



Exceptional service in the national interest

Cyberattacks and Defenses for EV Charging

Jay Johnson, Sandia National Laboratories

9th Embedded Security in Cars (escar) USA Conference

Ypsilanti, Michigan

June 15, 2022

SAND2022-XXXX

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





EV Charging Context

DOE public charger estimates:

- 2021: 46,500 chargers available today
- 2030: Demand for 600,000 chargers

\$1T infrastructure law included \$5B for EV charger installations

- Plan: **5-year roll-out of a network of EV chargers** along interstate highways, rural corridors, and underserved or disadvantaged communities
 - Target: **500,000 chargers with one every 50 miles of interstate highway**
 - States have until Aug. 1, 2022 to submit plans for their funding
 - There will be federal interoperability and **cybersecurity requirements** for state installations
 - Question: **what security issues need to be addressed?**

Transportation

Biden administration plan calls for \$5 billion network of electric-vehicle chargers along interstates

Grants included in the infrastructure law will help states build a charging network designed to reach highways in almost every corner of the country

By Ian Duncan

February 10, 2022 | Updated February 10, 2022 at 1:46 p.m. EST

Listen to article 5 min



THE WALL STREET JOURNAL. Subscribe Sign In

Politics

EV Charging Network Will Target Interstate Highways

Money approved by Congress for electric-vehicle chargers should first build out a network on high-use corridors, federal officials say



How the EV Industry Is Trying to Fix Its Charging Bottleneck

Electric-vehicle entrepreneurs are working on the industry's biggest bottleneck: charging infrastructure. Companies are building more chargers, but it may not be enough to make EVs work for people who can't plug in at home. Photo illustration: Carlos Waters/WSJ (Video from 7/6/21)

- <https://www.wsj.com/articles/ev-charging-network-will-target-interstate-highways-11644487200>
- <https://www.washingtonpost.com/transportation/2022/02/10/electric-vehicle-charging/>
- <https://afdc.energy.gov/stations/states>



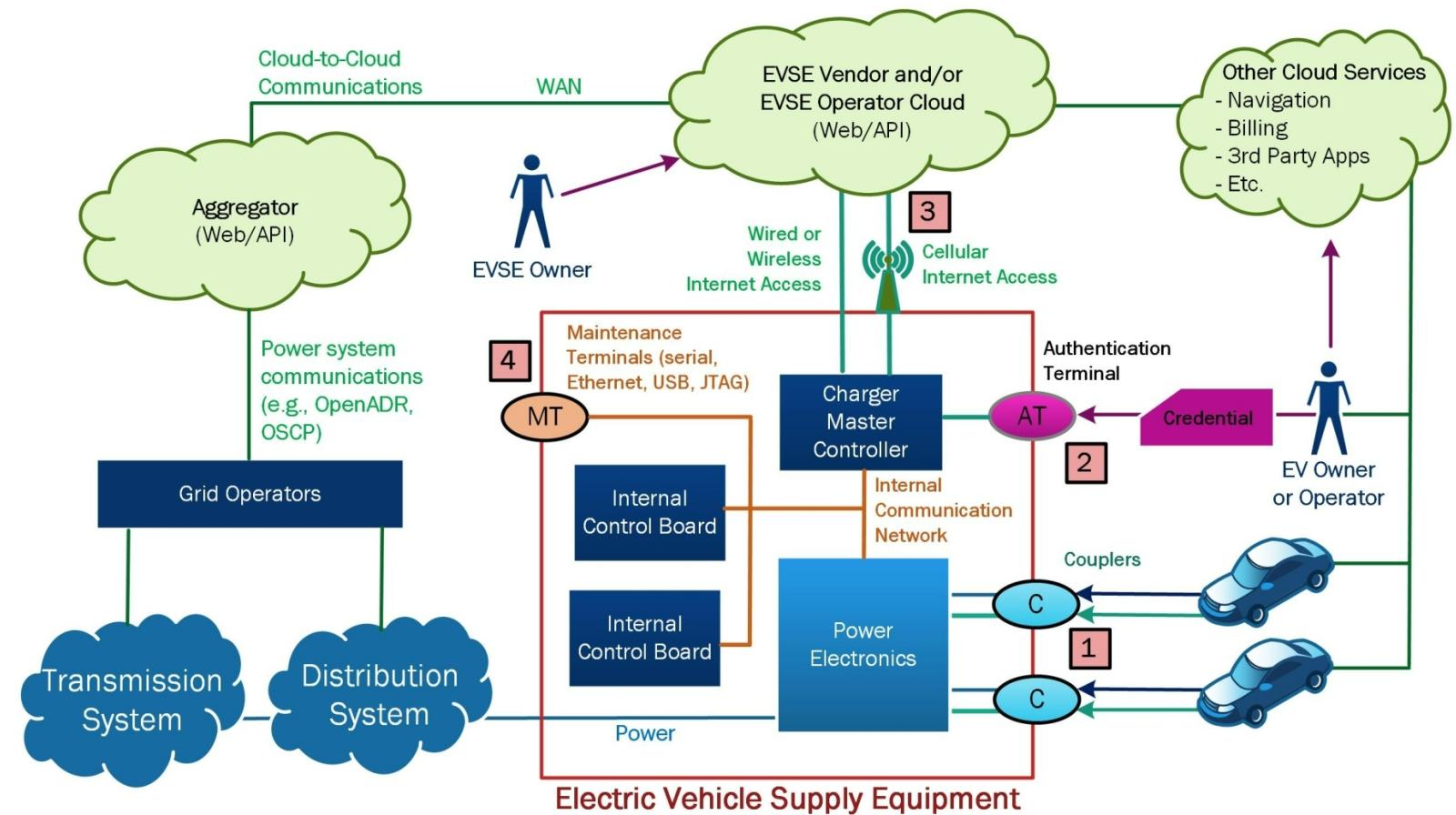
Electric Vehicle Charger Pen Testing Research

- Goal: **Discover and patch EV Supply Equipment (EVSE) vulnerabilities before exploitation**
- Sandia/ANL investigation
 - 8 high power and 4 Level 2 chargers (from 10 companies)
 - 2 backend cloud networks
 - OCPP 1.6
 - ISO 15118-2 PKI requirements
- Results
 - **Vulnerability information was provided to industry partners through secure channels**
 - **Partners addressed many of the findings**, or incorporated changes/mitigations into product roadmaps
- Sandia **surveyed known/published EVSE vulnerabilities and exploits** to understand risks faced by EV charging community



