Electric Vehicle Security and Privacy: A Comparative Analysis of Charging Methods

Gianpiero Costantino, Marco De Vincenzi, Fabio Martinelli, Ilaria Matteucci
IIT, Consiglio Nazionale delle Ricerche, Italy,
{firstname}.{lastname}@iit.cnr.it

2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) | 979-8-3503-1114-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/VTC2023-Spring57618.2023.10200030

***Abstract*—In the next decade, electric road vehicles have the potential to reduce climate change and improve mobility. However, not all charging methods are equally secure and private, so this work provides a comprehensive analysis of the security and privacy of various EV charging methods and highlights the importance of addressing vulnerabilities to meet homologation standards. Five charging methods are described in terms of physical components, communication protocols, and standards. This research identifies weaknesses in each method and determines which are less prone to cyber attacks or privacy disclosures. The impact of different charging methods on vehicle homologation is also discussed, as required by the cybersecurity regulation UNECE R155. A mapping is provided between vulnerabilities and suggested mitigations from the regulation. The evidence suggests that different charging methods result in different security and privacy levels, with conductive methods being more vulnerable to security attacks and privacy disclosure, while methods with fewer components may reduce security and privacy risks.**

***Index Terms*—Electric vehicle, conductive, inductive, battery swapping, security, privacy, UNECE R155.**

I. Introduction

The development of electric vehicles (EVs) such as full battery electric vehicles (BEVs) and plug-in hybrid electric vehicles (PHEVs) is contributing to the achievement of decarbonization goals and transforming road mobility [1]. Besides, many countries are planning to prohibit the production of new gas and diesel car models in the next fifteen years, which is expected to modify our daily routines and the cities' environments. To support this transition, an EV ecosystem, consisting of three main components, is required to supply energy: the EVs, the Electric Vehicle Charging Stations (EVCS) with their connections, and the power grids.

In this work, we focus on the EV charging ecosystem and in particular on EVCS which acts as an access point for EVs to the electric infrastructure. The EVCS is a regulated and standardized device that can be installed in a private or public area and includes various physical components, software solutions, and communication protocols. EVCS models vary based on their charging methods, such as conductive or inductive, which can determine the complexity of the charging ecosystem. At the same time, EVCS not only provides energy but can collect a wealth of sensitive personal data from payment to precise location or preferences data [2]. Different EVCS models, which use distinct charging methods, can have a different cybersecurity level [3]. Although the EVCS can be vulnerable to cyber attacks, limited best practices have been adopted by the industry to address security issues [4]. Our study investigates security and privacy concerns from a charging method perspective, which is a novel approach as security problems are typically considered from a single component or method perspective. Our work could have a real impact on the design of charging solutions, suggesting industry the less vulnerable or incentive to find mitigations. We start with the description of the different charging methods and compare them to retrieve security strengths and weaknesses, finding the most and the less secure method. Privacy is also a relevant topic because none of the existing standards or the Plug-and-Charge (PnC) provide privacy-preserving solutions to protect sensitive charging and billing data [5]. Our research provides valuable insights for the industry to comply with the UNECE R155 regulation [6]. This regulation requires not only ensuring the security of the vehicle but also of the external components that interact with it, such as back-end servers, which can be targeted by attackers to extract data or launch an attack on the vehicle. We identified possible vulnerabilities in the external vehicle ecosystem through literature references, which can help the industry to ensure compliance with UNECE R155 - Annex 5. To this purpose, in Section V we map each discovered EVCS security or privacy vulnerability with the mitigations suggested by the UNECE R155. Another relevant aspect of the EV life cycle is the *range anxiety*, namely the fear that the EV has not sufficient energy storage to cover the road distance to reach the destination or the next EVCS. This anxiety may increase with the security and privacy risks that the EVCS can suffer. For this reason, our work can contribute to describe the state of the art to find possible mitigations to be implemented by EVCS stakeholders.

The paper is structured as follows: Section II describes the related work, while Section III defines the security and privacy model that we use for our analysis. Section IV is the core of our work, where we describe the five charging methods and for each, starting from the scientific literature, we analyze the security and privacy issues. Section V contains the comparison among the different methods, summarizing the results of the previous section, and a mapping between the existing vulnerabilities with UNECE R155 mitigations. Section VI is the conclusion of our work with the findings and future possible research.

