

I Grid and Charging Infrastructure

I.1 Cyber Security

I.1.1 Securing Vehicle Charging Infrastructure

Jay Johnson, Principal Investigator

Sandia National Laboratories
P.O. Box 5800 MS1033
Albuquerque, NM 87185-1033
E-mail: jjohns2@sandia.gov

Lee Slezak, DOE Program Manager

U.S. Department of Energy
E-mail: Lee.Slezak@ee.doe.gov

Start Date October 1, 2018:

Project Funding (FY19): \$1,000,000

End Date: September 30, 2021

DOE share: \$1,000,000

Non-DOE share: \$0

Project Introduction

As the US electrifies the transportation sector, cyber attacks targeting vehicle charging could bring consequences to electrical system infrastructure. This is a growing area of concern as charging stations increase power delivery and must communicate to a range of entities to authorize charging, sequence the charging process, and manage load (grid operators, vehicles, OEM vendors, charging network operators, etc.). The research challenges are numerous and are complicated because there are many end users, stakeholders, and software and equipment vendors interests involved. Poorly implemented electric vehicle supply equipment (EVSE), electric vehicle (EV), or grid communication system cybersecurity could be a significant risk to EV adoption because the political, social, and financial impact of cyberattacks—or public perception of such—ripples across the industry and has lasting and devastating effects. Unfortunately, there is no comprehensive EVSE cybersecurity approach and limited best practices have been adopted by the EV/EVSE industry. There is an incomplete industry understanding of the attack surface, interconnected assets, and unsecured interfaces. Thus, comprehensive cybersecurity recommendations founded on sound research are necessary to secure EV charging infrastructure. This project is providing the power, security, and automotive industry with a strong technical basis for securing this infrastructure by developing threat models, determining technology gaps, and identifying or developing effective countermeasures. Specifically, the team is creating a cybersecurity threat model and performing a technical risk assessment of EVSE assets, so that automotive, charging, and utility stakeholders can better protect customers, vehicles, and power systems in the face of new cyber threats.

Objectives

The goal of this project is to protect US critical infrastructure and improve energy security through technical analysis of the risk landscape presented by the anticipated massive deployment of interoperable EV chargers. To improve the vehicle industry's cybersecurity posture, this project is:

- conducting adversary-based assessments of charging equipment,
- creating a threat model of EV charging, and
- analyzing power system impact for different attack scenarios.

This will provide DOE and automotive, EVSE vendors, and utility stakeholders with:

- clear documentation of gaps in EVSE cybersecurity and the path forward to address those weaknesses,
- a threat model for EVSEs and associated infrastructure and services,
- recommendations for the automotive industry based on EVSE penetration testing, and
- cyber attack impact analyses of the power system with remediation recommendations.

Approach

The team is executing on the following integrated cybersecurity R&D tasks:

1. Conduct threat modelling to understand what potential cyber hazards exist with EVSE communications;
2. Assess the current state-of-the-art cybersecurity posture of EVSE equipment using authorized, adversary-based assessment techniques (penetration testing and red teaming);
3. Establish credible attack vectors based on the cybersecurity assessments and threat model;
4. Determine the impact of current and potential vulnerabilities on distribution and transmission power systems; and
5. Create a risk matrix to prioritize mitigations that reduce the number of high-consequence/low-threat level attacks.

The task structure of this project is shown in Figure I.1.1.1, wherein the left side (blue) estimates the probability of different attack scenarios and the right side (green) estimates the consequence of attack scenarios. The cybersecurity risk of a particular attack is the combination of the likelihood and impact of the attack. By studying a range of attack scenarios, optimal mitigations can be determined to prevent attacks at specific points in the attack kill chain (i.e., the steps to accomplish adversary goals).