EVSE Cybersecurity Vulnerabilities

- Four interfaces of primary interest
 1. **EV couplers** – CCS, CHAdeMO, etc.
 2. **User terminals** – touch screens, credit card swipes, etc.
 3. **Internet connections** – cellular or wired backhaul networks
 4. **Maintenance terminals** – local debugging and service interfaces (USB, ethernet, etc.)
- **Vulnerabilities exist for each interface**
 - The following slides include a subset of vulnerabilities that may be of interest for the industry

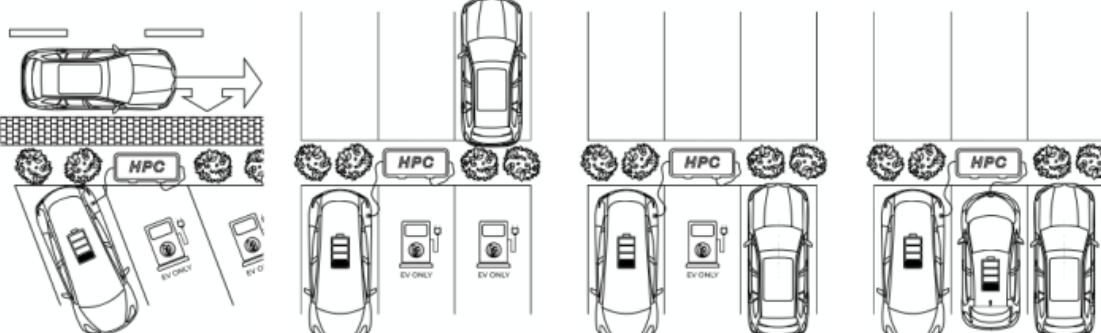


EV Connectors – Losing the Car Keys and Brokenwire

In 2019, University of Oxford showed you could **sniff Personally-Identifiable Information** (i.e., billing information) radiated from CCS charging cables

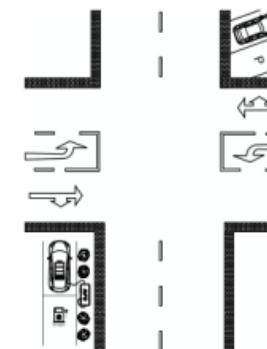
In 2022, the University of Oxford and Armasuisse S+T extended that work to **remotely terminate CCS sessions**.

- Radio frequency (RF) interrupts necessary CCS control communication between the vehicle and charger → **Aborts charge sessions**.
 - Inexpensive software defined radio (SDR)
 - **Less than 1 W of power.**
 - Successful at **distance of 47 m.**



Drive-by attack

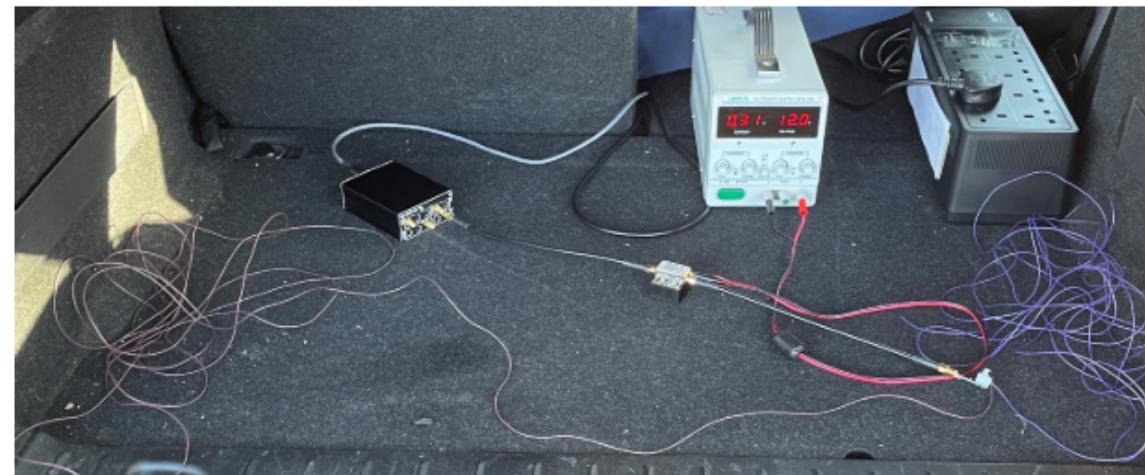
Proximity attacks: car-to-car



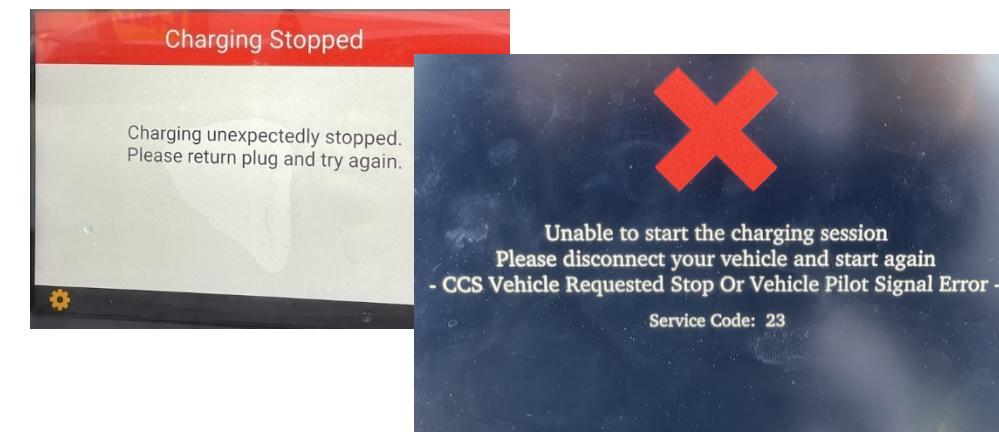
Remote attack



Vulnerability in the Combined Charging System for Electric Vehicles



Equipment for attack, including antennas, SDR, and UPS



<https://www.brokenwire.fail/>
<https://www.usenix.org/conference/usenixsecurity19/presentation/baker>





EV Connectors – Java Log4j/Log4Shell Privilege Escalation

Trend Micro used **CCS comms** to exploit Apache logging package Log4j.

