Cyber Security Research and Development

Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment

May 2018

INL/MIS-18-45521

Table of Contents

Introduction

The Idaho National Laboratory[1] (INL) partnered with the Department of Energy[2] (DOE) National Energy Technology Laboratory (NETL)[3] to perform cyber security assessments of several Smart Grid enabled Electric Vehicle Supply Equipment[4] (EVSE) devices that are being developed for production use. These EVSE units will be deployed in the future as the use of plug-in electric vehicles[5] (PEV) increases. These units were designed to be connected to the grid and managed by an electric utility company so that the charging of the vehicles will have little impact to the overall stability of the national electric grid. The EVSE devices need to be remotely managed to reduce the cost of management and maintenance for the electric utility. The first four EVSE tested were pre-production (prototype) devices two of which were intended for residential use and the other two for commercial deployment. The assessments of these four systems were done during 2014 and 2015.

INL also partnered with the DOE Vehicle Technologies Office (VTO) as part of the Grid Modernization Laboratory Consortium (GMLC) to assess two commercially available EVSE units from two of the most common vendors providing units for public use. These two units were designed to be remotely manageable by the owning company using the vendor provided web management interface. The assessments of these two systems were done during 2016 and 2017.

The cyber assessments performed by the INL were done in a manner to evaluate the accessibility of the EVSE from remote means (e.g. Wi-Fi[6] (802.11), Internet) as well as with physical access. The intent is to provide the manufacturer with information on how to secure their hardware and software so that the devices will be less likely to be used in nefarious ways. Each of the vendors received a detailed report identifying all of the vulnerabilities that were found during the assessments. These detailed reports were only shared with the vendor and were not shared with the DOE sponsors. Specifics regarding the identified vulnerabilities are not contained in this report to protect the vendors from public disclosure. The purpose of this report is to provide an overview of the state of security of EVSE and the potential cyber impacts to the EVSE infrastructure and the energy grid.

Consequence Driven Cyber Informed Engineering

One objective of this report is to provide an initial threat assessment of Level 2 AC charging stations (EVSE), and the potential impacts to utilizing PEV, charging infrastructure, and the electric grid. The first half of this report summarizes the vulnerabilities identified in all of the assessed EVSE. The final portion of this report will generate a basic threat analysis using the following methods.

Consequence conceptualization: During this stage, cybersecurity engineers worked with vehicle, charging infrastructure, and grid experts to identify High Consequence Events (HCEs). Given the assumption that attackers can gain access to elements in the system, the team identified what negative outcomes could result. This is a creative exercise, where researchers map a wide array of conceivable risks to potential consequences

---

[1] Idaho National Laboratory, http://www.inl.gov
[2] Department of Energy, http://www.energy.gov
[3] DOE NETL, http://www.netl.doe.gov/
[4] EVSE, http://en.wikipedia.org/wiki/Charging_station
[5] PEV, http://en.wikipedia.org/wiki/Plug-in_electric_vehicle
[6] Wi-Fi, http://en.wikipedia.org/wiki/Wi-Fi

across the entire system (e.g PEVs, charging infrastructure, DERs, and the grid). The team ranks HCEs by severity.

Analysis of system vulnerabilities: Next, the team performed a few technical investigations of systems to understand potential cybersecurity vulnerabilities (e.g. PEV and EVSE attack vectors, ability to manipulate messaging or controls, etc.). This process included a detailed review of communications and network protocol implementation, hands-on reverse engineering of hardware, and hacking experiments in a controlled laboratory environment. This work illuminates specific, plausible cyber-attack paths that might be used to produce a HCE. Researchers also identified the key information and access an attacker must obtain to discover and exploit these vulnerabilities. Based on the results of this step, researchers refined the list of conceivable HCEs and their severity. The team also created a basic rating index to indicate likelihood of occurrence of an HCE, based on the complexity of effort required to produce them.

Validation and prioritization of consequences: The next step conducted in-depth evaluation and validation of HCEs using basic prototype exploits. The team demonstrated the effects of cyber-attacks on PEVs, EVSEs, and the grid using real-time power hardware-in-the-loop (HIL) and other simulation methods. Results of this work validated HCEs and allowed the team to finalize priority ranking.