II. Related work

In the last years, several studies have discussed the different security and privacy aspects of the EV charging ecosystem, in

particular, the last three years can be considered the beginning of a relevant research interest in EVCS security and privacy.

In July 2022, the United States Department of Energy by National Technology and Engineering Solutions of Sandia released one of the main documents related to the cybersecurity of EVCS [4]. This report provides the power, security, and automotive industry with some recommendations founded on research that are necessary to secure EV charging ecosystem. Nasr *et al.* [7] analyze possible attacks against the EVCS like firmware and billing manipulation. They propose also possible mitigations and patching like enforcing authentication on all endpoints to patch information disclosure issues (Common Weakness Enumeration CWE-200). The review of Bharathidasan *et al.* [8], published in 2022, provides a significant study of the global market scenario for EVs with a focus on cybersecurity needs. The authors analyze the different charging methods describing present and future trends. They underline that the Electric Vehicle Supply Equipment (EVSE) interfaces have significant cybersecurity research needs, for instance, techniques to avoid the loss or tampering of charging signals through side-channel assaults. Regarding security mitigations, in 2020, Basnet *et al.* propose a deep learning-based intrusion detection system (IDS) to detect the Denial of Service (DoS) attacks in the EVCS. They underline the need for protection systems and, using long-short-term memory (LSTM) algorithms, they can achieve more than 99% detection accuracy.

About information privacy, in 2022, Islam *et al.* [9] propose an intelligent privacy preservation scheme for EVCS using local differential privacy while Almuhaideb *et al.* [10] propose an efficient privacy-preserving and secure authentication based on elliptic curve to fulfill the re-authentication protocol requirements to reduce the overhead of future authentication processes. Unterweger *et al.* [11] provide a deep analysis and overview of the EVCS ecosystem concerning privacy, suggesting a common naming convention and methodology to analyze privacy and establish common standards. Dedicated to the security issues and challenges of the Open Charge Point Protocol (OCPP), the work of Garofalaki *et al.* [12] describes the entities that take part in an OCPP-based smart charging scenario, identifying the security threats and possible solutions. Alcaraz *et al.* [13] focus on OCPP attacks which can cause energy theft or fraud.

To conclude, concerning the current literature, our work presents for the first time a comparative analysis among all the five charging methods focusing on cybersecurity and privacy aspects by highlighting the weakness of each charging mode and discussing them with respect to UNECE R155.

III. Threat Model

While an EV is connected to the charging station, it exchanges not only energy but also data with the infrastructure and external nodes. The goal is to discover which cyber attacks can be performed and their impact on each of the five different charging methods. As proposed in [14] and [4], we decide to use the STRIDE model, that is an acronym for:

- *S*poofing: gain illegal entry into a secure system using another user's authentication information;
- *T*ampering: an intentional but unauthorized act resulting in the modification of a system;
- *R*epudiation: a subject falsely denying having performed a particular action;
- *I*nformation Disclosure: unauthorized divulging of, or acquisition of, information;
- *D*oS: the prevention of authorized access to resources or the delaying of time-critical operations;
- *E*levation of Privilege: an unprivileged user that gains privileges to perform security-relevant actions.

We consider also physical security because the EVCS infrastructure can range from little to no supervision. This situation can allow an attacker to compromise the physical components which can be a vector to enter into the charging ecosystem. This type of situation can be called as "*cross-layer attack*" [15], when the weakness of a layer like the physical, with, for example, an accessible RS-232 port, is used to enter into another component, generating a sophisticated, more difficult to detect, and dangerous attack. The Open Web Application Security Project (OWASP) threat modeling process states that in the STRIDE model the Information Disclosure compromises the property of confidentiality, which is the mandatory property to preserve privacy. Thus, in our STRIDE model, privacy is represented by Information disclosure.

IV. Security and Privacy of Charging methods

The charging method defines the structure and the characteristics of the EVCS. We can identify three main categories of charging systems:

1) *Conductive charging*, a wired charging system to transfer energy using electrical contacts. It can use i) *Alternating current* (AC), an electric flow charge which changes polarity and direction over time for On Board Charger (OBC); ii) *Direct current* (DC), one-directional flow of electric charge for Off Board Charger Board Charger (DC Charger);
2) *Inductive charging*, also known as wireless charging. It uses electromagnetic induction to provide electricity to portable devices and it can be i) *Static*, when energy is delivered from an EVCS to the vehicle when it stopped; ii) *Dynamic*, when energy is delivered from the roadway, which is the EVCS, to the vehicle when it is in motion;
3) *Battery Swapping System (BSS)*, quick refilling with the substitution of the empty battery with a fully charged battery. It can be considered the shortest system to have a complete charge. According to NIO, a Chinese manufacturer of smart EVs, a swap station can take only 3 minutes to swap a battery [16].