- Log4j vulnerabilities + V2G *Injector* + HomePlug GreenPHY key collection flaws = **escalated access privileges** on simulated EVSE running the RISE-V2G Java stack.
 - Encoded XML payload delivered to EVSE using the Vehicle-to-Grid Transfer Protocol (V2GTP) layer.
- Vehicles also vulnerable to this attack.

LILY HAY NEWMAN SECURITY DEC 10, 2021 2:54 PM

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

Exploits & Vulnerabilities

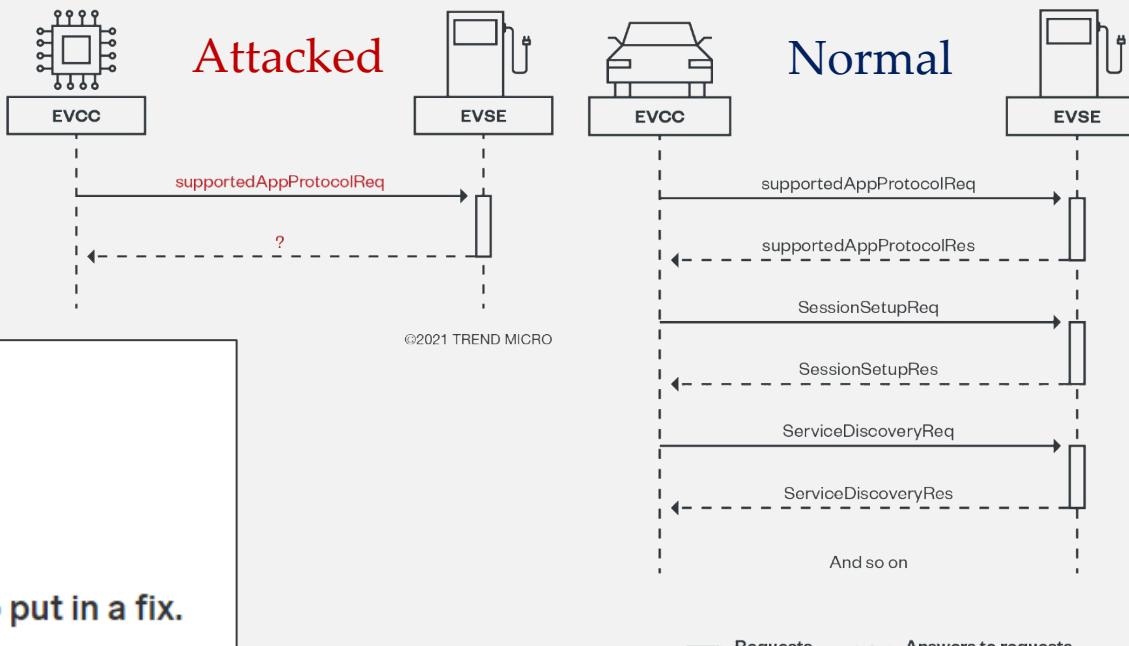
Examining Log4j Vulnerabilities in Connected Cars and Charging Stations

In this entry we look into how Log4j vulnerabilities affect devices or properties embedded in or used for connected cars, specifically chargers, in-vehicle infotainment systems, and digital remotes for opening cars.

By: Sébastien Dudek
December 23, 2021
Read time: 8 min (2288 words)

Subscribe

Attacked



- https://www.trendmicro.com/en_us/research/211/examining-log4j-vulnerabilities-in-connected-cars.html
- <https://www.wired.com/story/log4j-flaw-hacking-internet>



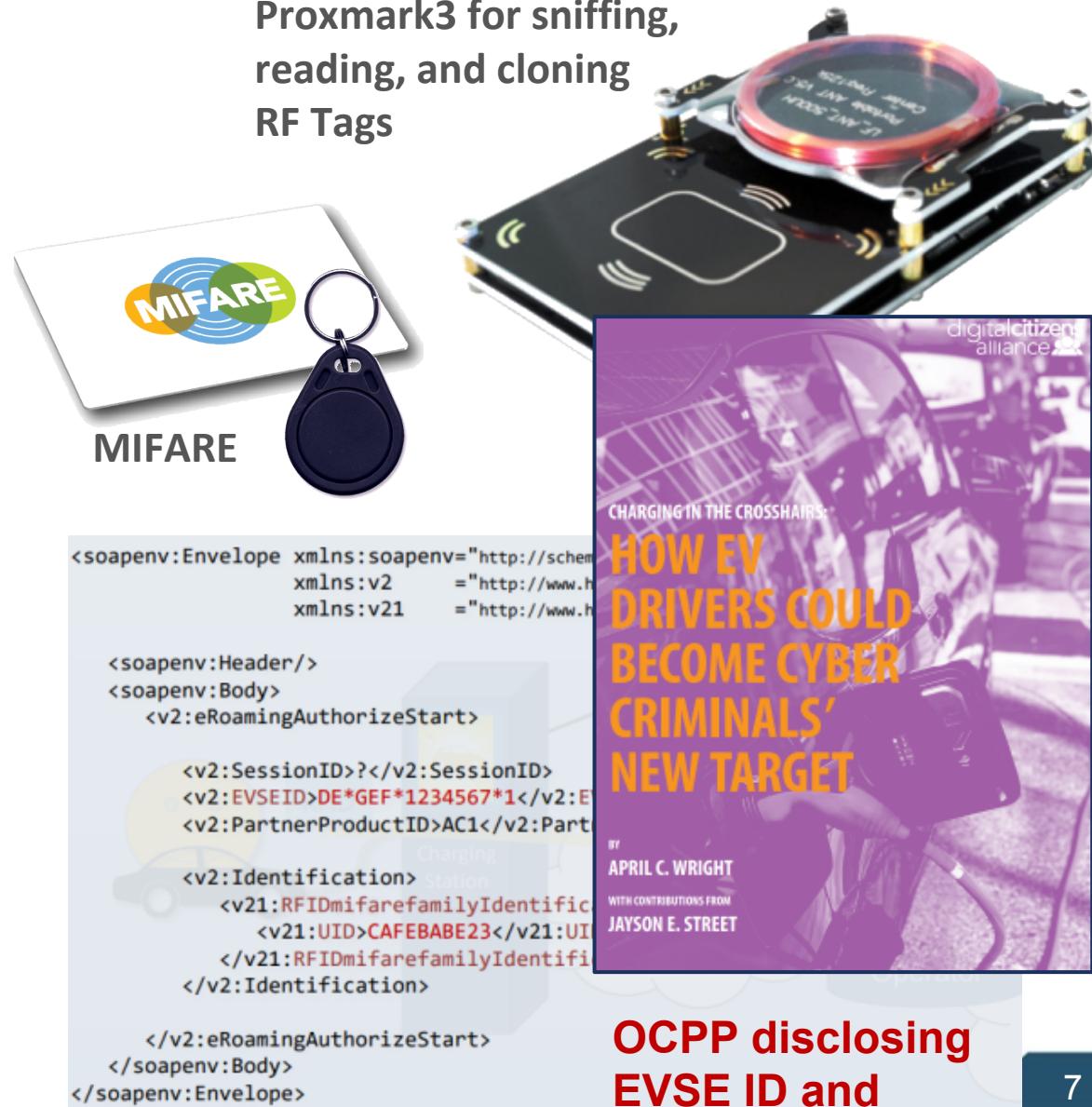
EVSE Operator Interfaces – Authentication Issues