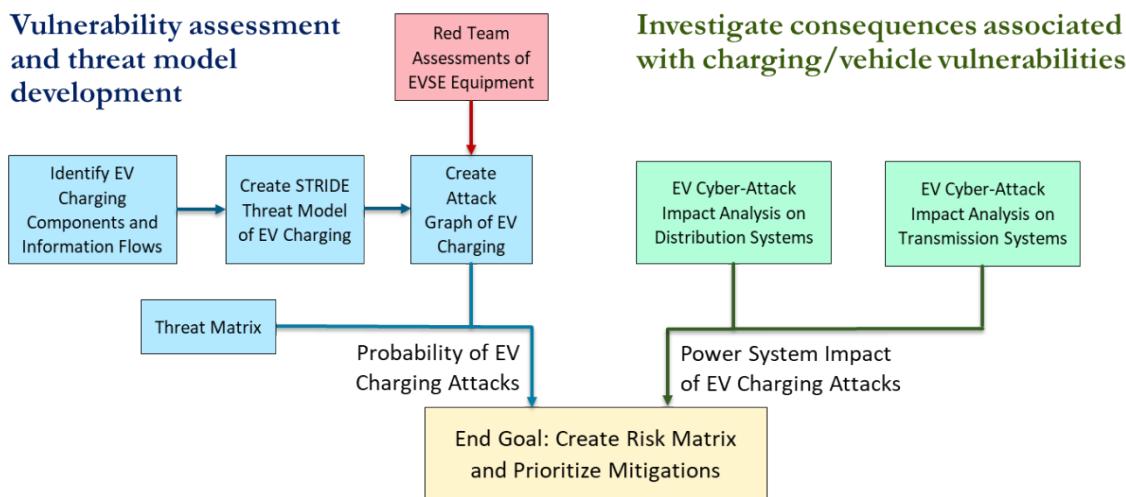


Figure I.1.1.1 Project tasking.

Results

The project team has evaluated probable attacks based on hands-on cybersecurity assessments with partner organizations and evaluated the probability of success against the skill level required to conduct the attack. A detailed threat model was created for different EVSE chargers with connections to external entities. Attack graphs were developed and then revised based on penetration testing of multiple EVSEs. A distribution simulation of EVSE charging with and without vehicle-to-grid (V2G) functionality was conducted to determine if malicious control of EVSEs could cause high or low voltages on feeder circuits. Transmission simulations of coordinated charging control was modeled for the Western Electricity Coordinating Council (WECC) were also performed to understand bulk system impact from coordinated cyber attacks.

EVSE Penetration Testing

Since year one, the team has worked closely with multiple EVSE vendors to better understand the vulnerabilities presented by EVSE equipment and associated networks. The project's second year focused on further understanding vulnerabilities that affect supporting IT systems. This included assessing remote access controls, use of insecure protocols, and the ability to fingerprint devices from their online presence. This involved working with the threat models and attack graphs from year one and validating some of the approaches. Findings from network traffic analysis, forensic analysis, and open source information gathering have led to vulnerability enumeration in both the EVSE as well as their supporting infrastructure. Use of insecure protocols, such as OCPP 1.6 and MQTT, on the globally routable Internet have resulted in several

findings that were disseminated back to EVSE manufacturers for remediation. Additionally, the team was able to use their findings to create a generalized "fingerprint" for EVSE deployments, allowing the team to search for and enumerate similar systems that were Internet connected. From these similar systems, specific characteristics such as open ports, software versions, or reports of vulnerabilities were used to identify other instances of EVSE deployments. The hands-on assessments for EVSE equipment found many areas for improvement, e.g., failure to physically secure EVSE enclosures; default passwords for internal systems, or credentials posted inside enclosure; data not encrypted at rest and only financial data is encrypted in transit; unnecessary ports and services are enabled. A list of best practices was generated from these assessments [1], shown in Figure I.1.1.2. In the final year of the project, an anonymized set of findings will be published. The assessment team also provided EVSE partners with the findings and potential mitigations for identified vulnerabilities. Some recommendations are included in Figure I.1.1.3.



Figure I.1.1.2 EVSE Best Practices [1].

