Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats

Devin Reeh[*], Francisco Cruz Tapia[†], Yu-Wei Chung[‡], Behnam Khaki[§], Chicheng Chu[¶], and Rajit Gadh[‖]
Smart Grid Energy Research Center (SMERC), University of California, Los Angeles
Los Angeles, CA, USA, 90095
Email: {[*]devinreeh, [†]focruztapia, [‡]ywchung, [§]behnamkhaki, [¶]peterchu, [‖]gadh}@ucla.edu

***Abstract*—The rapid pace of *Electrification* in the transportation sector, realized through plug-in electric vehicle (EV) integration, necessitates the smart charging infrastructures. These systems built on real-time data collection and decision making coordinate the charging demand to facilitate high penetration of PEVs in the power grids. Accordingly, the inherent cyber-physical characteristic of smart charging networks makes them susceptible to cyber-physical threats. Due to the lack of a consistent cyber-physical attack assessment in EV networks, this paper aims to propose the vulnerability analysis and risk assessment for the smart charging infrastructures. To this end, we define several potential failure scenarios for the WinSmartEV$^{\text{TM}}$ charging system on the UCLA campus and study the impacts of potential cyber-physical attacks. Moreover, we outline a codified methodology and taxonomy for assessing vulnerability and risk of cyber-physical attacks on the EV charging networks in order to create a generalizable and comprehensive solution. The outcome is a framework to prioritize the degree of the vulnerabilities and risks in the EV networks and to develop effective countermeasures.**

***Index Terms*—Cyber-physical threat, EV charging network, risk assessment, vulnerability analysis, WinSmartEV$^{\text{TM}}$.**

I. Introduction

In the energy sector, the transition from non-electric to electric consumers- *Electrification*- is the trend for improving the energy efficiency and having a sustainable infrastructure. *Electrification* can however, change the energy demand pattern significantly and affects power grid performance [1]. Therefore, electric power infrastructure is undergoing a transformation to accommodate the new consumers as well as increase electricity quality, reliability, and security. The goal is to turn the existing electric grid into a more advanced decentralized series of micro-grids equipped with digital communication infrastructure for grid monitoring, analysis, management, and control, also referred to as *smart grid*. Electric vehicles (EVs) are one of the most influential elements of that transition, which their charging infrastructure introduces new challenges regarding their accommodation in the power grids as well as their physical and cyber security. In this paper, we aim at analyzing the cyber-physical security of the EV charging infrastructures.

According to the National Institute of Standards and Technology (NIST) framework, seven domains are identified within the smart transportation and EV charging infrastructures for further research: (1) Markets, (2) Operations, (3) Service Provider, (4) Bulk Generation, (5) Transmission, (6) Distribution, and (7) Customer [2]. Here, we focus our study on the customer domain where the EV owners interact with the electric transportation (ET) cyber-physical system, which includes EV, EV supply equipment(EVSE), EV management server, and all of the communication among those devices.

Automotive manufacturers are expanding their electric vehicle (EV) offerings, and the car charging infrastructure is rapidly following. As of November of 2017, the total charging infrastructure for level II fast charging stations in the United States rose to fifty thousand [3]. As charging stations become smarter, they become more susceptible to cyber-physical attacks. Currently, a method for assessing the risk and impact of successful attacks against plug-in EV (PEV) charging networks does not exist. As a result, we aim to design a method by working through several case studies regarding potential mock cyber-physical attacks against the UCLA EV WinSmartEV$^{\text{TM}}$ charging platform.

To create the method outline for assessing the risk and impact, we will conduct a survey of attack feasibility and investigate the potential impact and risk of an individual carrying out such an attack. In the next sections, we will outline the UCLA charging network structure, conduct a vulnerability analysis of current systems, and provide a series of case study topics of cyber-physical attacks and the several corresponding ET impact failure scenarios.