Options for authenticating/billing driver for charging:

- Credit Card
 - Cyber criminals use **skimmers/shimmers** steal card information.
- RFID/MIFARE
 - **Cloning risks** of using RFID tags and MiFare Classic (13.56 MHz contactless smart cards)
 - **Drivers can be tracked** if RFID and Charging Station ID are broadcast (e.g., via unencrypted OCPP 1.6) to e-mobility roaming providers.
- NFC/phones
 - Some **smart phone apps** include **EVSE management and vendor cloud interface vulnerabilities**.
- Plug-and-Charge Functionality
 - Questions raised regarding the ISO 15118-2 **PKI** security implementation.
 - These are being addressed in ISO 15118-20/SAE PKI project.

- M. Dalheimer, "Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit (Charging infrastructure for electric cars: expansion instead of security)" in Proceedings of the 34th Chaos Communication Congress; 2017.
- A. Friedland, "Security and Privacy in the Current E-Mobility Charging Infrastructure. In Proceedings of the DeepSec; 2016.
- A.C. Wright, J.E. Street, "Charging in the Crosshairs: How EV Drivers Could Become Cyber Criminals' New Target; 2019.
- INL, "Cyber Security Research and Development: Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment," 2018.
- Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem, 2019.

Proxmark3 for sniffing,
reading, and cloning
RF Tags



**OCPP disclosing
EVSE ID and**



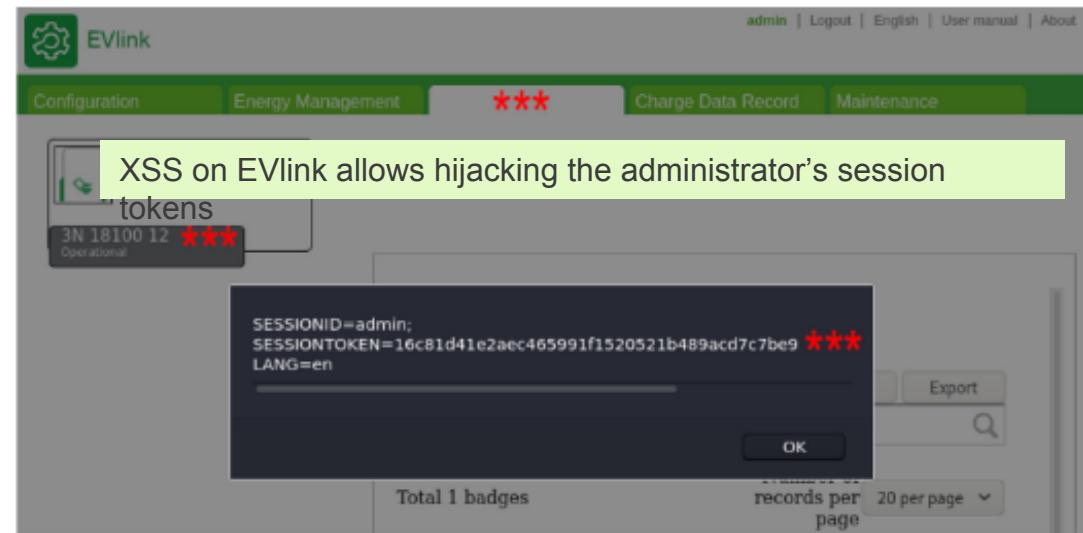
Internet Interfaces – Web

Nasr *et al.* reported multiple **web vulnerabilities** for the Schneider EVlink and other products including:

- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- javascript information exposure

INL found EVSE web vulnerabilities including:

- **Missing authentication** methods such as client-side validation
- **Unencrypted HTTP for logon credentials**
- Unsanitized logon fields vulnerable to **SQL injection** attacks



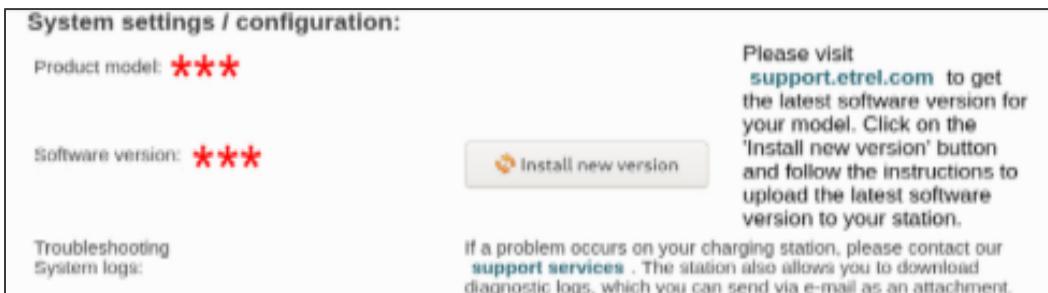
Vulnerabilities in EV Charging Management Systems														
		CVE-ID/Vulnerability												
		79	89	200	306	321	352	425	798	799	918	942	942	1236
Firmware	EVCSMS	Cross-Site Scripting (XSS)	SQL Injection (SQLi)	Information Disclosure	Missing Authentication	Embedded Secrets	Cross-Site Request Forgery (CSRF)	Forced Browsing	Hard-Coded Credentials	Missing Rate Limit	Server-Side Request Forgery (SSRF)	CORS Misconfiguration	FCDP Misconfiguration	CSV Injection (CSVi)
	EVlink	✓		✓			✓	✓	✓	✓	✓			✓
	xChargeln				✓					✓			✓	
	CSWI Etrel	✓			✓				✓		✓		✓	
Mobile	SmartFox													
	Keba				✓									✓
	ChargePoint					✓								
Web	Go					✓								
	EV Connect					✓								
	OASIS Portal	✓					✓							
	Base EVMS		✓											
	Ensto CSI				✓									
	FCBIS												✓	
	ICEMS													
	PiControl	✓					✓							
	Garo CSI													
	Lancelot													



