorithm to Increase Local Use of Solar Energy

- Ranks users according to their overall use of solar
- Encourages user to utilize solar energy to charge EV.
- **Correlation: solar -> pricing/incentives -> kwh**
- **If correlation broken, then we know that attack has occurred.**

Adjusted solar ratio =
solar energy used to charge / energy used to charge a car adjusted to daily solar generation increased after algorithm utilized

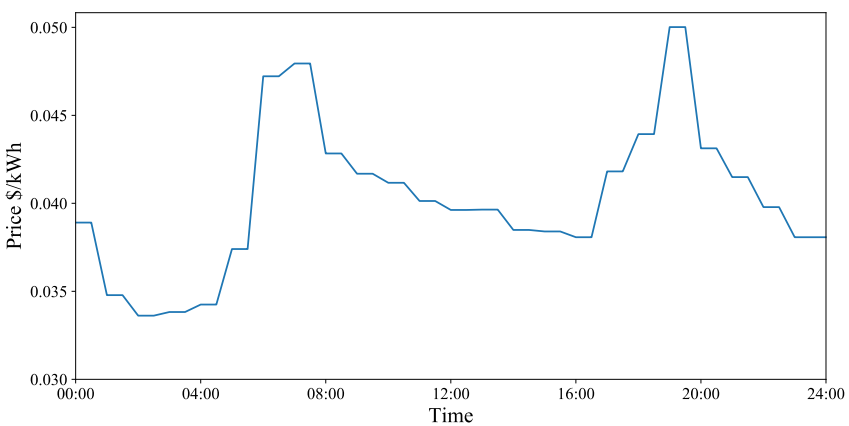
Solar usage ratio =
solar used locally to charge EV / total generated solar also increased

Funded by CEC

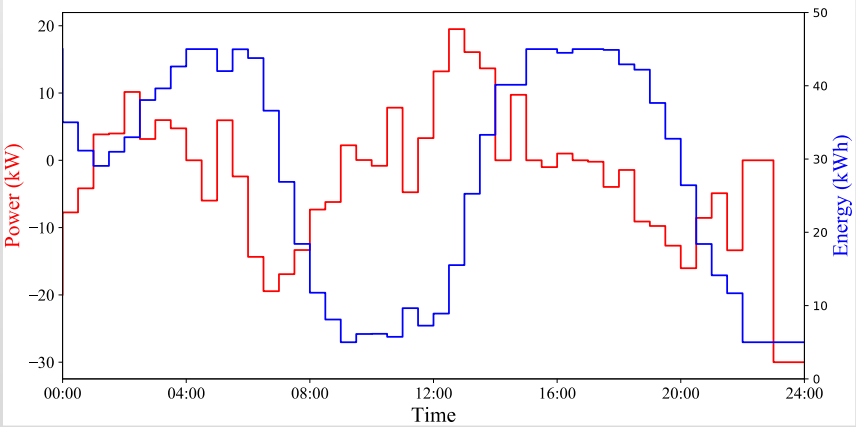
Reference:

23. T. Zhang, H. Pota, C. Chu and R. Gadh, "Real-Time Renewable Energy Incentive System For Electric Vehicles Using Prioritization and Cryptocurrency," Applied Energy, vol. 266, no. 15, pp. Pages 582-594, 2018.

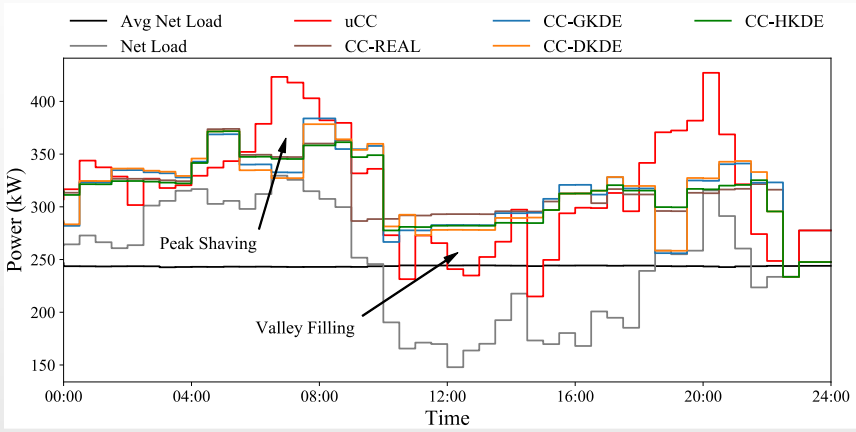
EV charging v.s. TOU price & load[24]



