DOCKETED	
Docket Number:	19-IEPR-04
Project Title:	Transportation
TN #:	228787-21
Document Title:	DOE DHS DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report - March 2018
Description:	Prepared by US Dept. of Transportation Volpe Center and US Dept. of Energy Office of Policy
Filer:	Wendell Krell
Organization:	California Energy Commission
Submitter Role:	Commission Staff
Submission Date:	6/19/2019 9:22:42 AM
Docketed Date:	6/19/2019

DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report

Prepared by:
United States Department of Transportation Volpe Center and
United States Department of Energy Office of Policy

Final Report—March 2018

DOT-VNTSC-DOE-18-01

Prepared for:
U.S. Department of Energy.
1000 Independence Ave., S.W.
Washington, DC 20585-1615

U.S. Department of Transportation
Volpe Center

Disclaimer

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE:	3. REPORT TYPE AND DATES COVERED
	March 2018	Technical Meeting Report

4. TITLE AND SUBTITLE	5a. FUNDING NUMBERS
DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report	VXU6A1/RE572
6. AUTHOR(S) Kevin Harnett, Brendan Harris, Daniel Chin, Graham Watson	5b. CONTRACT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Department of Transportation John A. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-DOE-18-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Energy 1000 Independence Ave., S.W. Washington, DC 20585-1615	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public on the National Transportation Library (NTL) Repository and Open Science Access Portal (ROSA P) website at: https://rosap.ntl.bts.gov/view/dot/34991	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (DOT) John A. Volpe National Transportation Systems Center (Volpe), held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. This report summarizes key takeaways and discussion points.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Electric Vehicle (EV), Electric Vehicle Supply Equipment (EVSE), Cybersecurity, Charging Station, Smart Grid, Utility, Building Energy Management Systems (BEMS), Vehicle Technology Office (VTO)	28
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASS	UNCLASS	UNCLASS	Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Acknowledgments

The Department of Energy (DOE) and U.S. DOT Volpe Center would like to thank subject matter experts (SMEs) from the California Public Utilities Commission's (CPUC) Vehicle-Grid Integration Communications Protocol Working Group, Idaho National Laboratory (INL), Lear Corporation, Fiat Chrysler Automotive (FCA), and Daimler AG for their insight on topics in this report. In addition, we would like to acknowledge and give thanks to all the organizations who participated in the DOE/DHS/DOT Volpe Center Technical Meeting on Electric Vehicle and Charging Station Cybersecurity on November 29-30, 2017, in Arlington, VA, and for providing their insights and expertise.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
BEMS	Building Energy Management System
CAN	Controller Area Network
CCC	Chaos Communications Conference
CCS	Combined Charging System
CD	Compact Disk
CDMA	Code Division Multiple Access
CEMS	Central Energy Management Systems
CharlN e.V.	The Charging Interface Initiative
DC	Direct Current
DCFC	DC Fast Charger
DHS S&T CSD	Department of Homeland Security Science and Technology Cybersecurity Division
DIN	Deutsches Institut für Normung e.V. (the German Institute for Standardization)
DOE	Department of Energy
DOS	Denial of Service
DOT	Department of Transportation
DSO	Distribution System Operator
ECU	Electronic Control Unit
EESA	Electrical Energy Storage Assemblies
ENCS	European Network for Cyber Security
ESCC	Electricity Subsector Coordinating Council
ESCSWG	Energy Sector Control Systems Working Group
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FISMA	Federal Information Security Management Act
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HAN	Home Area Network
HITB	Hack-in-the-Box
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INL	Idaho National Laboratory
IoT	Internet of Things
ISO	International Organization of Standardization
ISO	Independent System Operator

Abbreviation	Term
LEV	Light Electric Vehicle
MITM	Man In The Middle
NEC	National Electrical Code
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NFC	Near Field Communications
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
OBD	On-Board Diagnostic
OCA	Open Charge Alliance
OEM	Original Equipment Manufacturer
OP	Office of Policy
OTA	Over The Air
PEV	Plug-In Electric Vehicle
PHEV	Plug-In Hybrid Electric Vehicle
PIN	Personal Identification Number
RF	Radio Frequency
RTO	Regional Transmission Organization
SAE	Society of Automotive Engineers
SD	Secure Digital
SME	Subject Matter Expert
SMS	Short Message Service
TLS	Transportation Layer Security
TPMS	Tire Pressure Monitoring System
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VTO	Vehicle Technology Office
W3C	World Wide Web Consortium
WPT	Wireless Power Transfer
XSS	Cross-site scripting

Executive Summary

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. This report summarizes key takeaways and discussion points.

Electric vehicles are becoming a part of the transportation and mobility industry in the United States. It is during this initial development and deployment period for the EV environment that the opportunity exists to mitigate cybersecurity issues before they become widespread, ingrained, difficult, and expensive to remedy. The EV environment is a mix of multiple stakeholders, domains, hardware, and software. As the communication, electricity, and transportation systems become more integrated, cybersecurity vulnerabilities that would normally be localized, now have the ability to cause disruptions across these multiple sectors.

Modern day automobiles have cybersecurity vulnerabilities that the industry and government are working on addressing.[1] This report, and the preceding technical meeting, focuses on the cybersecurity vulnerabilities that are unique to electric vehicles and electric vehicle supply equipment:

- The two-way communication between the EVSE and the vehicle
- The connection between EVs, EVSE, and other systems (e.g., grid, telecommunications, buildings, etc.)

These differences could potentially lead to three main types of issues:

1) Public safety hazard to the vehicle operators and/or those in the immediate vicinity
2) Mobile, highly connected malware vectors
3) Initiating and/or exacerbating electric grid disruption

As a result of discussions during the Electric Vehicle and Charging Infrastructure Cybersecurity Technical Meeting, participants identified gaps and vulnerabilities in this threat space (see Chapter 7: Gaps and Conclusions for more detail on the gaps). The table below is a prioritized list of the gaps identified and provides a short description of each:

[1] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Identified Gap	Gap Description
EVSE Charging Infrastructure Lacks Cybersecurity Best Practices	The EV industry does not have secure software design and development methodology guidance to design and build "secure" EVSE capabilities. Purchasing agents who buy EVSEs do not typically specify cybersecurity protections (e.g. secure OTA firmware update capability, authentication) for their EVSE products due to lack of EVSE cybersecurity guidelines for the EVSE acquisitions.
End-to-End EV and Charging Infrastructure Lacks a Trust Model	There is no consensus on end-to-end trusted communication standards for securing communications between the electric vehicle and the charging infrastructure.
EV/Charging Infrastructure Lacks Cybersecurity Testing	There is a lack of formal cybersecurity testing and assessment applied to the entire EV charging infrastructure.
Wireless Chargers Lack Common Cybersecurity Guidelines	Light passenger EVs, electric buses and electric trucks have similar wireless charging communications paths, and none of them have guidance on the unique cybersecurity requirements specifically for wireless charging.
EV Over-the-Air (OTA) Infrastructure Update Capability Is Immature	Current EV infrastructure (i.e. EVSEs, Smart Meters, Advanced Metering Infrastructure-AMI, Demand Energy Response equipment, etc). OTA update capability is immature and insecure and vulnerable to cyberattacks. Insecure legacy equipment will need to be addressed at the same time as new EV equipment is designed to have better and more secure OTA capabilities.
Commercial EVSE Lack of Common Physical Security Guidelines	Physical damage to commercial EVSEs can result in non-operational units which could have an adverse effect on consumer confidence in EVs in general. Some types of physical damage whether intentional or not, may expose the public to harmful electric current levels. There is a lack of common Physical Security Guidelines for Commercial EVSE Physical Security.

Throughout the technical meeting, participants particularly focused on two of these gaps as critical for government and industry to address:

1. The lack of security best practices for EVSE charging infrastructure
2. The lack of an end-to-end trust model for validating communications

Addressing these critical gaps should help focus and frame coordination between the relevant stakeholders in the energy, transportation, and communication sectors.