Maintenance/Internet Interfaces – Malicious Firmware Updates

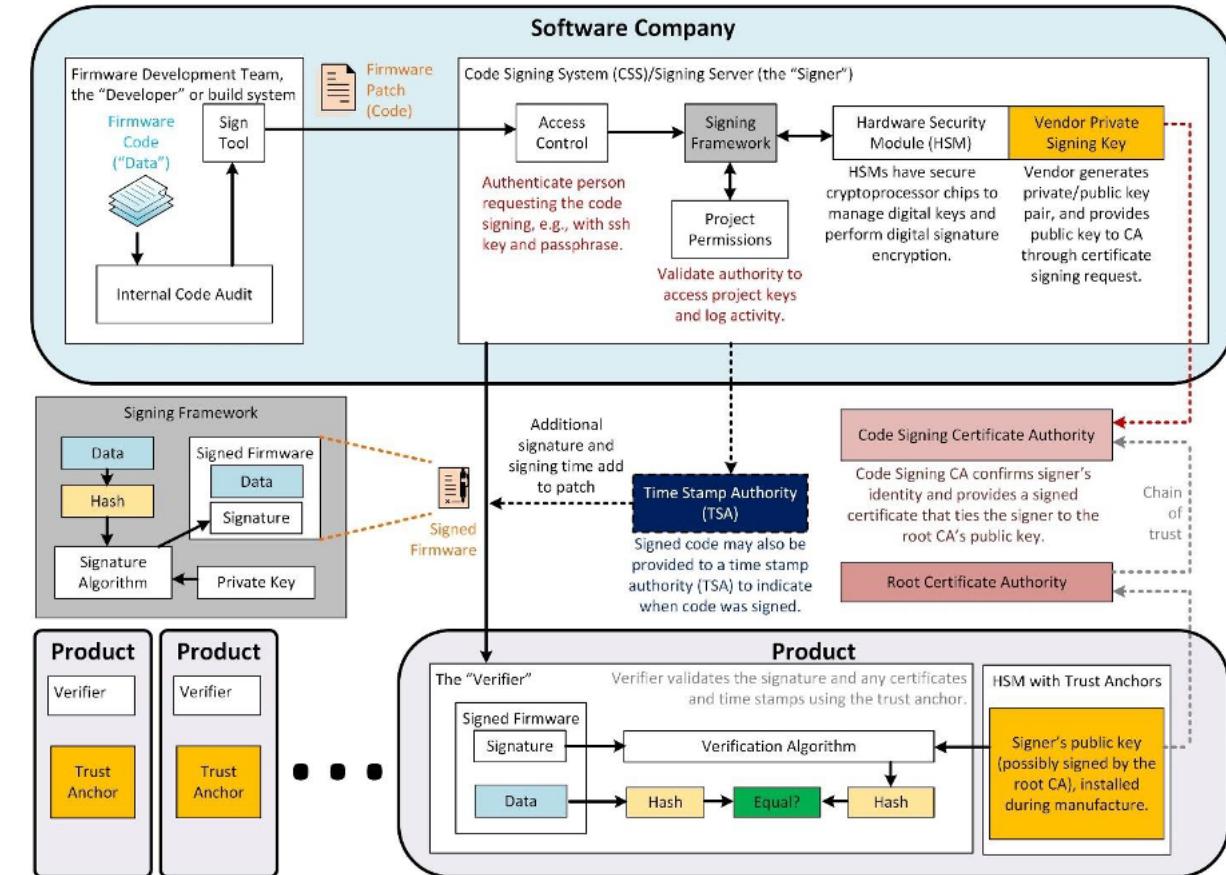
Many examples of **unsigned, unvalidated EV charging firmware**

- INL Case 1: Firmware automatically **updated when USB drive connected**
- INL Case 2: Sniff traffic, steal FTP credentials, compromised server, push out **modified firmware to all EVSE devices**
- Pen Test Partners: platform **without authorization did not require firmware signing**
- Nasr *et al.*: Etrel **firmware downgrade attacks**



Etrel allows attacker with administrator privilege to downgrade the EVSE firmware

- Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment, INL Technical Report INL/MIS-18-45521, May 2018.
- <https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/>
- T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, C. Assi, Computers & Security, Volume 112, 2022.
- J. Johnson, I. Hanke, "Recommendations for Distributed Energy Resource Patching," Sandia Report SAND2021-11150, September 2021.



Example Secure Code Signing Architecture

Malicious Firmware Updates and Supply Chain Vulnerabilities

Russian company, *Gzhelprom*, **outsourced components** in EV chargers to a Ukrainian Company, *Autoenterprise*

- Charging stations installed in 2020 on the M-11 route with backdoor access
- Recently the chargers were **disabled** and **displayed anti-Putin/pro-Ukraine messages**

Hacked electric car charging stations in Russia
display 'Putin is a d*ckhead' and 'glory to Ukraine'

Fred Lambert - Feb. 28th 2022 10:13 am PT @FredericLambert



<https://electrek.co/2022/02/28/hacked-electric-car-charging-stations-russia-displays-putin-dckhead-glory-to-ukraine/>

<https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html>

<https://jalopnik.com/russian-company-outsourced-the-main-components-in-ev-ch-1848603252>



Maintenance and Internal Interfaces

Maintenance interfaces are common on EVSEs, including:

- Serial (e.g., RS485, RS232, serial over USB, etc.)
- Wi-Fi or Ethernet (e.g., SSH, Telnet, HTTP, etc.)
- Bluetooth
- Front panel/screen codes

Fraunhofer found **USB ports that would copy logs and configuration data** including the OCPP server login and password, and **authentication tokens from previous users**.