Mitigation strategy development: With HCEs validated and prioritized, the team worked with the industry partners to develop mitigation solutions (where applicable and feasible). This was done by the creation of a detailed report documenting all of the research and guidance into how the vendors might address the HCEs. An ideal mitigation strategy eliminates the possibility of a HCE in system design, such as by isolating systems or physically limiting power capacity. When that is not feasible, protections and detection methods are designed to prevent or detect attacks that may lead to HCEs.

This report will document some of the general HCEs and mitigation strategies that can then be used by any of the vendors developing technology for use in the electric vehicle infrastructure.

EVSE System Design and Description

Each of the EVSE units evaluated at INL were designed very similarly. Two of the EVSE units were designed to be a single charging station capable of charging two PEVs simultaneously using power sharing features so that only a single 40A power source was required. The other EVSE were implemented with the intent of charging a single PEV. Typical user interaction with the EVSE includes authorization using a RFID token or cellphone application and then plugging in the PEV using the standard SAE J1772 connector. Figure 1 is a block diagram of the typical hardware components found in the EVSE units.

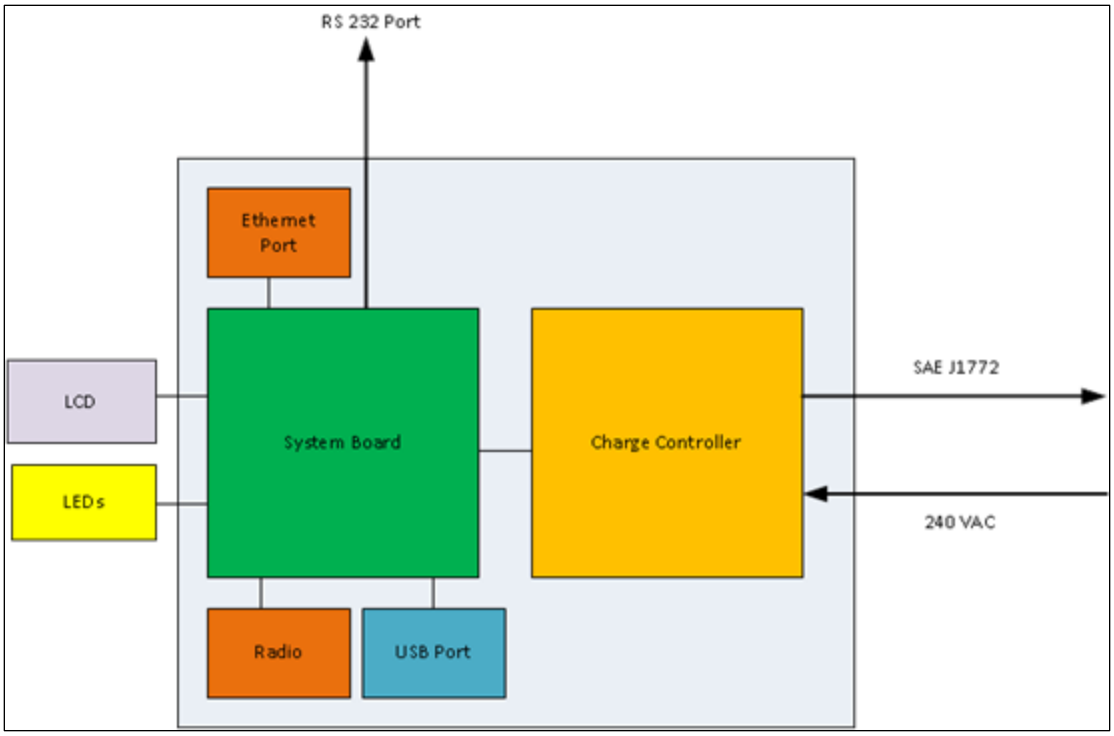


Figure 1 Example EVSE Block Diagram

Each of the EVSE were disassembled to inspect the various components used in the system and how they were interconnected. There is typically one main system board manufactured by the vendor. All of the evaluated system boards were ARM[7] Cortex processors along with some form of remote connectivity (e.g. cellular modem, wired Ethernet, Zigbee, etc.). The system board is connected to one or more charge controllers to manage each J1772 cordset. This connectivity was typically done using basic serial communications (RS232, I2C, SPI, etc.).