1 Background/Introduction

The global electric vehicle stock surpassed one million vehicles in 2015 and grew to more than two million electric vehicles in 2016.[2] Growing at a similar rate, the number of EV charging stations deployed globally reached two million in 2016.[3] In the United States, the EV stock was nearly 600,000 vehicles and EVs made up nearly one percent of total vehicle sales in 2016.[4] As EV and EVSE deployment continue their growth, research and development of technologies that ensure safe and secure operating conditions of the electric vehicle fleet would be cost effective and beneficial.

1.1 Structure of the Report

On November 29-30 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technology Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), and the U.S. Department of Transportation's (DOT) John A. Volpe National Transportation Systems Center (Volpe), held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity. The object of the technical meeting was not to obtain any group position or consensus. Rather, the organizers were seeking as many recommendations as possible from all individuals at the meeting.

The meeting brought together diverse stakeholders from the EV environment: vehicle manufacturers, charging station manufacturers and operators, academia, and federal and state governments. The purpose of the meeting was to explore current and future research and development in EV and EVSE cybersecurity. In their discussions at this meeting, the participants identified the takeaways and gaps contained in this report. The report also includes some background information and contextual information added for the convenience of the reader.

Section 1 gives a brief background on general vehicle cybersecurity and discusses unique electric vehicle cybersecurity concerns. Section 2 summarizes discussion and provides information on how organizations within this space can improve their cybersecurity preparedness through the structure of their organizations. Section 3 summarizes ideas expressed throughout the technical meeting on how to improve EV cybersecurity before deployment in order to increase security and save costs. Section 4 digs into the importance of establishing trust through verification, across and within systems. Section 5 discusses challenges around the supply chain of EV charging equipment and liability. Section 6 discusses how to improve sector cooperation and communication to address cybersecurity concerns early and effectively.

---

[2] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf

[3] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf.

[4] International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017. https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf.

Section 7 of the report contains gaps that were identified during the recent cybersecurity technical meeting, as well as through information gleaned from discussions with Energy Sector SMEs.

1.2 General Vehicle Cybersecurity Concerns Background

Today's automobiles are complex machines that can contain many embedded electronic control units (ECUs), networks to support these units, and a host of wired and wireless external interfaces. Wired interfaces include Universal Serial Bus (USB), compact disks (CDs), and secure digital cards (SD cards). Wireless interfaces include short range and long range connectivity through Bluetooth, Wi-Fi, radio frequency (RF), near-field communications (NFC), Global System for Mobile Communications (GSM), coded-division multiple access (CDMA), and Universal Mobile Telecommunications System (UMTS).

The wireless interfaces can support a host of features, including remote tire pressure monitoring systems (TPMS), telematics, and smart key/keyless entry/ignition start. They also enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications (collectively referred to as V2X communications), which could improve vehicle/driving efficiency, comfort, and safety. The continuing trend in vehicle architecture is a shift towards more open systems and away from the traditional closed/proprietary system type of architecture. This increased connectivity creates a number of potential security vulnerabilities in vehicles.

Supported by grants from the U.S. National Science Foundation, collaborations between researchers at the University of California San Diego and the University of Washington in 2010 and 2011 identified vehicle cybersecurity vulnerabilities:

- **Experimental Security Analysis of a Modern Automobile (2010)**[5]: The analysis assumed that unauthorized parties had (at least temporary) physical access to the vehicle's computer networks (e.g. able to plug their own hardware into a port underneath the dash). The researchers analyzed and evaluated the computers within the internal networks of a modern vehicle and described the range of security issues discovered in the process.
- **Comprehensive Experimental Analyses of Automotive Attack Surfaces (2011)**[6]: The major objective of this work focused on three key classes of remote attack vectors without physical contact with the vehicle: indirect physical, short-range wireless, and long-range wireless. The cybersecurity testing evaluated representative examples of each of these classes of remote attack vectors and clearly found it possible to exploit these vectors.

In 2017, the U.S. Department of Transportation's National Highway Safety Administration (NHTSA) took a proactive safety approach to protect vehicles from malicious cyber-attacks and unauthorized access by releasing proposed guidance for improving motor vehicle cybersecurity.[7] To ensure a comprehensive approach to cybersecurity, NHTSA has adopted a multi-faceted research approach that leverages the U.S. National Institute of Standards and Technology Cybersecurity Framework[8] and

[5] http://www.autosec.org/pubs/cars-oakland2010.pdf
[6] http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[7] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
[8] https://www.nist.gov/cyberframework

encourages industry to adopt practices that improve the cybersecurity posture of vehicles.

1.2.1 Telematics

Telematics in the automobile industry refers to the embedded system on board a vehicle that tracks the vehicle and combines wireless telecommunications and information processing to send, receive, and store information related to vehicles. For example, telematics include original equipment installed by the manufacturer, after-market add-on systems, and/or mobile device applications and programs. In addition, telematics involve a variety of applications such as GPS tracking, engine diagnostics, vehicle monitoring and drive identification, in-vehicle recording, and instant driver feedback. As the advancement in vehicle telematics/infotainment systems and integration of numerous technologies in them rapidly grow, the security vulnerabilities in vehicles equipped with telematics/infotainment systems expand exponentially.

In a basic telematics system, vehicles gather and send data on location and vehicle status to a telematics service center that stores the data which can be accessed by the account owners of that data (see Figure 1). Telematics should be thought of and treated as a system, from the vehicle to the on-board telematics devices to the communications cloud to the data management and storage systems.

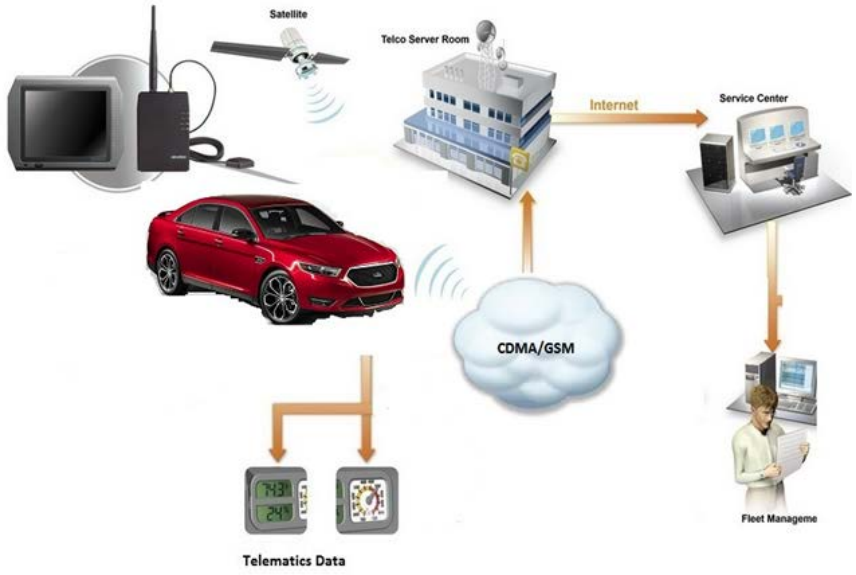

Image credit: Haulage Report Now

Figure 1. Typical Telematics System

The signal path of the data from the telematics device is also an area of concern as it is vulnerable to man-in-the-middle attacks. Cybersecurity penetration testing of after-market telematics devices has uncovered multiple vulnerabilities such as:

- Accepted unauthenticated administrative commands via Short Message Service (SMS)
- Loaded a home-grown trojan firmware
- Unauthenticated services on the Internet

- No encryption of data in transit

Of particular interest to the government fleet community is Executive Order 13693, which states:[9]

> *"If the agency operates a fleet of at least 20 motor vehicles, improve agency fleet and vehicle efficiency and management by … collecting and utilizing as a fleet efficiency management tool, as soon as practicable but not later than 2 years after the date of this order, agency fleet operational data through deployment of vehicle telematics at a vehicle asset level for all new passenger and light duty vehicle acquisitions and for medium duty vehicles where appropriate."*

Since most government fleet vehicles are older models, few, if any, have original equipment manufacturer (OEM) installed telematics, after-market telematics devices must be employed to meet the Executive Order.