Pen Test Partners noted issues with **secure storage** and **secure boot**.

Example exploit of eoHUB:

- Step 1: Remove the SD card
- Step 2: Inject root account
- Step 3: Boot device and SSH into system
- Step 4: Exfiltrate/modify anything of value
 - Full source code of device
 - FTP Credentials
 - SMTP Credentials
 - Cloud communication encryption/decryption keys

- https://media.ccc.de/v/34c3-9092-ladeinfrastruktur_fur_elektroautos_ausbau_statt_sicherheit
- <https://usa.kaspersky.com/blog/electric-cars-charging-problems/14357/>
- <https://www.pentestpartners.com/security-blog/owning-a-smart-car-charger-building-a-botnet/>
- <https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/>



```
#### CONSTANTS ####
self.OFFLINE_MODE = False
self.CONFIG_FILE = '/boot/hub.ini'
self.FW_ADDED_CHKSUM = "████████████████████████████████████████████████████████████████" # This charger firmware added the checksum into all packets
self.FILE_KEY = "████████████████████████████████████████████████████████████████" # As string for file encryption
self.CCS_ENC_SECRET_KEY = "████████████████████████████████████████████████████████████████" # CCSys decrypt/encrypt Key
self.EO_FLASH_SYNC_ADDR = "████████████████████████████████████████████████████████████████" # USED TO GLOBALLY TELL UNITS TO RE-SYNC THEIR FLASHING
self.UPDATE_FOLDER = "update" # Folder name for update
self.UPDATE_FILE_NAME = "update" # name of update script
self.CONST_TERM_RESEND = 10 # Seconds until a termination is being resent
self.CONST_TERM_FAILRE = 60 # Seconds till we think there is a problem with this message
self.CONST_TERM_SES_CHECK = 120 # Time until sessions are checked with server
self.CONST_CCS_FTP_SVR = "████████████████████████████████████████████████████████████████" # FTP Address for sending the log files
self.CONST_CCS_FTP_USR = "████████████████████████████████████████████████████████████████" # FTP Username
self.CONST_CCS_FTP_PASS = "████████████████████████████████████████████████████████████████" # FTP Password
self.CONST_CCS_FTP_PORT = 21 # FTP Port
```



PEN TEST PARTNERS



How can we
mitigate these
issues?

EVSE Cybersecurity Recommendations/Guidance/Defenses

NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cybersecurity Best Practices



ElaadNL procurement requirements, test plans, and architecture for EVSEs

Extreme Fast Charging (XFC)
Cybersecurity Threats, Use Cases and Requirements
For Medium and Heavy Duty Electric Vehicles

<https://github.com/nmfta-repo/nmfta-hvcs-xfc/>

July 2019

Prepared for:
National Motor Freight Traffic Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314-1798

Prepared by:
Volpe National Transportation Systems Center
Advanced Vehicle Technology Division
55 Broadway
Cambridge, MA 02142



U.S. Department of Transportation
Volpe Center

NMFTA/Volpe Center EVSE Requirements for medium and heavy duty charging



Sandia EVSE Cybersecurity Best Practices Infographic

PROTECTING TOMORROW: SECURITY RECOMMENDATIONS BASED ON EVSE PENETRATION TESTS



RISK MANAGEMENT

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



ASSET, CHANGE, AND CONFIGURATION MANAGEMENT

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



IDENTITY AND ACCESS MANAGEMENT

- Require individual credentials to log into systems. Do not reuse credentials across different systems.
- Disallow storage of common credentials inside the EVSE enclosure.
- Limit the use of system accounts. If required, this should be limited to one.
- Employ access-control systems that support two-factor authentication.
- Configure internal InfoNIST-compliant password multi-factor authentication to prevent compromised credentials from being used by an attacker.



THREAT AND VULNERABILITY MANAGEMENT

- Establish a threat profile for the types of attacks that are common on EVSE networks and back-end systems to effectively respond.



SITUATIONAL AWARENESS

- Ensure physical security and access logging for test chargers, manufacturing areas, and office spaces.
- Monitor network events and traffic for malicious anomalies. Consider using network-based and host-based intrusion detection systems.



INFORMATION SHARING AND COMMUNICATIONS

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



EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS

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



SUPPLY AND DEPEN- DANCY MANA- GEMENT

- Prepare EVSE for shipment process that includes steps to document the exact when it leaves the facility.
- Perform quality assurance manufacturing step to ensure components are used.
- Hardware is not present.
- Disassemble, inspect, and sample of equipment at partners and locations.
- Add security mechanisms to cryptographic material.
- Track all external library components for newly created and maintain gaps to check against tamper

Recommended Cybersecurity Practices for EV Charging Systems

CYBERSECURITY CONSIDERATIONS

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

CYBERSECURITY IMPACTS

- EVSE providers, grid operators, vehicle manufacturers, and government agencies must understand cyber-attacks targeting EVSE chargers can create both localized and widespread impacts:
 - Local impacts**
 - Theft of PII and financial information
 - Failure to charge vehicle
 - Damage to batteries or other EV components
 - Compromise of EVSE life-safety systems
 - Loss of EVSE service availability
 - Large-scale impacts**
 - Harvesting of PII and financial information
 - Segmentation of entire EVSE charging network
 - Exposure of upstream and partner IT networks
 - Misconfiguration of EVSE creating dangerous or dangerous conditions
 - Loss of consumer confidence in EVSE ecosystem
 - Bulk power system impacts

PREVALENT WEAKNESSES IN ELECTRIC VEHICLE SUPPLY EQUIPMENT

Physical Access

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

System Hardening

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

Network Protection & Monitoring

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

Best Practices

BUSINESS NETWORK & OPERATIONS

- Implement secure coding practices including integrity checks of code repositories and version controlling.
- Use separation of privilege for all EVSE-related operations.
- Ensure cybersecurity best practices like the NIST Cybersecurity Framework are used for internal assessments, cyber hygiene, patching, supply chain and insider threat mitigations, etc.

