Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations

Inna Skarga-Bandurova
School of Engineering, Computing and Mathematics
Oxford Brookes University
Oxford, United Kingdom
iskarga-bandurova@brookes.ac.uk
ORCID ID: 0000-0003-3458-8730

Igor Kotsiuba
Institute of Hazard, Risk and Resilience
Durham University
Durham, United Kingdom
igor.kotsiuba@durham.ac.uk
ORCID ID: 0000-0003-2878-6060

Tetiana Biloborodova
Saarland University of Applied Science
HTW Saar
Saarbrücken, Germany
beloborodova.t@gmail.com
ORCID ID: 0000-0001-7561-7484

***Abstract*—The paper analyses cyber security challenges of smart cities with a particular focus on the intelligent integrated and interconnected electric vehicle (EV) charging infrastructure. The analysis indicates that not all innovative elements and smart city solutions have adequate cybersecurity protection. Digital technologies vary considerably in terms of the level of potential risks, with certain novel technologies — such as V2G, smart charging, and smart energy management — posing higher risks than others. It is intended to lay a foundation for securing EV charging infrastructure by analysing problem context and data to be protected, including attack surfaces and cybersecurity threats and vulnerabilities in the EV ecosystem, analysing standardisation for the EV connection to the charging infrastructure, and providing a set of recommendations and best practices to securing EV charging infrastructure.**

Keywords—cyber security, electric vehicle, smart charging infrastructure, V2G

I. Introduction

The energy exchange and integration of e-mobility with the energy sector is one of the hottest topics in the growing electric vehicle (EV) market. Vehicle-to-grid (V2G) technology has the great potential to change the whole economic landscape promising a cleaner environment, lower running costs, reduced noise pollution, better driving experience and renewable electricity tariffs. However, there are considerable technical, social, and economic barriers to the widespread introduction of EVs. Poorly implemented cybersecurity and limited best practices are among the top barriers to EV adoption.

The success of EVs depends on a reliable, consistent network of charging stations. At the same time, electric car charging stations and smart home chargers are extremely vulnerable to cyberattacks. Table 1 shows a few EV charging incidents that have made headlines in the first half of 2022.

TABLE I. EV CHARGING VULNERABILITIES REPORTED IN 2022 [1].

Date	Cyber incidents with EV charging
January 2022	Remote attackers impersonated charging station admin users and carried out actions on their behalf, utilising vulnerabilities found in multiple charging stations.
February 2022	Russian EV chargers were hacked and disabled by a Ukrainian EV charging parts supplier as a part of the cyberwar effort.
April 2022	A new Combined Charging Stations (CCS) attack technique was found demonstrating the potential to disrupt charge EVs at scale.
April 2022	An EV charging station in the Isle of Wight was hacked to show inappropriate content. Some EV owners reported high voltage fault codes caused to strand.
May 2022	Rise in hacks of EV charging stations, including ransomware attacks against chargers and EV users.
May 2022	Rise in black-hat cyber criminals targeting EV charging stations to make money illegally, surpassing white-hat hackers working with stakeholders.
May 2022	Rise in EV charging station hacking incidents in the past few months of 2022, including incidents caused by load ransomware onto chargers to slow them down or stop functionality altogether. In addition, hackers could also lock users out of their user profiles until they pay a ransom fee or hack the chargers themselves to save on charging fees.
July 2022	A hacker gained control over a head unit of Korean automotive through the dashboard's API. By connecting to the dashboard's APIs, they were able to monitor the car status and control the locking mechanism through their app.

These incidents demonstrate the industry's immaturity in understanding attack surfaces, asset relationships, and multiple vulnerable interfaces. Cyber-attacks on components of EV charging infrastructure could affect nearly all critical infrastructure. Transferred data (personal and payment information) and involved entities (EVs, EV charging stations, smart grid and service platforms) are valuable assets that all require strong security. Combining many-faceted access with protection is well-established in other industries, and the approaches proven in similar use cases can be leveraged for e-mobility. Data attributed to vehicle operation and maintenance, as well as data attributed to the driver or owner containing personally identifiable information, whose integrity and authenticity need to be protected. The main tasks that need to be solved in this context include the following:

- Defining the most vulnerable points of EV infrastructure (objects, types of vulnerabilities and attack vectors) and analysing the links between users' activities on different devices.
- Analysing solutions for effective and efficient identification, investigation, mitigation, and reporting of realistic multi-dimensional cyber-attacks, ensuring privacy and security of sensitive information, pertaining to personal privacy for legal or ethical reasons.