II. EV Charging Netwrok

Charging networks are comprised of two primary components with varying levels of complexity. Many charging networks are connected to the primary power grid infrastructure. However, the existing power grid suffers from a tight coupling that exposes it to single points of failure for power distribution. Smart grids, localized power grids consisting of smart devices that can connect to a larger power grid or generate, store, and distribute electricity outside of the power grid, alleviate some of the single point of failures in the network as shown in Fig.1, UCLA EV WinSmart$^{\text{TM}}$.

The UCLA WinSmartEV$^{\text{TM}}$ Network is a smart grid EV charging network. It generates power through rooftop photovoltaic solar panels, stores the energy locally, and can send energy to electric vehicle charging terminals for drivers to

This work has been sponsored in part by grants from the award UCOP LFR-18-548175 - UC-Lab Center for Electricity Distribution Cybersecurity.

978-1-5386-9310-0/19/$31.00 ©2019 IEEE

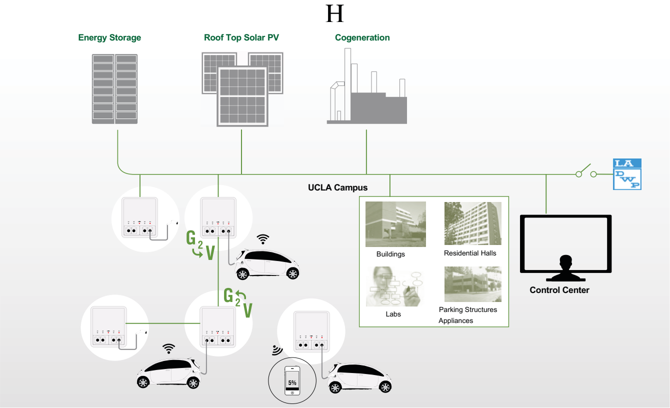

Fig. 1. UCLA EV WinSmart^{TM}

charge their electric vehicles. Localized EV charging terminals communicate information to make up a local charging network, and the drivers can access the them via the UCLA WinSmartEV^{TM} mobile application. The distributed charging network and mobile application client communicate through server, which also stores user records and electricity consumption in a database.

III. Potential Attacks and System Vulnerability

We define a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [2]. Since 2013, an estimated 14 billion data record records have been lost or stolen [4]. In the PEV network, cyber and physical vulnerabilities lie in the components as shown in Fig.2. Hackers have the advantage of choosing the time of attack and the vulnerability to exploit. In terms of cyber-physical compromise, both attacks and the impacts can be cyber or physical domain. Table I shows the causality of some common cyber-physical attacks [5].

TABLE I
The Impact of Cyber-Physical Device Compromise[5]

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

As shown in the Table.I, the impacts of the cyber-physical attacks can be categorized into 4 classes: Cyber-attack-Cyber-impact (CC); Cyber-attack-Physical-impact (CP); Physical-attack-Cyber-impact (PC); and Physical-attack-Physical-impact (PP). Understand the nature of the attacks would be helpful to come up with the solution for remedy and the corresponding protecting action.

This section will explore several typical attack vectors on the UCLA WinSmartEV^{TM} network components. It should be noted that while we cover five typical types of attacks we considered a multitude of others, and not all will be listed nor could all be sufficiently covered.

Following are the potential attacks:

A. Man-in-the-Middle Attack

The major risk of an attack comes from the router. The man-in-the-middle (MITM) attack refers to the attacker secretly replaying and possibly altering the communication between two parties by placing himself in the middle of communication [6, 7]. As in Fig.3, an attacker can intercept communication between the EV charging control center and drop, modify, or add data transmissions. This can lead to simultaneous fast charges that can cause a transformer overload.