From the federal perspective, the telematics system is considered an information system requiring Federal Information Security Management Act (FISMA) compliance. FISMA requires compliance with NIST standards. To help government fleet managers comply with FISMA, the U.S. Department of Transportation's Volpe Center, in cooperation with the U.S. Department of Homeland Security's Science and Technology Cybersecurity Division, created a document entitled *Cybersecurity Primer for Fleet Managers* which identifies 31 security controls for telematics from *Draft NIST 800-53: Security and Privacy Controls for Information Systems and Organizations*[10]. FedRAMP program provides requirements for cloud-based IT, which is relevant for telematics as well.[11]

1.2.2 Controller Area Network (CAN) Bus

The most common embedded network in a vehicle is the Controller Area Network (CAN) bus. All traffic to and from the components on the network is broadcasted simultaneously. Each component "listens" to all message traffic but only acts on messages explicitly addressed to it and ignores all others.

The CAN bus connects almost all of the components responsible for the operation of the vehicle and was originally designed with maintenance in mind. Maintenance personnel focused on the operations, troubleshooting, and fine-tuning of the automobile must have access to the network. This access is provided via an on-board diagnostics (OBD) port located within the cabin of the vehicle, usually under the steering wheel. Starting in 1996 in the United States, and 2001 in Europe, every vehicle is required to contain a standardized common access port to the CAN, such as OBD-II.

Anyone can control the flow of data by sending a data packet to a target electronic control unit (ECU) through the CAN bus. This method of injecting data packets can match any data packet transmitted

[9] Executive Order 13693: Planning for Federal Sustainability in the Next Decade. March 19, 2015. https://www.gpo.gov/fdsys/pkg/FR-2015-03-25/pdf/2015-07016.pdf

[10] National Institute of Standards and Technology. NIST 800-53: Security and Privacy Controls for Information Systems and Organizations. August 2017. https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[11] https://www.fedramp.gov/

across the network, including data packets that control functions like vehicle speed, braking, and steering. Since all CAN data packets are passed unauthenticated across the network, all messages are assumed to be legitimate messages originating from within the vehicle. With an open access port such as the OBD-II, any entity or device with access to that port can influence the vehicle systems on the network. Currently, there are many software and hardware tools that allow a user to broadcast custom CAN messages through the OBD-II port.

One of the greatest dangers with any kind of attack is repeatability. Once an attacker develops an attack, they can publish the attack steps on the web, or produce a "canned" version of the attack. A cursory search of the Internet will illustrate the extensive breadth of information shared and vehicle hacks performed utilizing the OBD-II port and CAN bus. This gives potential actors with less technical expertise the ability to carry out the attack.

Integrating after-market features, often used in fleet management, results in an expansion of the access points into the CAN bus. Many, if not all, of these devices allow external access directly to the vehicle's CAN bus, and, thus, all vehicle components connected to it.

1.3 Cybersecurity Considerations for the Electric Vehicle

In addition to the vulnerabilities present in newer vehicle models, EVs present unique cybersecurity vulnerabilities because of their connections to other infrastructure and communication systems. When an EV refuels, it is physically and electronically connected to and exchanges information with EVSE (see Table 1.). The EVSE is an additional external interface into the internal network of the vehicle and to the electricity grid. While there are standards for the communications between the vehicle and the grid (Appendix A), further work could ensure that EVSE and EV cybersecurity is not compromised.

Information	Description
Customer/vehicle/charger ID	Unique identifying numbers for the user, vehicle, and charging station (may also include charging station location)
Control commands	Commands issued or received by the vehicle or charger
Software/firmware downloads/updates	Software downloaded or uploaded to vehicle or charger to facilitate charging process

Table 1. Typical Data Elements Exchanged Between an EV and Charging Station

Compromised EVs and EVSE could be a potential public safety concern, similar to other compromised vehicles or utility distribution equipment.

Power flow between EVSE and electric vehicles need not (necessarily) flow in only one direction. Vehicle-to-grid (V2G) technology is being studied by DOE, the national labs,[12] and the Energy Sector as a

[12] https://www.anl.gov/energy-systems/group/vehicle-grid-interoperability

way to improve the grid's resiliency, reliability, and flexibility in load management. Future EVs could send electricity from their batteries back into the grid via smart chargers during peak times and also reverse the flow during off-peak hours to charge the EV. [13] Ensuring cybersecurity protections are in place is an important part of utilizing this potential use of EVs.

Compromised EVs could spread malware to the EVSE they connect to. This could then be used to spread malware to other EVs connected to that network should the network architecture not be adequately segmented. The mobility of the EVs then could then be leveraged to "infect" other EVSE and, ultimately, other connected systems. Participants at the technical meeting mentioned that the EVSE could be used as a potential entry point for malware to spread to other systems, networks, and grid components.

In many cases, the EVSEs are connected to building energy management systems (BEMS), the electricity grid, telecommunications networks, and billing systems. Participants discussed at the meeting that due to these connections, EVs and EVSE could potentially be leveraged to cause electricity load management disruptions for buildings or the electric grid. For example, traditionally in the BEMS environment power draw is spread across multiple devices making the instance of rapid cycling of large power demands a rare if not impossible occurrence. The advent of large EVSE systems being integrated into the BEMS environment creates a concentrated system with a relatively large power draw. The accessibility and power draw of an EVSE system is a potential mechanism for disrupting the power of a building, or the electricity distribution service in a specific area. In addition, if the attacker installs persistent malware in the EVSE, the duration of the grid disruption can be extended even further.

Listed below are some potential cybersecurity issues which pertain to EVs:

- **Man-in-the-middle at charging station** - Attacker inserts themselves between the EV and the EVSE leading to possible tracking issues, monetary issues, and other privacy issues
- **Payment fraud** at charging station
    - The charger cycle does not last the full amount of time paid for
    - The charger is spoofed into providing free service
- **Privacy/tracking issues** with using EVSEs linked into Smart Grid
- **Intentional overcharging of batteries** via a cybersecurity attack causing possible severe damage to batteries/EV
- **Intentional discharging of batteries** taking the EV out of service/degrading range
- **Denial of service (DOS) attack at EVSEs** - Taking vehicles out of service if unable to re-charge
- **A malware infected EV** - A vehicular "Typhoid Mary" which passes its malware to other EVs via the EVSE
- **Malware infected EV** that passes onboard malware through an EVSE to the Smart Grid or onboard malware through networked EVSEs
- **Rapid cycling of heavy loads** to the grid through multiple compromised EVSEs in order to cause grid failure

[13] https://www.anl.gov/energy-systems/project/ev-smart-grid-interoperability-center

There has been a body of EVSE security testing research conducted by DOE's Idaho National Laboratory (INL):

- **2014-2015**[14]: INL conducted unbiased and independent EVSE testing for efficiency, reliability research, and cybersecurity posture (i.e. remote compromise, unauthorized access, firmware modifications, potential grid impact) on four (4) pre-production systems delivered by Siemens, Eaton, GE, and Delta. Listed below are some potential cybersecurity issues which pertain to EVs:
    - Software Development mistakes (i.e. implementation of "complex" code on a small embedded device leads to poor decision making)
    - Sanity checking of remote input lacking
    - Processes are executed with extensive privileges (i.e. root)
    - Memory corruption vulnerabilities (i.e. ARM, X86)
    - Poor web application implementation SQL injection, cross-site scripting (XSS), input validation, and insecure credentials
    - Billing and price information were manipulated
    - Remote updating was very poorly implemented
    - Malicious firmware lead to full compromise of all units from one vendor

- **2016-2018**[15]: INL conducted cybersecurity testing on two production Level 2 EVSEs and the testing results were only shared with the vendors. INL also conducted cybersecurity testing on a DC Level-2 Fast Charger (DCFC) with both a CHAdeMO and a SAE J1772-Combo cordset. Cybersecurity testing revealed the following findings:
    - A compromised Plug-In Electric Vehicle (PEV) charge module can infect the DCFC vehicle controllers and local servers and vice versa
    - A compromised PEV is not only a potential safety concern, but it is also a grid network access concern. The biggest potential problem is for a coordinated charging event that causes widespread disruption of the grid
    - The cybersecurity testing identified some unknown issues that need to be resolved (e.g. who owns the EVSEs and network connections, are EVSEs considered part of the Utilities network perimeter, and can Utilities handle increased electrical loads)