The present research work was conducted within several research initiatives including European Union's Horizon 2020 research and innovation programme (RESPONSE, grant agreement No. 957751) which aims to establish a strategic vision for Smart Cities Energy Transition: Climate-neutral cities by 2050 [2]. The project builds upon intelligent integrated and interconnected energy systems coupled with demand-oriented city infrastructures, governance models and services including a set of innovative elements (IEs) that foster energy sustainability. Connected cars are one of the IEs of smart cities and part of the internet of things (IoT). Beyond others, IEs also includes the development and test

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

implementation of automated driving and vehicle-to-vehicle communication robot cars via 5G, smart charging, and fast V2G Charging Station. In this context, our primary goal is to protect critical V2G infrastructure and improve energy security through technical analysis of the current threat landscape presented by interoperable EVs and EV chargers [3].

II. Problem Context and Data to be Protected

Typical smart city charging infrastructure (Fig. 1) includes different services such as vehicle-to-grid (V2G), vehicle-to-home (V2H), vehicle-to-building (V2B), enabling energy and data to be pushed from EV to smart grid, do both smart charging, and provide energy from the EV battery to the grid. Charging often starts at home or on-street charger points. The EV charging infrastructure incorporates the distribution system operators (DSOs) or power grids, network operators, building energy management systems (BEMS), EV charging stations and EV supply equipment (EVSE), including on-board charger (OBC), battery managed system (BMS) and battery. The V2G system (EV + charging station) has the capacity to charge and discharge an EV battery.

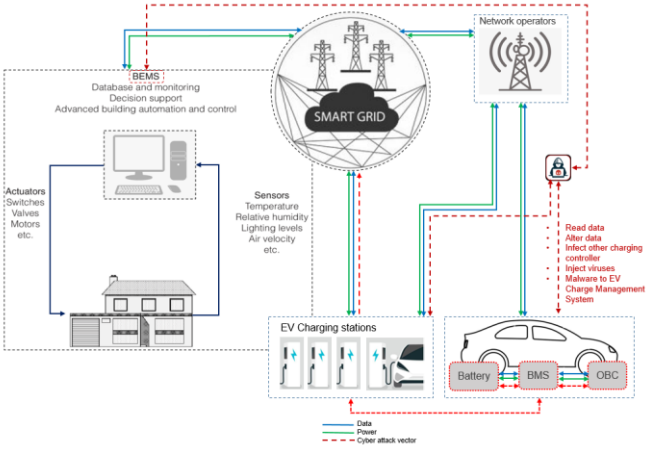

Fig. 1. Typical smart city charging infrastructure

Until now, V2G industrial products have been mainly used to provide balancing services to the overall electric system, for instance, by providing ancillary services to the Transmission System Operators (TSO). One of the objectives of the RESPONSE project [2] is usage V2G systems to provide the Energy Management System (EMS) of an eco-district with electric flexibility services and improve the self-consumption level of the eco-district. All the physical connections provide energy flow between the grid and the EV battery. The EV and the charger exchange data via a single cable, and the charging devices exchange data with a charging operator on the next layer. Beyond the vehicles, there are plenty of services connected to cloud platforms to support navigation, emergency services, telematics, music, browsing, infotainment, etc. Some of these systems are connected to third-party cloud environments to support billing and other services. With a variety of IoT devices using multiple communication platforms and web applications, the V2G components inherit the vulnerabilities of the adopted technologies generating new cybersecurity challenges to the whole architecture.

Any connected infrastructure is a potential target for cyber-security attacks and rightly, so such a broad variety and tight interconnection significantly expand the attack surface for hackers making its protection a challenging task. In some cases, a connection of EVSE with the entire electrical grid is so poorly secured that influencing charging sessions, e.g. via the EV-to-EVSE one day, may destabilise entire electrical grids [4].

Different protocols exist for each connection between participants, but since smart EV charging is relatively new, the protocol landscape for this infrastructure is still changeable. New protocols and extensions are constantly being developed and are not uniform. The Open Clearing House Protocol (OCHP) is used to connect the service provider to the backend networks of another service provider to verify charging transactions on third-party chargers. Connection to grid operators is performed using Open Smart Charging Protocol (OSCP), OpenADR, or other protocols [5]. OpenADR is an open, secure, two-way communication model which enables information between vehicles and the electricity grid and helps to balance grid supply and demand. Open Charge Point Protocol (OCPP) is used for communication between the smart EV charging station and the backend systems of charge station operators. When the EV charging station is turned on, the software confirms its identity, and OCPP sends a transaction message about the start of charging. When users want to stop charging, they can use a smartphone app to verify their identity. Open Charge Point Interface (OCPI) manages communication between charge station operators and the e-Mobility service providers facilitating roaming for EV drivers across several charging stations. This protocol provides information about the charge station (location, real-time billing, accessibility, etc.). However, all the infrastructure components and communication channels of EV charging could be potential targets of the cyberattacks. By intruding on a V2G communication line, an attacker can impersonate a charging station for communication and harm the car's BMS or electronic control unit (ECU). Fig. 1 also demonstrates some possible threats [5], including impersonation, theft of payment-related information, communication spoofing, eavesdropping, denial of service (DoS), and breach of privacy.