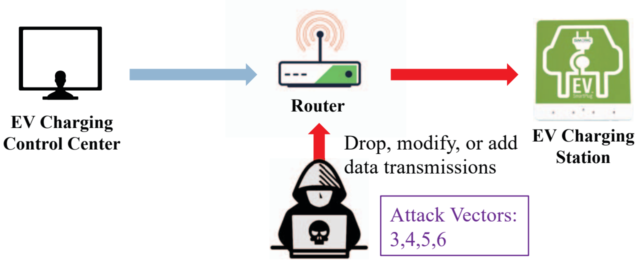

Fig. 3. Man-in-the-Middle Attack

B. 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 [7, 8]. In this scenario, the hacker can attack via the server and block an EV user from the charging station as shown in Fig.4. For example, unavailable communication blocks customer use of EV preferential rate. This can lead to a delay for high priority vehicles such as ambulance and firetruck. There is an advanced DoS called distributed DOS(DDoS), which can lead to a more severe outcome. 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.

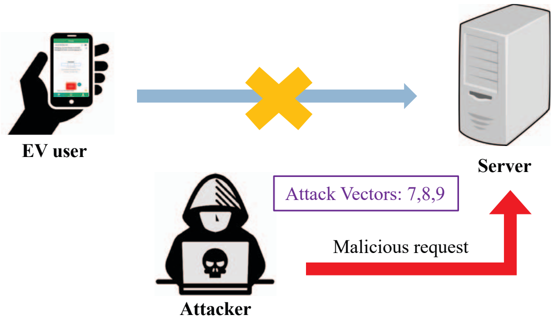

Fig. 4. Denial-of-Service Attack

C. Packet Replay Attack and Eavesdropping

As illustrated in Fig. 5, packet replay attack or eavesdropping occurs when an attacker intercepts a request from an EV user, captures and repeats or delays valid data transmissions, resulting in modified messages or spoofed on demand response automation system(DARS) communications channels, or collect private EV user information [7, 9, 10]. This can lead to EV registration ID theft to falsifying credentials to access preferential rate of high priority EV users.

