I Grid and Charging Infrastructure

I.1 Cyber-Physical 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

Thomas E. Carroll, Principal Investigator

Pacific Northwest National Laboratory
PO Box 999 MS-IN J4-45
Richland, WA 99352
E-mail: Thomas.Carroll@pnnl.gov

Roland Varriale, Principal Investigator

Argonne National Laboratory
9700 South Cass Ave
Lemont, IL 60439
E-mail: rvarriale@anl.gov

Lee Slezak, DOE Program Manager

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

Start Date October 1, 2018: End Date: September 30, 2021
Project Funding (FY22): $1,000,000 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 provided 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 created a cybersecurity threat

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.

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 the project was 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:

- conducted adversary-based assessments of charging equipment,
- created a threat model of EV charging, and
- analyzed power system impacts for different attack scenarios.

This provided 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 executed the following integrated cybersecurity R&D tasks:

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

The task structure of the 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).

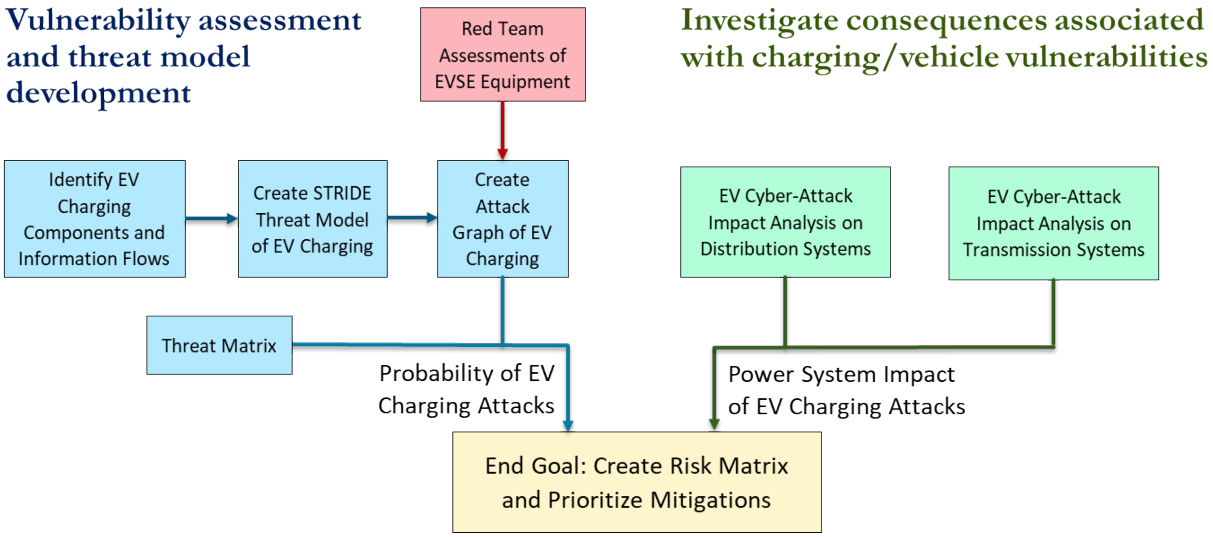

Vulnerability assessment and threat model development
Red Team Assessments of EVSE Equipment
Investigate consequences associated with charging/vehicle vulnerabilities
Identify EV Charging Components and Information Flows
Create STRIDE Threat Model of EV Charging
Create Attack Graph of EV Charging
EV Cyber-Attack Impact Analysis on Distribution Systems
EV Cyber-Attack Impact Analysis on Transmission Systems
Threat Matrix
Probability of EV Charging Attacks
Power System Impact of EV Charging Attacks
End Goal: Create Risk Matrix and Prioritize Mitigations

Figure I.1.1.1 Project tasking.