There are at least three charging attack surfaces in this infrastructure:

- EV-to-EVSE – charging fraud via vehicle impersonation.
- Grid to EV – attacks against charging networks could disrupt the ability to charge electric vehicles at scale.
- Grid to Fleet – charging stations attacking multiple vehicles.

Charging stations authorize users and vehicles using RFID cards, Bluetooth, or Wi-Fi, and studies of widely deployed EV Charging Station Management Systems and are a potential attack vector into the larger energy grid. They are just as vulnerable as any connected device have shown an array of vulnerabilities in their communication components that suggest a susceptibility to remote cyberattacks. These vulnerabilities can be potentially exploited by hackers to compromise the availability, integrity, and confidentiality of a network of charging stations, or even the power grid. Adversary control of EVSE may also compromise the safety of the basic functionality of the devices, leaving the user stranded or injured. Therefore, it is critical to protect vital information against attacks during transactions between vehicles and charge points.

Potential security issues of smart charging include: 1. MITM - a form of eavesdropping, where communication between two users is monitored and/or modified by an unauthorized party. In the process, the two authorized parties appear to communicate normally. The transmitter does not recognize that the receiver is an attacker or an unauthorized party, trying to access or modify the message before retransmitting to the receiver. MITM attacks can also overload distribution transformers and sometime power grid frequency and voltage stability disturbances leading to power grid failure via rapid cycling of a large number of EV loads. 2. DoS - an attacker prevents a legitimate user from using services, e.g., deprives the customer of charging the EV. 3. Denial-of-charge (a type of DoS in V2G system), e.g., Brokenwire - a way to wirelessly abort vehicle charging en masse from up to 47m (151ft) away. This process can have mass implications if the charging of emergency or government vehicles were stopped and did not have enough energy for their shifts. 4. Malware – mostly used to penetrate a charging station network, targeting one OEM. An attack can unravel manufacturer reputations and/or expose personal data, giving hackers insight into a vehicle's charging habits, locations, and other personal information. 5. Attack on two-way power flow - by hacking into charging stations, vehicles of a certain type or in a controlled region may be programmed to simultaneously demand or send power at a specific time, overloading the power grid. A compromised vehicle can be a hazard to pedestrians, networks, cloud data, and other critical road-safety initiatives.

Potential security issues in fast chargers are: 1. False Data Injection Attack (FDIA) – is one of the crucial attacks that can cause several damages to the EVs, EVSE, V2G system, and even to the grid. FDIA aims at manipulating the V2G system and its integrated system-related various data such as [6]: (a) energy request, (b) energy usage, (c) price signal from a utility, (d) demand response bidding from EVSE, (e) demand response needs from the utility, (f) event messages, (g) EV ID, (h) premise location ID, (i) utility ID, and (j) customer ID, communicated between EVs, EVSE, and V2G system. FDIA can cause overcharging to batteries and several damages to EVs and the grid. 2. MITM - an attacker can intercept communication between EVs, EVSEs, and V2G system and modify, drop, and falsify data transmission. When attackers insert between EVs, EVSEs, and V2G system, they can create tracking issues, payment fraud (e.g., the charging cycle does not last the full amount of time paid for, the charger is spoofed into providing free service), and violate other personal privacy. An attacker can also cause intentional overcharging/discharging of PEV batteries causing damage to the EV and its batteries and taking the EVs out of service or degrading range. 3. DoS – in the case of the V2G system and its entities, attackers can attack servers and block valid requests from EVs resulting in rejecting requests from legitimate PEV users. Due to denial-of-charge (a type of DoS in the V2G system), important emergency vehicles (e.g., ambulances, firetrucks, and security vehicles) may be denied from charging, resulting in detrimental effects on the various emergency services and society. 4. Malware injections via EVs – can cause the theft of sensitive information such as payment information (debit/credit card information), personal information, charging time, payment amounts, etc. The malware-injected EVSE not only affects individual EVSEs but also has a probability of propagating to a network of EVSEs. The malware injected in EVSEs can also pass to EVs, the V2G system, and the power grids resulting in detrimental effects to all the stakeholders.

Table 2 summarises the most common cyber security threats and their impact on EV chargers.

TABLE II. COMMON CYBER SECURITY THREATS AND ATTACKS AGAINST EV CHARGES (ADAPTED FROM [4]).