Vehicle Control and Interface

Each of the assessed EVSE are traditional Level 2 AC units that simply provide AC power directly to the PEV. Each PEV is responsible for managing the charging process and ensuring vehicle safety. The only communications between the EVSE and the PEV is provided by a pilot signal found on one of the pins in the SAE J1772 cord and connector. This pilot signal is just a basic pulse-width modulated signal that is used to indicate the charging state and the available power from the EVSE. As such there we no identified methods that could lead to vehicle compromise from a compromised EVSE.

In the future, vehicle compromise from a compromised EVSE might be possible as the EVSE evolve into higher power charging stations We have already observed the enhanced communications available in today's DC Fast Charging systems that operate providing DC power directly to the vehicle. These systems use the CHAdeMO or SAE J1772 CCS connectors and have advance communications with the vehicle to manage the charge. Details of these communication methods are beyond the scope of this report, but it is important to note that Level 2 AC charging is but a portion of the electric vehicle infrastructure.

Future charging systems, including Level 2 AC EVSE, will likely start implementing additional protocols for charge management features from the grid. This will include protocols such as SAE 15118 and can be implemented over the existing AC powerlines using Power Line Carrier (PLC) technology. When this happens, there will be increased communications between the PEV and the Level 2 EVSE that might also be used for

[7] ARM Architecture, http://en.wikipedia.org/wiki/ARM_architecture

potential compromise. So far we are unaware of any vehicles or EVSE implementing these enhanced communication methods.

Physical Access Assessments

One phase in each of the assessments was to determine what information and vulnerabilities were discoverable given physical access to the EVSE. The intent is to determine what might be done to the system if it was in the hands of someone with malicious intent. In cyber security it is generally assumed that physical access to hardware more often than not leads to severe system compromise. These assessments confirmed that assumption. It is important to note that devices such as EVSE are going to be publicly accessible due to the nature of their use (i.e. they will be outdoors in public areas). With physical access to the EVSE, the assessment team was able to further test and analyze the behavior of the system while interacting with it using the vendor provided management clients.

Identified Vulnerabilities

The following list is a summary of the range of vulnerabilities identified during the disassembly, reverse-engineering, and penetration testing of the various EVSE. This list is not in any particular order.

- The system board (used for remote communications and management) were all Linux based systems marginally configured and running very old kernels and ancillary services (telnet, ftp, etc.). Several of these Linux systems used weak password hashing algorithms. The stored passwords were cracked in a reasonable amount of time and also found to not be unique to the specific EVSE.
- All of the vendor processes running on the EVSE ran as the Linux **`root`** user. In most cases this allows the process to access system functionality that it doesn't necessarily require for operation. And if/when the vendor processes are exploited, the attacker gains full access to the EVSE.
- Charge controller firmware, in addition to the system boards, was all successfully extracted using a variety of techniques. Extraction of the firmware was done using JTAG, Flash memory readers, serial interfaces, or USB. This was successful on all devices but one because of the secure boot loader settings.
- Vendor provided firmware updates were not signed, and modified firmware was easily loaded back onto the EVSE. Some systems even periodically checked for an external drive to be present and would automatically update firmware from the drive.
- A few of the EVSE units provided a local web server using ad hoc wireless networking. This service was provided for quick configuration and commissioning of the EVSE unit. Several issues were identified with these webservers that ultimately lead to unauthorized access to the configuration files and data on the EVSE.
- A few of the EVSE units provided Android or iOS applications to remotely manage or authorize charge sessions. These applications were easily revere engineered and revealed several weaknesses in the management interface of the EVSE, and gave insight into the vendor cloud server API calls.
- Serial ports, Ethernet jacks, or USB ports were found on the outside of the EVSE cases. These ports were all easily accessible and active, and the assessment team was able to use this access for varying levels of control or update to the system.
- Weak password hashing was found in use on the local databases (if used) and in the backend database systems. When extracted, the user names and passwords were easily cracked.