Attack Graphs

Attack graphs show the steps an attacker must take to move from a system/network access point to a consequence or objective. The use of attack graphs simplifies the identification of key steps an attacker must take to achieve their objectives, allowing those actions to be detected or prevented. Figure I.1.1.4 illustrates access points, staging areas, and consequences of concern related to a generic EV charger network. In this figure, one of the attack paths involves an attacker using an initial compromise of an EVSE provider's business network to impact the bulk power system. By analyzing the steps in this attack path, detective or preventive controls – such as monitoring for unusual Network Time Protocol traffic or requiring code signing of EVSE updates – can be implemented. The team used the information gathered from their assessments, publicly available information regarding vulnerabilities, and knowledge regarding the tactics, techniques, and procedures used by attackers to advise the attack graph. In the case of coordinated EVSE attacks that disrupt the power system, there were two major questions:

- Can the attacker "pivot" between the components, systems, and networks in the EV/EVSE ecosystem to compromise the necessary information flows?
- Can an attacker synchronize their attack to affect large portions of the grid simultaneously?

From the assessment activities, it appears both are possible so an attacker *could* manipulate large networks of EVSEs and cause distribution and transmission impacts.



Figure I.1.1.3 EVSE vendor recommendations based on penetration tests of EVSE equipment and networks [1].

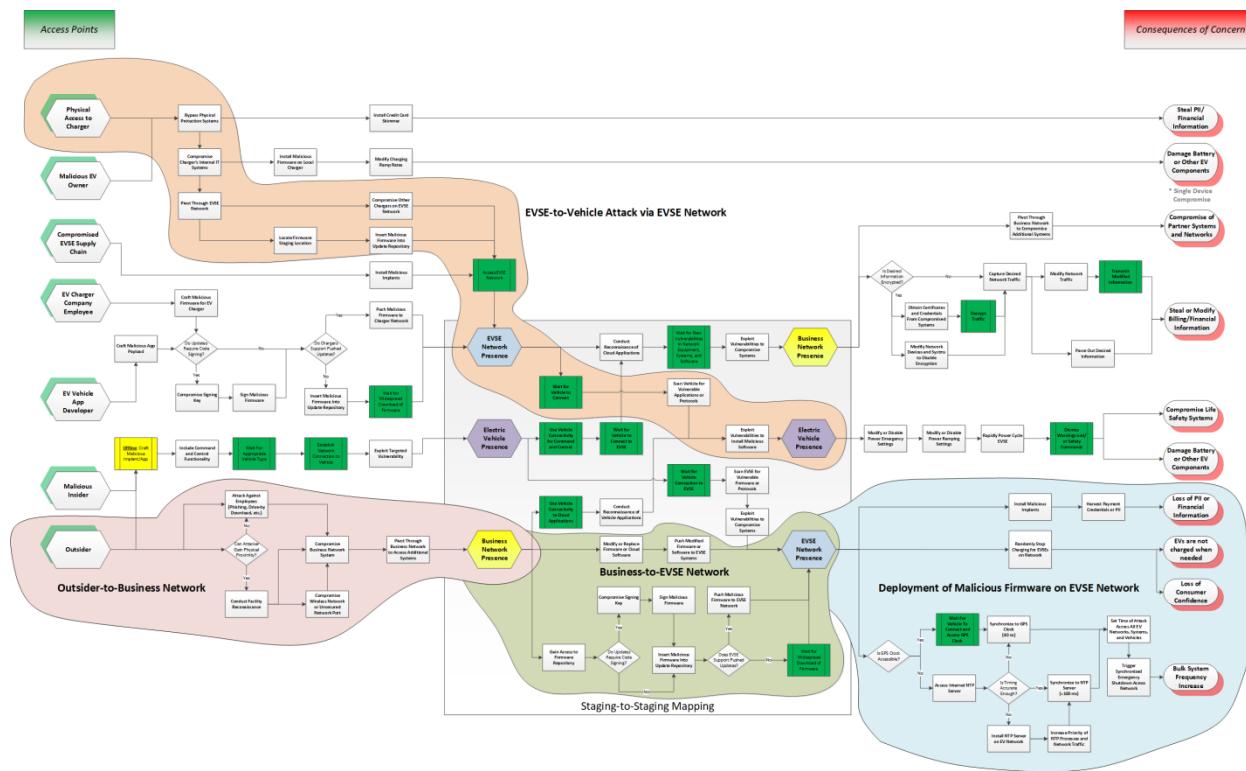


Figure I.1.1.4 Complete graph. Details presented in [2].