Note that there is also the possibility, called *trickle charge*, to connect directly the vehicle to the normal current sockets of the house, without any other intermediate component. However, this charging system is not allowed in some countries and it can not be considered an EVCS because it lacks the main elements of an EVCS like a charger or a control device.

A. EVCS common components

Table I reports the vulnerabilities of the common components of the different charging methods. The Power Grid

TABLE I
COMMON ELEMENTS' LIST OF VULNERABILITY OR ATTACK METHOD FOLLOWING THE STRIDE MODEL. IN SQUARE BRACKETS AND BOLD THE IDENTIFIER OF EACH VULNERABILITY.

Element	Security Attack Class					
	S	T	R	I	D	E
Power Grid	-	-	-	-	**[V.1.1]** Increase in Charging Demand / Switching Attack [17] / **[V.1.2]** Under-frequency load event [18]	**[V.1.3]** Consumption patterns can be used to observe and infer properties that many would consider private [19]
Power Link	-	-	-	-	**[V.1.4]** Sites are often located in remote areas and difficult to monitor, leaving them vulnerable targets [19]	-
EMS	**[V.1.5]** The used protocols are vulnerable to sniff [14]	**[V.1.6]** False Data Injection Attack (FDIA) [20]	-	**[V.1.7]** Malware [20]	**[V.1.8]** Malware [20]	-
OSCP	-	-	-	-	**[V.1.9]** Electromagnetic attack [20]	-
CSMS	-	-	-	**[V.1.10]** Malware [20]	**[V.1.11]** Malware [20]	-
OCPP	**[V.1.12]** Highjack the communication and gain control [21]	-	-	**[V.1.13]** Passive traffic analysis [13] / **[V.1.14]** Man in the middle on data privacy [22]	**[V.1.15]** Electromagnetic attack [20]	-

represents the physical network to deliver electricity from the producer to the users, connected by a power link. Both of them can suffer DoS attacks, but also, with an escalation of privilege, there is the possibility, starting from the consumption patterns, to inferring personal information of the users, compromising also privacy. The Energy Management System (EMS) is a remote computer-aided tool used by power system operators to monitor, manage, and serve optimal energy [23]. Usually, EMS uses OSCP to communicate with EVCS components. The Charging Station Management System (CSMS) is a software and hardware component that manages the EVCS operations and its security and authentication. The EMS and the CSMS can suffer malware attacks. Two communication protocols are defined as follows:

- *Open Smart Charging Protocol (OSCP)* is used to communicate from the management system of a power grid and the CSMS. The actual version, OSCP 2.0 released in 2020 provides a 24-hour forecast of the available grid capacity. Regarding security, the endpoints (HTTP) are protected with SSL and token-based authentication;
- *Open Charge Point Protocol (OCPP)* is used to communicate from CSMS and the physical EVCS. The actual version, OCPP 2.0.1 released in 2018 supports ISO 15118. Regarding security, it implements three different profiles, chosen according to the security needs of the EVCS ecosystem: Basic security profile, TLS with Basic Authentication, and TLS with Client Side Certificates.

The communication protocols can both suffer electromagnetic attacks, which can cause DoS. According to literature, only OCPP can suffer sniffing and information disclosure.

B. Conductive Charging

Fig. 1 reports a schematic structure of a conductive charging EV ecosystem which can be considered descriptive for both AC and DC solutions.

We consider EVCS not only the station where the vehicle connects to charge but also the incoming and outcoming wired and wireless connections. For instance, it could be a wallbox for home charging or a column in a parking area. In any case,

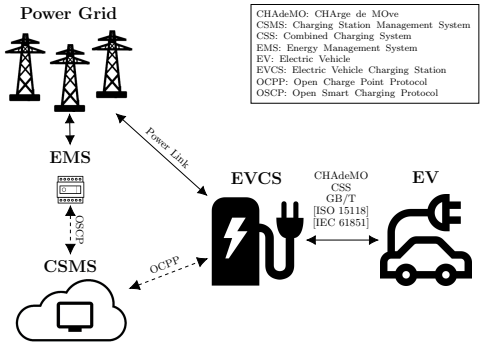

Fig. 1. EV ecosystem with the most commonly used communication solutions. Solid lines represent the wired connections, while dotted lines are wireless connections.