EVSE SECURITY

- Implement tamper-detection sensors and alarms on EVSE enclosures.
- Prioritize alarms and ensure timely actions on critical log events.
- Encrypt all information storage devices within the EVSE.

EVSE NETWORK

- Use network segmentation and VLANs to isolate EVSE installations.
- Install firewalls and IDSs at key network locations.
- Encrypt all network traffic using a FIPS 140-2 compliant cryptographic module.
- Disable unnecessary services and ports.
- Ensure proper defense in depth by limiting external access to device to only authorized users and devices using access control technologies.

EVSE OPERATIONS

- Validate all network traffic and EV inputs before routing them into the EVSE OT network.
- Utilize secure trust principles such as HSM signing, secure boot, and secure firmware and software to update processes.
- Manufacturers and developers should follow secure software development practices.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

https://www.researchgate.net/publication/344888849_Recommended_Cybersecurity_Practices_for_EV_Charging_Systems



EVSE Cybersecurity Recommendations – Lots more out there!

Organization/Researchers	Cybersecurity Hardening Suggestions, Technologies, or Topics
U.S. DOT Volpe Center, 2019	Collection of XFC requirements: design, logging, cryptography, communication, assurance, hardening, resiliency, secure operation, etc.
Chan and Zhou, 2014	Cyber-physical challenge-response charging authentication
Sandia, 2021	Broad cyber recommendations for business and EVSE network & operations, EVSE physical and logical interfaces, and EVSE ecosystem.
NREL, 2019	Encrypt data-at-rest and data-in-flight, remove external ports, add tamper alarms, and certify cloud services with FedRAMP.
ElaadNL, 2016	Design, cryptography, communications, system hardening, resilience, access control, logging, product lifecycle, governance, assurance.
ElaadNL, 2019	Access control, cryptography, communications, physical/information, operational (backup, logging, vulnerability management) security.
Eekelen <i>et al.</i> , 2014	Recommendations for design, implementation, infrastructure, and incident issues; stronger authentication of customer identity; end-to-end encryption; add data-centric security and publish/subscribe middleware to OSCP
Baker & Martinovic, 2019	Prevent remote sideband CCS data extraction via electromagnetic shielding; improve EVSE key distribution; add new SLAC initialization steps
Chan & Zhou, 2014	Add cyber-physical challenge-response mechanism for J1772 authentication
Vaidya & Mouftah, 2020	Employ ISO 15118 Multimodal and Multi-pass Authentication mechanisms
INL, 2017 and 2018	Deploy intrusion detection systems to allow for logging based on EV security requirements
DigiCert, ChargePoint, and Eonti, 2019	Create certificate policy for all V2G and V2V exchanges, improve certificate revocation policies, create a management requirements, etc.
Fuchs <i>et al.</i> , 2019; Fuchs <i>et al.</i> , 2020	Use Security Modelling (SMod) Protection Profile to define the security functions of the ISO 15118 communication protocol
Lee <i>et al.</i> , 2014	Handshake ISO 15118 with additional security mechanisms, verify message validity, and using a third-party auditor to thwart EV-EVSE collusion
Höfer <i>et al.</i> , 2013	Add protection mechanisms to provide greater privacy in ISO 15118
Bao <i>et al.</i> , 2018	Add clock synchronization, EV On-Board clocks within the EVSE, and mandatory TLS encryption to ISO 15118
Mültin, 2018	Move to PnC identification mechanisms to avoid the insecurity of RFID and other nearfield authorization technologies
Rubio <i>et al.</i> , 2018	Adding ISO 15118 profiles, endpoint security, and role-based access control (RBAC) security mechanisms to OCPP
Van Aubel <i>et al.</i> , 2019	Use extensions to ISO 15118, OCPP, and OCPI to provide secrecy and nonrepudiation at the individual data field level
Vaidya & Mouftah, 2018	Use a role-based access control system on the OCPP Control Center server
INL, 2018	Use TLS, code signing, unique username/password combinations, improve mobile APIs, and securing sessions with a signed certificate
Moroson & Pop, 2017	Neural network trained to detect malicious OCPP traffic
Carlson, 2021	Monitor EV charger operations with intrusion detection framework
Gottumukkala <i>et al.</i> , 2019	Use secure-by-design principals, software security, hardware security, and tamper monitoring and resistance
Ghatikar, 2021	Secure Network Interface Card (S-NIC) with secure boot and tamper resistant technologies
Yang, <i>et al.</i> ; 2011; Liu <i>et al.</i> 2014	Privacy-preserving technologies for V2G applications

There's a vibrant community of
cyber researchers working to
secure EV charging systems!

Research Needs – A Call to Arms!

Interface

Research Areas

1

EV-to-EVSE

- Techniques to **prevent** loss or manipulation of charging communications via **side-channel attacks**.
- Improved authentication and authorization** mechanisms for EV and EVSE equipment, including those established **with PKIs**.

2

EV Operator

- New **privacy-preserving authentication solutions** for EVs and EV operators.
- Improved EVSE credential, data, and **PII storage**.
- Hardened and sanitized local web services**.