- JTAG interfaces (populated or unpopulated) were all found on the system and charge controller boards. This interface was used with varying degrees of success, but more often than not allowed direct control of the board processor.
- Most of the EVSE systems lacked secure boot protections. This allowed the boot loader to be interrupted enabling the assessment team to modify boot parameters, change the system to operate in single-user mode, and even extract flash memory contents.
- A few of the systems implemented some form of proximity detection (micro switches, light sensors, etc.), but these mechanisms were ineffective so long as the system was never powered on when the case was removed.
- User information, including personal billing history, was stored locally on the EVSE systems and retrieved from the local embedded databases.
- Reverse engineering of vendor specific binaries (applications) revealed several different types of vulnerabilities in the applications themselves (buffer overflow, string injection, system command injection, etc.). None were investigated very deeply, but they should be resolved with secure coding practices.
- Several vendor specific binaries contained hard coded usernames and passwords to access other system components and/or remote management applications. This information was then used to access the management systems from assessment computers and impersonate the EVSE. The primary impact was the loss of personal information from the management system.
- Several EVSE units relied upon shared memory pages to allow for Inter-Process Communications (IPC), but this shared memory was not protected from arbitrary use. Rouge or compromised applications on the EVSE were able to access the IPC memory and arbitrarily control messages between processes. This allowed for not only the capture of potentially sensitive data but also the manipulation of normal EVSE charge functions.

Mitigation Recommendations

The following is a list of the recommendations provided to mitigate some of the vulnerabilities found during the physical access assessment.

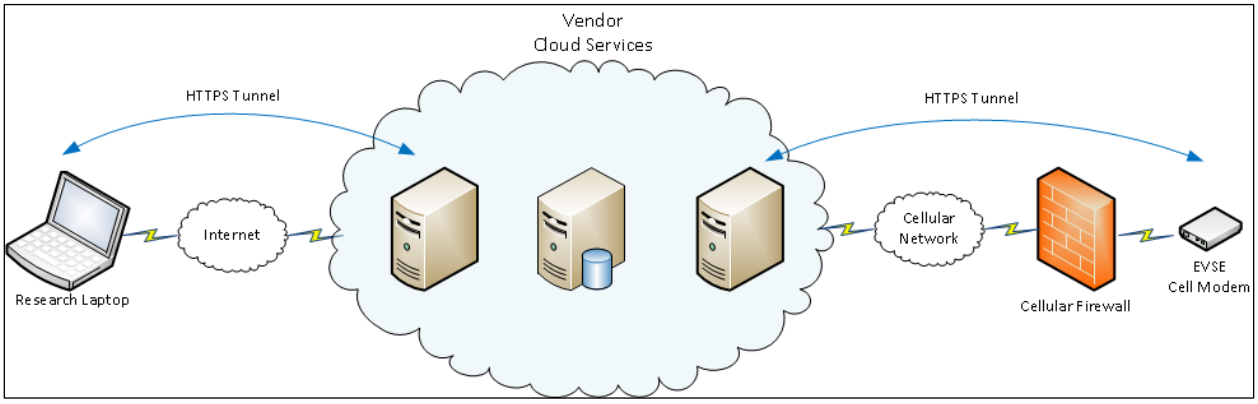
- Remove external access jacks (RJ45, DB9, USB) from the EVSE case.
- Lock the boot loaders so that the firmware boot options cannot be modified. The BeagelBone Black, for example, uses a version of U-Boot that does not allow U-Boot environment variable modifications.
- Lock, encrypt, and/or sign the system board and charge controller board firmware.
- Strip all vendor compiled binaries that are running on the system board.
- Remove hard-coded usernames, passwords, and connection string information from all source code.
- Audit all source code used for basic secure coding practices (deprecated functions, boundary issues, SQL injection, etc.).
- Remove the Linux system calls found in any vendor binary files ***or*** make sure the arguments to the system call are completely sanitized.
- Disable or turn on the security lock features for the JTAG interface.
- Encrypt board-to-board communications (if possible) to prevent reverse engineering of the control commands.
- Obscure IC part names to make reverse engineering more difficult.
- Do not use HTTP Basic Authentication for any web access control.

- Ensure all input values (length fields, strings, etc.) from users ***and*** external sources (e.g. shared memory) are sanity checked prior to use.
- Do not provide a mechanism for such easy firmware updates as simply plugging in a USB drive into the EVSE.
- When storing passwords, use a cryptographically secure hashing algorithm. Use a long, unique random salt for each password.
- Use semaphores to prevent concurrency problems and enforce access control for shared memory and IPC.
- Consider the use of a read-only file system, such as **`squashfs`**[8], to prevent persistent storage of malicious files.
- Make the external housing more difficult to access.
- Require a password for direct console access via tty (serial) interfaces.
- Use the POSIX[9] API instead of the System V[10] API to interface with shared memory. This will provide better security and concurrency management (integrity) for all processes accessing a shared memory resource (thread safety).
- Turn off services not actively used.

