irdeto

Whitepaper

Empowering Secure EV Charging

Cyber Defense in Public EVSE Infrastructure

In partnership with PTR

Table of Contents

CONTENTS

1. INTRODUCTION

The transportation sector is rapidly moving towards Electric Vehicles (EVs) due to countries' goals of reducing carbon emissions and phasing out Internal Combustion Engines (ICEs). The rapid growth of EVs and the increasing demand for EV charging infrastructure has led to the development of smart and connected charging stations. These offer a range of benefits, including remote monitoring, real-time data collection and enhanced user experience. However, as with any connected device, they also face a range of cybersecurity threats that could compromise the safety and reliability of the charging network.

This white paper provides a comprehensive overview of the challenges encountered by the public EV charging industry, with an emphasis on Europe and North America. These regions have witnessed substantial growth in EV adoption and charging infrastructure deployment, making them pivotal markets for addressing the need for robust cybersecurity measures. In the realm of Electric Vehicle Supply Equipment (EVSE) cybersecurity, attention is often directed towards public chargers due to their heightened vulnerability to cyber-attacks. These chargers, accessible to a diverse range of users and required to operate in remote, sometimes hostile environments, inherently possess an increased potential for malicious activities. By examining the specific threats and vulnerabilities associated with these charging stations, this paper aims to cultivate an understanding of the criticality of cybersecurity within this rapidly evolving industry.

In the second section of this paper, an overview of the EV charging market and the growing demand for smart and connected charging stations is discussed. This section also explores the benefits and challenges associated with these devices and highlights the importance of cybersecurity in ensuring the safety and reliability of the charging network.

The third section focuses on the types of threats that EV charging stations face, including denial of service, delay/replay attacks and physical security threats. Drawing on examples of EVSE cyber-attacks and vulnerabilities from across the industry, this section highlights the potential impact of these threats on the charging network and outlines the vulnerabilities and weaknesses that can be exploited by attackers.

The fourth section of this whitepaper covers the latest research and development efforts in the field of EVSE cybersecurity, including emerging trends and innovations, efforts by national laboratories, Charge Point Operators (CPOs) and Original Equipment Manufacturers (OEMs), government plans and regulations, as well as standards and protocols in the EVSE industry. The section aims to provide valuable insights into the key trends and developments that are shaping the EVSE cybersecurity landscape.

In the fifth section of the whitepaper, the focus has been put on the relationships between cybersecurity in EVSE and other related industries. More specifically, this section draws comparisons between the cybersecurity concerns and solutions found in the EVSE industry and those found in the EVs and grid industries.

In the final section, this paper concludes with a set of high-level recommendations for mitigating cyber risks in EV charging infrastructure. These recommendations are based on the insights and findings from the preceding sections and are designed to provide practical guidance for policymakers and stakeholders in this field.

In this white paper we use specific terms defined below:

Electric Vehicle	Electric Vehicles (EVs) rely on electric energy stored in onboard battery packs for propulsion and use electric motors as their primary source of power. In this white paper, EVs include both Battery Electric Vehicles (BEVs) and Plug-in Hybrid Electric Vehicles (PHEVs).
e-Passenger Car	Electric-powered passenger vehicles used for the carriage of passengers, typically equipped with no more than eight seats in addition to the driver seat.
e-Bus	Electric-powered passenger vehicles with over eight seats plus a driver or a maximum mass exceeding 3.5 metric tons.
e-Truck	Electric-powered commercial vehicles designed for transporting goods, with a weight exceeding 3.5 tons.
e-LCV	Electric-powered vehicles used for the transportation of goods, with a maximum mass not exceeding 3.5 tons (this category includes Pick-Up trucks).
Charging Point	A charge point connects and charges a single vehicle at a time.
Charging Station/Charger	A charging station is an appliance that can be either fixed to the wall or self-standing and is connected to an electrical supply point. It is designed to provide charging capability for one or more vehicles, depending on the number of charging points it has.
Public Charge Point	A charging infrastructure that is generally available for use by the public. It encompasses a wide range of charging points installed along destination and en-route locations.
Destination Charging	Destination charging refers to the provision of charging infrastructure in locations such as shopping centers, restaurants, public parking garages, shopping malls, cinemas, hotels, resorts, educational institutions, hospitals, metro stations, airports, etc.
En-Route Charging	Includes charging infrastructure located at locations including gas stations, public roads and highways.

2. GROWING DEMAND FOR SMART/CONNECTED EV CHARGERS AND IMMINENT NEED FOR CYBERSECURITY

The rising popularity of EVs has generated substantial demand for EV chargers, creating a notable strain on the electrical grid infrastructure. To connect millions of chargers effectively, utilities are faced with the substantial challenge of investing billions of dollars in grid upgrades and expansions. This issue is being tackled by the implementation of connected/smart chargers, which are equipped with advanced software and communication capabilities. These chargers can interact intelligently with the grid and other devices in the EV ecosystem, allowing for efficient and effective charging.

As smart charging involves network communication and data exchange between EVs, chargers and grid operators, it creates potential vulnerabilities that cyber attackers can exploit. Therefore, as the adoption of smart charging grows, it is important to ensure that cybersecurity measures are put in place to protect the integrity of the EVSE system.

Did you know?

The security researchers from Tencent's Blade Team demonstrated the use of a Raspberry Pi-based tool called "XCharger" to execute a man-in-the-middle attack on the communication between an EV and a charging pile. Their focus was on the security of the communication protocol between the two devices. They developed the XCharger tool using a Raspberry Pi or STM32 microcontroller along with the CANSPY car hacking tool. It allowed them to capture, modify, replay and fuzz data packets exchanged during the communication process.

An attack like this can result in potential financial loss due to weak security in the communication protocol between the EV and the charging pile, affecting the integrity of charging payment system.

Source: www.i.blackhat.com/

2.1 Overview of growth of EVs and smart/connected EV chargers

The increasing demand for environmentally friendly transportation has led to significant growth in the EV market. According to the analysis by PTR, the global EV market is expected to grow at a significant Compound Annual Growth Rate (CAGR) of around 20% between 2022 and 2030. The projected CAGR for e-passenger cars is 18%, while for e-buses it is 22%, e-trucks 50% and for e-Light Commercial Vehicles (e-LCVs) it is 41% [1].

As a result, there has been a rapidly expanding network of charging stations, both public and private. As e-passenger cars are expected to be the most widely adopted type of electric vehicle in the coming decade, public charging stations are likely to be predominantly utilized by them, indicating the need for adequate infrastructure to support the charging needs of these vehicles.

Figure 1 shows the projected growth of the passenger EV market in 2022, 2025 and 2030, which highlights the expected rapid adoption of these vehicles in the coming years. The analysis by PTR indicates that the market for public chargers is expected to grow at a CAGR of over 11%, from 2022-2030 [1]. Furthermore, in 2022, 91% of public chargers were smart chargers and this figure is predicted to increase to 96% by 2030, as shown in Figure 2 [2]. While this growth in the market for EVs and EVSE is promising, it has raised cybersecurity concerns, especially for public smart chargers.

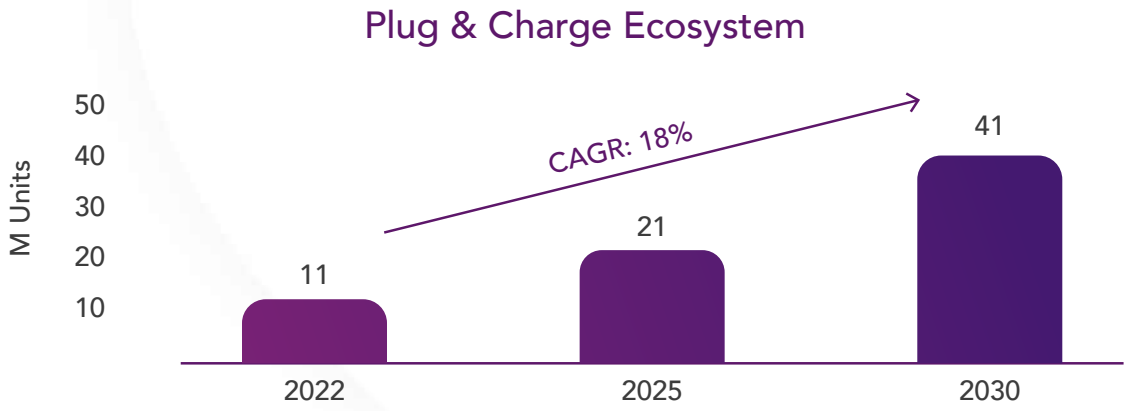


Figure 1: Forecast of global passenger EV annual market (source: PTR)