In addition, there have been two hacker conferences discussions on EVSE hacking and vulnerabilities. In December 2017, the Chaos Communication Congress (CCC) Conference in Germany featured a talk titled "Charging Infrastructure for Electric Cars: Expansion Instead Of Security."[16] The security researcher probed different components of the EVSE system and found security problems, such as:

- Insecure third-party ID tokens that allow copying personal card data and successfully charging with the copy
- Outdated versions of the OCPP protocol based on HTTP that allow setting up a man-in-the-middle attack by relaying the transaction
- Insecure EVSE USB ports that allow logs and configuration data to be copied to the drive via an empty flash drive which provide access to the login/password for the OCPP server via spoofed token numbers

In 2013, the Hack in-the-Box (HITB) conference in Malaysia, featured a talk titled "Who Can Hack a Plug: Infosec risk of Charging Electric Cars." The security researcher identified potential EVSE vulnerabilities

[14] https://www.energy.gov/sites/prod/files/2014/03/f13/vss096_francfort_2013_o.pdf
[15] https://avt.inl.gov/sites/default/files/pdf/presentations/VSATTOctober2015CANBusOverview.pdf
[16] https://www.v3.co.uk/v3-uk/news/3024499/kaspersky-warning-over-electric-car-charging

based on public information (e.g. vendor web sites):[17]

- Firmware can be extracted to identify eavesdropping points and access encryption keys
- RFID and protocol analysis to determine vulnerabilities
- Short range communications (RS-485) bandwidth and latency limits encryption and makes eavesdropping and man-in-the-middle attacks easier
- RFID short range communication is easy to eavesdrop and costly to patch
- If the same symmetric key is used for all EVSEs and payment cards does not scale and is open to relay and card attacks
- Internet of Things (IoT) protocols and web/mobile control are typically insecure
- Charge station Owners charging configuration and Driver payment methods need to be secured

1.3.1 Stakeholders

There many stakeholders in the EV environment (see Table 2). Section 6 of this document addresses the importance of coordination and harmonization of research and development efforts between stakeholders.

[17] https://conference.hitb.org/hitbsecconf2013ams/materials/D2T2%20-%20Ofer%20Shezaf%20-%20The%20Infosec%20Risks%20of%20Charging%20Electric%20Cars.pdf

Stakeholder Type	Examples	Links to the EV environment
Government agencies	- Departments of Energy (DOE) - Department of Transportation (DOT) - Department of Homeland Security (DHS) - State, local, and international governmental agencies	Vehicle and human safety; protection of critical infrastructure; advanced research on EV and EVSE technologies and cybersecurity
Standards bodies	- Institute of Electrical and Electronics Engineers (IEEE) - National Institute of Standards and Technology (NIST) - Society of Automotive Engineers (SAE) - International Organization of Standardization (ISO) - National Electrical Code (NEC)	Implementation of standards and best practices for safety, security, and interoperability
OEMs and Tier 1 Suppliers	- Automobile manufactures	Design and build safe and reliable EVs
Grid owners	- Regional Transmission Organizations (RTOs)/Independent System Operators (ISOs) - Utilities	Produce and transmit electricity, load balance the grid
Technology suppliers	- EVSE vendors and operators - BEMS suppliers - Information and communications technologies (ICT) - Central Energy Management Systems (CEMS) - Payment systems - DER Vendors	Supply the hardware and software systems that allow the EV environment to operate
Researchers	- Academics - White hat hackers - Independent researchers	Study the EV environment for possible vulnerabilities and mitigations, design the next generation EV environment
EV consumers	- General public - Commercial fleets - Government fleets	End users of EV environment technologies

Table 2. EV and Charging Infrastructure Stakeholders

2 Organizational Structure

Cybersecurity should be incorporated into every stage of electric vehicle and EVSE development. To build secure products and then manage identified vulnerabilities, organizations must have structures and corporate policies that support cybersecurity awareness throughout the design, development, and deployment of their devices and systems.

During the design process, domain architects, engineers, and security personnel should coordinate to create secure systems. Once electric vehicles and EVSE leave the manufacturer's floor, they could be monitored regularly to detect irregular behavior. This can help identify vulnerabilities being exploited. If a vulnerability is identified, that information should be shared with the owner, manufacturer, appropriate Information Sharing and Analysis Center (ISAC), and those who can provide solutions to address the vulnerability in a timely manner.

To accomplish the aforementioned goals, some organizations have created an executive position in the c-suite who is in charge of product and/or information security. This officer's responsibilities may include the following functions:[18]

- **Protect, shield, defend and prevent:** Taking preemptive measures to ensure products and information are proactively secured from cyber threats.
- **Monitor, detect, and hunt:** Identifying irregular activity as it occurs.
- **Respond, recover, and sustain:** Minimizing the impacts of the exploited vulnerability and restoring the system to normal operations.
- **Govern, manage, comply, educate, and manage risk:** Creating a work environment where security is a concern in all parts of operation, rather than an afterthought when an incident occurs.

While an executive who oversees security is an important step for integrating cybersecurity into the core of an organization, it is also necessary to define clear paths of information flow. Quick information sharing between security and engineering teams allows identified problems to be remedied quickly which can prevent vulnerabilities from being widely exploited.

An example scenario that a vehicle manufacture or EVSE vendor could think through:

How would our company respond to a compromised charger, charging system, or EVSE vendor?

Relevant sub-questions may include:

- Could our company simply deny any attempt for a vehicle trying to charge at that vendor's stations?
- How would we communicate the denial of charging ability to vehicle owners and operators?
- What happens internally at our company when making these decisions that could potentially impact the reputation of our company?
- Who would need to be brought in on the decision making process?

By testing how an organization responds to an identified vulnerability, the flow of information can be

[18] https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

mapped out and the process for how information gets to those who need to act can be refined. An efficient information sharing procedure will enable an organization to respond in a timely manner to an identified vulnerability. Threat modelling is another way through which an organization can systematically evaluate, identify, assess and address the security risks and vulnerabilities associated with a process or an application. It is one of the ways to map out the attack surface of the application which can assist personnel in devising effective strategies to mitigate those attacks.

3 Incorporating Cybersecurity into Design

Cybersecurity incorporated into the design of EVs and EV charging infrastructure equipment from the onset reduces product vulnerabilities and risk of exploitation far greater than addressing cybersecurity after a system is deployed. Having cybersecurity protections from the start may help prevent basic attacks and provide a solid foundation for improving security and mitigations within the EV environment in the future.

With each addition of a new system, whether software or hardware related, security should be considered a crucial factor in the system development. Since no platform is protected from all vulnerabilities, a way to safely and securely patch the platform is needed. Developers could also establish a vulnerability disclosure program in case vulnerabilities are discovered after production has begun on the system in order to quickly respond to vulnerabilities before they are exploited.

3.1 Segmentation

Separating and securing key components with in a system is an essential element of secure design. Segmentation can prevent a vulnerability from compromising the whole system, by limiting an attacker's access to a small portion of the system. If the attacker wants to move to another part of the system they would need to find another vulnerability to exploit. The attacker will be unable to move freely throughout the network which will limit the damage caused from an exploit.

Segmentation in EVs is crucial because most of the important operational functions of the vehicle communicate through the CAN bus, which can easily be compromised or misused. ECUs are allowed to communicate freely with vehicle systems by broadcasting messages throughout the CAN bus. These messages reach every component in the vehicle that is connected to the network, even if the message is not intended for that component. The correct component responds if the message was addressed specifically to it. This allows for any compromised ECU within the network to broadcast messages to other ECUs it was not intended to interact with. An example of this behavior would be an attacker gaining access to the vehicle's CAN bus through the infotainment system, then broadcasting a message to the vehicle's headlamps turning on the high beams. Segmentation will prevent unrelated communications between components and systems from reaching each other, such as the infotainment system communicating with critical components in the vehicle. If a component or system needs to send information to another within the network, security checks would need to be in place to authenticate the sender, its receiver, and the message itself.

3.2 Chipsets

The use and integration of newer chipsets (integrated circuits that manage data flows) could improve

cybersecurity within a system. Older chipsets are generally basic and only provide features to carry out the task given, excluding cybersecurity. Newer chipsets provide added resources which can include extensive cybersecurity solutions as well as cybersecurity features built in on the chipset. Sometimes, when a vulnerability is found on an older chipset, it can be mitigated by adding an additional process within the chipset; however, it can be difficult to implement additional processes due to the lack of resources on the chipset.