Results

The project team 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

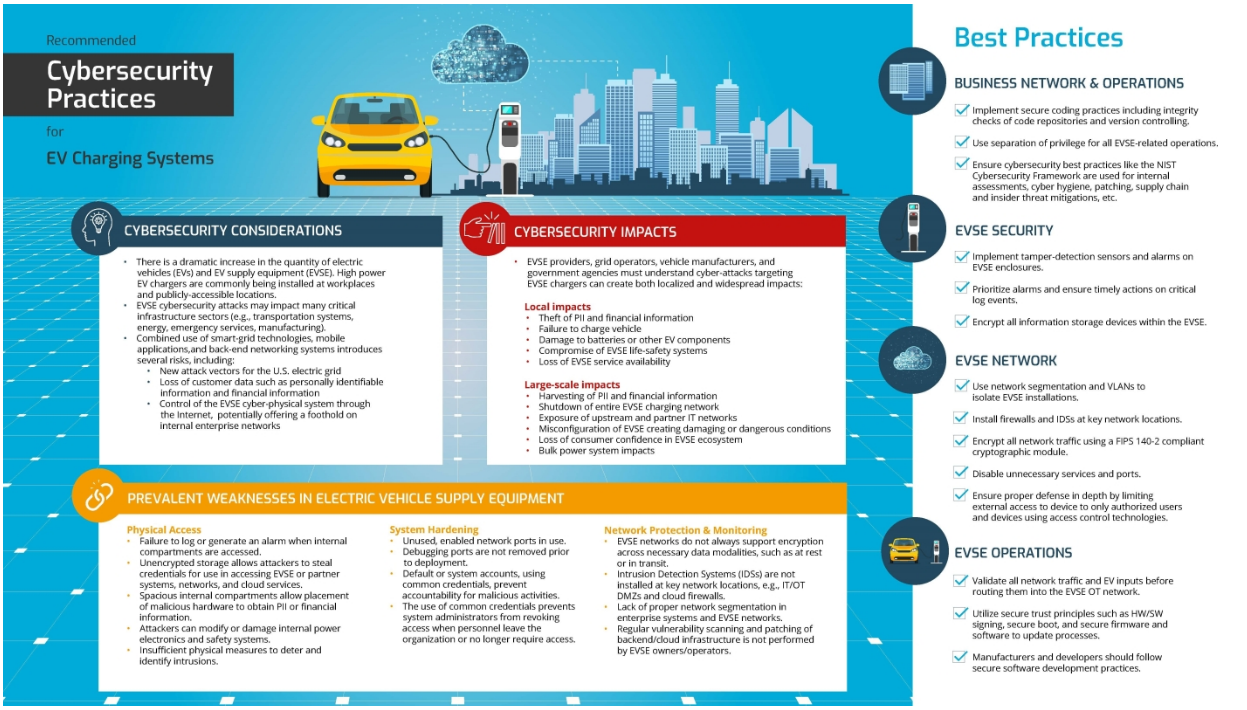
From the beginning of the project, the team worked closely with multiple EVSE vendors to better understand the vulnerabilities presented by EVSE equipment and associated networks. The project also studied vulnerabilities that affect supporting IT systems. This included assessing remote access controls, use of insecure protocols, and the ability to fingerprint devices from their online presence. This required working with the threat models and attack graphs and validating threat modelling 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. Some of these findings, enumerated through open-source intelligence (OSINT) means, were disseminated to EVSE manufacturers. These manufacturers confirmed our findings and advised that they indicate software or security misconfigurations. 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. The project final report included an anonymized set of findings [2]. 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. A large set of additional recommendations and areas for future R&D for this space was provided in [4].

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.



Recommended

Cybersecurity Practices

for

EV Charging Systems

CYBERSECURITY CONSIDERATIONS

- There is a dramatic increase in the quantity of electric vehicles (EVs) and EV supply equipment (EVSE). High power EV chargers are commonly being installed at workplaces and publicly-accessible locations.
- EVSE cybersecurity attacks may impact many critical infrastructure sectors (e.g., transportation systems, energy, emergency services, manufacturing).
- Combined use of smart-grid technologies, mobile applications,and back-end networking systems introduces several risks, including:
    - New attack vectors for the U.S. electric grid
    - Loss of customer data such as personally identifiable information and financial information
    - Control of the EVSE cyber-physical system through the Internet, potentially offering a foothold on internal enterprise networks

CYBERSECURITY IMPACTS

- EVSE providers, grid operators, vehicle manufacturers, and government agencies must understand cyber-attacks targeting EVSE chargers can create both localized and widespread impacts:

Local impacts

- Theft of PII and financial information
- Failure to charge vehicle
- Damage to batteries or other EV components
- Compromise of EVSE life-safety systems
- Loss of EVSE service availability

Large-scale impacts

- Harvesting of PII and financial information
- Shutdown of entire EVSE charging network
- Exposure of upstream and partner IT networks
- Misconfiguration of EVSE creating damaging or dangerous conditions
- Loss of consumer confidence in EVSE ecosystem
- Bulk power system impacts

PREVALENT WEAKNESSES IN ELECTRIC VEHICLE SUPPLY EQUIPMENT

Physical Access

- Failure to log or generate an alarm when internal compartments are accessed.
- Unencrypted storage allows attackers to steal credentials for use in accessing EVSE or partner systems, networks, and cloud services.
- Spacious internal compartments allow placement of malicious hardware to obtain PII or financial information.
- Attackers can modify or damage internal power electronics and safety systems.
- Insufficient physical measures to deter and identify intrusions.