- Update the local website to include a more robust authentication mechanism such as the built-in Django Authentication Middleware.[11]
- Strengthen any of the commission/configuration pages by requiring physical access to the device during setup. This can be done by simply requiring the press of a button.
- Strengthen management application APIs by requiring authentication, using certificate pinning, replacing Basic Authentication with secure sessions, and using signed certificates.
- Encrypt flash memory where the firmware is stored locally.
- Add a tamper alarm that reports to the managing body if the housing is opened, even when powered off (i.e. backup battery).

Remote Access Assessments

The second phase of each assessment was done using only remote access methods. This allowed for the determination of what might be done to the unit without prior knowledge of its intended function, and what might be done from across a traditional internet connection. The remote management for the internet-based EVSEs was provided by cellular modems connected to a vendor network or cloud server.



[8] SquashFS Overview, http://en.wikipedia.org/wiki/SquashFS
[9] POSIX Overview, http://en.wikipedia.org/wiki/POSIX
[10] UNIX System V Overview, http://en.wikipedia.org/wiki/UNIX_System_V
[11] https://docs.djangoproject.com/en/1.8/ref/middleware/#module-django.contrib.auth.middleware

Figure 2: Example Remote Management Architecture

The assessment team was given valid credentials to the vendor's management system to allow normal management functionality of the system under test. The assessment was done using these credentials or other credentials harvested during the physical access portion of the assessment.

Identified Vulnerabilities

The following is a list summarizing the types of vulnerabilities discovered during the remote portion of these assessments.

- Several of the remote management applications lacked proper authentication methods. This included mistakes such as client side validation, processing logon credentials using basic HTTP authentication methods, and un-sanitized logon fields allowing for SQL injection.
- Some of the cloud managed systems were vulnerable to multiple web exploit types. This included SQL injection possibilities in input fields and Cross-site Scripting (XSS) attacks that allowed for restricted page access.
- Some systems allowed authenticated users to manage or manipulate equipment that was not their own. This was done after some basic reverse engineering of the webserver API calls that then allowed manipulation of the calls in transit to expose other EVSE systems.
- Although the cellular modems were not configured with public IP addresses (Network Address Translation (NAT) provided by the cellular carrier) some of the cellular modems were reachable from other devices connected to the same provider. The semi-private network provided by the cellular company is good basic protection, but the actual deployed network layout depends on the carrier configuration (e.g. differences between Europe and US).
- Remote firmware updates, in some cases, were provided by poorly configured FTP servers. The credentials used to connect to the FTP server were easily stolen by monitoring the network traffic, and the assessment team gained access to the FTP server. Because of the use of unsigned firmware, a modified firmware was uploaded to the server and it was later pushed out to all of vendors EVSE during the next update cycle (not just the system under test).
- System call injection was possible on a few of the vendor binaries. This was due to applications passing user controlled data as the command string to the Linux **`system`** function. This resulted in privileged system commands being run on the management server based upon input fields found in the management web pages.

Mitigation Recommendations

The following is a list of the recommendations provided to the vendors to address some of the security findings.

- Wrap the remote management commands inside of a higher level protocol so that connections to the EVSE are authenticated and/or authorized (e.g. all commands are sent via HTTPS, not just logon attempts).
- Properly configure the Cellular modem so that the default usernames and passwords are unique to the EVSE.
- Turn off ancillary services not actively used, or replace them with known secure versions of similar services (e.g. replace FTP with SFTP or SCP).
- Strengthen mobile API authentication using certificate pinning, replacing basic authentication with secure sessions, and using a signed certificate.

- Ensure the firmware and patch management servers are extremely secure.
- Use code-signing techniques for firmware update verification.

Grid Impacts

The INL also performed some power engineering tests of each of the EVSE units. A number of these tests focused on system functionality, efficiency, and power quality, but another test was designed to monitor the natural response of an EVSE and a PEV to a dynamic grid event. The EVSEs were connected to a Grid Simulator capable of producing atypical grid events such as a frequency deviation or voltage sag. The research team subjected the three EVSE and plug-in electric vehicles, while charging at a rate between 3 to 7 kW, to a supply voltage sag from 240 VAC to 100 VAC for a duration of 12 cycles (0.2 seconds) as shown in Figure 3. Two of the vehicle charging systems (PEV-A and PEV-B) responded by increasing current in an attempt to maintain constant power to the vehicle energy storage system. Conversely, PEV-C stopped charging at the initiation of the voltage sag, but resumed charging approximately five seconds after the completion of the voltage sag.