it has a wired connection with the power grid, and, usually, a wireless or wired link with a CSMS using OCPP. The EVCS has a socket outlet with a fixed or removable cable that is used to connect the EVCS with the EV, using a charging connector, which is usually classified by the rate at which the batteries are charged. *Level 1* connectors, following the standard J1772, are the most basic and slowest charging solution. They use AC, usually 120 V, for example, in a private context. *Level 2* plugs are AC 240 V chargers in public areas, following J1772 standard or having Tesla connectors. The last category is *Level 3*, using DC fast charging only for public contexts. Some charging connectors examples are:

- *CHArge de MOve (CHAdeMO)* is a fast-charging system developed by Japanese carmakers since 2010 following the standard IEC 61851. It is used in the DC stations. It works with the Controller Area Network (CAN)-based protocol: its messages are sent to the EV via CAN bus;
- *Combined Charging System (CSS)* is a charging system developed by European and North American car manufacturers since 2011. CSS allows AC and DC charging, following the IEC 61851. For DC connections, CSS1 is mainly used in North America, while CSS2 is in Europe and the rest of the world;
- *Guobiao standards (GB/T) 18487.1/20234/27930* are a

TABLE II
CONDUCTIVE CHARGING LIST OF VULNERABILITY OR ATTACK METHOD FOLLOWING THE STRIDE MODEL

Element	Security Attack Class					
	S	T	R	I	D	E
EVCS	**[V.2.1]** Hard-Coded Credentials [21] / **[V.2.2]** Side-channel attack [20]	**[V.2.3]** Cross-Site Scripting (XSS) [21]	**[V.2.4]** Repudiation caused by manipulation and obscuration of the transaction details [4]	**[V.2.5]** SQL Injection [21]	**[V.2.6]** Server-Side Request Forgery (SSRF) [21]	**[V.2.7]** Loss of financial/energy transaction or nonrepudiation [4]
CHAdeMO	**[V.2.8]** The cybersecurity threats will follow the vehicle's CAN communication security threats [24]					
CSS	**[V.2.9]** TLS is not required [24] / **[V.2.10]** Sniff data using unencrypted ISO 15118 traffic [25]	**[V.2.11]** Fabrication of metering and tariff information can result in free charging [24] / **[V.2.12]** Injected a Log4Shell payload [26]	-	**[V.2.13]** Eavesdropping if information not encrypted properly [24]	**[V.2.14]** Attack on communication channels to inhibit the charging [24] / **[V.2.15]** Brokenwire attack [27]	-
GB/T	**[V.2.16]** The cybersecurity threats for GB/T 20234 will follow the vehicle's CAN communication security threats [28]					
ISO 15118	**[V.2.17]** Sniff data using unencrypted ISO 15118 traffic [25] [28]	-	-	**[V.2.18]** Privacy concerns [21]	-	-
IEC 61851	**[V.2.19]** Authentication was considered outside the scope of this protocol [21]	-	-	-	-	-
EV	**[V.2.20]** Side-channel attack [20]	-	-	**[V.2.21]** Exposure of the EV driver's sensitive data [20]	-	-
EV Driver	**[V.2.22]** Side-channel attack [20]	-	-	**[V.2.23]** Through smartphone app access to personal EV driver and vehicle information [29]	-	-

set of charging standards developed in China since 2011 containing requirements for safety and connection issues. GB/T allows AC and DC charging, following IEC 61851.

Note that the possible configuration could be different, especially for the connection EVCS-EV. For example, another possible connector is the Tesla version, used in all markets for Tesla vehicles, following the North American standard J1772 for AC and DC chargers.