System Hardening

- Unused, enabled network ports in use.
- Debugging ports are not removed prior to deployment.
- Default or system accounts, using common credentials, prevent accountability for malicious activities.
- The use of common credentials prevents system administrators from revoking access when personnel leave the organization or no longer require access.

Network Protection & Monitoring

- EVSE networks do not always support encryption across necessary data modalities, such as at rest or in transit.
- Intrusion Detection Systems (IDSs) are not installed at key network locations, e.g., IT/OT DMZs and cloud firewalls.
- Lack of proper network segmentation in enterprise systems and EVSE networks.
- Regular vulnerability scanning and patching of backend/cloud infrastructure is not performed by EVSE owners/operators.

Best Practices

BUSINESS NETWORK & OPERATIONS

☑ Implement secure coding practices including integrity checks of code repositories and version controlling.

☑ Use separation of privilege for all EVSE-related operations.

☑ Ensure cybersecurity best practices like the NIST Cybersecurity Framework are used for internal assessments, cyber hygiene, patching, supply chain and insider threat mitigations, etc.

EVSE SECURITY

☑ Implement tamper-detection sensors and alarms on EVSE enclosures.

☑ Prioritize alarms and ensure timely actions on critical log events.

☑ Encrypt all information storage devices within the EVSE.

EVSE NETWORK

☑ Use network segmentation and VLANs to isolate EVSE installations.

☑ Install firewalls and IDSs at key network locations.

☑ Encrypt all network traffic using a FIPS 140-2 compliant cryptographic module.

☑ Disable unnecessary services and ports.

☑ Ensure proper defense in depth by limiting external access to device to only authorized users and devices using access control technologies.

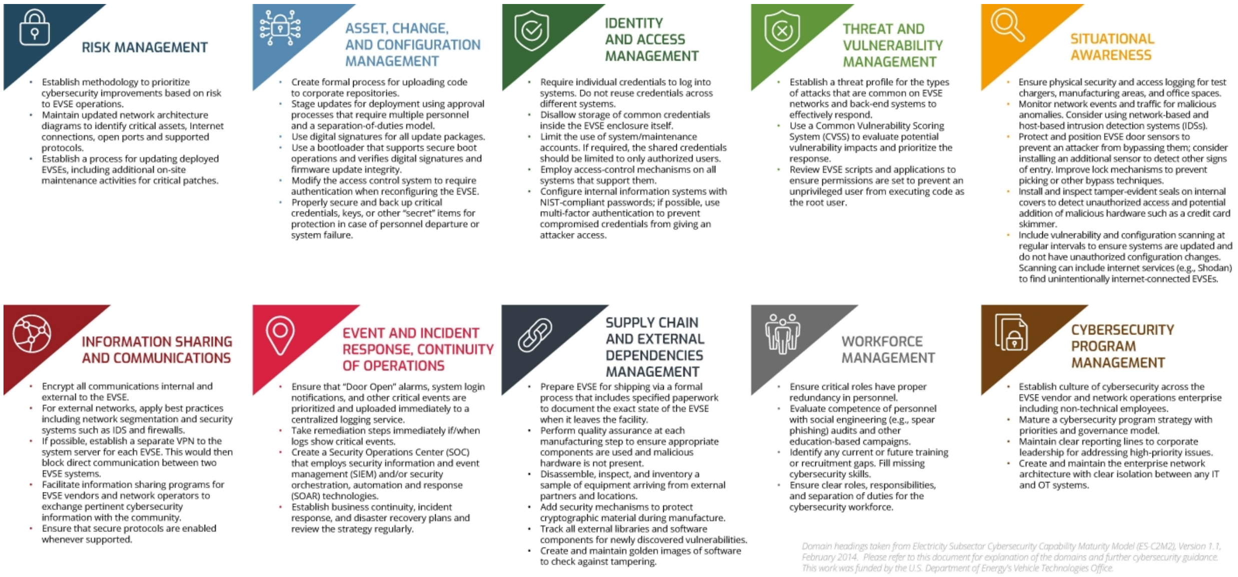
EVSE OPERATIONS

☑ Validate all network traffic and EV inputs before routing them into the EVSE OT network.