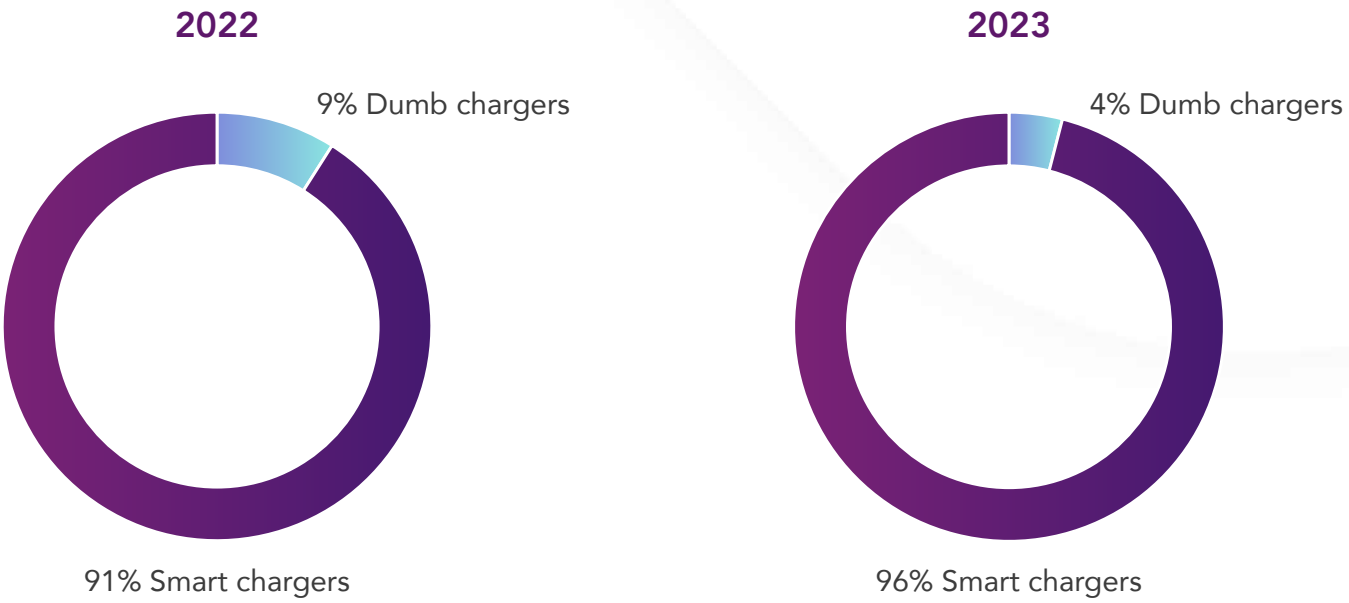


Figure 2: Public smart and dumb chargers' annual market in 2022 and 2030 (source: PTR)

As discussed above, smart electric vehicle chargers play a critical role in promoting grid flexibility and stability. With Vehicle-to-Grid (V2G) capabilities, smart charging can even replace high-demand power generation plants. Smart chargers connect to utilities, grid operators, EV owners and CPOs through a data connection, enabling them to receive and transmit information and control commands as shown in Figure 3. This allows chargers to adjust charging rates based on various factors such as energy availability and time of day, as well as automatically adjust speeds based on grid conditions to avoid grid overload and reduce costs for EV drivers.

The adoption of V2G technology is currently in its early stages and relies heavily on smart EV charging software to manage bi-directional charging and optimize energy usage based on signals from the grid. In addition, V2G systems must be capable of tracking energy flow for accurate billing and payment, and not only charge the EV battery but also enable the vehicle to feed power back into the grid when it's idle. This feature can help to stabilize the grid and create additional revenue streams for EV owners.

With the increasing deployment of EVs and the need for grid operators to enhance the grid's flexibility and resilience, the V2G charger market is expected to grow significantly in the coming years. Already, over 20 EVSE manufacturers offer V2G chargers – and with the new Regulation for the deployment of Alternative Fuels Infrastructure (AFIR) connectivity with backend and the grid will be mandatory for certain types of chargers. According to PTR's analysis, the market size of V2G technology for public chargers was 16 million USD in 2022. It is projected that the V2G market will grow at a CAGR of 51% and is expected to reach a market size of 57 million USD for public chargers in 2030 [1].

In addition to V2G, Plug&Charge (PnC) technology, based on the ISO 15118 standard, plays a pivotal role in simplifying the electric vehicle charging process. By enabling seamless charging through automatic authentication and payment, Plug&Charge enhances user convenience and removes the need for additional steps or physical tokens. However, weak encryption or improper implementation of the authentication process can expose loopholes for attackers to bypass authentication or impersonate legitimate vehicles. Moreover, if the charger's firmware is compromised or if vulnerabilities exist in the firmware update process, malicious actors could gain unauthorized control over the charger or access sensitive data.

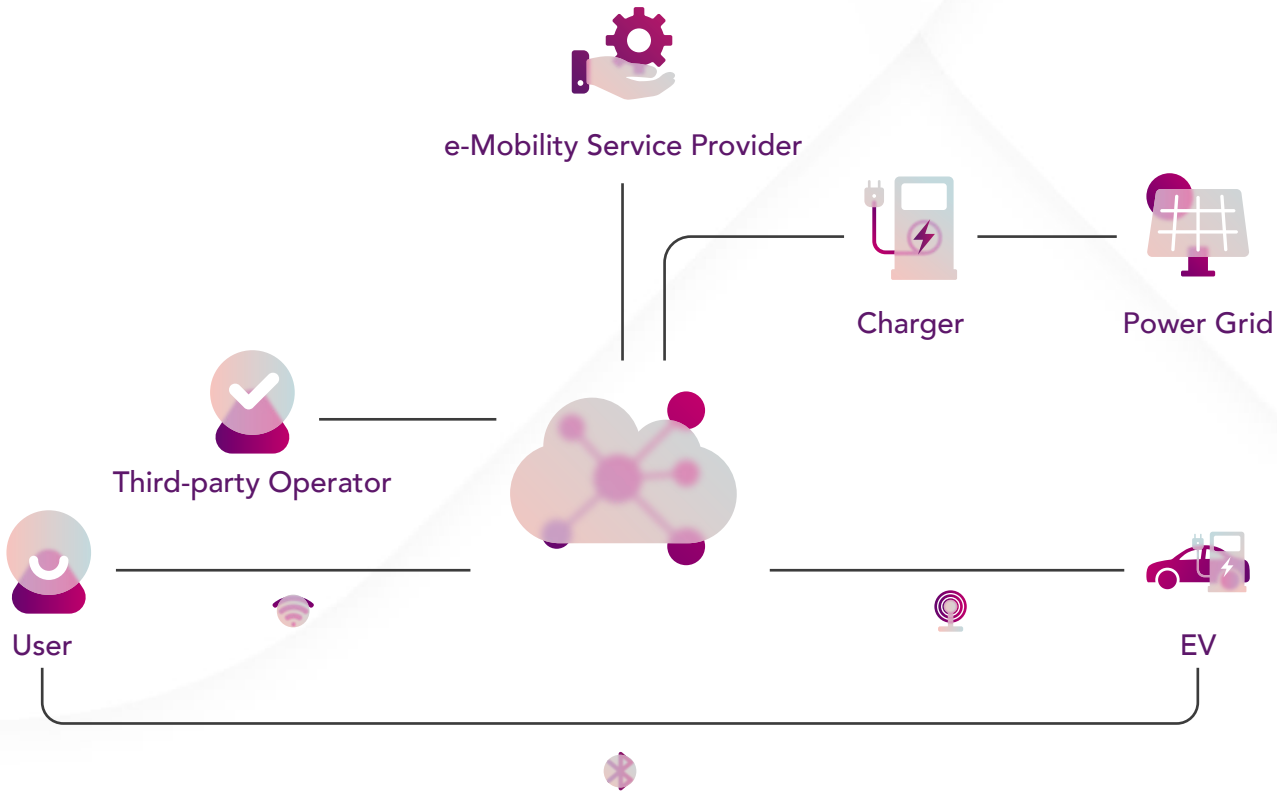


Figure 3: Smart Charger Ecosystem (Source: PTR)

Figure 4 shows the Plug&Charge ecosystem. The EV automaker manages security certificates for the car, including a provisioning certificate installed in the EV. Additionally, an ISO 15118-compliant V2G root certificate is installed in the car. The charging station, connected to a CPO's backend, has its digital certificate, authenticated by a third-party V2G root Public Key Infrastructure (PKI). Both the EV and the charging station have the V2G root certificate installed in their respective communication controllers. Once the EV is purchased, the owner can sign up for charging services with a mobility operator establishing a contractual relationship with the EV owner.