Table II reports the result of our analysis on the possible vulnerabilities of each component of the EVCS ecosystem. From a physical security perspective, Levels 2 and 3 require more protections because they are installed in a public context, where an attacker could have more interest to perform an attack. At the same time, the connection between the EVCS and the EV is standardized by ISO 15118 and IEC 61851. The EVCS is the core of the ecosystem and it can be attacked by injecting malicious code to infer data or cause a DoS, with also the possibility to cause financial loss with an elevation of privilege. Among the different versions of connectors, CSS seems to be the most studied and also prone to several attacks like the recent *brokenwire* attack [27], causing sessions to abort. While the other two connectors type CHAdeMo and GB/T use the CAN protocol for handshaking and to exchange configuration parameters, so they can suffer the vulnerabilities of the CAN bus like the lack of confidentiality. The standard ISO 15118 can suffer the sniffing of unencrypted traffic, while the only application of the standard IEC 61851 can not guarantee any security protection. Through its charging systems, EVs can suffer different attacks like the side-channel or the exposure of the driver's sensitive data. The driver of the EV should be considered as part of the ecosystem and could be used as a vector to inject malicious code like using the charging app installed on the driver's smartphone.

To summarize, in this scenario, it seems that security may be compromised in several components with high impact on service availability, but also privacy could be risked in almost all the software components of the ecosystem.

C. Inductive Charging

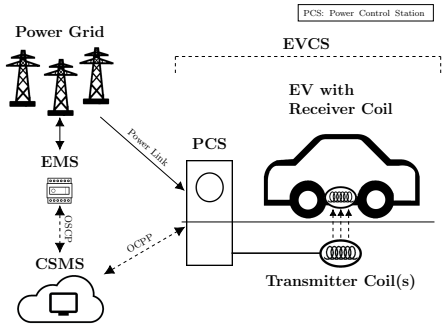

Fig. 2. EV ecosystem of the inductive static charging method. The PCS can be located in a public or private area.

In the two inductive static charging methods, charging is carried out when the EV is stopped in a public or private area (Fig. 2). Concerning the conductive method, the main differences are the presence of the transmitter and receiver coil, and the presence of a Power Control Station (PCS), which can be considered as the physical component to manage the charging. The set of the transmitter coil and the PCS forms the EVCS. The other parts of the schema reported in Fig. 2 are the same as the conductive charging with the same scope to manage and provide energy to the EVCS. The PCS with

its hardware/software components can be prone to spoofing attacks, causing possible eavesdropping that can cause a leak o the privacy of users' information.

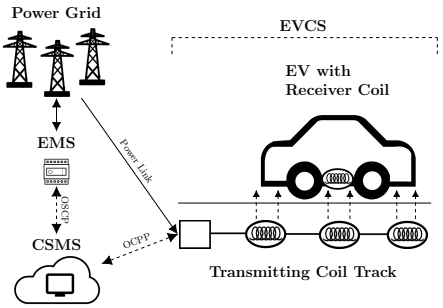

Fig. 3. EV ecosystem of the inductive dynamic charging method. The Transmitting Coil Track is a road that can transmit inductive charge like the Stellantis project in Chiari (Italy) [30].

During the driving, the receiver coil installed at the bottom of the EV receives energy directly from the road in which it is installed a transmitting coil track, composed of different subsequent coils (Fig. 3). This method has several advantages allowing theoretically infinitive driving. This technology is under study and test: in the Swedish island of Gotland, where, in 2021, it was installed a 1.6-kilometer trail track to test truck charging. Regarding the physical component like the coils, the only attack that can suffer is a DoS caused by jamming to interfere with electromagnetic waves.

TABLE III
INDUCTIVE CHARGING LIST OF VULNERABILITY OR ATTACK METHOD FOLLOWING THE STRIDE MODEL

Element	Security Attack Class					
	S	T	R	I	D	E
PCS	**[V.3.1]** The unshielded charging cable leaks signals of the PLC-based charging communication, which allows an adversary to eavesdrop wirelessly on the communication [28]	-	-	-	-	-
Trasmitter coil	-	-	-	-	**[V.3.2]** Broadband noise jamming [28]	-
EV (Receiver coil)	-	-	-	-	**[V.3.3]** Broadband noise jamming [28]	-

D. Battery Swapping

The battery swapping method (Fig. 4) can be considered the fastest among the different charging methods because it consists only of the substitution of the empty battery with a fully charged battery. This operation can be completed in a few minutes in specific battery swapping stations (BSS) that contains a different charged battery. When a user needs one, it can independently change the battery for motorbike or wait some minutes in a station for a road vehicle [16].

Today in the world, the BSS network is not enough developed to support the daily use of EV with battery swapping. However in China, NIO is planning to have more than 1300 battery swap stations by the end of 2022 and to install 1000 BSS outside China by 2025.