☑ Utilize secure trust principles such as HW/SW signing, secure boot, and secure firmware and software to update processes.

☑ Manufacturers and developers should follow secure software development practices.

Figure I.1.1.2 EVSE Best Practices [1].



RISK MANAGEMENT

- Establish methodology to prioritize cybersecurity improvements based on risk to EVSE operations.
- Maintain updated network architecture diagrams to identify critical assets, Internet connections, open ports and supported protocols.
- Establish a process for updating deployed EVSEs, including additional on-site maintenance activities for critical patches.

ASSET, CHANGE, AND CONFIGURATION MANAGEMENT

- Create formal process for uploading code to corporate repositories.
- Stage updates for deployment using approval processes that require multiple personnel and a separation-of-duties model.
- Use digital signatures for all update packages.
- Use a bootloader that supports secure boot operations and verifies digital signatures and firmware update integrity.
- Modify the access control system to require authentication when reconfiguring the EVSE.
- Properly secure and back up critical credentials, keys, or other "secret" items for protection in case of personnel departure or system failure.

IDENTITY AND ACCESS MANAGEMENT

- Require individual credentials to log into systems. Do not reuse credentials across different systems.
- Disallow storage of common credentials inside the EVSE enclosure itself.
- Limit the use of system/maintenance accounts. If required, the shared credentials should be limited to only authorized users.
- Employ access-control mechanisms on all systems that support them.
- Configure internal information systems with NIST-compliant passwords; if possible, use multi-factor authentication to prevent compromised credentials from giving an attacker access.

THREAT AND VULNERABILITY MANAGEMENT

- Establish a threat profile for the types of attacks that are common on EVSE networks and back-end systems to effectively respond.
- Use a Common Vulnerability Scoring System (CVSS) to evaluate potential vulnerability impacts and prioritize the response.
- Review EVSE scripts and applications to ensure permissions are set to prevent an unprivileged user from executing code as the root user.

SITUATIONAL AWARENESS

- Ensure physical security and access logging for test chargers, manufacturing areas, and office spaces.
- Monitor network events and traffic for malicious anomalies. Consider using network-based and host-based intrusion detection systems (IDSs).
- Protect and position EVSE door sensors to prevent an attacker from bypassing them; consider installing an additional sensor to detect other signs of entry. Improve lock mechanisms to prevent picking or other bypass techniques.
- Install and inspect tamper-evident seals on internal covers to detect unauthorized access and potential addition of malicious hardware such as a credit card skimmer.
- Include vulnerability and configuration scanning at regular intervals to ensure systems are updated and do not have unauthorized configuration changes. Scanning can include internet services (e.g., Shodan) to find unintentionally internet-connected EVSEs.

INFORMATION SHARING AND COMMUNICATIONS

- Encrypt all communications internal and external to the EVSE.
- For external networks, apply best practices including network segmentation and security systems such as IDS and firewalls.
- If possible, establish a separate VPN to the system server for each EVSE. This would then block direct communication between two EVSE systems.
- Facilitate information sharing programs for EVSE vendors and network operators to exchange pertinent cybersecurity information with the community.
- Ensure that secure protocols are enabled whenever supported.

EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS

- Ensure that "Door Open" alarms, system login notifications, and other critical events are prioritized and uploaded immediately to a centralized logging service.
- Take remediation steps immediately if/when logs show critical events.
- Create a Security Operations Center (SOC) that employs security information and event management (SIEM) and/or security orchestration, automation and response (SOAR) technologies.
- Establish business continuity, incident response, and disaster recovery plans and review the strategy regularly.

SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT

- Prepare EVSE for shipping via a formal process that includes specified paperwork to document the exact state of the EVSE when it leaves the facility.
- Perform quality assurance at each manufacturing step to ensure appropriate components are used and malicious hardware is not present.
- Disassemble, inspect, and inventory a sample of equipment arriving from external partners and locations.
- Add security mechanisms to protect cryptographic material during manufacture.
- Track all external libraries and software components for newly discovered vulnerabilities.
- Create and maintain golden images of software to check against tampering.