EVs and EVSEs contain many chipsets to communicate within themselves and with each other. One of the most important chipsets is the chipset responsible for communication between the EVSE and the EV related to charging the vehicle. It is important to protect theses communications because they can provide the charging rate, vehicle identification, and billing information. Whether it's through a chip in the chipset or processes to authenticate and check the communication, chipsets that handle this sensitive information should have security features to keep the data safe.

3.3 Penetration Testing

Penetration testing is an important step when incorporating cybersecurity into a system. Penetration testing is used by the manufacturer/designer to find and exploit vulnerabilities in a system before being released to the public. If a vulnerability is discovered, it shows the developers if the mitigations put in place were effective and where improvements can be made in the system to prevent a future attack. Vulnerabilities could be corrected through a patch if the issue is software related or through a redesign if the hardware contains the vulnerability.

It is best to address cybersecurity during the design phase, when it is easier to make changes with the system. Mitigations for identified vulnerabilities can be incorporated into the system and retested with another penetration test to ensure the issue has been resolved. In order to improve cybersecurity in system design most effectively, penetration testing could be done when designing the system as well as to test systems after they have been patched or redesigned in order to maintain the strongest level of security from cyberattacks. Periodic tests should also be conducted to ensure vulnerabilities weren't missed in previous tests.

Within the EVSE, BEMS, and electrical grid network, penetration testing can help ensure the whole system is more secured against attacks and if each system has an effective mitigation solution. The test could also demonstrate that an exploited system will not have a negative impact on other systems and cause issues that can impact public safety. The results of the test will show a level of competency in the whole system to deal with vulnerabilities and the exploits used against them.

The National Electric Sector Cybersecurity Organization Resource (NESCOR) wrote a guide for penetration testing electrical utilities which can be applicable to both electric vehicles as well as electrical vehicle supply equipment.[19] NESCOR's guide breaks down penetration testing into six major

[19] http://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

segments: Penetration Testing Scope, Architecture Review, Target System Setup, Penetration Tasks, End-to-End Penetration Test Analysis, and Result Interpretation and Reporting.

Penetration Testing Scope determines which part of the system the penetration test should focus on. Architecture Review allows the team performing the penetration test to understand the system and possible vulnerabilities in the system. Target System Setup is setting up the test environment in a non-production system that operates as closely to the production system as possible to provide the most accurate test and results possible. Penetration Tasks is testing of each critical component in the system and can be broken down into four categories: server OS, server application, network communication, and embedded device. End-to-End Penetration Test Analysis is a communication gap analysis throughout the system. Result Interpretation and Reporting is the documentation of vulnerabilities discovered and possible mitigation solutions inside a report for future referencing.

3.4 Vulnerability Assessment

The NESCOR Guide to Vulnerability Assessment for Electric Utility Operations Systems can also help provide guidance in mitigating vulnerabilities found within an EVSE or BEMS.[20] The use of the guide could help ensure that the network, system, and system applications are prepared to deal with attackers. The guide explains the methodology the assessors should follow and how they should analyze, interpret, and report their findings. Like penetration testing, not all possible vulnerabilities will be found, but a vulnerability assessment would help mitigate a possible attack and keep the EVSE or BEMS safe.

3.5 EVSE Cybersecurity Procurement Guidelines

Cybersecurity procurement guidelines specify security requirements for new EVSE systems. These guides will tell buyers what cybersecurity measures to look for in EVs, EVSEs, and other systems related to the EVSE when acquiring them for their own use.

Two guides related to cybersecurity procurement language have already been written, though they are not directly related to EVSE systems. The Department of Homeland Security wrote the *Cyber Security Procurement Language for Control Systems*[21] Guide and the Energy Sector Control Systems Working Group (ESCSWG) wrote the *Cybersecurity Procurement Language for Energy Delivery Systems*[22]. It is recommended that both documents are used to produce procurement language for cybersecurity in EVSE systems as they cover both software and hardware security.

[20] http://smartgrid.epri.com/doc/nescor%20vuln%20scan%2006-26-14.pdf
[21] https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf
[22] https://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

In August 2017, the European Network for Cyber Security (ENCS), Commissioned by ElaadNL developed a document titled *EV Charging Systems Security Requirements*.[23] In addition, an EVSE Threat Assessment for Secure EV Charging Systems (April 2016) and EV Charging Systems Security Architecture (April 2016) documents were developed. These requirements can be used as part of the security requirements when new EVSE server systems are procured or set up.

[23] https://www.elaad.nl/uploads/files/Security_Requirements_Charge_Points_v1.0_april2016.pdf

4 Trust

Electric vehicles and charging infrastructure need a method to ensure secure trusted communication between the EV and EVSE. An essential concept in cybersecurity, trust is when computers prove their identities to each other through the use of applied cryptography. Key aspects of trusted communications include authentication, data integrity, and data secrecy.

- **Authentication** – The sending and receiving parties identities are verified
- **Data integrity** – Data is not able to be altered by a 3rd party during the transmission process
- **Data secrecy** – Data is not able to be read by a 3rd party during the transmission process

EVSEs and the networks that will carry the communications (e.g. demand response, price charging, authentication and authorization) between the EVSE, the utility and other connected devices like CEMS, smart meters, etc. must have a secure trusted end-to-end communications path. If the malware/attacks can be propagated from one node to another node (e.g. EVSE), it will be only a matter of time before all the nodes are compromised. Options to secure these interfaces will be encryption and authentication:

- **Encryption** – In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted
- **Authentication** – For a positive authentication, elements that could be verified include:
    - **Knowledge factors**: Something the user knows (e.g., a password, partial password, pass phrase, or personal identification number (PIN), challenge response, security question)
    - **Ownership factors**: Something the user has (e.g., wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token)
    - **Inherence factors**: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier).

In effect, trusted communication allows two parties, such as a customer and a store, to use an untrusted medium, such as the Internet, for a specific purpose, such as buying or selling goods, without fear that a third party will manipulate their order (violate data integrity) or steal their financial information (violate data secrecy). Currently, there is no consensus on a trusted communication standard for securing communications between electric vehicles and charging infrastructure. However, there are a number of existing standards and technology for securing end to end communications in use today (see Appendix A). Instead of creating a new standard, existing Internet security standards and best practices can be adapted for use in the EV and EVSE domain.

The Internet, and the range of mature security technologies which support it, is one of the best places to look for existing technologies to adapt to electric vehicle charging networks. One common security concept which the internet relies on is the concept of zero-trust, or that the network itself is untrustworthy. This means that communications over that network are secured in an end-to-end

manner (through encryption and/or authentication), and that the end devices themselves are responsible for authenticating, and ensuring integrity and secrecy of their communications. Some of the standards and technologies that enable this are X.509, which defines the format of public key certificates, a common method of authentication, and Transport Layer Security (TLS) which allows the two endpoints to establish a secured session which ensures data integrity and secrecy. TLS enables protocols, such as HTTP, to be run in a secure manner, such as HTTPS. This robust system for exchanging keys, validating identities, and establishing a secure session is the keystone which supports e-commerce, and can be adapted to the electric vehicle charging ecosystem to enable secure communications between any combinations of stakeholders in the industry. The World Wide Web Consortium (W3C) has expressed interest in adapting web protocols and technology for use in the automotive domain and is a potential partner for this effort. In order to use this technology, industry must adopt a trust anchor or root of trust, upon which the rest of chain of trust is derived.

In cryptographic systems with hierarchical structure, a trust anchor is an authoritative entity for which trust is assumed and not derived. For example in X.509 certificates, a "root certificate" is the trust anchor from which the whole chain of trust, and therefore authentication process, is derived. The trust anchor must be in the possession of the trusting party beforehand to make any further certificate path validation possible. Vehicles and charging infrastructure have unique trust challenges related to their physical properties. Unlike personal computers and servers, which are usually kept behind locked doors, charging stations and automobiles are frequently left unattended in public and need periodic maintenance. These properties make secure storage of trust anchors a significant challenge. Both devices need some form of tamper-proof storage for keys and a method to revoke keys which have been compromised. The Society of Automotive Engineers (SAE) is currently in the process of developing *Standard J3101*: *Requirements for Hardware-Protected Security for Ground Vehicle Applications* which addresses the need for hardware-based trust anchors in the car. It is possible to leverage the trust anchors proposed in this standard to address electric vehicles. The Hybrid Communication and Interoperability Task Force has also published the *Technical Information Report J2931/7*: Security for Plug-In Electric Vehicle Communications. The report establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).