Threat Model Development

PNNL led the task to develop a threat model of high-power electric vehicle charging infrastructure and systematically analyze it for threats that have the potential to bring wide-ranging consequences to the electric grid and transportation systems. PNNL derived a novel consequence-centric variant of the STRIDE threat modeling methodology to: (i) discover consequences that potentially impact vehicles, the electric supply, and

transportation; and (ii) focus subsequent modeling and analysis on threats that may precipitate the consequence. STRIDE is an industry-accepted approach to threat modeling, first made popular for its application at Microsoft. Examples of the system models used for the threat modeling are depicted in Figure I.1.1.5, which show decomposition of chargers and vehicle into components, how data flows between components, and the relationships of components to external entities. After the threats are enumerated, safeguards and countermeasures are identified to mitigate the vulnerabilities. By focusing on consequences, insights into the security and resiliency of the EV charging ecosystem is gained. Importantly, the threat model analysis suggests that no single entity (for example, charging station vendor or charging network operator) is ideally situated to secure the ecosystem, but instead, requires the concerted effort of the ecosystem. The threat model, analysis, and results are detailed in [3].

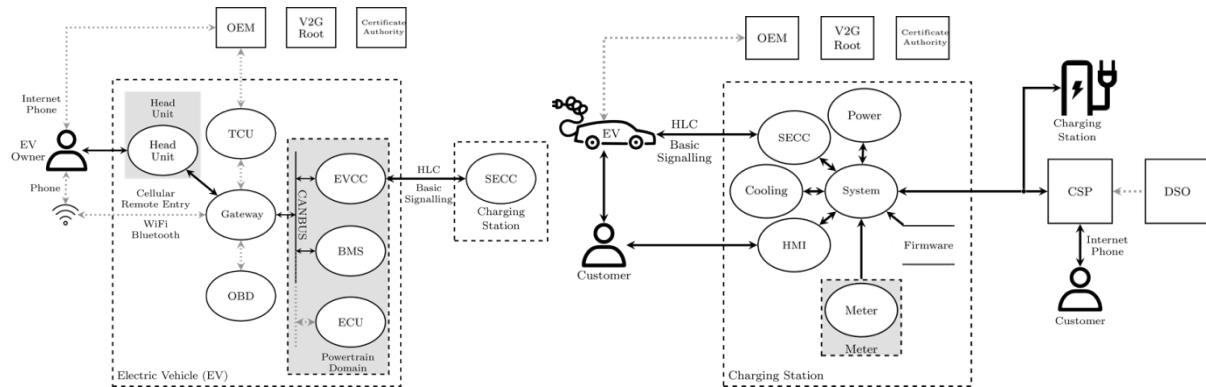


Figure I.1.1.5 The vehicle system model (left) depicts the components of the vehicle and their relationship to the charger. The charger system model (right) illustrates the relationship of the components and information flows.

Transmission System Consequence Analysis Simulations

PNNL's Consequence Analysis results indicate that for the specific events studied in this work, the impact on the WECC system is minimal. Two different types of studies were simulated: a large discrete WECC-wide EV load drop across the region intended to raise frequency, and several smaller EV load modulation events intended to excite system inter-area oscillations along the California Oregon Intertie (COI). Figure I.1.1.6 illustrates this procedure. Here the green and blue dots indicate a distributed load to modulate on either side of the COI. The graph above the map shows that the loads are 180 degrees out of phase. Conceptually, if loads in the north are high and loads in the south are low, this will create a flow north along the COI. Similarly, when loads are low in the north and high in the south, this will tend to generate flows south along the COI. No significant adverse effects were observed in either set of simulations, however, COI flows of up to 3 times the oscillating load size were observed in the load modulation studies. Inter-area oscillations are of concern in that they put the grid in elevated state of risk during system events as well as making it difficult to achieve ideal transfer capacities and optimal power flows. Further details are presented in [4-7].