Security threat	**Attack scenario**	**Impact**
No API authorization	Unsanctioned remote control of the charger	Allows attacker to get the full remote control of the charger and potentially switch all chargers on and off synchronously, there is potential to cause stability problems for the power grid, owing to the large swings in power demand as reserve capacity struggles to maintain grid frequency.
No firmware signing	A new firmware to be pushed remotely and the charger used as a pivot onto the home network	Allows attackers to gain unauthorised access to the server via a network interface card with unsigned firmware used by each of the big three server manufacturers. Once the firmware on any of these components is infected, the malware stays undetected by any software security controls.
Malicious firmware update	Disable chargers with malicious firmware update, privilege escalation, and other attacks	EV operators cannot charge which impacts emergency and medical services, food and agriculture, manufacturing, defence, etc.
EV chargers used the low-cost modules	Extraction of all stored data, including credentials and the Wi-Fi pre-shared key, or PSK	Allows attackers to use EV charging stations to gain unauthorized entry into a business network, or hack user accounts to bill charges to the wrong account, e.g., weak code used in the EV charging stations can expose the credit card details of drivers causing monetary loss.
Weak code used in the charging stations	Exposing the credit card details of drivers causing monetary loss	Allows attacker to gain unauthorized entry into a business network.
V2G control mis-coordination	EVSE V2G control mis-coordination produced active and reactive power flows	Minimal distribution voltage outside of ANSI Range A at end of feeder.

Potential security issues related to cloud-based ECUs are [7]: 1. DoS - this happens when attackers overwhelm a resource, making it unavailable for users. 2. MitM attack - this occurs when an entity intercepts all network communications between the cloud and the car. This attack can modify, drop, delay the transfer of, or steal data, causing critical malfunction in the car. 3. Hijacking of services - this takes place when some of the services that are used by the cloud-based architecture are hijacked by an entity, modifying data. 4. Latency issues - if the network latency continuously fluctuates (because of network issues or an attack) the car will continuously context-switch between cloud and local processors, which may introduce errors in operations. 5. Data privacy - any cloud architecture is bound to store critical and private data such as driver profiles, car maintenance data, destination data, and financial information, among other pieces of sensitive information. 6. Loss or alteration of this data becomes a contentious issue in the event of a data breach. 7. Authentication and management issues. Incorrect data - in this case, a car receives incorrect critical real-time data. 8. Misconfiguration issues - this is a common and recurring issue with cloud-based servers and as such is not unique to connected cars. 9. Cloud supply chain issues - could adversely affect the connected cars.

Moving further, we have also analysed the most critical vulnerabilities that were proven to be present in the EV ecosystem [8] and summarize them in Table 3. This helps to understand EV attack impact on power grid operation and expand the landscape of possible solutions and best practices in cyber security for V2G systems.

TABLE III. THE MOST CRITICAL VULNERABILITIES PRESENT IN THE EV ECOSYSTEM (ADOPTED FROM [9, 10]).

Vulnerability	Attack scenario	Impact
SQL Injection	Backend database manipulation to access information that was not intended to be displayed	Allows the attacker to gain access to privileged user information and manipulate the Electric Vehicle Charging Station (EVCS) firmware.
XML/External Entity Injection	Manipulation or compromising the logic of an XML application or service	Allows the attacker to inject HTTP requests into the system and in some cases gain remote access to the EVCS.
Server-Side Request Forgery (SSRF)	Sending requests from the server to other resources, both internal and external, and receive responses	Allows the attacker to redirect traffic towards internal/external endpoints causing denial of service and reading files and record logs of the EVCS.
Cross-Site Scripting (XSS)	Malicious script is injected directly into a vulnerable web application.	Allows the attacker to inject malicious code into the EVCS allowing them to highjack user accounts or even administrator accounts in some cases.
Comma-Separated Values (CSV) injection	Manipulation of EVCS functionality	Allows attackers to embed XSS payloads that get triggered and stored on the EVCS leading to hijacking administrator session tokens.
Cross-Site Request Forgery (CSRF)	Control of the EVCS	Allows the attacker to induce target users to perform unintentional actions that lead to setting modification and manipulation of EVCS functionality.
Hard-Coded Credentials	Embedding authentication data (user IDs and passwords) directly into the source code of a program or other executable object	Allows attackers to recover the hardcoded login credentials in the source code of the EVCS or the associated application and gain unauthorized access to the EVCS.
Missing Authentication	Unauthorized access to user accounts	Allows the attacker to gain unauthorized access to user accounts without being properly verified by the EV management system.
Open Charge Point Protocol (OCPP) MITM vulnerabilities	OCPP MITM attack; backend system compromise; malicious firmware update	May lead to power market disruptions affecting generator scheduling and economic dispatch.

III. STANDARDIZATION LANDSCAPE FOR THE CONNECTION TO THE CHARGING INFRASTRUCTURE

This section details the standardization activities focusing on the communication interface between the electric vehicle and the charging spot, but further connections to the backend are also considered. The main focus is placed on standardization activities from the ISO/IEC. Standardization activities of ISO/IEC and SAE can be divided into four categories [11]: charging connector, charging communication, charging topology, and safety (see Fig. 2).