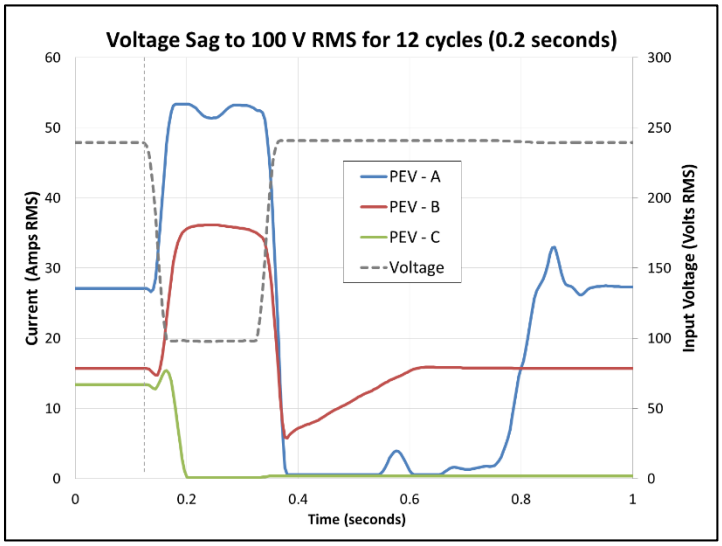


Figure 3: Dynamic Response of EVSE and PEV during 12 Cycle Voltage Sag

The response from the three charging systems during a 240 VAC to 100 VAC voltage sag was used with a grid distribution model as the input for a simulation of 4,000 plug-in vehicles and EVSE on a 34-node distribution feeder. The grid distribution feeder model was previously validated using data from PG&E feeder network in the San Francisco bay area. The simulation results from the 4,000 plug-in vehicles and EVSE on the 34-node distribution feeder resulted in grid voltage and frequency oscillation on the distribution feeder system. Figure 4 and Figure 5 show the response of the voltage and frequency following the voltage sag event while 4,000 plug-in vehicles are charging at a level 2 rate. Note the oscillation that resulted from the event which naturally dampened within 15 seconds.

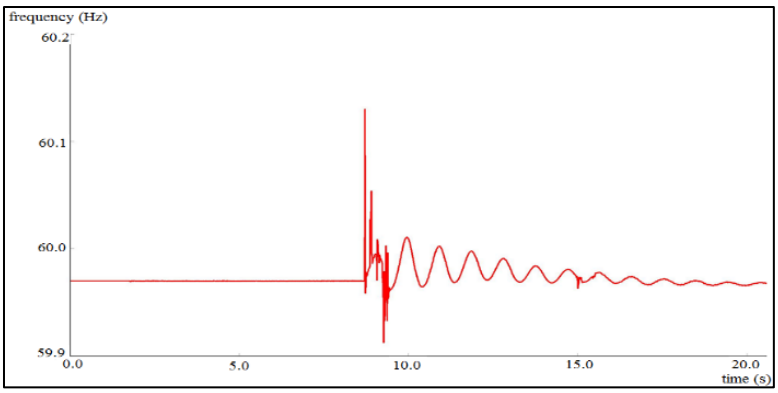


Figure 4: Simulated Effects of Dynamic Frequency Response of 4,000 EVSE and PEVs on a Distribution Feeder

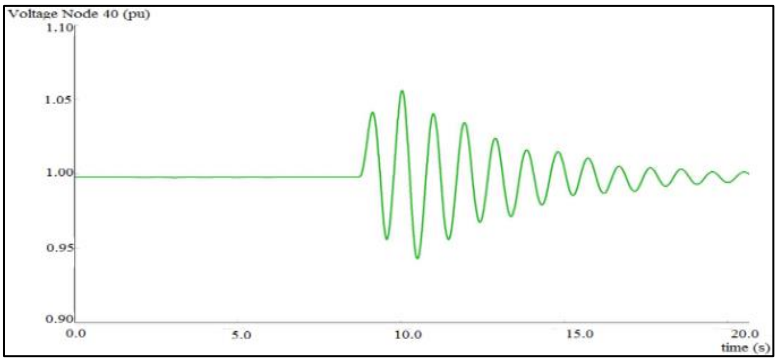


Figure 5: Simulated Effects of Dynamic Voltage Response of 4,000 EVSE and PEVs on a Distribution Feeder

Even though the simulated distribution feeder response showed in the previous figures occurred due to a non-malicious intent (electrical fault), this response demonstrates the potential vulnerability from grid instability of voltage and frequency as dependent upon electrical load mix and composition. With increased EV market penetration, there is a change in the load mix towards more constant power load due to more power electronic loads and therefore increased potential risk due to malicious intent by manipulating the inherent instability characteristics of higher constant power mix.