WORKFORCE MANAGEMENT

- Ensure critical roles have proper redundancy in personnel.
- Evaluate competence of personnel with social engineering (e.g., spear phishing) audits and other education-based campaigns.
- Identify any current or future training or recruitment gaps. Fill missing cybersecurity skills.
- Ensure clear roles, responsibilities, and separation of duties for the cybersecurity workforce.

CYBERSECURITY PROGRAM MANAGEMENT

- Establish culture of cybersecurity across the EVSE vendor and network operations enterprise including non-technical employees.
- Mature a cybersecurity program strategy with priorities and governance model.
- Maintain clear reporting lines to corporate leadership for addressing high-priority issues.
- Create and maintain the enterprise network architecture with clear isolation between any IT and OT systems.

Domain headings taken from Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1, February 2014. Please refer to this document for explanation of the domains and further cybersecurity guidance. This work was funded by the U.S. Department of Energy's Vehicle Technologies Office.

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

Threat Model Development

PNNL led the task to develop a threat model of high-power electric vehicle charging infrastructure and systemically 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 information is exchanged among 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 were gained into the security and resiliency of the EV charging ecosystem. 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 [2].

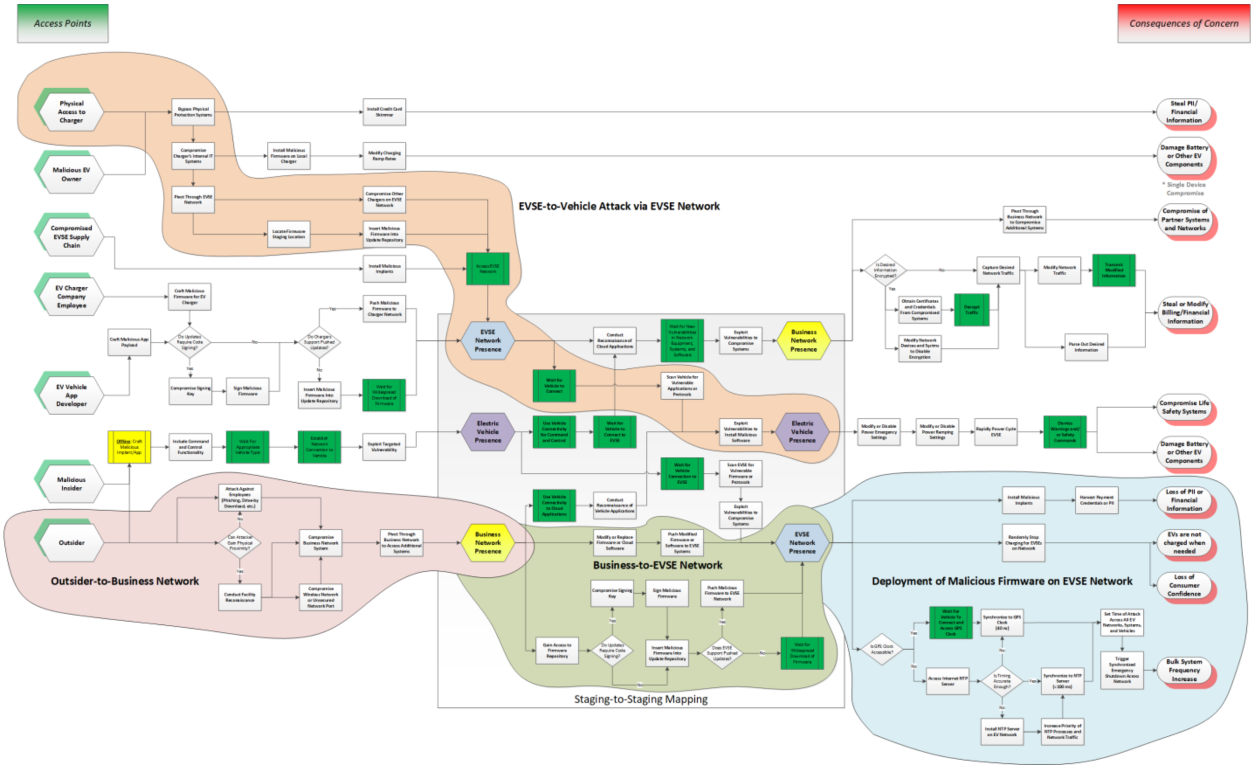

Access Points
Consequences of Concern
Physical Access to Charger
Malicious EV Owner
Compromised EVSE Supply Chain
EV Charger Company Employee
EV Vehicle App Developer
Malicious Insider
Outsider
Bypass Physical Protection Systems
Compromise Charger's Internal IT Systems
Pivot Through EVSE Network
Install Credit Card Skimmer
Install Malicious Firmware on Local Charger
Modify Charging Ramp Rates
Compromise Other Chargers on EVSE Network
Locate Firmware Staging Location
Insert Malicious Firmware Into Update Repository
Install Malicious Implants
Access EVSE Network
Craft Malicious Firmware for EV Charger
Craft Malicious App Payload
Do Updates Require Code Signing?
No
Yes
Do Chargers Support Pushed Updates?
Push Malicious Firmware to Charger Network
Compromise Signing Key
Sign Malicious Firmware
Insert Malicious Firmware Into Update Repository
Wait for Widespread Download of Firmware
Offline: Craft Malicious Implant/App
Include Command and Control Functionality
Wait For Appropriate Vehicle Type
Establish Network Connection to Vehicle
Exploit Targeted Vulnerability