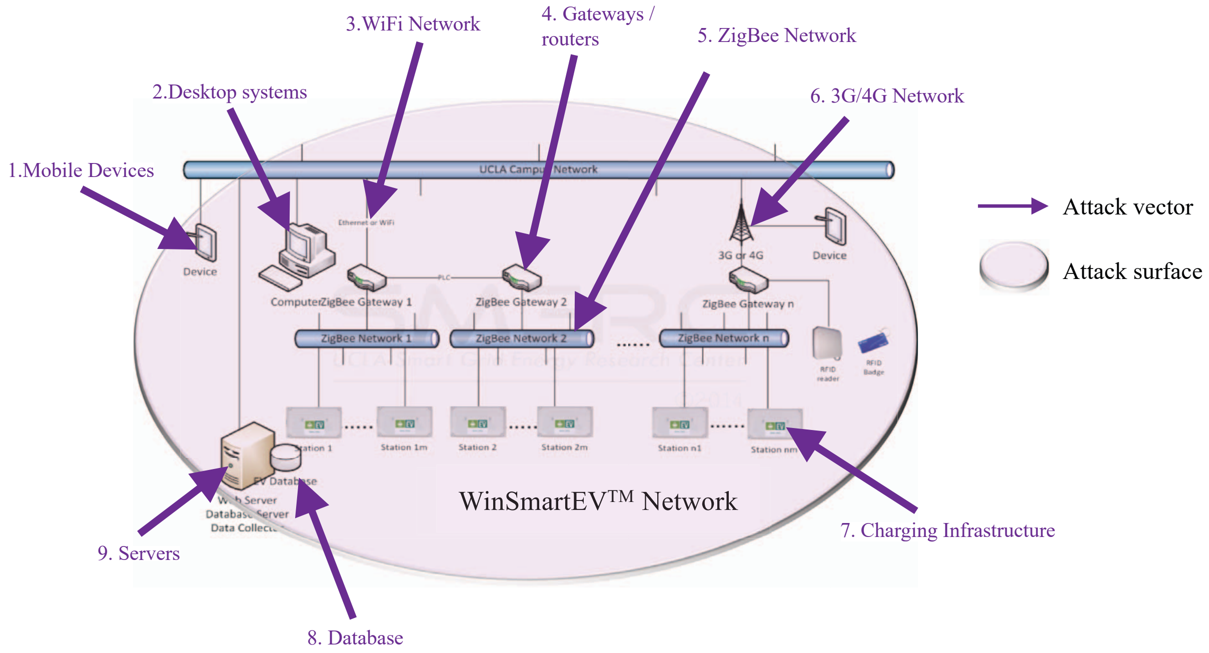

Fig. 2. Attack vectors and the attack surface of UCLA EV WinSmartEV$^{\text{TM}}$ network

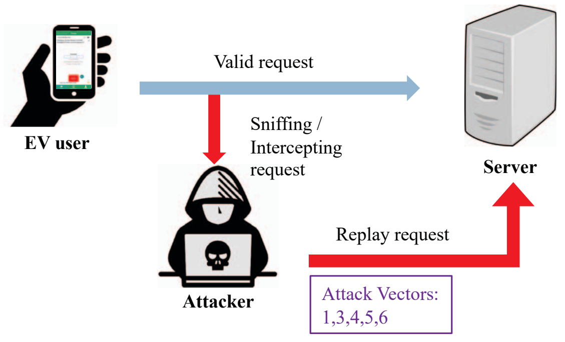

Fig. 5. Packet Replay Attack and Eavesdropping

D. Address Resolution Protocol 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 attackers 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]. The ARP spoofing is illustrated in Fig.6.

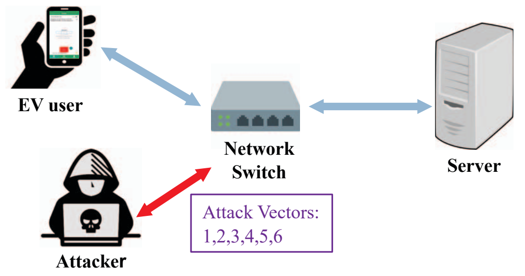

Fig. 6. ARP Spoofing

E. 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 as shown in Fig.7. An insider can be employees, contractors or an insider from outside [9].

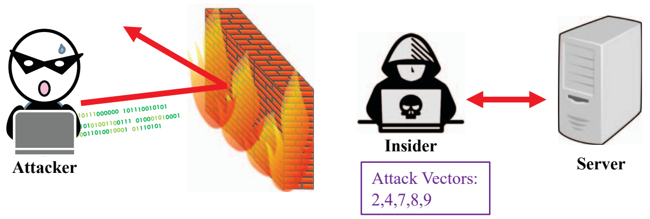

Fig. 7. Insider Attack

IV. Risk Assessment

When investigating the cyber-physical attacks on EV networks, we found that there exists two broad categories: (1) impact (2) cost. The impact is the impact and effects on likelihood and opportunity of a successful attack. The cost refers to the cost or resources necessary for the attacker to be successful [11]. To capture the relationship of impact and cost, we defined the risk as the ratio of impact to cost.

$$Risk = \frac{Impact}{Cost}. \tag{1}$$

The impact can be quantified as a 0, 1, 3, or 9 that represent the severity of a specific failure scenario, in which 0 is least significant and 9 most significant. Similarly, cost can take on the values 0.1, 1, 3, or 9. Higher values of risk indicate risker systems. The potential parameters for each variable were chosen to make calculating risk easier and understandable. The distance between the values also makes it easier for users to understand the different levels of risk, impact, and cost. These