5 Ownership and Maintenance

In the EV environment, ownership, maintenance, customization, and repair of hardware and software can be a complex issue. For EVSEs, the multitude of ownership models for charging stations makes it difficult to know who is responsible for physical and software upkeep, especially if the installer, owner, and operator are different entities. For PEVs, repairs can require specially trained personnel due to the high voltages involved in the batteries, and some owners may want to customize the software of their vehicle.

Physical maintenance issues will be relatively easy to detect (e.g. frayed or broken cables, non-functioning displays). The electric current levels associated with EVSE can be harmful if not handled properly, an important consideration for technicians.

Cyber monitoring and anti-tamper hardware, such as an intrusion detection system (IDS) and video surveillance, could be used to detect abnormalities in the operation of the EVSE. When an abnormality has been detected, a software patch needs to be applied. This is often accomplished by remotely applying the patch using a secure over-the-air (OTA) download method. In the event of a catastrophic failure of an EV or EVSE, forensics for analysis requires a means to record the device's data.

Vehicle software updates present another ownership issue. If consumers need to accept or opt into an update, software in the vehicles on the road may not be uniform, even within a certain make and model year, because of time delays in accepting the update. Another issue arises when consumers make modifications to vehicles after they have purchased them. These aftermarket changes to the vehicles may create unique vulnerabilities to those vehicles. While a customer likely voids any warranty with the car manufacturer when this is done, these modified vehicles may not respond the same way to software updates issued by a vehicles manufacturer, leaving identified vulnerabilities in cars. Finally, software issues may be much more difficult to detect, whether the issue is caused by a cyber attack or bug in the vendors update.

6 Coordination

In order to address the unique cybersecurity challenges in electric vehicle cybersecurity, coordination and harmonization among stakeholders is essential. Coordination helps to reduce parallel research efforts, define clear roles and responsibilities for various stakeholder groups, and maximize return on investment for the greater research community. The cross-domain nature of electric vehicle cybersecurity, which bridges two critical infrastructure groups, energy and transportation, places an even greater emphasis on inter-organizational and interdisciplinary approaches to information sharing, research and development activities, standards development, and technology transfer than is seen in other large scale cybersecurity programs.

Coordination efforts can be broken into three major categories: public sector coordination, private sector coordination, and public-private coordination. Public sector coordination involves all stakeholders representing a government entity, including federal agencies, international governments, and state or local governments. Private sector coordination involves stakeholders from the electric and automotive industries, including OEMs, trade associations, and standards bodies. Public-private coordination involves the necessary communication between these two groups.

6.1 Standards Coordination

Standards are the basic building blocks for interconnectivity and interoperability. Even voluntary standards make it easier to develop unambiguous requirements. Without standards (even competing ones) there would be no hope of achieving interoperability within the EV environment. Appendix A contains a brief overview of some of the more technical standards found in the EV environment that address EV and charging infrastructure cybersecurity.

6.2 Public Sector Coordination

Public sector coordination involves stakeholders from all levels of government, from state and local governments, to federal agencies, and to international partners. Each of these public sector organizations have a unique role regarding electric vehicle cybersecurity and the communication and coordination between these organizations is essential.

One of the major challenges in public sector coordination is the lack of a centralized hub for communication between public sector stakeholders, such as: DOE, National Labs, NIST, DOT (i.e. NHTSA, FHWA, FMCSA and the Volpe Center), DHS (Cybersecurity Division), OSTP's National Science and Technology Council (NSTC), and DoD. This lack of coordination results in confusion about stakeholders roles and responsibilities regarding cybersecurity for electric vehicles and the infrastructure on which they depend. Coordination requires dedicated understanding of the complex challenges underpinning electric vehicle cybersecurity and the response effort to those challenges.

It may be beneficial to develop a joint task force across relevant agencies to help support public sector coordination. A coordinating body could help align strategic objectives through:

- Defining, prioritizing, and funding key research gaps in electric vehicle and infrastructure cybersecurity
- Establishing and disseminating industry best practices and standards
- Addressing and defining regulatory and enforcement concerns

6.3 Private Sector Coordination

Private sector coordination involves stakeholders from the electric and automotive industries. Both are mature industries with complex supply chains. Currently, each industry has its own set of industry standards bodies, such as IEEE for electricity and SAE for automotive.

In the automotive domain, original equipment manufacturers (OEMs) integrate components manufactured by Tier 1 suppliers. The OEM then sells the vehicle on the primary market to the primary consumer, which may be an individual or a company with a fleet. After a period of time, the vehicles can be resold on the secondary market, generally to individual consumers. Once a vehicle is sold, there is an entire industry dedicated to aftermarket enhancements, such as up-fits and fleet management technology.

Another challenge in the private sector is that there are a number of nascent businesses which are developing, installing, and maintaining EVSE. Since the EVSE segment of the electric industry is relatively new, they have a limited amount of resources to dedicate to solving EVSE cybersecurity concerns individually. EVSE providers can address this concern by working with existing trade associations, like NEMA, which can leverage resources from its members to establish industry best practices for cybersecurity.

6.4 Public-Private Coordination

Public-private coordination is necessary in order to address electric vehicle and infrastructure cybersecurity concerns both nationally and internationally. Agreeing upon and setting international standards is frequently a time consuming and difficult task. One of the greatest challenges is determining which organizations and government agencies should be a part of the standards making process.

In addition to working together to set standards, government and industry in the automotive and electricity sectors have established their own Information Sharing and Analysis Centers, which are organizations dedicated to sharing and analyzing threat intelligence and vulnerability information with their stakeholders in a timely manner. Below is information on both ISACs:

- **Automotive ISAC**[24] - The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. Members embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators.
- **Electricity ISAC**[25] - The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for, and respond to cyber and physical threats, vulnerabilities and incidents.

One way to close the communications gap between these industries is to leverage organizations which are common to both industries, such as the ISACs, trade associations, and standards bodies. Formal communications between these entities improve response and coordination during a cyber incident and could also help each industry stay aware of cross-sector threats.

[24] www.automotiveisac.com
[25] www.eisac.com

7 Gaps and Conclusions

7.1 Identified Gaps

One of the goals of the EV and EVSE Cybersecurity Technical Meeting was to identify gaps, challenges, and opportunities in cybersecurity R&D around the interdependencies between the transportation, electricity, and communications sectors. This section of the report contains gaps that were identified during the technical meeting and gleaned from discussions with subject matter experts.

7.1.1 EV Charging Infrastructure Lacks Cybersecurity Best Practices

Hundreds of thousands of electric vehicle charging stations currently exist for public and residential charging. EVSEs are a key element in the EV infrastructure; however, their use in the EV environment presents several unique cybersecurity vulnerabilities. EVSEs, particularly DC fast charging stations, could be used as a potential entry point for malware to spread to other systems, networks, and grid components. Compromised EVs and EVSEs not only present potential public safety concerns similar to other compromised vehicles or utility distribution equipment, but are also potential malware vectors to other systems because of the shared connectivity and mobility of EVs. In many cases, an EVSE is connected to a BEMS, the electric grid, telecommunications networks, and back-end billing systems. Using these connections, EVs and EVSEs could be leveraged to cause electricity load management disruptions for buildings or the grid. Corrupted EVSEs could cause damage not only to the EV that is directly connected but also to other EVSEs on the same network. In addition, EVSE have physical security vulnerabilities that can allow attackers access to interior components.

With thousands of EVSEs in service, acting as not only loads but also potentially as distributed energy resources, quick notification of a compromised EVSE is important. It is currently unknown how many manufacturers provide Intrusion Detection System (IDS)[26] monitoring both for technical and financial intrusion events. After an event, forensic data can be used to determine the method of attack which can provide the basis for designing mitigations. It is currently unknown what post event forensic data, if any, manufactures collect for after-event analysis.