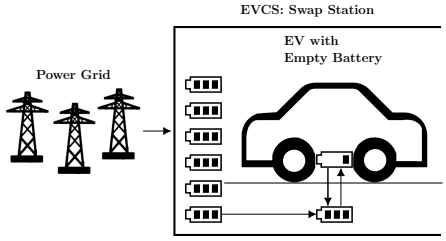

Fig. 4. EV Battery swapping ecosystem. The empty battery of the vehicle is exchanged with a fully charged battery. The swap station is connected to the power grid with a power line.

The main security problem may be related to the presence in the batteries of a memory, which can store usage and user information. In the case that the battery memory is not erased after each usage, the information could be read by an attacker.

TABLE IV
BATTERY SWAPPING LIST OF VULNERABILITY OR ATTACK METHOD FOLLOWING THE STRIDE MODEL

Element	Security Attack Class					
	S	T	R	I	D	E
Battery	-	-	-	**[V.4.1]** If the battery has a memory, the attacker can extract critical information such as the driver's habits and location [15]	-	-

V. DISCUSSION

The charging methods can be compared from a security and privacy perspective to identify their strengths and weaknesses. Starting from the previous single analysis, all the charging methods share the vulnerabilities of the power grid, power link, EV, and EV driver. However, the conductive charging methods (both AC and DC) suffer the weaknesses of the communication protocols and applied standards, while the inductive method and the BSS are not prone to this category of security issues. The most common and studied threats are the DoS and the elevation of privileges to perform cross-layer attacks.

Moreover, the five methods have different charging speeds that can change according to the vehicle (Table V) and may influence the exposure to cyber attacks. Generally speaking, AC charging can be considered a slow method as static inductive charging. DC charging is considered the fastest between the conductive and inductive methods. However, battery swapping is the fastest among all methods to have a fully charged battery. The location of the stations can vary from private to public. Nevertheless, until today, only the AC and the static inductive charging are usually installed in private areas like houses.

A. UNECE R155 Mitigations

To homologate the new road vehicles, cybersecurity regulation UNECE R155 requires that all implemented processes should consider the probable sources of security risk, providing an adequate assessment. During our analysis, we

TABLE V
COMPARISON OF FIVE DIFFERENT CHARGING METHODS

Charging Method	Charging Speed	Usual location	S	T	R	I	D	E
AC Conductive Charging	Slow	Private / Public	●	●	●	●	●	●
DC Conductive Charging	Fast	Pubic	●	●	●	●	●	●
Static Inductive Charging	Slow	Private / Public	●	○	○	○	●	●
Dynamic Inductive Charging	Continuous	Public	●	○	○	○	●	●
Battery Swapping	Fastest	Public	○	○	○	●	●	●

discover that the vulnerabilities, found in the different charging methods, correspond to the risks identified in UNECE R155 Annex 5 Table A1 and that should be treated.

In Table VI, we report each discovered vulnerability with the relative mitigation suggested by UNECE R155. For example, the side-channel attack (V.2.2) on EVCS is a threat identified in Table A1 (4.3.2 Threats to vehicles regarding their communication channels, 4.1 Spoofing), which needs to be mitigated to receive the vehicle homologation. In particular, Table B1 suggests mitigation M10 where *the vehicle shall verify the authenticity and integrity of messages it receives* [6]. Regarding the connectors CHAdeMo and GB/T standards in Table A1, point 11.1, UNECE R155 identifies the malicious CAN messages as a possible threat (V.2.8, V.2.16). So, in Table B1, the mitigation M15 suggests adopting measures to detect malicious CAN internal messages. Note that the vulnerability V.2.4, related to repudiation, following the OWASP definition, can be classified as an attack on the transaction details and logs. Thus, we map V.2.4 with mitigation M7, which can fix unauthorized deletion/manipulation of system event logs.

In Table III, regarding the physical component of the inductive charging like the coils, the only attack that can suffer is a DoS caused by jamming to interfere with electromagnetic waves (V.3.2, V.3.3). UNECE R155 requires to treat also this last attack. Table A1, (4.3.5 Threats to vehicles regarding their external connectivity and connections, 16.3 Interference), considers the possible interference with short-range wireless systems or sensors, which the transmitting coils can be. In Table B1, mitigation M20 suggests adding security controls that shall be applied to systems that have remote access or, we can infer, that can suffer remote DoS attacks.