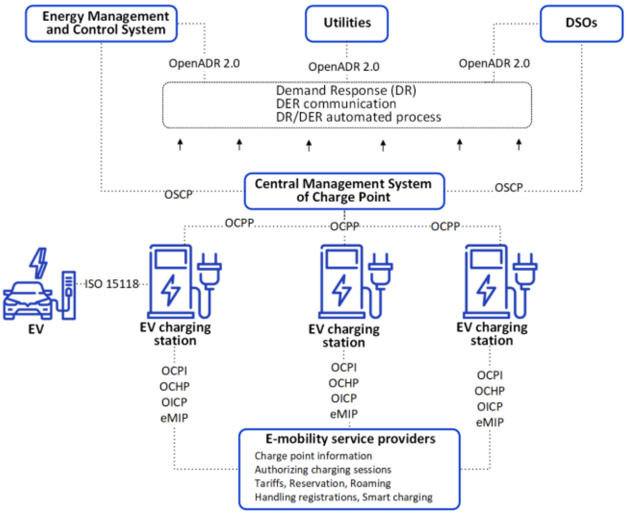

Fig. 2. Communication standards for the electric vehicle charging infrastructure

Alternatively, the most relevant standards and protocols of battery-electric mobility, are presented on the information layer of the E-Mobility Systems Architecture (EMSA) model [12] and can be classified into six main categories with respect to their functionality:

- Communication with end user devices via a specific REST-API.
- EV charging and automatic authorization, e.g., IEC/ISO 15118.
- Managing the CSa, e.g., the Open Charge Point Protocol (OCPP).
- Exchanging information between the CSO and the E-Mobility Service Provider (eMSP), e.g., Open Charge Point Interface protocol (OCPI).
- Roaming, e.g., the Open Clearing House Protocol (OCHP) and the Open InterCharge Protocol (OICP).
- Communication with the grid operators, e.g., the Open Smart Charging Protocol (OSCP).

The most EV charging stakeholders are still in the early stages of implementing advanced cyber security platforms and are not yet required to follow regulations and standards similar to UNECE WP.29 R155 and ISO/SAE 21434 [13].

In this regard, safety objectives should encompass not only vehicles, but also the surrounding infrastructure and related ecosystems.

Table 4 summarizes information about relevant standards.

TABLE IV. COMMUNICATION STANDARDS AND THEIR SCOPE FOR THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE.

Standard	Scope	Content
IEC 62196	Charging Connector	Plugs, socket-outlets, vehicle couplers and vehicle inlets – Conductive charging
SAE J1772	Charging Connector	Electric Vehicle Conductive Charge Coupler
ISO 15118	Charging Communication	Road vehicles - Communication protocol between electric vehicle and grid
SAE J2293	Charging Communication	Energy Transfer System for Electric Vehicles
SAE J2836	Charging Communication	Use Cases for Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
SAE 2847	Charging Communication	Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
IEC 61850	Power Systems Communication	Communication networks and systems in substations
IEC 61851	Charging Topology	Electric vehicle conductive charging system
IEC 61439	Charging Topology	Low-voltage switchgear and control gear assemblies

The IEC 61851 [14] standard describes four different EV charging modes. The first three modes assume delivering AC current to the EV on-board charger while the fourth one delivers DC current directly to the EV battery bypassing the on-board charger:

- Mode 1: EV is directly connected to a standard household socket outlet. The mode does not support any communication between the EV and changing point.
- Mode 2: EV charges from a standard household socket outlet with an in-cable control and protection device (IC-CPD) equipped with the required control and safety functions.
- Mode 3: EV charges using a dedicated EVSE socket outlet and plug with the EV on-board charger.
- Mode 4: fast charging mode using an off-board charger with a DC output. The charging connector is permanently connected to the station.

The communication between the vehicle and the charging spot depends on the mode applied. There is no data communication in Mode 1 and Mode 2. In Mode 3, only the control pilot communication exists, while in Mode 4 additional communication functions are available to allow battery management. Common to all modes is that IT-security is not provided. Nevertheless, for vehicle integration into a smart-grid-connected charging infrastructure, (secure) communication is required for tariff exchange, billing, optimization of charge cost and grid load, value-added services, etc. To support these functions in the future, ISO/IEC 15118 is currently being specified to address these communications needs, including an integrated security concept.

ISO 15118 [15] is an international standard that outlines digital communication between an EV and the EV charging station to charge an EV's high-voltage battery. ISO 15118 provides standard methods for secure communication, smart charging and the Plug & Charge features. The connection between EV and the grid must be secure to exchange private and payment-related information to provide Confidentiality, Integrity, and Availability (CIA). This process is also known as plug & charge, where mutual authentication for payment processes is done automatically. V2G implementation must include well-planned cybersecurity measures to achieve CIA along with identification, authentication, authorization and accountability.

The security measures defined in ISO/IEC 15118-2 [16] build upon existing standards. The access media for AC/DC charging will be power line communication in the first step. Support of inductive charging will most likely use wireless communication. As both features have a different OSI layer 1+2, security measures have not been placed here to allow an independent solution. As shown in Fig. 2, ISO/IEC 15118-2 applies TCP/IP to provide communication between the vehicle and the charging spot. Consequently, security is applied on the transport layer using TLS [17], ensuring a protected channel between both of them. Since ISO/IEC 15118 targets the communication between the vehicle and the charging spot, this might be sufficient at first glance, but security measures on the application layer have also been defined by applying XML security (digital signatures and encryption). Application layer security became necessary, as the communication also targets billing and payment-relevant information, which is exchanged with the backend in contract-based payment scenarios. Moreover, to enable contract-based payments, the vehicles need authentication means. The EV possesses a digital vehicle certificate and a corresponding private key to secure communication with the backend. These security measures go beyond the communication hop between the EV and the charging spot.