TABLE II
ELECTRIC TRANSPORTATION (ET) FAILURE SCENARIOS I: IMPACT C: COST R: RATIO

Scenarios	Description	I	C	R	Ranking	Class
ET1	Custom Malware causes EV Overcharge and Explosion	3	3	1	Low	CP
ET2	Simultaneous Fast Charges cause Transformer Overload	9	9	1	Low	CP
ET3	Virus Propagated between EVs and EV Service Equipment (EVSE)	9	3	3	Low	CP
ET4	EV Charging Locations Disclosed via Utility Database	1	1	1	Low	CC
ET5	Compromised Protocol Translation Module Enables Control of EVs	3	3	1	Low	CP
ET6	EVSE Connects Wirelessly to Wrong Meter and Compromises Billing	3	3	1	Low	CC
ET7	Private Information Disclosed in Transit between EV and EVSE	3	3	1	Low	CC
ET8	Customer Misuses their EV Registration ID to Obtain Preferential Rate	0	0.1	0	Negligible	CC
ET9	EV Registration ID Stolen to Obtain Preferential Rate	0	0.1	0	Negligible	CC
ET10	High Priority EV Registration Identity Misused to Obtain Faster Charging	0	1	0	Negligible	CC
ET11	All EV Registration IDs Stolen from Utility	3	1	3	Low	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	High	CP
ET16	An EV is Exploited to Threaten Transformer or Substation	9	9	1	Low	CP
ET17	EVSE Meter Bypassing Result in Wrong Billing	3	1	3	Low	PC
ET18	EVSE Destruction Result in Unavailability of Charging Service	1	1	1	Low	PP

values are obtained by surveying individuals knowledgeable on cyber-physical system attacks. This formula highlights the areas of highest risk and provide a ranking system that prioritizes remediation effort.

This approach has been successfully used by a NESCOR member company in the past [11]. Using NESCOR as a reference, we quantified the impact of a failure scenario as an impact score, which can take on the value 0, 1, 3, or 9. The values represent increasing severity of impact. For example, impact scores could be:

- 0: one customer out of power for 15 minutes, petty cash expenses,
- 1: small generation plant offline,
- 3: 20% of customers experience defect from smart meter deployment,
- 9: large transformer destroyed and major city out of power for a week.

Additionally, we created a cost score that represents the cost and difficulty to the threat agent to carry out the failure scenario, which can take on values 0.1, 1, 3, or 9. For example cost scores could be:

- 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).

These scores are collected via a survey given to researchers familiar with the resources required to carry out such cyber-physical attacks. In both cases, the scores increase in severity as the number assigned increases. In cases, where scores are not the same values, we proposed using equation(1) to calculate risk, since the likelihood of the impact of cyber-physical attack and the means of carrying one our are directly proportional. In other words, as the potential impact of a cyber-physical attack increases the amount of resources necessary to carry one out also increases. Thus, a higher ratio means a higher level of urgency.

Case Study I: Low Risk

A possible vulnerability could exist in a protocol translation module where unauthorized changes can be made. A successful attempt to exploit this may enable unauthorized control of EVs. The resources to accomplish this would require expertise and planning, so the cost score would be a three. The impact scenario could be altering charging levels for a large number of vehicles within a short time period, which can have varied impacts ranging from inconveniencing customers. The impact value is also three because it primarily targets inconvenience to consumers but it can have an impact to multiple consumers at the same time. Since the impact and cost are both three the risk ration is one which is not high but is important to know to figure out if an attacker would target this vulnerability.

Case Study II: Low Risk

A possible vulnerability is the installation of malware in an EV. An attacker can propagate a virus between EVs and EV Service Equipment (EVSE). Malware could affect driving mechanisms that could result in serious injury or loss of life. The impact would be severe as it affects multiple EV drivers, so well assign an impact score of nine. The resources and cost to the attacker would require the installing a virus, so well assign it a cost score of 3. This scenario has risk ratio of three, and can be used to prioritize this issue above the previous.

Case Study III: High Risk

A possible scenario is malware causing discharge of the electric vehicle to the microgrid. Relevant vulerabilities in the system would be changes to code in the charging station management system and protocol translation module or design, implementation, or maintenance permits system to enter a hazardous state by overloading of the distribution transformer if many EVs are discharged. The impact of such an attack could be Critical damage to electric vehicles and associated costs, violation of customer contracts and loss of customer confidence, or even sudden discharges that damage a transformer. In this scenario, the impact could be assigned a 3 and the cost could be considered a 0.1 which results in a risk score of 30.