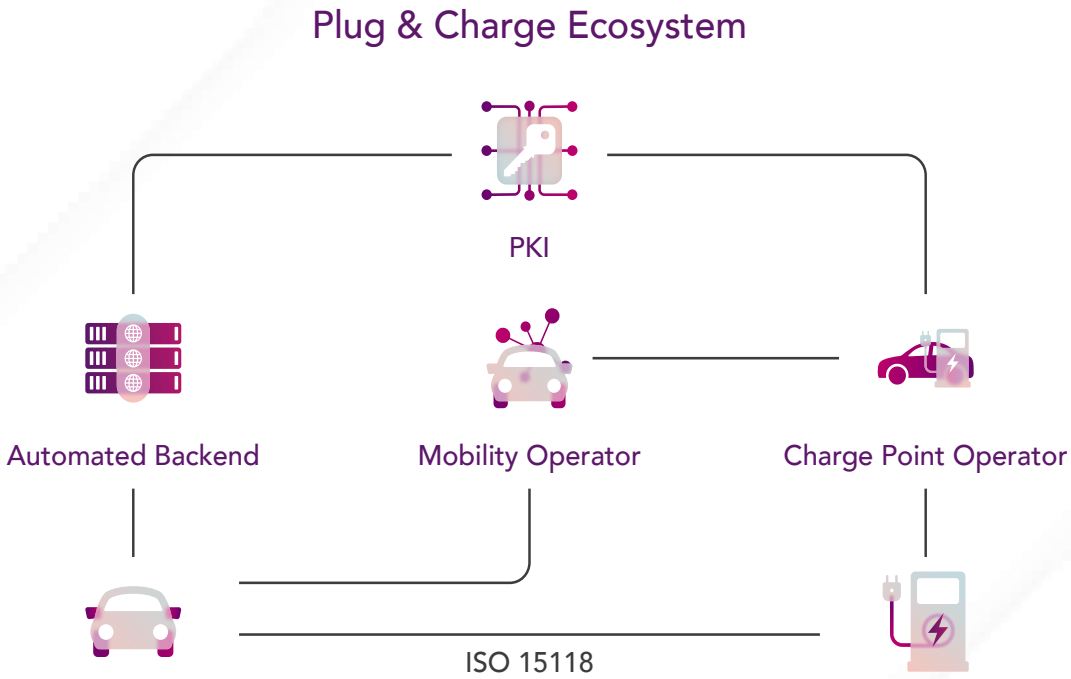


Figure 4: Plug&Charge ecosystem (source: PTR)

The incorporation of advanced algorithms in smart chargers optimizes the charging process, resulting in the most efficient use of available energy, while also allowing for the integration of energy storage systems, increasing the charging infrastructure's flexibility and reliability. However, network communication and data exchange between EVs, chargers and grid operators create potential cybersecurity vulnerabilities that cyber attackers can exploit.

2.2 Bottlenecks faced by different stakeholders in EVSE ecosystem

The EVSE ecosystem involves several stakeholders, including EV manufacturers, charge point operators, utilities and end-users. While the growth of this ecosystem presents several opportunities, it also brings its fair share of challenges. One of the significant challenges faced by stakeholders in the EVSE ecosystem is the intricacy of the regulatory approval process. CPOs must obtain permits from utilities to install charging stations, which can be a time-consuming and challenging process. Additionally, different regions and utilities have varying permit requirements and approval processes, leading to further delays and bottlenecks.

Although certain aspects of EV charging ecosystem are well standardized, another bottleneck faced by stakeholders is the lack of standardization in communication protocols and data exchange formats. This can create interoperability issues between charging stations, EVs and backend systems, as well as increased costs for CPOs. Moreover, the limited availability of charging infrastructure poses a significant inconvenience for EV drivers.

Table 1 shows some of the bottlenecks faced by different stakeholders in the EVSE ecosystem.

Table 1: Bottlenecks faced by stakeholders in EVSE ecosystem

	STAKEHOLDERS			
BOTTLENECKS	**EV manufacturers**	**Charge Point Operators**	**Utilities**	**End-users**
	Raw material availability for battery production	High capital expenditure for setup	Difficulty in demand forecasting for charging	Limited charging station availability and interoperability
	Supply chain issues	Challenges in obtaining permits from utilities for EV charging stations	Additional grid infrastructure investment needed	Charging speed and convenience concerns
	Low uptake of EVs due to limited charging infrastructure availability	Optimizing station utilization and retrofitting chargers in existing infrastructure poses significant challenges	Complex grid integration regulations	High upfront EV cost

Stakeholders in the EVSE ecosystem face several challenges, including limited charging infrastructure, high costs, interoperability and complex regulations. However, as EVs and EVSE become more prevalent, cybersecurity is emerging as a critical issue for chargers.

2.3 Cybersecurity risks and importance in the smart/connected EV charger ecosystem

Smart chargers are advanced charging devices that enable efficient and intelligent management of EV charging. During charging, sensitive information such as billing details, Personal Identifiable Information (PII) and location data may be transmitted. Additionally, the connection between the charging device and the power grid creates a potential target for cyberattacks that could disrupt the power grid or compromise the integrity of the charging process.

Cybersecurity is of paramount importance in the EVSE industry since it involves the integration of software, hardware and networks. A successful cyberattack on an EVSE can compromise the entire network, leading to the theft of personal information, financial loss and damage to the reputation of the CPOs, eMobility Service Providers (eMSPs), OEMs and other parties involved in the EVSE ecosystem. Ensuring cybersecurity in the EVSE industry is pivotal to safeguard the privacy and security of users, maintain the integrity of the charging infrastructure and sustain the growth of the industry.

Did you know?

Engineers at Southwest Research Institute (SwRI) conducted a cybersecurity research project to assess potential threats in EV charging hardware. They successfully disrupted the charging process by reverse-engineering the signals and circuits of an EV and a J1772 charger, a commonly used interface for EV charging in North America. Using a spoofing device (developed in their laboratory), the team manipulated the charging process by limiting the charging rate, blocking battery charging and overcharging. They demonstrated that malicious attacks on charging infrastructure could cause significant disruptions as EV adoption increases.

Source: www.swri.org

2.4 Possible attack vectors in the EVSE ecosystem

The EVSE ecosystem presents several possible attack vectors that malicious actors can exploit to compromise the security of the charging infrastructure. Following are the possible attack vectors in the EVSE ecosystem as depicted in Figure 5, where the arrows visualize the data flow:

- OEM: Cyberattacks on EV chargers' OEMs can result in malware being inserted into software updates for charging points, potentially infecting multiple charging points, including third-party charging stations using the same software.
- EVSE: Hacking a charging station can cause various threats, such as overloading, overheating, physical tampering and vandalism. Attackers can manipulate the charging rate, leading to damage to the EV battery or stealing sensitive information, such as payment details.
- CPMS: The Charge Point Management System (CPMS) is a back-office system that oversees multiple charge points and manages billing, payments and customer support. If hacked, attackers can access sensitive customer information, including names, addresses and payment card data.
- eMSP: Service providers are targets for cyberattacks due to handling sensitive information such as customer names, charging data and payment cards. Successful attacks can result in personal and payment information theft.
- Mobile App: An eMSP's mobile app is a potential target for cyberattacks as it contains sensitive data, including login credentials and charging behavior. Attackers may attempt to steal login credentials, install malware or exploit vulnerabilities to gain unauthorized access.
- Roaming Hub: The roaming hub transmits information between the eMSP and the CPO, making it vulnerable to attacks that can compromise the data transmitted.
- Grid: The Distribution System Operators (DSOs) responsible for the power grid are also a cyberattack surface. Manipulating the grid could alter the loading behavior of multiple charging networks, causing widespread disruption and damage. Attackers can target the grid's communication and control systems to carry out attacks, such as causing a blackout or disrupting the grid's stability.