IV. RECOMMENDED ACTIONS AND OPEN ISSUES IN CYBER-SECURITY AND PRIVACY OF EV

The EV charging infrastructure is a complex ecosystem consisting of several entities that interact with each other and share (often personal) user data. The charging ecosystem must be able to interface seamlessly between various vehicles, charge station service providers, banks and payment platforms. EV charging stations combine IoT technology to manage payment and data analytics providing multiple cyberattack vectors. The compromised V2G infrastructure not only threatens vehicles and networks, but also compromises privacy and results in the loss of personal data. As a result, all vehicle Original Equipment Manufacturers (OEMs) and charging station manufacturers may have a huge financial impact depending on regional legislation.

The standard ISO/IEC 15118 requires vehicles to store only a fixed, limited number of root certificates to enable issuer verification. Moreover, it also restricts the number of supported intermediate certification authorities. Besides the validity and issuer, the client also needs to check the certificate revocation status. One option to avoid handling certificate revocation lists is the usage of short-term certificates from the server side. Another option is the provisioning of the revocation state by the server itself, e.g., by attaching a fresh Online Certificate Status Protocol (OCSP) response to the certificate during the authentication phase. To keep a balance regarding the implementation and operational effort, the current ISO/IEC 15118 proposal features both short-term certificates for the server-side certificates and OCSP responses for intermediate CAs.

A. *Best practices to ensure EV ecosystem security*

Devices that meet this specification are resistant to physical attacks and implement security features, including authentication, encryption and cryptography, that help secure connected systems using protected keys.

TABLE V. BEST PRACTICES TO ENSURE EV ECOSYSTEN SECURITY (ADAPTED FROM [18]).

Vulnerability	Best practices
Protocol vulnerabilities	A standardized set of protocols must be enforced on the EV ecosystem instead of allowing different vendors and manufactures to use their own set of protocols. Furthermore, the optional authentication and encryption schemes must be enforced, and no data should be allowed to be transmitted in plain text.
SQL Injection	Use parametrized queries to distinguish code from data.
XML/External Entity Injection	Disable external entities whenever possible.
Server-Side Request Forgery (SSRF)	The IP addresses used should be validated and only pre-approved (pre-mapped) clients should be allowed to access the system.
Cross-Site Scripting (XSS)	HTTP parameters must be filtered, and user inputs must be encoded to prevent them from being manipulated by attackers.
Comma-Separated Values (CSV) injection	The system should parse the received data and reject the data that contains special characters used to trigger or execute codes.
Cross-Site Request Forgery (CSRF)	Add random values to the communication process with each HTTP request to ensure the attacker cannot craft fake messages and cause system modification.
Hard-Coded Credentials	The hardcoded credentials should be replaced by hash values of the credentials instead of the actual message in plain text.
Malware injection	Provide cyber security related testing and assessment while installing EVSEs.
Missing Authentication	Authentication should be enforced on all functionalities especially the critical functions that can be used to manipulate the charging session parameters.

As presented here, many best practices have been proposed for user interfaces and communication protocols. These must be carefully considered by standards development organizations and network operators to improve the security of the EV ecosystem. Our analysis shows that currently available EV and V2G charging infrastructures are immature for cyber security best practices:

- The V2G standard has not been released yet
- There are many challenges related to business models (e.g., the need for incentives to car owners - how would they be compensated?)
- Current V2G applications are mostly on the DC side. AC side is more challenging for V2G since the car or V2G station needs to be responsible for grid code compliance.
- Local grid companies may require specific grid code compliance documentation for AC side V2G.

Given the fact that there is physical access to both vehicle and charging station, physical attacks must also be considered in the attacker model. As was mentioned in [19], a recognized risk for the V2G is the fact that only a few car manufacturers are enabling V2G at this stage. It implies that in order to test V2G, we need to cooperate with the car manufacturers. This cooperation between OEMs, charging networks and smart mobility stakeholders could enforce the development of a new cyber security paradigm that ensures consumers can trust the charging infrastructure in use and EVs are always protected [13].

The main direction of securing V2G systems is to respond to the evolving threat landscape by continuously improving defensive postures. To that end, several major technical trends, research opportunities, and other habits in charging industry best practices can be proposed [4]:

- Techniques to prevent loss or manipulation of charging communications via side-channel attacks.
- Improved authentication and authorization mechanisms for EV and V2G equipment, including those established with public key infrastructure (PKIs) and their continuous revision and update.
- 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.
- At the policy level, state and federal governments should seek legislation to improve the security of EVSE systems by creating EVSE cyber security requirements, expanding information-sharing programs, and establishing incident-response strategies - especially in cases of coordinated or widespread attacks.