V. Result and Discussion

Table II shows the the impact scenarios that can occur as a result of different attack types on EV networks. Table III maps each scenario to the potential attacks.

TABLE III
Mapping of potential ET impact scenarios of listed attack types.

Attack Type	ET Failure Scenarios
Man in the Middle	ET2, ET5, ET6, ET15, ET16
Denial of Service	ET12, ET14
Packet Replay	ET14
Eavesdropping	ET4, ET7, ET9, ET10
ARP Spoofing	ET4, ET7, ET9, ET10, ET13
Insider	ET1, ET2, ET3, ET6, ET15, ET16

The goal of the scoring mechanism is to rank risk in order to highlight areas of highest risk and prioritize remediation effort and the mapping attacks is to identify the nature of the attacks, thereby helps to find the corresponding solution. It is noted that high ranking does not necessary to have the highest impact. For ET15, a malware may be injected by an angry worker form EV maintenance service or anyone who has access to the EV. An EV without malware detection can affect the EVSE when plug in. On the other hand, low ranking can also result in high impacts as ET2, ET3, and ET16. For those cases, the attackers require a higher level of computer skill to compromise the system and thus increase the cost of the attacks. The nature of the attack-impact causality is marked in the ”Class” column. Generally, preventing cyber attacks relies on stronger authentication process and avoiding cascading of physical impacts requires physical protection mechanism such as circuit breaker. Fault detection is important for both cyber and physical consequences. Physical attack, which is relatively rare, can be avoided by physically secure the access to the infrastructures. The strategy of mitigation for each scenario is summarized in Table IV.

VI. Conclusion

This paper presents a comprehensive cyber-physical system vulnerabilities analysis for ET domain. We analyze the UCLA WinSmartEV$^{\text{TM}}$ charging network and identify the potential attack vectors and its attack surface. Since cyber-security issue is an unfair advantage for hackers as they can choose the time and place of battle and attack only a single weak point of the system, understand the weakness and strengthen the protection scheme is vital of importance to secure the system. Therefore, we reviewed the potential attack types to the system weakness

TABLE IV
Mitigation action for each ET scenario

Scenarios	Mitigation Act
ET1	Overcharge-prevention hardware for EV battery[12]; A stronger authentication mechanism for modifying EV firmware [13].
ET2	A stronger authentication mechanism for configuring fast charging management system[13]; Fault-detection scheme for an unusual fast charging load[14]; Set an upper limit of EVs that can charge simultaneously; Deploy a circuit breaker to protect distribution transformer.
ET3	Anti-virus program in charging system to detect unauthorized software; Fault-detection scheme to detect abnormal events or functionality[14].
ET4	Enforcement of user password rule; Improve data encryption method[15]; A stronger authentication process to access the database[13].
ET5	Strengthen the integrity protections for translation modules;
ET6	A stronger authentication check between EVSE and the smart meter[16]; A stronger authentication process to pair smart meter and EVSE configuration[16].
ET7	Improve data communication encryption method between EV and EVSE [17].
ET8	Deploy a power usage monitoring program to recognize EV charging pattern and identify abnormal usage pattern[14]; A stronger authentication process to verify the EV identity[16].
ET9	Use multisignature method to authorize EV charging;[18].
ET10	Use multisignature method to authorize EV charging;[18].
ET11	A stronger authentication process to access the database[13]; Improve data encryption method[15]; Use multisignature method to authorize EV charging;[18]; Enable user to dispute the abnormal charging event and re-issue an EV ID.
ET12	Design resilient communication paths for EV identity verification.
ET13	Design resilient communication paths for EV identity verification; Use an alternative authentication method to verify EV identity.
ET14	Design resilient communication paths for EV identity verification; Use an alternative authentication method to verify EV identity.
ET15	A stronger authentication mechanism for configuring charging management system [19]; Require EV users' authorization for discharging; Deploy a circuit breaker to avoid over reverse power flow to the grid.
ET16	A stronger authentication mechanism for configuring charging management system[19]; Fault-detection scheme for an unusual charging load[14]; Set an upper limit of EV charging load; Deploy a circuit breaker to protect distribution transformer.
ET17	Secure the access to the EVSE.
ET18	Secure the access to the EVSE.