TOU price



Charging/ discharging of BESS according to TOU price



- **EV charging control to achieve peak shaving/ valley filling of total load**
- **If unusual peak that does not follow this pattern, then it may be a cyber attack**

uCC: uncontrolled charging (+Net Load)
Net Load: building netload
GKDE: Gaussian Kernel Density Estimator
DKDE: Kernel Density Estimator via Diffusion
HKDE: Hybrid Kernel Density Estimator

Reference:

24. Y. Chung, B. Khaki, C. Chu and R. Gadh, "Electric Vehicle User Behavior Prediction Using Hybrid Kernel Density Estimator", In 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), pp. 1-6. IEEE, 2018.

Steps to realize the attack detection system (3.2)

- **STEP1:** Modeling for Invariant network and vanishing correlation
  - Discover significant pairwise correlations among massive set of time series in addition to TOU price, total load and solar generation under smart EV charging control scheme.
  - Create an EV invariant charging network
  - Model the vanishing correlation (broken link)

- **STEP2:** Ranking causal anomalies
  - Simulate the propagation of a causal anomaly within a network
  - Analyze the impact of causal anomalies and rank them

- **STEP3:** System setup and implementation
  - Expand the current SMERC control and monitoring center with the attack detection function

  - Year 2: Testing of framework in field

Course Development and Revision

- Detailed plan for on-line three course certificate on Electric and Autonomous Controls being developed. Contains material pertaining to cybersecurity of EV infrastructure
- Addition of new cybersecurity material for ”Design and Analysis of Smart Grids C237 class”
- Year 2
  - Approval of on-line certificate and teaching for first time
  - Advertise to industry and utility partners.
  - Teach the on-line course

Software, Patents and I.P.

- Software:
  - WINSmartEV software environment being readied for vulnerability and risk assessment
  - Designed a series of questionnaires to conduct a survey, leveraging statistical sampling methods with people who have computer science background to evaluate risk of attacks on WINSmartEV
- Patent
  - Being investigated for research on invariant network

- Year 2
  - Software testing for above attack to be done in UCLA parking lot 9 installation.
  - Potential of work leading to patent will be explored in partnership with utility advisory board
  - Anticipated one patent filing in Year 2.

Training Career Development and Outreach

- Students and researchers getting trained on the research and infrastructure testbed
- Students working on publications (one paper published)
- Students showed demonstrations in P9 microgrid in UCLA to get feedback from industry and government
- Outreach via conference organized in 2018

- Year 2
  - Continue research and training
  - Train next set of student with expanded curriculum for Smart Grid class C237
  - Outreach via conference organized in Sacramento (Summer) and UCLA (Fall)

- **RCSec and SMERC Testing (Testbed, 3.1)**
  - Testbed being readied for cyber attack testing
  - Test plans developed
  - Attack related questions identified

  - Year 2
    - Testbed to be completed.
    - Students to be given instructions on carrying out attacks
    - Measurement and analysis of attack vector, risk and propagation.

Industry Board Formation, Recommendations and Dissemination to Policy Makers (3.2)

- Leverage SMERC advisory for this project. Following are advisory board members at SMERC that have been briefed about this project during a board meeting in UCLA.
  - Southern California Edison (SCE)
  - Los Angeles Department of Water and Power (LADWP)
  - UCLA SMERC held one conference for industry and policy makers on May 1, 2018 with theme of DER – EV, PV and Microgrid, at which a variety of topics were discussed pertaining to EVs including cyber security.
  - Industry/Government Round Table held in September 2018 in which SCE, LADWP and EV manufacturers were invited to discuss infrastructure issues – which pertain to stability and security. Companies attending include SCE (board member), LADWP (board member), eVelozcity (board member), Mercedes, Porsche, and several others.