The issue V.4.1 in Table IV, related to the BSS, can be the vulnerability of UNECE R155 Table A1 (4.3.1 Threats regarding back-end servers related to vehicles in the field, 3.5 Information breach), where it is reported the unintended sharing of data. UNECE R155 Table C1 reports as mitigation M8 the security controls that can be found in OWASP documents.

With respect to the UNECE R155, all the charging methods require actions to mitigate the possible threats. In particular, a single mitigation can treat several vulnerabilities. For example, mitigation M12, which requires the verification of the messages authenticity and integrity, can mitigate nine discovered vulnerabilities. However, a conductive charging station seems to need more solutions than a battery swapping station. UNECE R155 Table B1 and C1 can provide the necessary mitigations to the retrieved threats, but, until today, each carmaker like Tesla seems to adopt propriety solutions with a wide range of standards and different connectors, which can increase the security risks.

To conclude, the conductive methods can be considered more exposed to security attacks and lack of privacy with the information disclosure, while the other methods with less components and communication protocols seems to reduce the security and privacy risks.

VI. CONCLUSION

This work provides a comprehensive analysis of the security and privacy of various EV charging methods and highlights the importance of addressing vulnerabilities to meet homologation standards. Besides, it provides industry a complete security analysis to design the future EVCS. We also describe how vulnerabilities, even if out of the vehicle, should be treated to reach the UNECE R155 homologation and we map the vulnerabilities with the possible mitigations.

From this work, we can infer that the conductive methods with more components and protocols seem to be more vulnerable, because, following the cross-layer attacks, the most vulnerable node defines the level of security of the entire ecosystem while the BSS seems to be the most secure and fastest method because the substitution of the battery can bring only an information disclosure. However, until now, BSS security seems to be an understudied topic, so, as future research, it may be useful to study its possible vulnerabilities and security mitigations. To conclude, this work can serve as a valuable resource for industry professionals and researchers working on the design and development of secure and reliable EVCS.

ACKNOWLEDGMENT

The activity leading to this work has received funding from program under grant agreement No 883135 (E-Corridor), PTR 22-24 P2.01 (Cybersecurity), and SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

REFERENCES

[1] The global electric vehicle market overview in 2022; statisics and forecasts. Accessed on October 28, 2022. [Online]. Available: https://www.virta.global/en/global-electric-vehicle-market

[2] J. Banda. Electric vehicle charging stations may be a privacy risk. Accessed on October 28, 2022. [Online]. Available: https://iapp.org/news/a/electric-vehicle-charging-stations-may-be-a-privacy-risk/

[3] H. ElHussini, C. Assi, B. Moussa, R. Atallah, and A. Ghrayeb, "A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid," *ACM Trans. Internet Things*, vol. 2, no. 2, mar 2021. [Online]. Available: https://doi.org/10.1145/3437258

[4] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt, T. Carroll, L. O'neil, B. Dindlebeck, P. Maloney, J. O'brien, D. Gotthold, R. Varriale, T. Bohn, and K. Hardy, "Cybersecurity for electric vehicle charging infrastructure," 07 2022.

TABLE VI
UNECE R155 MITIGATIONS TO ADDRESS DISCOVERED VULNERABILITIES

UNECE R155 Mitigation Reference	UNECE R155 Mitigation Description	Addressed Vulnerabilities
M1	Security controls are applied to back-end systems to minimise the risk of insider attack	V.1.3
M2	Security controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP	V.1.5
M7	Access control techniques and designs shall be applied to protect system data/code. Example Security controls can be found in OWASP	V.2.11, V.2.4
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of security controls can be found in OWASP	V.2.19, V.2.23, V.4.1
M9	Measures to prevent and detect unauthorized access shall be employed	V.2.1
M10	The vehicle shall verify the authenticity and integrity of messages it receives	V.1.12, V.1.14, V.2.2, V.2.3, V.2.5, V.2.6, V.2.12, V.2.20, V.2.22
M12	Confidential data transmitted to or from the vehicle shall be protected	V.1.13, V.2.7, V.2.9, V.2.10, V.2.13, V.2.17, V.2.18, V.2.21, V.3.1
M13	Measures to detect and recover from a denial of service attack shall be employed	V.1.1, V.1.2, V.1.4, V.1.9, V.1.15, V.2.14, V.2.15
M14	Measures to protect systems against embedded viruses/malware should be considered	V.1.7, V.1.8, V.1.10, V.1.11
M15	Measures to detect malicious internal messages or activity should be considered	V.2.8, V.2.16
M20	Security controls shall be applied to systems that have remote access	V.3.2, V.3.3
M22	Security controls shall be applied to external interfaces	V.1.6