Participants stated that in today's environment, purchasing agents who buy EVSEs do not typically specify cybersecurity protections (e.g. secure OTA firmware update capability, authentication) for their EVSE products due to lack of EVSE cybersecurity guidelines for the EVSE acquisitions. In August 2017, the European Network for Cyber Security (ENCS), Commissioned by ElaadNL developed a document titled *EV Charging Systems Security Requirements* which can be leveraged by the US Energy Sector.[27]

Also, another gap mentioned is the EV industry lacks secure software design and development

[26] An Intrusion Detection System is a device or software application that monitors a network or systems for malicious activity or policy violations.

[27] https://www.elaad.nl/uploads/files/Security_Requirements_Charge_Points_v1.0_april2016.pdf

methodology guidance to design and build “secure” EVSE capabilities.

7.1.2 End-to-end EV and Charging Infrastructure Lacks a Trust Model

The connected infrastructure for electric vehicles goes beyond the electric vehicle and electric vehicle supply equipment. Connections to BEMS, smart metering systems, utility billing, and, ultimately, the grid itself are all a part of the EV environment. In this environment, electric vehicles, the charging infrastructure, and other stakeholder groups exchange information which is critical to maintaining interoperability. This information needs to be exchanged in a secure environment to ensure quality and creditability.

There is no consensus on a trusted communication standard for securing communications between the electric vehicle and the charging infrastructure. In the future it is likely that legacy equipment updates and interoperability will also be a concern.

7.1.3 EV/Charging Infrastructure Lacks Cybersecurity Testing

Penetration testing is an important aspect of cybersecurity for any device in development. Today, there is a lack of formal cybersecurity penetration testing and assessment applied to the entire EV environment. Existing EV/EVSE penetration testing has been piecemeal and not necessarily thorough. This lack of formality makes it difficult to design a functional reference security architecture as there is no clear picture of the EV and charging infrastructure’s vulnerabilities.

Participants discussed a number of areas in the EV environment which could benefit from additional and more robust penetration testing between:

- The EV and EVSE
- The EVSE and EVSE networks
- The EVSE and BEMs
- The EVSE and electric utility

Participants stressed that in today’s environment, EVSE and connected networks could be utilized to propagate malware/attacks from one node to another node, leading to potential impacts on grid operations. In addition, participants discussed the possibility that persistent malware could be utilized to increase the duration of the grid disruption. The attacker could take advantage of:

- The inadequate integrity protections for code in the protocol translation module
- The absence of cybersecurity monitoring tools to detect the malicious activity

7.1.4 Wireless Chargers Lack Common Cybersecurity Guidelines

While industry works to develop new types of charging for electric buses, electric trucks, and light passenger EVs, there is no clear guidance on the unique cybersecurity requirements for wireless power transfer (WPT) charging systems specifically.

WPT charging systems utilize an electromagnetic field to transfer energy via electromagnetic induction. A typical wireless charging system consists of a fixed unit, which supplies an alternating electrical field to a fixed induction coil. On-board the vehicle, a second induction coil receives the power from the electrometric field which is converted back into electric current and used to charge the electric vehicle's battery pack. To charge efficiently, the vehicle coil needs to be positioned over the fixed coil within a tolerance of a few inches in the X and Y directions and several inches in the Z direction. To maintain the convenience that wireless charging offers, all communication between the EV and EVSE occurs over-the-air.

WPT charging systems face the same issues as traditional wired charging systems, but because a physical wired connection is not available in a WPT charging system, unique issues need to be considered such as:

- Additional remote attack vector to the EV where a malicious actor could potentially compromise the safety, privacy, or operation of not only charging, but other vehicle functions without physically interacting with the EV.
- Similarly, additional remote attack vector to the EVSE where a malicious actor could compromise the safety, privacy, or operation of not only charging, but other infrastructure functions without physically interacting with the EVSE.
- The physical and cyber security mitigations used for a traditional, wired charging system need to be redesigned because the same threat model does not apply. Two-way communication between the EV and EVSE is exposed to eavesdroppers and vulnerable to denial of service, message injection, and Man-in-the-middle (MITM) over the air. It is harder to detect a remote attack due to lack of physical evidence (e.g. surveillance cameras can be avoided and equipment does not need to be damaged/modified). Critical remote software updates can be sent over the air via the two-way communication either from the EV to the EVSE or from the EVSE to the EV depending on the implementation and deployment needs.
- Different attacker goals including influencing the positional information of the vehicle, dangerously enabling energy transfer when a vehicle isn't present or when a human is between the vehicle and the fixed coil, and eavesdropping on vehicle charge status or payment information need to be considered.

7.1.5 Security of EV Over-the-Air (OTA) Infrastructure Update Capability

EVs and EVSEs have external connectivity, such as:

- Wi-Fi technology to allow for remote power monitoring and control of the charging state of the connected vehicle
- Gateway cellular modems and cell phone applications
- Over-the-air (OTA) firmware update capability,
- Building Energy Management Systems BEMS interfaces

Today's EV infrastructure (i.e. EVSEs, Smart Meters, Advanced Metering Infrastructure-AMI, Demand Energy Response equipment, etc.) currently has or will have OTA firmware and software update (such as

remote flash capabilities) to quickly distribute software changes and security patches.[28] OTA in the context of the EV infrastructure includes distributing new software/firmware, configuration settings, and updating encryption keys. The OTA technology generally is immature and vulnerable to cyber attacks. For example, many of the major IT companies in the world, like Microsoft, Adobe, and Apache have had their OTA repositories attacked.

Participants were uncertain about how secure the update methods for EVSE are and suggested that research is needed to address potential OTA update insecurities. The following are potential vulnerabilities that participants discussed:

- Man-in-the-middle (MITM) attacks outside or inside the EVSE
- Manipulations of EVSE configuration and firmware updates via USB ports. Since this update mechanism is frequently insecure, arbitrary code could be inserted into the EVSE. By this method, an attacker for example can make charging free for all or can steal customers' card numbers to make charges at their cost
- Compromised keys used to sign updates or servers that store these keys
- For EVSEs with OTA upgrade capability for downloading software files, an attacker could make the EVSE download malicious software files
- Attackers could target the EVSE to achieve one or more of the following goals:
    - *Read updates*: Attackers aim to learn the contents of software updates in order to reverse-engineer the EVSE firmware and/or steal intellectual property
    - *Deny functionality*: Attackers try to stop the EVSE from functioning correctly, thus causing the EVSE to fail abnormally, either temporarily or permanently
    - *Control*: Attackers try to modify the EVSE performance and functionality
- Physical access, such as an attacker manually tampering with the EVSE (e.g. ports)
- Firmware updates not digitally signed or encrypted
- Weak or no authentication (e.g. default credentials), authorization or encryption for firmware updates and use of insecure internet protocols

Insecure, legacy equipment will need to be addressed at the same time as new EV equipment is designed to have better and secure OTA capabilities.

There are secure OTA frameworks the sector could investigate or utilize. For example:

- Internet Engineering Task Force (IETF) develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP).[29]
- Uptane is a compromise-resilient software update security system for the automotive industry that was funded by DHS Science and Technology (S&T) Cybersecurity Division (CSD) developed by New York University's Tandon School of Engineering, the University of Michigan's Transportation Research Institute, and the Southwest Research Institute.[30]

[28] For example, ChargePoint (https://www.chargepoint.com/products/commercial/ct4000/) and Siemens (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=BTLV_44824)
[29] https://tools.ietf.org/html/draft-moran-suit-architecture-00
[30] https://ssl.engineering.nyu.edu/papers/kuppusamy_escar_16.pdf

- NEMA Smart Grid Standards Publication SG-AMI 1-2009 - *Requirements for Smart Meter Upgradeability* (December 2016) defines functional and security requirements for the secure Smart Meter/AMI upgrade—both local and remote for industry stakeholders such as regulators, utilities, and vendors.[31]
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (March 2015) describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009.[32]

7.1.6 Commercial EVSE Lack of Common Physical Security Guidelines

There are many differing types of EVSEs each having their own unique properties. Commercial EVSEs are public facing devices which have unique physical security challenges. Unlike personal computers and servers, which are usually kept behind locked doors, commercial charging stations are situated in public areas and are frequently left unattended and open to physical damage. Commercial EVSE equipment is often placed in public places with low to zero security. In such instances, there are windows of opportunity for potential attackers to tamper and damage the EVSE equipment physically.