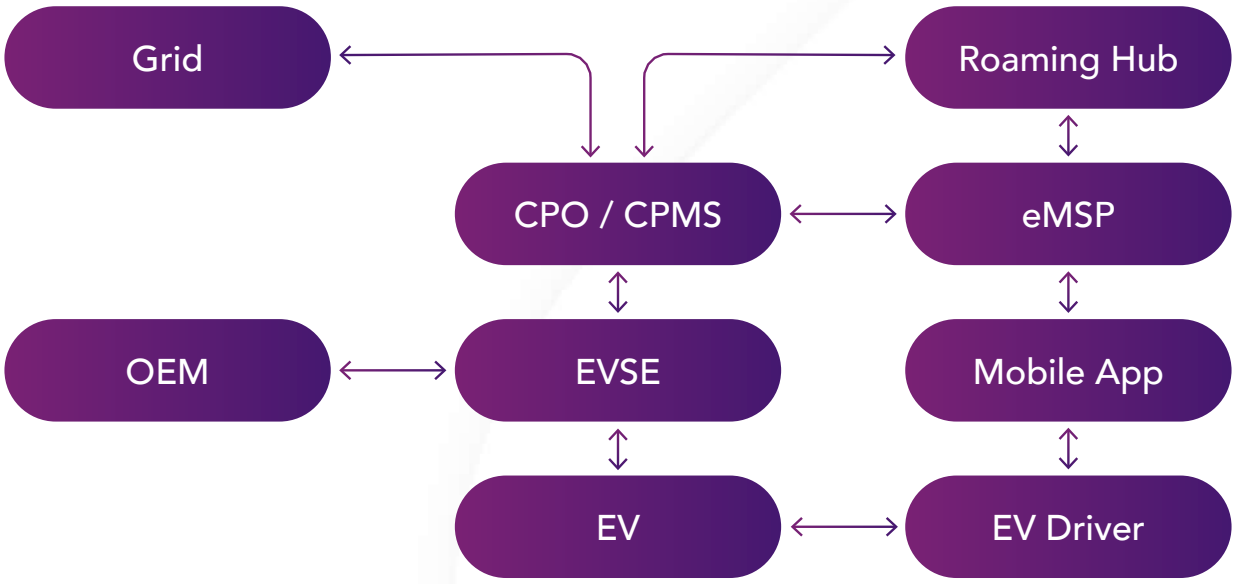


Figure 5: Possible Attack Vectors in EVSE Ecosystem (Source: PTR)

3. TYPES OF THREATS POSED TO EV CHARGING

Vulnerabilities in EV charging pose a potential risk as they can be used to carry out attacks or hinder the detection of attacks. These weaknesses can be evaluated based on the extent of damage caused, the level of skill needed to conduct an attack and the scope of the damage if an attack were to occur.

3.1 EVSE vulnerabilities

Connected infrastructures are susceptible to cyberattacks, which can be motivated by information theft, cyber warfare or organized crime. Risk and threat modeling exercises have highlighted potential vulnerabilities in the EVSE system, which could lead to severe consequences such as data loss, spoofing and denial of service attacks. It is essential to ensure the cybersecurity of interconnected devices and the entities responsible for managing them as these vulnerabilities may emerge from the interface between the charging infrastructure and associated systems.

There are generally two major categories of vulnerabilities that exist: physical attacks and remote attacks. Physical attacks involve physically accessing a system, while remote attacks are carried out over a network or the internet.

3.1.1 Physical access

EVSE enclosures provide insufficient physical protection against unauthorized access and insufficient physical measures to deter and identify intrusions. This can make EV charging systems vulnerable to various types of attacks, including:

- Unauthorized access: EV charging systems lack locks or sensors to prevent access to internal system components, allowing attackers to modify equipment, steal sensitive information or override safety features.
- Tampering: Failure to log or generate an alarm when internal components are accessed can lead to tampering that compromises the safety and reliability of the equipment, making it more susceptible to hacking attempts or malicious attacks.
- Credential theft: Attackers can steal login credentials from EVSE enclosures by exploiting unencrypted storage or finding usernames and passwords, potentially compromising all EVSEs within a provider's network.
- Persistent storage vulnerabilities: EV chargers commonly lack encrypted hard drives, which can be removed, copied and searched for hardcoded credentials or other sensitive information, allowing attackers to extract data.
- Software/firmware vulnerabilities: EV chargers often use bootloaders that do not require digital signatures for updates, making it easier for attackers to insert malicious code into the update package, compromising the EVSE's integrity and security.

- Use of default/system accounts: The use of default or system accounts with common credentials presents a significant weakness in EV chargers, allowing attackers to gain unauthorized access to internal systems and manipulate settings without being detected.
- Network port vulnerabilities: EV charging systems often have unused network ports that are enabled, creating a security vulnerability. Debugging ports are often left enabled in EVSEs even after deployment, allowing attackers to gain access to sensitive information or control the EVSE's functions.

It is crucial to implement robust physical security measures to prevent unauthorized access and deter attacks on EV charging systems. This includes implementing locks, sensors and alarms to monitor access to internal components, as well as encrypting sensitive data and verifying firmware and software updates.

Did you know?

The Brokenwire attack represents a significant advancement in the field of automotive cybersecurity, specifically targeting the widely deployed Combined Charging System (CCS) used for DC rapid charging in EVs. By exploiting the Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, the attack disrupts vital control communication between the EV and the charging infrastructure, causing charging sessions to abruptly terminate.

What sets Brokenwire apart is its wireless execution using electromagnetic interference, enabling attackers to remotely disrupt individual vehicles or entire EV fleets simultaneously. The attack leverages off-the-shelf radio hardware and requires only limited technical expertise, highlighting the urgent need to address the vulnerabilities within CCS and implement effective mitigation strategies to secure the future of EV charging infrastructure.

Source: www.brokenwire.fail

3.1.2. Remote access

Remote access to EVSE is essential for maintenance and troubleshooting, but it poses significant security risks. The following are some of the common security risks associated with remote access to EVSE:

- Default or shared credentials: Use of default or shared credentials can lead to unauthorized access to all EVSEs in the network and make it difficult to revoke access. This can compromise the security of the charging infrastructure and leave it vulnerable to cyberattacks.
- Lack of encryption: Lack of encryption for data at rest or in transit leaves EVSE networks vulnerable to cyberattacks, allowing information to be intercepted or modified. The susceptibility of communication protocols to hacking and cyber threats is a valid concern in the realm of EV charging infrastructure.
- Lack of network security measures: If the EVSE network does not use segmentation Virtual Private Networks (VPNs) or include protection devices such as an Intrusion Detection Systems (IDSs) or firewalls, an attacker who compromises a single EVSE can access the entire EVSE network without being detected. Without IDS in place, malicious actors can infiltrate the system undetected, causing damage and stealing sensitive data.
- Insecure remote access tools: The use of insecure remote access tools can pose a significant security risk. Attackers can exploit the lack of encryption in these tools to gain unauthorized access to the EVSE network and steal sensitive data.

- Neglecting vulnerability scanning and patching: Neglecting regular vulnerability scanning and patching of backend and cloud infrastructure leaves the EVSE network vulnerable to cyberattacks since unpatched vulnerabilities can be exploited to gain unauthorized access or disrupt the system.
- Local log storage: Logs are stored locally on the systems rather than being uploaded to a server for analysis. This allows attackers to perform malicious activities and then delete the related log entries to avoid detection.

To mitigate these security risks, EVSE network owners and operators should deploy comprehensive security measures such as using strong, unique credentials, supporting encryption across all necessary data channels, implementing network security best practices, using secure remote access tools, performing regular vulnerability scanning and patching and storing logs on a server for analysis.

3.2 Examples of EVSE cyber-attacks and vulnerabilities

The EVSE market, despite being at the early stages of its evolution, has already witnessed instances where charging infrastructure has been compromised. These instances serve as important reminders of the challenges that need to be addressed as the EVSE market continues to grow and mature. Following are a few examples of EVSE cyber-attacks and vulnerabilities:

- Shenzhen Growatt Network Vulnerability: In July 2021, a vulnerability in the Shenzhen Growatt network allowed chargers to be locked and unlocked with a predictable serial number and unvalidated username, potentially stopping all charging on the network. [3]
- Schneider Electric Patches 7 Bugs in EVlink Products: In December 2021, Schneider Electric fixed seven vulnerabilities in its EVlink products, including critical and high-severity issues that could have allowed attackers to take control of an operator's account and tamper with the charging process. [4]
- Russian EV Chargers Hacked: In March 2022, several electric car charging stations outside Moscow were hacked, disabling EV owners from charging their vehicles. [5]
- Isle of Wight Council's Electric Vehicle Chargers Hacked: In April 2022, charging points in the Isle of Wight Council's three car parks were hacked, displaying explicit images on the charging screens as users plugged in their vehicles. The council shut down the charging points and launched an investigation. [6]
- Brokenwire: In March 2022, researchers discovered a novel attack called Brokenwire that could be used against the Combined Charging System (CCS), causing charging sessions to abort by interrupting necessary control communication wirelessly from a distance. This attack affects all vehicles that use the CCS protocol. [7]
- ChargePoint App Vulnerability: Kaspersky Lab found that the ChargePoint smartphone application had a website vulnerability that could remotely tamper with a charging session via Wi-Fi, potentially stopping charging sessions or causing overheating, tripping breakers, or fires by increasing the maximum charging current above the circuit rating [8].
- European Union (EU)-Wide Outage: On April 23, 2023, an EU-wide outage occurred within the Ionity network, resulting in widespread disruption of electric vehicle charging services. The exact cause of the outage remains unknown, with initial indications suggesting 'IT issues.' However, considering the possibility of external factors influencing IT systems, it is important to recognize that such incidents can be the result of deliberate actions.