- Year 2
  - Invite SMUD, SDGE, and PG&E to the industry board to get coverage of California.
  - Invite EV companies – BMW, Tesla, and others. To the industry board
  - Have a second on-side board meeting to present, show them the testbed and get feedback on the research, testbed and test plan
  - Provide recommendations on testbed to industry
  - UCLA is hosting an event in Sacramento in June 2019 to educate/inform policy makers on electric vehicles, smart grids, and cybersecurity will be one of the topics.
  - UCLA is hosting an event in March 2019 to bring EV industry and policy makers to campus.

References - 1

1. EPRI (2018). Grid Resiliency. [Online] https://www.epri.com/#/pages/sa/grid_resiliency?lang=en
2. Clark-Ginsberg, A. (2016). What's the Difference between Reliability and Resilience?. [online] https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_MAR_16/reliability%20and%20resilience%20pdf.pdf
3. Breach Level Index. [Online] https://breachlevelindex.com
4. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195-209.
5. Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys and Tutorials*, *19*(1), 446-464.
6. NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010
7. National Electric Sector Cybersecurity organization Resource (NESCOR), Technical Working Group 1 (2014). Electric Sector Failure Scenarios and Impact Analysis.
8. Rahim, R. (2017). Man-in-the-middle-attack prevention using interlock protocol method. *ARPN J. Eng. Appl. Sci*, *12*(22), 6483-6487.
9. Carter, C., Cordeiro, P. G., Onunkwo, I., & Johnson, J. T. (2018). *Cyber Assessment of Distributed Energy Resources*(No. SAND2018-0281C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
10. Bijral, R., Gupta, A., & Sharma, L. S. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. *International Journal of Advanced Research in Computer Science*, *8*(5).
11. Sadi, M. A. H., Ali, M. H., Dasgupta, D., & Abercrombie, R. K. (2015, April). OPNET/simulink based testbed for disturbance detection in the smart grid. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (p. 17). ACM.
12. Potteiger, B., Emfinger, W., Neema, H., Koutosukos, X., Tang, C., & Stouffer, K. (2017, September). Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed. In Resilience Week (RWS), 2017(pp. 177-183). IEEE.
13. 37 Most Powerful Penetration Testing Tools (Security Testing Tools) [online] https://www.softwaretestinghelp.com/penetration-testing-tools/
14. The Hacker News: "TSMC Chip Maker Blames WannaCry Malware for Production Halt". August 6, 2018.

References - 2

15. Lee, E. K., Gadh, R., & Gerla, M. (2012, November). Resource centric security to protect customer energy information in the smart grid. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on* (pp. 336-341).
16. Daily Burin: New Dining Services online feature optimizes meal-time efficiency. May 25, 2017
17. The privacy Point: Announcing CrowdZen. May 23, 2017.
18. C. Alcaraz, J. Lopez and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452-2459, Sept. 2017.
19. Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid [Online] https://avt.inl.gov/sites/default/files/pdf/presentations/INLCyberSecurityDCFC.pdf
20. Open Charge Alliance [online] **https://www.openchargealliance.org/about-us/appraisal-ocpp/**
21. ISO15118 Standardization and Rollout [Online] https://assets.vector.com/cms/content/events/2017/EMOB17/Vector_EMOB_2017_Michael_Schwaiger.pdf
22. W. Cheng, K. Zhang, H. Chen, G. Jiang, Z. Chen and W. Wang, "Ranking Causal Anomalies via Temporal and Dynamical Analysis on Vanishing Correlations," ACM Transactions on Knowledge Discovery from Data (TKDD), p. 11(4): p. 40, 2017.
23. T. Zhang, H. Pota, C. Chu and R. Gadh, "Real-Time Renewable Energy Incentive System For Electric Vehicles Using Prioritization and Cryptocurrency," Applied Energy, vol. 266, no. 15, pp. Pages 582-594, 2018.
24. Y. Chung, B. Khaki, C. Chu and R. Gadh, "Electric Vehicle User Behavior Prediction Using Hybrid Kernel Density Estimator", In 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), pp. 1-6. IEEE, 2018.