and discuss their impacts. Eighteen ET failure scenarios are presented and categorized based on the attack-impact causality. We also conduct a risk assessment to each scenarios and rank them in order to prioritize the remediation effort and allocate security resources accordingly.

References

[1] T. T. Mai, P. Jadun, J. S. Logan, C. A. McMillan, M. Muratori, D. C. Steinberg, L. J. Vimmerstedt, B. Haley, R. Jones, and B. Nelson, “Electrification futures study: Scenarios of electric technology adoption and power consumption for the united states,” National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2018.

[2] National Institute of Standards and Technology (NIST), “Guidelines for smart grid cyber security,” U. S. Department of Commerce, Technical Report, 2010.

[3] E. W. Wood, C. L. Rames, M. Muratori, S. Srinivasa Raghavan, and M. W. Melaina, “National plug-in electric vehicle infrastructure analysis,” National Renewable Energy Lab. (NREL), Golden, CO (United States), Technical Report, 2017. [Online]. Available: https://www.nrel.gov/docs/fy17osti/69031.pdf

[4] Breach Level Index, “Data breach statistics - data records lost or stolen since 2013,” https://breachlevelindex.com, accessed: 2019-04-20.

[5] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber-physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[6] R. Rahim, “Man-in-the-middle-attack prevention using interlock protocol method,” *ARPN J. Eng. Appl. Sci*, vol. 12, no. 22, pp. 6483–6487, 2017.

[7] C. Carter, P. G. Cordeiro, I. Onunkwo, and J. T. Johnson, “Cyber assessment of distributed energy resources.” Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2018.

[8] J. Qin, M. Li, L. Shi, and X. Yu, “Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks,” *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2018.

[9] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, “A survey on smart grid cyber-physical system testbeds,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2017.

[10] R. Bijral, A. Gupta, and L. S. Sharma, “Study of vulnerabilities of arp spoofing and its detection using snort,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[11] A. Lee, “National electric sector cybersecurity organization resource (NESCOR),” Electric Power Research Institute (EPRI), Incorporated, Technical Report, 2014.

[12] H. K. Lim, J. H. Seo, S. H. Kim, Y. C. Jeon, J. S. Choi, and E. K. Kim, “Overcharge prevention device of battery,” Sep. 29 2015, uS Patent 9,147,872.

[13] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

[14] F. Harrou, Y. Sun, B. Taghezouit, A. Saidi, and M.-E. Hamlati, “Reliable fault detection and diagnosis of photovoltaic systems based on statistical monitoring approaches,” *Renewable energy*, vol. 116, pp. 22–37, 2018.

[15] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, “A new payment system for enhancing location privacy of electric vehicles,” *IEEE transactions on vehicular technology*, vol. 63, no. 1, pp. 3–18, 2014.

[16] L. Mazur, J. Xie, S. D. Daniel, and C. J. Saretto, “Authenticating using cloud authentication,” Nov. 12 2013, uS Patent 8,584,221.

[17] Z. Yang, S. Yu, W. Lou, and C. Liu, “$\hat{p}\{2\}$: Privacy-preserving communication and precise reward architecture for v2g networks in smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[18] A. Boldyreva, “Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme,” in *International Workshop on Public Key Cryptography*. Springer, 2003, pp. 31–46.

[19] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, “Role-dependent privacy preservation for secure v2g networks in the smart grid,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, 2014.