It is imperative for stakeholders across the industry, including EV manufacturers, CPOs and cybersecurity experts, to collaborate and prioritize the development and implementation of effective security measures.

3.3 EVSE security threats and impact

EVSE security attacks disrupt operations and can result in the dysfunctionality of many chargers. By understanding these threats and their impact, appropriate measures can be taken to secure the charging infrastructure, ensuring the safe and reliable operation of EVSE. Following is a list of threats and their definitions:

- Elevation of privilege: Attacker gains unauthorized access to the EV charging station and escalates privileges to manipulate charging sessions, billing systems or access sensitive customer data.
- Spoofing: Attacker impersonates a legitimate user, device or system to gain unauthorized access to a network or system, including impersonating an EV driver or charging station to steal data or manipulate charging data.
- Phishing: Attacker attempts to trick users into revealing sensitive information by posing as a legitimate entity, such as a charge point operator, through fraudulent websites, emails, text messages or social engineering tactics.
- Energy repudiation: Attacker manipulates energy consumption data in EVSE to deny or dispute energy usage or billing charges through false reduction or increase of energy consumption, replaying attacks or generating false records.
- Man-in-the-middle (MitM)/tampering: Attacker intercepts and manipulates communication between the EV charging station and the driver or back-end system to manipulate charging data, steal personal information or take control of the charging station.
- Code injection: Attacker inserts malicious code into the charging infrastructure of the EV to control the system or manipulate charging data by exploiting vulnerabilities, physical access, or intercepting firmware or software updates.
- Delay/replay attack: Attacker intercepts a legitimate communication between a charging station and a device, such as an EV, that is being charged and replays it later, repetitively or delays it to manipulate the charging process, steal personal information or disrupt the normal operation of charging station, leading to grid overload.
- Denial of Service (DoS): Attacker uses flood, distributed, or protocol attacks to disrupt the normal operation of the charging station, prevent EV drivers from accessing charging infrastructure, or cause grid overload, inconvenience, or safety risks.

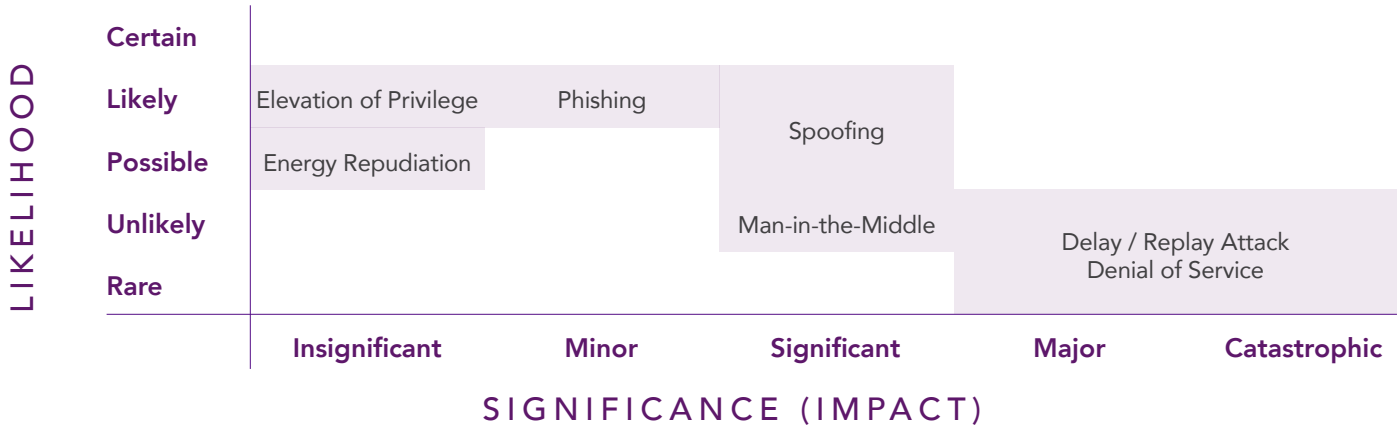
Table 2 presents an assessment of possible cyber threats on EVSE and their associated risk factors, likelihood and security measures. This serves as a comprehensive guide for evaluating and prioritizing potential risks and determining appropriate security measures to mitigate them. Moreover, Figure 6 illustrates how cyber threats are plotted on the Risk Matrix.

Table 2: Assessing the risk: EVSE cyber threats and security measures

Threats	Risk Factor	Likelihood	Security measures
Elevation of Privilege	Low	Medium	Least privilege access, encryption, regular software updates and monitoring and logging
Spoofing	Low	High	Authentication and authorization measures, encryption, network security, identity management, user education
Phishing	Low	High	User education, multi-factor authentication, email and website authentication, monitoring and response
Energy Repudiation	Low	Medium	Authentication and authorization measures, encryption, secure software and firmware updates, monitoring and logging
Man-in-the-middle/ Tampering	Medium	Medium	Authentication and authorization mechanisms, secure communication protocols, firmware and software updates, intrusion detection, tamper-proof hardware, integrity protection
Code Injection	Medium	Medium	Firmware and software updates, tamper-proof hardware, integrity protection, intrusion detection
Delay/Replay Attack	High	Low	Secure communication protocols, time synchronization, data monitoring andlogging, intrusion detection
Denial of Service	High	Low	Load management, network segmentation, intrusion detection and prevention systems, regular security testing and upgrades

The extensive attack surface necessitates end-to-end security across the EV charging ecosystem to ensure the safety of the charging network, personal and payment data and the grid. Also, it is crucial to invest in research and development of new and innovative cybersecurity measures.

Figure 6: Cyber threats mapped onto the risk matrix (source: PTR)



4. RESEARCH AND DEVELOPMENT IN EVSE CYBERSECURITY

Research and Development (R&D) plays a significant role in addressing the cybersecurity concerns within the EVSE market, as it enables the development of innovative solutions and strategies to safeguard charging infrastructure from potential vulnerabilities.

4.1. Emerging trends and innovations

The field of EVSE cybersecurity is rapidly evolving and there are several emerging trends and innovations that are worth noting. Here are a few key areas of research and development that are currently underway:

- Secure communication protocols: As the number of smart EV chargers continues to grow, there is an increasing need for secure communication protocols that can protect against hacking attempts. One emerging trend in this area is the use of blockchain technology to create a secure and decentralized communication network for EV chargers.
- Advanced authentication methods: Traditional password-based authentication methods are often vulnerable to hacking attempts, so researchers are exploring more advanced authentication methods, such as biometric authentication and digital signatures. These methods can help to prevent unauthorized access to EV chargers and protect against cyber-attacks.
- Machine Learning and Artificial Intelligence: Machine learning and Artificial Intelligence are increasingly being used to detect and prevent cyber-attacks on EV chargers. By analyzing large amounts of data, these technologies can identify patterns and anomalies that may indicate a security breach and take action to mitigate the risk.
- Secure firmware updates: Firmware updates are critical for ensuring that EV chargers remain secure and up to date. However, these updates can also be a vulnerability if they are not implemented securely. Researchers are developing new methods for securely updating firmware on EV chargers, such as using encrypted channels and digital signatures.
- Cybersecurity standards and regulations: As the importance of EVSE cybersecurity becomes more widely recognized, there is a growing need for industry-wide cybersecurity standards and regulations. Researchers are working to develop these standards and regulations, which will help to ensure that all EV chargers are designed and built with cybersecurity in mind.

Standardization plays a pivotal role in mitigating the risk of cyber vulnerabilities within the EVSE market. By establishing uniform protocols, specifications and security measures across charging infrastructure, standardization ensures a consistent and robust approach to cybersecurity. With standardized practices in place, the possibility of cyber vulnerabilities is reduced, as potential weaknesses can be identified and addressed systematically, ultimately enhancing the overall security of EVSE systems.

Irdeto is working with a leading CPO to establish baseline security requirements for EVSE testing/validation and certification process. Through these standardized security requirements, it aims to identify and address any vulnerabilities in the software, firmware or network infrastructure promptly. This will help in strengthening the overall cybersecurity posture of charging infrastructure, protecting both the infrastructure and vehicle from potential cyber threats and unauthorized access.

4.2. R&D investment and partnerships: Research labs, CPOs, OEMs

Investment in research and development is critical for improving the cybersecurity of EVSE, and companies and organizations are making significant investments in this area. Labs, CPOs, OEMs, government projects and cybersecurity service providers are all contributing to the advancement of EVSE cybersecurity.