Attack Against Employees (Phishing, Drive-by Download, etc.)
Can Attacker Gain Physical Proximity?
Conduct Facility Reconnaissance
Compromise Business Network System
Compromise Wireless Network or Unsecured Network Port
Pivot Through Business Network to Access Additional Systems
Outsider-to-Business Network
EVSE-to-Vehicle Attack via EVSE Network
EVSE Network Presence
Business Network Presence
Electric Vehicle Presence
Conduct Reconnaissance of Cloud Applications
Wait for New Vulnerabilities in Network Equipment, Systems, and Software
Exploit Vulnerabilities to Compromise Systems
Wait for Vehicle to Connect
Scan Vehicle for Vulnerable Applications or Protocols
Use Vehicle Connectivity for Command and Control
Wait for Vehicle to Connect to EVSE
Exploit Vulnerabilities to Install Malicious Software
Wait for Vehicle Connection to EVSE
Scan EVSE for Vulnerable Firmware or Protocols
Use Vehicle Connectivity to Cloud Applications
Conduct Reconnaissance of Vehicle Applications
Modify or Replace Firmware or Cloud Software
Push Modified Firmware or Software to EVSE Systems
Business-to-EVSE Network
Push Malicious Firmware to EVSE Network
Gain Access to Firmware Repository
Does EVSE Support Pushed Updates?
Staging-to-Staging Mapping
Steal PII/ Financial Information
Damage Battery or Other EV Components
* Single Device Compromise
Pivot Through Business Network to Compromise Additional Systems
Compromise of Partner Systems and Networks
Is Desired Information Encrypted?
Capture Desired Network Traffic
Modify Network Traffic
Transmit Modified Information
Obtain Certificates and Credentials From Compromised Systems
Decrypt Traffic
Modify Network Devices and Systems to Disable Encryption
Parse Out Desired Information
Steal or Modify Billing/Financial Information
Modify or Disable Power Emergency Settings
Modify or Disable Power Ramping Settings
Rapidly Power Cycle EVSE
Dismiss Warnings and/ or Safety Commands
Compromise Life Safety Systems
Install Malicious Implants
Harvest Payment Credentials or PII
Loss of PII or Financial Information
Randomly Stop Charging for EVSEs on Network
EVs are not charged when needed
Loss of Consumer Confidence
Deployment of Malicious Firmware on EVSE Network
Is GPS Clock Accessible?
Wait For Vehicle To Connect and Access GPS Clock
Synchronize to GPS Clock (40 ns)
Access Internet NTP Server
Is Timing Accurate Enough?
Synchronize to NTP Server (<100 ms)
Install NTP Server on EV Network
Increase Priority of NTP Processes and Network Traffic
Set Time of Attack Across All EV Networks, Systems, and Vehicles
Trigger Synchronized Emergency Shutdown Across Network
Bulk System Frequency Increase

Figure I.1.1.4 Complete graph. Details presented in [3].