Intentional physical attacks on EVSEs can occur to gain access to the EVSE's electronics to perform a cyber-based attack, to steal components such as cabling which have a high re-sale value, or to vandalize the equipment.

In addition to intentional attacks, unintentional physical damage to EVSEs can be caused by vehicles striking the EVSE, charging cabling being cut or torn out, and miscellaneous damage to user interfaces located on the EVSE such as displays and payment systems.

Physical damage to commercial EVSEs can result in non-operational units which could have an adverse effect on consumer confidence in EVs in general. Some types of physical damage whether intentional or not, may expose the public to harmful electric current levels.

7.2 Conclusions and Critical Gaps

The EV and charging infrastructure cybersecurity environment is a complex mix of many sectors and stakeholders. The joint DOE/DHS/DOT-Volpe Center EV and Charging Infrastructure Cybersecurity Technical Meeting was a first of its kind to bring together these disparate entities. Through presentations, breakout sessions, and general discussions, participants were able to discuss the issues at hand, identify gaps within the industry, talk about possible solutions, and establish connections between all the different stakeholders in attendance.
As these gaps identified in Section 7.1 illustrate, there are multiple challenges to securing the EV

[31] https://www.nema.org/Standards/Pages/Requirements-for-Smart-Meter-Upgradeability.aspx#download
[32] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7823.pdf

environment. Throughout the technical meeting, participants particularly focused on two of these gaps as critical for DOE and private industry to address:

1. The lack of security and security best practices for EVSE charging infrastructure
2. The lack of an end-to-end trust model for validating communications

There areas are critical because they have potential implications for the entire EV environment. Addressing these critical gaps should help focus and frame coordination between the relevant stakeholders in the energy, transportation and communication sectors.

Security analysis of this large and complex problem is necessary and requires coordinated and collaborative research across the different systems impacted by EVs and EVSE. Several federal agencies and offices (including DOE, DHS, and DOT) and industry are pursuing R&D in this space, with potential for further collaboration with each other and other entities. As transportation, telecommunications, and electricity system become more interconnected and interdependent, it is necessary to take a comprehensive look at the threat space and vulnerabilities and coordinate various efforts to reduce technical and policy gaps and ensure the effectiveness of existing programs.

Appendix A - Electric Vehicle Technical Standards Overview

There are many standards to be found in the EV environment such as those that apply to EVSEs e.g. type of charger (DC or AC), type of charging plug etc. However without standards (even competing ones) there would be no hope of achieving interoperability within the EV environment and the table below contains a brief overview of some of the more technical standards found in the EV environment that could be impacted by EV and charging infrastructure cybersecurity. Standards also make it easier to develop requirements that can be unambiguous.

Standards Body	Standard	Standard Title	Remarks
Deutsches Institut für Normung e.V. (the German Institute for Standardization)- (DIN)	70121:2014-12	Electromobility - Digital communication between a D.C. EV charging station and an electric vehicle for control of D.C. charging in the Combined Charging System	(For DC charging) that has no security but it is communication only from the vehicle to the off-board inverter in the EVSE. This has options for payment and authentication but not widely used.
The Charging Interface Initiative (CharIN e. V.)	Combined Charging System (CCS)1.0	Combined Charging System Specification 1.0	DIN 70121:2014-12 Harmonized with SAE J2847/2
The Charging Interface Initiative (CharIN e. V.)	CCS 2.0	Combined Charging System Specification 2.0 (Mid 2018, introduction)	Retains DIN 70121:2014-12 but adds ISO 15118 ED 1. Has security but is optional.
The Charging Interface Initiative (CharIN e. V.)	CCS 3.0 (Under Development)	Combined Charging System Specification 3.0	Under development to include existing SAE and ISO standards plus updating for more Wireless Power Transfer (WPT) features such as adding more control and communication for vehicles approaching the ground assembly (starting from 10-50 meters out) than currently exist.

			Security will be required (not optional).
Society of Automotive Engineers (SAE)	J2847/2	Communications between Plug-In Vehicles and Off-Board DC Chargers	Establishes requirements and specifications for communication between Plug-in Electric Vehicle (PEV) and the DC Off-board charger.
Society of Automotive Engineers (SAE)	J2931/7	Security for Plug-In Electrical Vehicle Communications	Establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).
Society of Automotive Engineers (SAE)	J2836	Use Cases for Communication Between Plug-in Vehicles and the Utility Grid	Establishes use cases for communication between plug-in electric vehicles and the electric power grid, for energy transfer and other applications.
International Organization for Standardization (ISO)	15118 (ED 2 expected end of 2018)	Road vehicles-Vehicle to grid communications Interface	Specifies the communication between Electric Vehicles (EV), including Battery Electric Vehicles and Plug-In Hybrid Electric Vehicles, and the Electric Vehicle Supply Equipment (EVSE).
IEEE	2030.5 (formally SEP 2.0)	Adoption of Smart Energy Profile 2.0	Defines the mechanisms for exchanging application messages, the exact messages exchanged

			including error messages, and the security features used to protect the application messages.
Underwriters Laboratories	UL2202	Standard for Electric Vehicle (EV) Charging System Equipment	Conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off board and on board chargers
Underwriters Laboratories	UL2231	Standard for Personnel Protection Systems for Electric Vehicle (EV) Supply Circuits	Requirements cover conductive charging system equipment intended to be supplied by a branch circuit of 600 volts or less for recharging the storage batteries in over-the-road electric vehicles (EV). The equipment includes off board and on board chargers
Underwriters Laboratories	UL2251	Standard for Plugs, Receptacles and Couplers for Electric Vehicles	Requirements cover EV plugs, EV receptacles, vehicle inlets, vehicle connectors, and EV breakaway couplings, rated up to 800 amperes and up to 600 volts ac or dc. These devices are intended for use with conductive electric vehicle supply equipment (EVSE), and are intended to facilitate the

			conductive connection from the EVSE to the vehicle.
Underwriters Laboratories	UL2271	Batteries for use in Light Electric Vehicle (LEV) Applications	Requirements cover electrical energy storage assemblies (EESAs) such as battery packs and combination battery pack-electrochemical capacitor assemblies and the subassembly/modules that make up these assemblies for use in light electric-powered vehicles (LEVs) as defined in this standard.
Underwriters Laboratories	UL2594	Electric Vehicle Supply Equipment	Conductive electric vehicle (EV) supply equipment with a primary source voltage of 600 V ac or less, with a frequency of 50 or 60 Hz, and intended to provide ac power to an electric vehicle with an on-board charging unit.
Open Automated Demand Response (ADR) Alliance	Open ADR 2.0	Open ADR 2.0	OpenADR 2.0a and b Profile Specifications provide specific implementation related information in order to build an OpenADR enabled device or system.
Open Charge Alliance (OCA)	OSCP 1.0	Open Smart Charging Protocol	Protocol between charge point management system and energy management system of the site owner or the

			Distribution System Operator's (DSO) system.
North American Electric Reliability Corporation (NERC)	CIP-002-51.a	Cybersecurity-Bulk Electrical System Categorization	Identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.
North American Electric Reliability Corporation (NERC)	CIP-005-5	Cybersecurity-Electronic Security Perimeter(s)	Manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.
NIST	7628	Guidelines for Smart Grid Cybersecurity	Analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related

			characteristics, risks, and vulnerabilities.
NIST	Handbook 44-Section 3.40	Electric Vehicle Fueling Systems (Tentative Code)	Code applies to devices, accessories, and systems used for the measurement of electricity dispensed in vehicle fuel applications wherein a quantity determination or statement of measure is used wholly or partially as a basis for sale or upon which a charge for service is based.
NIST	Handbook 44-Section 5.55	Timing Devices	This code applies to devices used to measure time during which services are being dispensed This code also applies to Electric Vehicle Supply Equipment (EVSE) when used to assess charges for time-based services in addition to those charged for electrical energy.