Additionally, basic cyber hygiene procedures could notably improve the security landscape. These include using proper encryption, locking physical ports, removing unneeded services, keeping software up to date, etc.

The UK government has developed the Smart EV Charging Point Regulations [20], which have made concise arrangements for the use of EV changes and ensures that charging points have reasonable functionality and safety. The first part of the rules on smart charging stations contains measures to help manage the growing demand for electricity from electric vehicles and came into force on June 30, 2022. The second part of the regulations is aimed at strengthening security and will enter into force on December 30, 2022.

B. *Digital forensic readiness*

The embedding of digital components into V2G and smart charging represent a new threat surface for attackers. In this context, Digital Forensics Readiness (DFR) plays an important role, as it is the only way that an IoT-enabled environment could minimize the potential of digital evidence while minimizing the costs for a digital forensic investigation. Compared to conventional computing devices, the IoT has special features that make it critical for the IoT environment to be prepared for possible cyber-attacks and intrusions [21].

The goals of implementing DFR processes in organizations are specified in ISO/IEC 27043 [22] and include:

- Maximize the potential use of digital evidence.
- Minimize digital research costs incurred directly within the system or related to the system's services.
- Minimize interference and prevent interruption of the organization's business processes.
- Maintain or improve the current level of information security within the organization.

As a result, the DFR can be effectively used as a way to counter the cyber-attacks and maximize the potential use of digital evidence while minimizing the cost of conducting a digital forensic process in IoT environments, which are one of the core elements of many IEs in the RESPONSE project [2].

DFR process groups based on the ISO/IEC 27043 include the planning processes group, the implementation processes group and the assessment processes group. As discussed by Mohay [23], DFR is the degree to which computer systems or computer networks are capable of recording activities and data. Therefore this is important to ensure that the records are sufficient to their extent for subsequent forensic purposes, and that the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations.

The forensic readiness phase is the initial step in the planning process used to determine the level of forensic capabilities, including the presence of suitable data sources and toolsets [24]. First, an analysis of potential data sources is performed, where a determination of digital components (IoT, EV, V2G, etc.) and used technologies are applied. In general, most EVs implement similar data sources. Used technologies differ between manufacturer and model. A more in-depth or abstract analysis of potential data sources is feasible. Depending on the questions a forensic investigation should answer, the type of analysis differs. Common vehicle literature and, if available, OEM documentation are usable as an instrument.

The second step of this phase is a determination of interfaces and data exchange methods. Depending on the type of forensic investigation (live or post-mortem) as well as the acquisition method (online and offline), different exchange methods and interfaces are applicable. For example, in the case of EV, to acquire data using JTAG, direct access to an ECU is necessary. OBD-II allows to acquire data without physical access to an ECU. This phase must ensure to fulfil of the integrity requirement and therefore not tamper potential evidence. Next, the level of development for automotive forensics and the availability of a toolset must be evaluated. The goal of this step is to determine how much forensic analysis experience is available for automotive forensics. It allows forensic analysts to use known as well as functioning technologies and methods during forensic investigations. If the level of development for a specific domain is extensive, the acceptance requirement is attainable. In addition, solutions for digital forensics challenges might be present and applicable. Documentation should be provided during all of the performed steps. The reproducibility requirement is fulfilled if final documentation is available. By using this report, any third party should be able to reproduce results. For the implementation of DFR in an organization, systematic and complex work must take place, including the incorporation of a range of operational and infrastructural readiness strategies, such as risk assessment, staff training, tool deployment, and evaluation metrics.

CONCLUSION

The research gaps and vulnerabilities identified in electric vehicle and charging station cyber security are the follows.

- Currently available EV and EVSE charging infrastructures are immature for cyber security best practices.
- Most of the EV industries do not have security software and development methodologies and guidelines.
- Buyers of EVSEs do not typically specify the cybersecurity-related protection requirements because of limited knowledge.
- Cyber security-related testing and assessment are not accessible to most of the EVs and charging infrastructure industries. Further research in this field is inevitable.
- The guidelines and guidance on cyber security requirements for wireless charging infrastructures for light passenger EVs, electric buses, and electric trucks are still in the testing and demonstration phase.
- Currently available EV infrastructures such as EVSEs, smart meters, advanced metering infrastructure, and demand response equipment are yet to be matured with up-to-date technologies.
- Commonly available EVSEs are still struggling with proper physical security guidelines and guidance.
- Unavailability of such guidelines has adversely affected the consumer’s confidence in EVs.

We have also considered other potential cyber risks, but in our opinion, they should be analysed with specific stakeholders in accordance with their demands and the data provided. As it was mentioned, with increasing demands in this area, all can be quickly changing, covering in greater detail some of the requirements for certification, accreditation, training, and how the model is to be rolled out in the coming months. The specific ideas can cover preparedness for cyber threats, testing of the cyber security level, monitoring of cyber security at the operational level, and reacting to the implementation of the cyber threat.