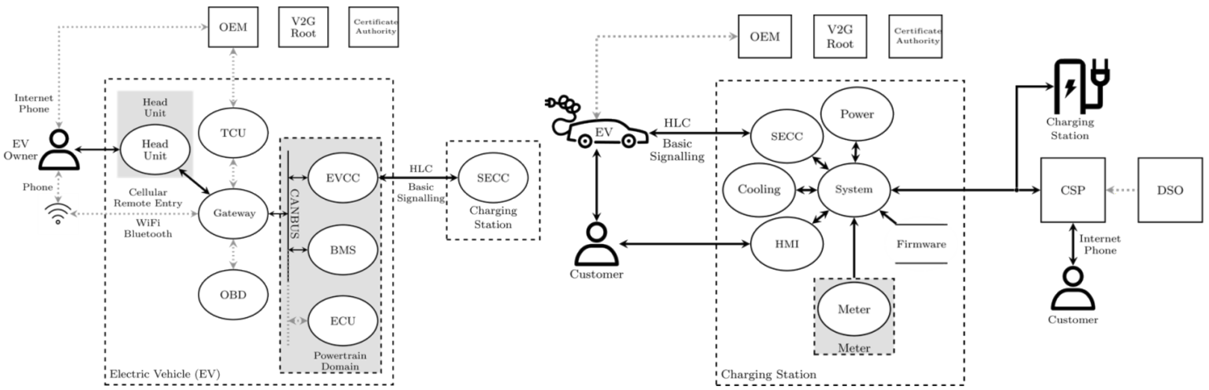


Figure I.1.1.5 The vehicle system model (left) depicts the components of the vehicle and their relationship to the charger. The charger system model (right) illustrates the relationship of the components and information flows.

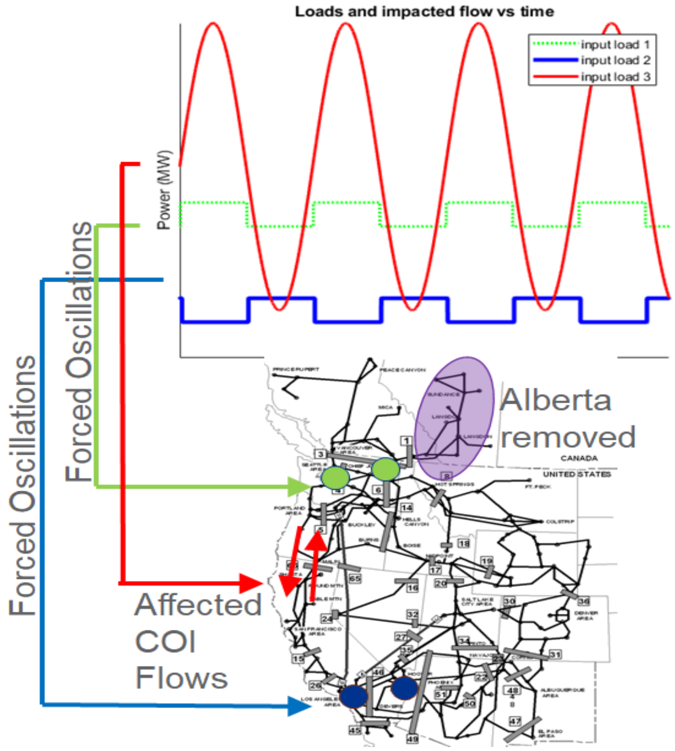


Figure I.1.1.6 Load oscillation simulation

Transmission System Consequence Analysis Simulations

PNNL's Consequence Analysis indicates that for the specific events studied in this work, the impact on the WECC system is concerning but generally manageable. 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 [2].

Conclusions

This project helped identify 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.
- Providing search terms and key identifiers that can quickly identify potential misconfigurations and security gaps.
- 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] J. Johnson et al., “Cybersecurity for Electric Vehicle Charging Infrastructure,” SAND2022-9315, July 2022.

[3] B. Anderson, “Securing Vehicle Charging Infrastructure Against Cybersecurity Threats,” 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020.

[4] J. Johnson, T. Berg, B. Anderson, B. Wright, “Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses,” Energies, vol. 15, no. 11, p. 3931, May 2022, https://doi.org/10.3390/en15113931.

[5] Varriale, Roland, Ryan Crawford, and Michael Jaynes. "Risks of Electric Vehicle Supply Equipment Integration Within Building Energy Management System Environments: A Look at Remote Attack Surface and Implications." *National Cyber Summit*. Springer, Cham, 2021.

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.