3

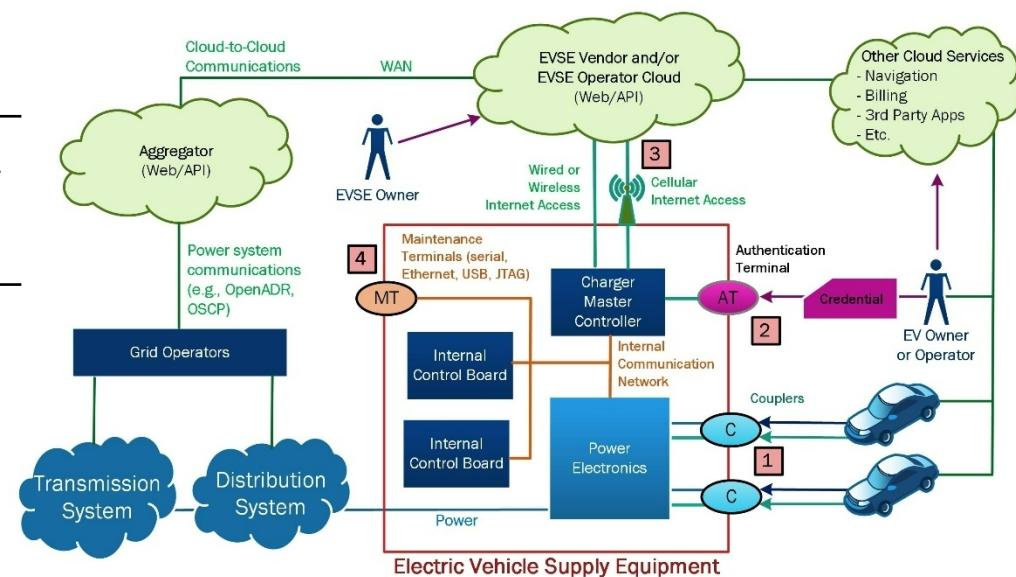
EVSE Internet

- Communication solutions with **end-to-end confidentiality, integrity, authentication, authorization, non-repudiation, and auditing**.
- Novel **EVSE firmware update mechanisms** that account for key/certificate provisioning and storage.
- EVSE network-based intrusion detection and mitigation systems**.
- Cloud, website, and API security solutions** that prevent manipulation or information disclosure with authentication on all endpoint operations.

4

EVSE Maintenance

- Host-based intrusion detection systems** and **tamper-resistant technologies** for physical and logical access.
- Device-level security features**, including secure storage, secure bootloaders, and other software/hardware hardening technologies.





Shameless Plug

Publication covering information from this talk (and lots more!)

- Additional discussion of public EVSE vulnerabilities
- Survey of functional, financial, privacy, safety, and power system impacts from EVSE cyberattacks
- Security suggestions and other defensive solutions

J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," *Energies*, vol. 15, no. 11, p. 3931, May 2022, doi: 10.3390/en15113931.



energies



Review
Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses

Jay Johnson *, Timothy Berg , Benjamin Anderson and Brian Wright

Sandia National Laboratories, Albuquerque, NM 87123, USA; tberg@sandia.gov (T.B.); brander@sandia.gov (B.A.); bjwright@sandia.gov (B.W.)

* Correspondence: johns2@sandia.gov; Tel.: +1-505-284-9586

Abstract
Worldwide growth in electric vehicle use is prompting new installations of private and public electric vehicle supply equipment (EVSE). EVSE devices support the electrification of the transportation industry but also represent a linchpin for power systems and transportation infrastructures. Cybersecurity researchers have recently identified several vulnerabilities that exist in EVSE devices, communications to electric vehicles (EVs), and upstream services, such as EVSE vendor cloud services, third party systems, and grid operators. The potential impact of attacks on these systems stretches from localized, relatively minor effects to long-term national disruptions. Fortunately, there is a strong and expanding collection of information technology (IT) and operational technology (OT) cybersecurity best practices that may be applied to the EVSE environment to secure this equipment. In this paper, we survey publicly disclosed EVSE vulnerabilities, the impact of EV charger cyberattacks, and proposed security protections for EV charging technologies.

Keywords:
cybersecurity; electric vehicle supply equipment (EVSE); electric vehicle (EV); EV chargers; power system security

check for updates

Citation:
Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* **2022**, *15*, 3931. <https://doi.org/10.3390/en15113931>

Academic Editor:
Mario Marchesoni

Received:
10 May 2022

Accepted:
24 May 2022

Published:
26 May 2022

Publisher's Note:
MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

CC BY

Copyright:
© 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Electric vehicle charging is expected to drastically increase in the next decade. Charging points in the EU and UK increased from approximately 34,000 in 2014 to 250,000 in September 2020, and the European Commission has set a target of 1 million charging points by 2025 to curb greenhouse gas emissions [1]. Similarly, the United States experienced a 9.2% quarterly growth rate in public chargers in 2020 Q4 [2] and recently passed the 100,000 public charger mark in March 2021 [3]. In the U.S., a bipartisan infrastructure bill passed in November 2021 in which USD 7.5B was allocated for developing an EV charging network across the country [4]. In addition to the expanding prevalence of electric vehicles and chargers in the passenger vehicle area, there is also an increased adoption of electric vehicles for medium and heavy duty (i.e., freight) applications [5].

Even with growing vehicle battery capacities, users are expecting faster turnarounds at chargers. As a result, chargers are becoming increasingly powerful. Extreme fast charging (XFC) draws 350–400+ kW to provide 200 miles of range in about 15 min [6]. For medium and heavy duty applications ranging from school and city buses to commercial delivery and over-the-road trucks, current designs are supporting more than 1 MW per vehicle [7–9].

Charging providers and users alike seek to optimize their use of the growing network of fast chargers through a variety of highly interconnected and internet-enabled tools. EVSE must communicate with cloud services, EVs and their battery management systems, and much more. For example, EV chargers may be integrated into distributed smart grid EV charging, or interconnected with Building Automation Systems (BAS) or Building Energy Management Systems (BEMS) [10]. On a larger scale, EV chargers are taking a role in smart city technologies to help ensure the sustainability of urban living [11]. Automated and networked connections to grid and microgrid power management and controls round out the picture of the complexity of EVSE connectivity.

Energies **2022**, *15*, 3931. <https://doi.org/10.3390/en15113931>

<https://www.mdpi.com/journal/energies>



Conclusion

Cybersecurity researchers continue to identify EV charger vulnerabilities

- Part of a **continuous process of hardening charging infrastructure** against cyberattacks
- EVSE vendors should have **bug bounty programs** and support **responsible disclosure processes**
- EVSE vendors and 3rd parties should consider adopting **zero-trust principles** in addition to traditional perimeter defenses

Federal and state governments should **seek policies to improve the security of EVSE systems**

- National Electric Vehicle Infrastructure (NEVI) Formula Program adding cybersecurity requirements
- **Similar issues exist for the distributed energy resource (DER) industry** – there is a growing community addressing those issues (e.g., SunSpec/Sandia DER Cybersecurity Workgroup)

Comprehensive national cybersecurity approach must include:

- **Information sharing programs** in conjunction with EVSE/cloud **anomaly/intrusion detection systems**
- **Incident response strategies**, especially for coordinated/widespread attacks on grid infrastructure