ACKNOWLEDGMENT

This research was funded by European Union’s H2020 programme as part of the RESPONSE project (integRatEd Solutions for POsitive eNergy and reSilient citiEs), Grant Agreement ID 957751 and ELECTRON project (rEsilient and seLf-healed EleCTRical pOwer Nanogrid), Grant Agreement No. 101021936.

REFERENCES

[1] AutoThreat® Intelligence Cyber Incident Repository, https://upstream.auto/research/automotive-cybersecurity/?id=null

[2] RESPONSE project https://h2020response.eu/about/ (assessed 12-10-2022).

[3] J. Johnson, Securing Vehicle Charging Infrastructure. 2020 DOE Vehicle Technologies Office Annual Merit Review (assessed 10-10-

2022) https://www.researchgate.net/profile/Jay-Johnson-11/publication/341911722_Security_Vehicle_Charging_Infrastructure/links/5ed923db299bf1c67d3c25f9/Security-Vehicle-Charging-Infrastructure.pdf

[4] J. Johnson, T. Berg, B. Anderson, B. Wright. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* 2022, *15*, 3931.

[5] Automotive cybersecurity: The future of EV charging stations https://www.telematicswire.net/automotive-cybersecurity-the-future-of-ev-charging-stations/#:~:text=Vehicle%20Threats%20%E2%80%93%20In%20V2G%20communication,onboard%20port%20for%20charging%20gun.

[6] S. Abedi, A. Arvani, and R. Jamalzadeh, Cyber Security of Plug-in Electric Vehicles in Smart Grids: Application of Intrusion Detection Methods. Singapore: Springer Singapore, 2015, pp. 129–147.

[7] N. Huq, C. Gibson, V. Kropotov, R. Vosseler. Cybersecurity for Connected Cars Exploring Risks in 5G, Cloud, and Other Connected Technologies. Trend Micro Research. https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf

[8] Cyber assessment report of level 2 ac powered electric vehicle supply equipment, 2018. https://avt.inl.gov/sites/default/files/pdf/reports/Level2EVSECyberReport.pdf

[9] M.A. Sayed, Atallah R., Chadi M. A., Mourad Debbabi (2021) Electric Vehicle Attack Impact on Power Grid Operation.” *ArXiv* abs/2111.11317 (2021): n. pag.

[10] D. Skylar. ChargePoint Home security research, Technical Report. Kaspersky Lab Security Services, 2018.

[11] R. Falk, S. Fries, Siemens Ag. (2012) Electric Vehicle Charging Infrastructure - Security Considerations and Approaches. https://www.semanticscholar.org/paper/Electric-Vehicle-Charging-Infrastructure-Security-Falk-Fries/be40e8690fae1518db474a393228496e934e1f2f

[12] B. Kirpes, P. Danner, R. Basmadjian, H. De Meer, C. Becker. E-mobility systems architecture: a model-based framework for managing complexity and interoperability. Energy Inf 2(1):15, 2019.

[13] G. Serio, EV Charging Stations Cyber Vulnerabilities Could Be EVs Achilles Heel https://upstream.auto/blog/ev-charging-cyber/

[14] IEC 61851-25:2020 Electric vehicle conductive charging system - Part 25: DC EV supply equipment where protection relies on electrical separation, https://webstore.iec.ch/publication/31531

[15] ISO 15118-1:2019 Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition, https://www.iso.org/standard/69113.html

[16] ISO 15118-2:2014 Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements, https://www.iso.org/standard/55366.html

[17] FINSENY – Future Internet for Smart Energy, http://www.fi-ppp-finseny.eu/

[18] A. Walker, J. Desai, D. Saleem, T. Gunda. Cybersecurity in Photovoltaic Plant Operations. United States. https://doi.org/10.2172/1774870, 2021.

[19] Recommended cybersecurity practises for EV charging systems https://energy.sandia.gov/download/63318/

[20] Guidance Regulations: electric vehicle smart charge points https://www.gov.uk/guidance/regulations-electric-vehicle-smart-charge-points

[21] V.R. Kebande, N.M. Karie, H.S. Venter (2018) Adding Digital Forensic Readiness as a security component to the IoT domain, Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 1, doi: 10.18517/ijaseit.8.1.2115.

[22] ISO/IEC 27043: 2015: Information technology -- Security techniques -- Incident investigation principles and processes.

[23] G. Mohay Technical challenges and directions for digital forensics. Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering; 2005 Nov. 7–9; Taipei, Taiwan. Piscataway, NJ: IEEE Computer Society Publishers,;155–61, 2005.

[24] K. K. Gomez Buquerin, Analysis of Digital Forensics Capabilities on State-of-the-art Vehicles, Technical University Ingolstadt, 2020.