[5] D. Zelle, M. Springer, M. Zhdanova, and C. Krauß, "Anonymous charging and billing of electric vehicles," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ser. ARES 2018. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3230833.3230850

[6] UNECE, "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," United Nations Economic Commission for Europe, Geneva, CH, Regulation Addendum 154 – UN Regulation No. 155, 2021. [Online]. Available: https://unece.org/sites/default/files/2021-03/R155e.pdf

[7] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102511, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003357

[8] M. Bharathidasan, V. Indragandhi, V. Suresh, M. Jasiński, and Z. Leonowicz, "A review on electric vehicle: Technologies, energy trading, and cyber security," *Energy Reports*, vol. 8, pp. 9662–9685, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235248472201410X

[9] S. Islam, S. Badsha, S. Sengupta, I. Khalil, and M. Atiquzzaman, "An intelligent privacy preservation scheme for ev charging infrastructure," *IEEE Transactions on Industrial Informatics*, pp. 1–10, 2022.

[10] A. M. Almuhaideb and S. S. Algothami, "Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ecqv," *Journal of Sensor and Actuator Networks*, vol. 11, no. 2, 2022. [Online]. Available: https://www.mdpi.com/2224-2708/11/2/28

[11] A. Unterweger, F. Knirsch, D. Engel, D. Musikhina, A. Alyousef, and H. Meer, "An analysis of privacy preservation in electric vehicle charging," *Energy Informatics*, vol. 5, 04 2022.

[12] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," *IEEE Communications Surveys Tutorials*, vol. 24, no. 3, pp. 1504–1533, 2022. [Online]. Available: https://doi.org/10.1109\%2Fcomst.2022.3184448

[13] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.

[14] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.

[15] A. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A security perspective on battery systems of the internet of things," *Journal of Hardware and Systems Security*, vol. 1, pp. 1–12, 06 2017.

[16] Nio power swap. Accessed on October 28, 2022. [Online]. Available: https://www.nio.com/nio-power

[17] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers Security*, vol. 112, p. 102511, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003357

[18] G. S. Morrison, "Threats and mitigation of ddos cyberattacks against the u.s. power grid via ev charging," 2018.

[19] L. A. Maglaras, M. A. Ferrag, H. Janicke, N. Ayres, and L. Tassiulas, "Reliability, security, and privacy in power grids," *Computer*, vol. 55, no. 9, pp. 85–88, 2022. [Online]. Available: https://doi.org/10.1109/MC.2022.3184425

[20] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," *IEEE Communications Surveys &amp Tutorials*, vol. 24, no. 3, pp. 1504–1533, 2022. [Online]. Available: https://doi.org/10.1109%2Fcomst.2022.3184448

[21] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, "Electric vehicle attack impact on power grid operation," *International Journal of Electrical Power &amp Energy Systems*, vol. 137, p. 107784, may 2022. [Online]. Available: https://doi.org/10.1016%2Fj.ijepes.2021.107784

[22] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.

[23] Igi global, ems definition. Accessed on October 28, 2022. [Online]. Available: https://www.igi-global.com/dictionary/energy-management-system-ems/9856

[24] C. Hodge, K. Hauck, S. Gupta, and J. Bennett, "Vehicle cybersecurity threats and mitigation approaches," 2019.

[25] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, p. 3931, 05 2022.

[26] S. Dudek. Examining log4j vulnerabilities in connected cars and charging stations. Accessed on October 28, 2022. [Online]. Available: https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html

[27] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire : Wireless disruption of CCS electric vehicle charging," *CoRR*, vol. abs/2202.02104, 2022. [Online]. Available: https://arxiv.org/abs/2202.02104

[28] S. Kohler, S. Birnbach, R. Baker, and I. Martinovic, "On the security of the wireless electric vehicle charging communication," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, Singapore, 2022.

[29] O. G. M. Khan, E. El-Saadany, A. Youssef, and M. Shaaban, "Impact of electric vehicles botnets on the power grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*, 2019, pp. 1–5.

[30] Stellantis inductive track. Accessed on October 28, 2022. [Online]. Available: https://www.stellantis.com/en/news/press-releases/2022/june/arena-del-futuro-demonstrates-capability-of-dynamic-inductive-recharging-technology-for-electric-vehicles