High Consequence Events (HCEs)

The following is an overview of some of the High Consequence Events (HCEs) scenarios that were generated during these assessments. It is important to note that each assessed EVSE was not vulnerable to all of these HCEs, but each EVSE could be compromised using at least one of these scenarios.

Compromise of the Management Interface

Most of the EVSE units provided a management interface for the system that was available from a vendor owned cloud service. Some of these units were managed using a custom vendor application that ran locally on a network connected to the EVSE or on a mobile device. In a majority of the cases, vulnerabilities were identified that allowed unauthorized access to the management functions. In some cases it was also possible to remotely manage EVSE units that did not belong to the credentials used to access the management application.

Impact

The impact caused by unauthorized access to the management server varied widely in the overall impact. In some cases the assessment team was only able to view and manage EVSE units not assigned to their user

credentials. In other cases it was possible to compromise the vendor management server directly leading to unauthorized use, access, and data theft.

Compromise of the Firmware Update Process

A few of the EVSE were compromised by manipulating the provided firmware update process. In one case the firmware was automatically updated when a USB drive was connected to the EVSE. In other cases the firmware was located on a remote server. In all cases, however, the firmware was never signed or validated. This allowed for modified firmware to easily be used.

Impact

The impact caused by these vulnerabilities is quite severe. Modifying the firmware of the EVSE allowed the assessment team to change any or all of the subsystems running on the management board. This is the most complete form or compromise because the systems can be completely controlled by a hostile entity and can keep the vendor from ever regaining access to their EVSEs.

Compromise of Payment Data

The loss of payment data and other personal information was accomplished by either gaining access to the data stored locally on the EVSE or by compromising the data on the remote management or payment servers. Although this data can often include sensitive information such as credit cards, it most often only included customer IDs, charge time, and payment amounts.

Impact

The impact of this HCE is rather low compared to other HCEs due to only a loss of information. This is more of a concern for payment services than it is for network providers and management systems. But the loss of sensitive personal information still needs to be addressed.

Compromise of the EVSE System

Through various means, most of the EVSE units were able to be directly compromised. The result of system compromise is that a hostile entity has unauthorized system access, and can use the EVSE system in a manner it wasn't designed.

Impact

In all cases, system compromise of the EVSE resulted in the assessment team having system or root level access to the EVSE hardware. This allowed for a number of potential impact scenarios to be realized, most of which are considered fairly severe. However, considerations must be made to determine if the compromise is just to a single EVSE unit or if the compromise leads to unauthorized access of all the networked EVSE. Regardless of how widespread this might be, the result can ultimately mean loss of control of the unit by the vendor.

Measurable Grid Disturbances

Although the measured responses of the EVSE and charging PEV were a natural response to typical grid events, it is hypothesized by the assessment team that similar results can be created via a cyber mechanism. The hypothesis is that compromise of the EVSE might allow a hostile entity to control charging functions in a coordinated fashion (e.g. starting or stopping all vehicle charges at the same time) that might lead to a measurable grid event that is beyond the acceptable limits of noise or harmonics.

Potential Impact

The assessment team at INL has not yet performed any tests or experiments to test this hypothesis.

Conclusion

Although Level 2 AC EVSE stations are considered low-power by today's standards, they are still the most widely deployed charging stations for PEV. The overall potential impacts may currently be considered small due to the low numbers of EVSE units deployed nationwide, but these numbers will only increase over the next several years. Additionally it must be recognized that Level 2 EVSE will also be located in homes where disruption to the grid may cause wide spread effects on the portion of the distribution system that can affect many households.

It is important to note, however, that although all of the EVSE units involved in these assessments were compromised in some fashion, the assessment team was never able to cause the EVSE or the PEV to enter an unsafe state.