Automakers are developing their proprietary cybersecurity solutions, while others are partnering with cybersecurity firms to integrate advanced security features into their EV charging infrastructure. National labs and research centers are conducting extensive research in the field of EVSE cybersecurity, developing new technologies and protocols to secure EV charging infrastructure and collaborating with industry partners to test and refine their solutions.

The "Securing Vehicle Charging Infrastructure" project is just one example of these efforts. A collaboration between Sandia National Laboratories, Pacific Northwest National Laboratory and Argonne National Laboratory, the project aimed to enhance the cybersecurity of EVSE and develop strategies for mitigating emerging threats [9]. Other institutions, including National Renewable Energy Laboratory, Oak Ridge National Laboratory, Idaho National Laboratory, Concordia cybersecurity researchers, European Commission Joint Research Centre and Electric Power Research Institute, are also making significant contributions to the field of EVSE cybersecurity.

Companies within the industry have invested heavily in research and development to improve the cybersecurity of their chargers. They have developed new technologies and protocols and worked collaboratively with government agencies and industry stakeholders to identify emerging threats and develop effective mitigation strategies.

4.3. Government plans and regulations

Governments have recognized the importance of regulations and guidelines for ensuring the cybersecurity and privacy of electric vehicle charging infrastructure. For instance, the European Union Agency for Cybersecurity (ENISA) has published a set of cybersecurity guidelines recommending the implementation of secure communication protocols, secure firmware updates and security-by-design principles to safeguard networks from cyberattacks [10].

The Cybersecurity Act, which strengthens the ENISA, establishes a certification framework that aims to ensure that products and services are designed and developed with robust cybersecurity measures, including threat modeling, secure coding and security testing, among other things [11]. In response, several plans and projects have been implemented to address this issue. Here are some of these strategies, along with a brief description:

- National Electric Vehicle Infrastructure (NEVI) Plan: The NEVI Plan allocates $5 billion over five years to prioritize EV charging infrastructure cybersecurity and encourage private sector partnerships for publicly available charging stations.
- National Institute of Standards and Technology (NIST): NIST funded a $3.1 million research project on EVSE cybersecurity in partnership with Virginia Tech, Georgia Tech, Utah State University and industry partners, including Ford Motor Co., Qualcomm and Commonwealth Edison Company.
- National Cybersecurity Strategy: Launched by the White House to bolster the US's protection against cyber threats while collaborating with private companies and governments to build a connected network of EV chargers, alternative fuel infrastructure and electric transit fleets.

The Charging Interface Initiative e.V. (CharIN e.V.) is working to promote interoperable and unified charging standards like the Combined Charging System (CCS) and the Megawatt Charging System (MCS) for vehicles of all kinds. CharIN is working in collaboration with Irdeto on the implementation of a Public Key Infrastructure (PKI) to enable Plug and Charge [12].

- ElaadNL and European Network for Cyber Security (ENCS): ElaadNL and ENCS have collaborated on a project related to EVSE cybersecurity. This EV Charging Security project aims to identify potential security risks associated with EVSE and develop new technologies to mitigate these risks. Also, ElaadNL highlighted several criteria for device fortification, including eliminating unnecessary interfaces, securing accounts and implementing physical security measures [13].
- The European Telecommunications Standards Institute (ETSI): ETSI and the NIST are both investing resources in the development of cybersecurity standards for EVSE. These organizations recognize the need to establish industry-wide standards to ensure the security of EVSE infrastructure and protect against potential cybersecurity threats.
- Communications Security Establishment Act (CSE): While threats continue to evolve, the Government of Canada has made cybersecurity a priority. Investments include the passage of the CSE Act, which gave the Communications Security Establishment the ability to better intercept and disrupt foreign threats.
- The Network and Information Security (NIS) 2 Directive: The US Dept. of Energy Vehicle Technologies Office partnered with ABB and other companies for a $2.1 million project to develop a resilient AC input eXtreme Fast Charger that reduces the risk and impact of cyber intrusions.

In addition to these plans, several regulations and acts have been enacted to ensure information security in EV chargers. Following are some of the major regulations and acts that pertain to the security and confidentiality of data, accompanied by a summary of their objectives.

- General Data Protection Regulation (GDPR): The GDPR enables EU citizens to have greater control and protection over their data, which is relevant as personal data is collected through EV charging points. It outlines principles for processing personal data, including obtaining consent before collecting or processing personal data.
- National Security Act, Electronic Communications Act and Regulation: Various laws and regulations, such as the Personal Data Act, National Security Act, Electronic Communications Act and Regulation, Energy Act and Information and Communication Technology (ICT) Regulation, aim to regulate cybersecurity in specific sectors. These laws seek to ensure secure communication, protect personal data, prevent threats to national sovereignty and secure power supply.
- Privacy Act: The Privacy Act permits data processing for public interest purposes and certain criminal offenses. It also allows exemptions for research or statistical purposes and allows seeking injunctions for GDPR or Privacy Act violations. Violations can result in fines and criminal sanctions, except for public sector entities.
- Critical Infrastructure Act: The Critical Infrastructures Act mandates security measures for critical infrastructure in key sectors such as energy, transport, finance and electronic communications. It requires the appointment of a security officer and a mandatory reporting obligation for incidents that pose a threat to the infrastructure's security.
- The Classification Act: The Classification Act of Belgium mandates the classification of data that may pose a threat to national security or interest. It maps security practices to assigned classification levels, including information related to EV charging infrastructure.
- The EU Cybersecurity Act: The EU Cybersecurity Act's emphasis on certification reinforces the importance of robust and trustworthy cybersecurity practices in the European Union, promoting a safer and more resilient digital landscape. It emphasizes the need for risk management, incident response and continuous monitoring to safeguard against cyber threats.

To sum up, the regulations and plans discussed in this section demonstrate the increasing awareness of the importance of cybersecurity in the EVSE. While these regulations have helped establish a baseline for cybersecurity requirements, there is still a need for further regulations to address the ever-evolving cyber threats and vulnerabilities.

4.4. EVSE standards and protocols

The development of EVSE standards and protocols is a crucial step in ensuring the security and reliability of the charging infrastructure. Standardization in the EVSE industry provides a common language and framework for different stakeholders to follow [14].

Figure 7 provides an overview of protocols and standards that enable interoperability and communication between different components. Certain protocols have clear and specific applications, evident from their purpose-driven design, which is represented by solid lines.

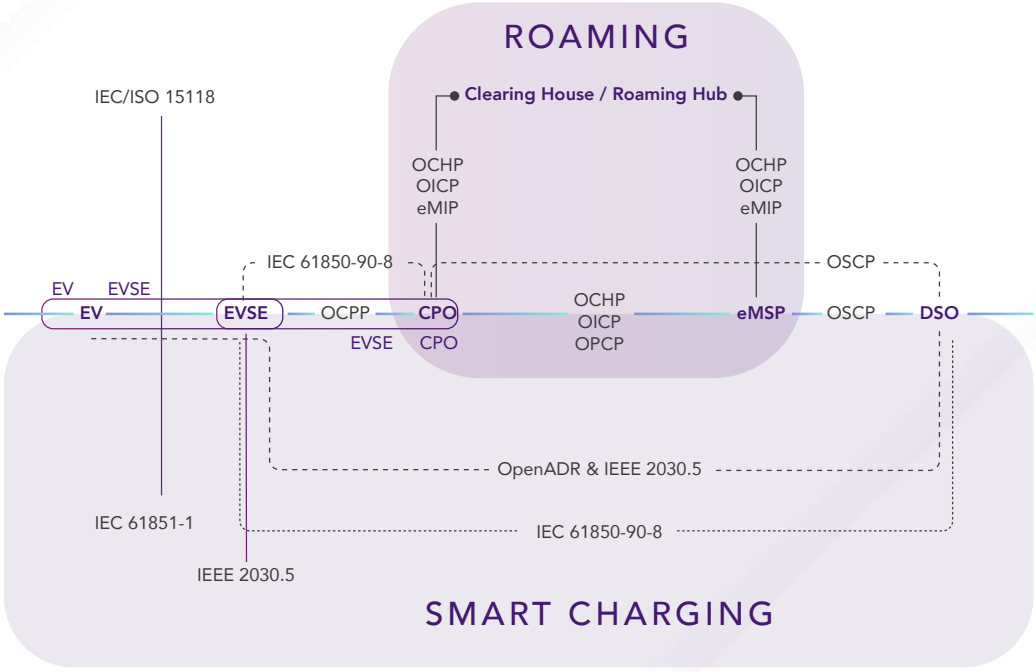


Figure 7: Smart charger ecosystem protocols and standards (source: PTR)

Conversely, protocols like IEEE 2030.5 and OpenADR are more versatile and generic, making them suitable for various stages within the EV market ecosystem. These adaptable protocols are depicted with dotted lines, indicating their potential for use in multiple areas of the EV industry.