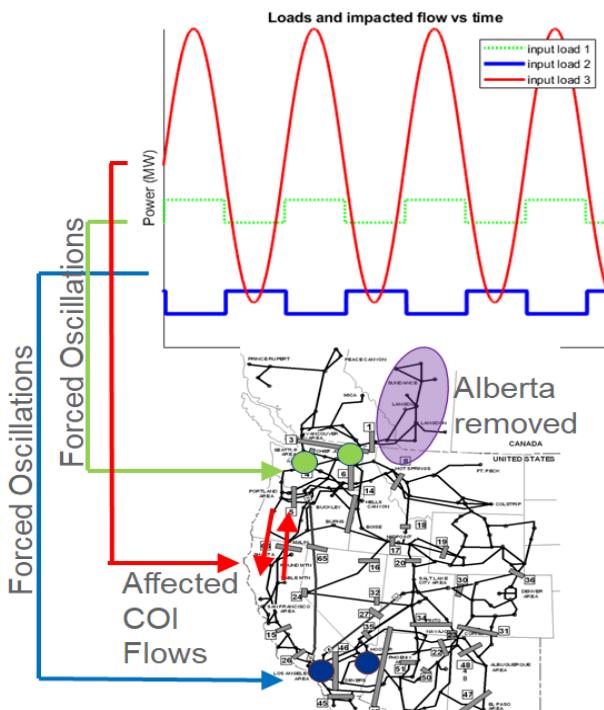


Figure I.1.1.6 Load oscillation simulation

Conclusions

This project is helping identify potential EV charger vulnerabilities and quantify the risk to critical infrastructure when vehicle chargers are maliciously controlled. This risk assessment is only an initial step in a continuous process of hardening charging infrastructure against cyber-attacks. There is much more work to secure charging infrastructure from cyber attacks, including:

- Developing standardized policies for managing chargers and other assets in the charging ecosystem.
- Designing effective perimeter defenses to protect the assets including firewalls, access control mechanisms, data-in-flight requirements (encryption, authentication), etc.
- Creating situational awareness systems and intrusion detection/prevention systems in an ecosystem of diverse communication networks and systems.
- Researching response mechanisms to prevent further adversary actions on the system, nonrepudiation technologies, and dynamic responses.
- Creating hardware- and software-based fallback and contingency operating modes.

Key Publications

- [1] J. Johnson, B. Anderson, B. Wright, J. Daley, R. Varriale, "Recommended Cybersecurity Practices for EV Charging Systems," Sandia National Laboratories, SAND2020-11401 D, doi.org/10.13140/RG.2.2.11141.37602.
- [2] B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020.
- [3] T.E. Carroll, G.B. Dindlebeck, R.M. Pratt, L.R. O'Neil, "A Threat Model of High-Power Electric Vehicle Charging Infrastructure," Journal of Information Warfare (forthcoming).
- [4] J. G. O'Brien, P. R. Maloney, U. Argrawal, T. E. Carroll, and R. M. Pratt, "Electric Vehicle Infrastructure Consequence Assessment," Pacific Northwest National Laboratory, Technical Report PNNL-29121, 2019.
- [5] Pratt R.M., T.E. Carroll, G.B. Dindlebeck, P.R. Maloney, and J.G. O'Brien. 06/02/2020. "Cybersecurity: Securing Vehicle Charging Infrastructure - Consequence Analysis and Threat Assessment.", United States. PNNL-SA-152801.
- [6] J.G. O'Brien, P.R. Maloney, U. Agrawal, T.E. Carroll, R.M. Pratt, "Electric vehicle infrastructure consequence assessment," Pacific Northwest National Laboratory Technical Report PNNL-29514, 2019.
- [7] Pratt R.M., T.E. Carroll, J.G. O'Brien, P.R. Maloney, L. O'Neil, and U. Agrawal. 2019. PNNL Cyber VTO Annual Progress Report. PNNL-29374. Richland, WA: Pacific Northwest National Laboratory.

References

N/A

Acknowledgements

DOE and the PI wish to thank the multi-laboratory team for this work: SNL (Ben Anderson, Brian Wright, , Josh Daley, Jimmy Quiroz), PNNL (Rick Pratt, Tom Carroll, Lori Ross O'Neil, Brian Dindlebeck, Patrick Maloney, James O'Brien) and ANL (Roland Varriale, Ted Bohn, and Keith Hardy).

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.