One of the important standards is the IEC 61851-1 standard which played a crucial role in facilitating the deployment of EV charging infrastructure around the world. It defines the technical requirements for EVSE and EVs to ensure interoperability between different charging stations and EVs.

In addition to the standards, a range of protocols and technologies are used to secure EVSEs, such as Transport Layer Security (TLS) encryption, PKI certificates and secure boot mechanisms. These measures are implemented to safeguard against common cybersecurity threats such as unauthorized access, malware and denial of service attacks.

Open Charge Point Protocol (OCPP) is a widely used communication protocol in the EVSE industry that enables interoperability between different charging station manufacturers and network operators. OCPP provides a standardized set of messages that facilitate communication between charging stations and back-end systems, enabling charging sessions to be monitored and controlled remotely.

Starndards/Protocols	Details
ISO 15118	ISO 15118 is for the communication protocol between EVs and charging stations. It enables instant authorization at linked charging stations through its Plug&Charge feature, with charging stations ensuring encryption and authentication to comply with the standard.
ISO 15118-2	ISO 15118-2:2014 provides details on the communication between EV and EVSE for energy transfer, including detection and IP-based communication.
ISO 15118-20	ISO 15118-20 is an extension that adds support for wireless power transfer and defines components for automatic connection and disconnection processes for conductive energy transfer, with second generation network and application layer requirements specified.
IEC 61850-90-8	IEC 61850-90-8 defines a communication protocol for the integration of EVSE with the electrical grid. It provides the framework for communication between the grid and EVSE for control and monitoring purposes, including the requirements for cybersecurity.
IEC 61851-1	IEC 61851-1 defines the general requirements for conductive charging of electric vehicles. It specifies the characteristics of the charging process and the connectors used for EV charging. The purpose of IEC 61851-1 is to ensure that EVs can be charged safely and efficiently from any compatible charging station, regardless of the manufacturer or location.
IEEE 2030.5	This standard is a suite of communication protocols to connect and directly control devices. It enables secure and reliable communication and data exchange, supporting advanced energy management functions like demand response, voltage control and energy storage management.
OCPP	OCPP is a protocol for communication between EV charging stations and a central management system. It provides interoperability and flexibility for charging infrastructure and is used by manufacturers, software providers and network operators. OCPP offers cost optimization, risk mitigation and support for EV driver access. The latest version, OCPP 2.0.1, includes advanced features for device management, transaction handling, security, smart charging and extensibility.
OCHP	The Open Clearing House Protocol (OCHP) is an open-source protocol that simplifies communication between a charging management system and a clearing house system/roaming hub. This protocol facilitates e-roaming, enabling limitless electric vehicle charging across charging station networks. eMobility service providers can use OCHP to connect with EV charging operators and providers, providing access to their network.
eMIP	eMobility Interoperation Protocol (eMIP) enables charging service roaming through charge authorization and data clearinghouse Application Programming Interfaces (APIs), along with access to a comprehensive charging point database.

OCPI	The Open Charge Point Interface (OCPI) is an interface that facilitates the exchange of charge point information between operators and service providers, enabling automated and scalable EV roaming.
OpenADR	Open Automated Demand Response (OpenADR) is a secure protocol that enables automated demand response and communication between utilities, energy management systems and distribution system operators. It standardizes demand response and distributed energy resource communications, streamlines energy management for customers and helps balance energy demand during peak times. The latest version is OpenADR 2.0.
OSCP	Open Smart Charging Protocol (OSCP) is an open communication protocol between a charge point management system and an energy management system, allowing real-time prediction of grid capacity to enable capacity-based smart charging of EVs.
OICP	Open Intercharge Protocol (OICP) is a communication standard for eMSPs and CPOs. It was developed to facilitate roaming and establish technical connections and contractual arrangements for e-roaming within EVSE.
OPCP	Open Plug&Charge Protocol (OPCP) marks a significant milestone in the advancement and interoperability of Plug&Charge technology. By enabling free access and standardizing the EV ecosystem, OPCP enhances compatibility among market participants and establishes uniform shared usage options.
OPnC	Open Plug&Charge is a standard-driven protocol that enables access to and standardization of the EV ecosystem. It is being developed as an open protocol for handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118 (-2/-20).

The EVSE industry needs to adopt and implement these standards and protocols to ensure the security and reliability of the EV charging infrastructure. Furthermore, the development of additional standards and protocols specific to EVSE cybersecurity is necessary to keep up with the evolving threat landscape and ensure the long-term sustainability of the EV charging ecosystem.

5. COMPARISON WITH ADJACENT INDUSTRIES

The EVSE cybersecurity industry is still in its early stages, so drawing comparisons with adjacent sectors, such as EVs and grid can provide practical insights for securing EV charging infrastructure. By adopting similar cybersecurity measures, EV charging providers can establish a robust and resilient system that can withstand cyber threats.

5.1. Comparison with the EV industry

The EV industry has been around for over a decade and has developed comprehensive cybersecurity standards and regulations specific to EVs. For example, the Trusted Information Security Assessment Exchange (TISAX) serves as a vital cybersecurity framework, facilitating the evaluation and enhancement of EV security.

Additionally, ISO 21434 provides guidelines for establishing a cybersecurity management system in road vehicle engineering, while UN Regulation No.155 outlines requirements for cybersecurity management in the design and production of EVs. These standards cover a range of cybersecurity areas, including secure communication protocols, secure software development practices and secure hardware design.In contrast, the EV charging industry is still in its infancy and lacks industry-wide cybersecurity standards and regulations.

The development of Connected and Autonomous Vehicles (CAVs) has led to an increased focus on cybersecurity, as these vehicles rely heavily on software and communication networks. The United Nations Economic Commission for Europe (UNECE) WP.29 Cybersecurity and Cybersecurity Management Systems (CSMS) regulation (R.155), and Software update and software update management system regulation (R.156) require cybersecurity measures for connected vehicles.

It sets requirements and recommendations for vehicle OEMs, component suppliers and mobility services to ensure cybersecurity throughout the vehicle's lifecycle. A CSMS is a structured approach to managing cybersecurity risks.

Similar to EV charging infrastructure, the automotive industry also faces cybersecurity risks such as data breaches, malware attacks and system manipulation. Therefore, the automotive industry has implemented various cybersecurity measures to safeguard their vehicles, including:

- Secure communication protocols: These protocols are designed to ensure that the communication between various components in the vehicle is secure and cannot be intercepted or tampered with.
- Secure boot process: The secure boot process ensures that the vehicle's software and firmware are securely loaded and verified before the vehicle is allowed to operate.
- Encryption: Encryption is used to protect sensitive data, such as personal information, financial data and communication between the vehicle and the cloud.
- Over-The-Air (OTA) updates: OTA updates are used to deliver updates and patches to the vehicle's software and firmware, ensuring that the vehicle is always running the latest and most secure version.
- Data privacy: EVs generate a vast amount of data, including location, charging behavior and personal information. Protecting this data from unauthorized access is crucial to ensure user privacy.

EV charging infrastructure can adopt similar measures to secure their systems, such as secure communication protocols and encryption to protect sensitive data and OTA updates to ensure that the charging infrastructure is always up to date with the latest security patches.

5.2. Comparison with the grid industry

The EVSE industry and the grid industry are critical infrastructure systems that are increasingly becoming digitized, interconnected and vulnerable to cyber-attacks. Like the EVSE industry, the grid industry is facing growing risks and challenges associated with cybersecurity, including the potential for physical damage, financial loss and reputational damage.

The EVSE industry and the grid industry both rely on complex networks of hardware, software and communication protocols that are subject to a wide range of potential vulnerabilities and threats. The grid industry has already experienced several high-profile cyber-attacks, including the 2015 Ukraine power grid attack [15] and the 2019 US Department of Energy data breach [16], which have underscored the need for robust cybersecurity measures across the entire energy sector.

To address these threats, the grid industry has developed a wide range of cybersecurity standards, guidelines and best practices, including the NIST Cybersecurity Framework, the ISO 27001 standard and the Critical Infrastructure Protection (CIP) cybersecurity standards from the North American Electric Reliability Corporation (NERC) [17]. The EVSE industry can draw on these standards and best practices to develop its comprehensive cybersecurity strategies and protocols, leveraging the existing knowledge and expertise from the grid industry to protect against potential threats and vulnerabilities.

However, the cybersecurity requirements for EV charging systems go beyond those of the grid due to their direct connection to the Internet, user interaction and the increased risk of cyberattacks. Therefore, EV charging systems need to comply with both the grid cybersecurity standards and additional cybersecurity measures to ensure the safety and security of the charging infrastructure.

Here are some of the cybersecurity measures that the grid industry has implemented to safeguard their systems, which can also be applied to EV charging systems:

- Access controls: Access controls limit access to critical infrastructure and sensitive information, ensuring that only authorized personnel can access them.
- Network segmentation: Network segmentation is used to separate critical infrastructure from less critical systems, reducing the attack surface and limiting the potential impact of a cybersecurity breach.
- Incident response plans: Incident response plans are put in place to detect and respond to cybersecurity incidents in a timely and effective manner.
- Continuous monitoring: Continuous monitoring can help detect and respond to security incidents in real time, minimizing the impact of cyber-attacks and improving overall system security.

Both industries also face similar challenges in terms of balancing security needs with operational efficiency, as cybersecurity measures can sometimes create additional costs and complexities that must be managed carefully to avoid disruption to critical services and systems. The grid is a highly regulated and complex system with numerous cybersecurity standards in place, such as NIST SP 800-53, ISA/IEC 62443 and ISO/IEC 27001, which provide a framework for managing and protecting sensitive information using a risk management approach.

To summarize, the EV charging industry can learn from adjacent industries, such as EVs and grid cybersecurity, to develop a more resilient cybersecurity framework for EVSEs. While the EV industry has established cybersecurity standards and regulations, the EVSE industry is still in the developmental stages of cybersecurity.

6. CONCLUSION AND RECOMMENDATIONS

As the demand for smart/connected EV chargers continues to grow, it is becoming increasingly important to address the cybersecurity risks associated with them. EVSE vulnerabilities are commonly exposed through remote and physical access points, which can compromise the EVSE firmware or PII.

Remote threats to EVSE, on the other hand, include attacks that can be launched over a network, such as the internet, cellular network, or the backend management system. To secure the EVSE against both physical and remote threats, it is essential to implement a multi-layered approach to cybersecurity. Following are some recommended measures to enhance EVSE cybersecurity:

- Establish a cybersecurity risk management program: To prioritize cybersecurity improvements based on risk to EVSE operations, it is recommended to establish a methodology that includes assessing and managing risks to the system. This can include best cybersecurity practices like the NIST cybersecurity network for internal assessments, patching and threat mitigations.
- Develop a threat profile: To evaluate potential vulnerability impacts and prioritize response, it is important to establish a threat profile for the types of attacks that are common on EVSE networks and back-end systems.
- Maintain network architecture diagrams: Keep updated network architecture diagrams to identify critical assets, Internet connections, open ports and supported protocols and ensure that all necessary security controls are in place.
- Monitor network activity: Continuously monitor network activity to detect and respond to unauthorized access attempts, and to identify and remediate any security vulnerabilities.
- Implement a central Vehicle-Specific Security Operations Center (VSOC): Public EV charging stations are susceptible to physical or close-range attacks and each charging station provides potential network access to all affiliated stations. By implementing a central VSOC with cloud-based monitoring, data can be contextualized and analyzed to identify any abnormal activities or anomalies at various levels, such as individual stations, regional clusters, or even across widespread networks.
- Conduct regular security assessments: Conduct regular security assessments to identify potential vulnerabilities and implement appropriate security measures to prevent or mitigate security threats.
- Secure the EVSE physically: Install the EVSE in a location that is protected against unauthorized access and vandalism and implement physical security measures such as security cameras and alarms.
- Use strong password policies: Implement strong password policies to prevent unauthorized access to the EVSE and change default passwords immediately after installation.
- Implement network segmentation: EV charger installations require secure and reliable network connectivity to function efficiently. Network segmentation and Virtual Local Area Networks (VLANs) can be used to isolate EVSE installations and provide an extra layer of security.
- Utilize secure trust principles: Utilize secure trust principles such as hardware/software signing, secure boot, secure firmware and software to update processes. Use firewalls to protect the EVSE from unauthorized network access and to prevent hacking attempts.

Overall, the implementation of these recommendations will help in protecting the EVSE ecosystem from cyber threats, ensuring the secure and reliable operation of the charging infrastructure and maintaining the trust of the users.

To ensure the long-term security of EVSE networks, it is essential to maintain an ongoing investment in research and development. This includes collaborating with industry partners and government agencies to identify emerging threats, develop new cybersecurity technologies and share best practices.

GLOSSARY

API	Application Programming Interface
CAGR	Compound Annual Growth Rate
CAV	Connected and Autonomous Vehicle
CCS	Combined Charging System
CIP	Critical Infrastructure Protection
CPMS	Charge Point Management System
CPO	Charge Point Operator
CSMS	Cybersecurity Management Systems
CSE	Communications Security Establishment Act
DoS	Denial of Service
DSO	Distribution System Operator
e-LCV	e-Light Commercial Vehicle
eMIP	eMobility Interoperation Protocol
eMSP	eMobility Service Provider
ENCS	European Network for Cyber Security
ENISA	European Telecommunications Standards
ETSI	European Telecommunications Standards
EU	European Union
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
GDPR	General Data Protection Regulation
ICE	Internal Combustion Engine
ICT	Information and Communication Technology
IDS	Intrusion Detection System
MitM	Man-in-the-Middle
NERC	North American Electric Reliability Corporation
NEVI	National Electric Vehicle Infrastructure

NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OCHP	Open Clearing House Protocol
OCPI	Open Charge Point Interface
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer
OICP	Open Intercharge Protocol
OPCP	Open Plug&Charge Protocol
OpenADR	Open Charge Point Interface
OSCP	Open Smart Charging Protocol
OTA	Over-The-Air
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PnC	Plug&Charge
R&D	Research and Development
TISAX	Trusted Information Security Assessment Exchange
TLS	Transport Layer Security
UNECE	United Nations Economic Commission for Europe
VLAN	Virtual Local Area Network
VPN	Virtual Private Networks
VSOC	Vehicle-Specific Security Operations Center
V2G	Vehicle to Grid

REFERENCES

[1] "PTR_EV+EVSE_Global_Database" PTR Inc. EVSE Service Update January 2023 https://ptr.inc/services/e-mobility/evse-charging/

[2] "PTR_EV+EVSE+Software_Global_Database" PTR Inc. EVSE Service Update January 2023 https://ptr.inc/services/e-mobility/evse-charging/

[3] https://industrydigits.com/cyber-attacks-ev-charging-stations/

[4] https://latesthackingnews.com/2021/07/20/schneider-electric-patched-security-bugs-in-evlink-charging-stations/

[5] https://insideevs.com/news/570958/russia-electric-car-chargers-hacked/

[6] https://www.bbc.com/news/uk-england-hampshire-61006816

[7] https://arxiv.org/abs/2202.02104

[8] Johnson, J., Berg, T. Anderson, B., & Wright, B. (2022). Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts and defenses. Energies, 15(11), 3931. Available: https://www.mdpi.com/1996-1073/15/11/3931

[9] Anderson, B. R., & Johnson, J. B. (2021). Securing Vehicle Charging Infrastructure (No. SAND2021-5745PE). Sandia National Lab. (SNL-NM), Albuquerque, NM (United States). Available: https://www.energy.gov/sites/default/files/2021-06/elt198_johnson_2021_o_5-11_558pm_LR_TM.pdf

[10] https://www.enisa.europa.eu/securesme/downloads

[11] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[12] https://www.charin.global/news/charin-irdeto-and-ul-solutions-announce-partnership-to-roll-out-plug-and-charge-in-europe/

[13] https://elaad.nl/en/projects/cybersecurity/

[14] Klapwijk, P., & Driessen, L. (2017). EV Related Protocol Study. Adresse: https://www. elaad.nl/uploads/files/EV_related_protocol_study_v1, 1. Available: https://www.researchgate.net/publication/317265159_EV_Related_Protocol_Study

[15] Case, D. U. (2016). Analysis of the cyber-attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf

[16] https://www.eenews.net/articles/experts-assess-damage-after-first-cyberattack-on-u-s-grid/

[17] https://static.tenable.com/marketing/whitepapers/Guide-NERC-CIP-Standards-and-ICS-Security-Compliance.pdf

Irdeto is the world leader in digital platform security offering cyber services and technology solutions that protect platforms, digital assets and software applications across multiple industries. Irdeto's products meet the rapidly changing mobility demands and exceed cybersecurity regulations for automotive, rail and beyond. We provide solutions throughout the product lifecycle to prevent cyberattacks and help protect assets for connected cars, commercial fleet, rail and construction equipment. With a rich heritage of security innovation and rapid adaptation to the changing demands of the cyber security space, Irdeto is the preferred partner to empower a secure world where people can connect with confidence.

Last modification: 9-08-2023 / 09:41 am GMT+01:00