Vulnerability analysis of an electric vehicle charging ecosystem*

Roland Plaka, Mikael Asplund, Simin Nadjm-Tehrani

Department of Computer and Information Science,
Linköping University, Sweden
{roland.plaka,mikael.asplund,simin.nadjm-tehrani}@liu.se

Abstract. The increase of electric vehicles has exacerbated the need for adequate security measures in the electric vehicle charging ecosystem (EVCE). Integrating IT services into the electric vehicle charging infrastructure exposes it to several new attack vectors. In this paper, we apply a vulnerability analysis method to assess the current security posture of the internet-connected EVCE components. Our method is based on penetration testing principles using open-source cybersecurity search engines. Using this method, we gathered security-related information apparently associated with eight charging station vendors and three management systems, and we found 13 vulnerable technologies containing 81 vulnerabilities. Based on the information provided by vulnerability databases, we classified the threats according to the STRIDE model and analyzed the potential consequences of the vulnerabilities in terms of the security properties that can be violated.

Keywords: EV charging · cybersecurity · vulnerability analysis

1 Introduction

Integrating IT services in the electric vehicle charging stations introduces several attack surfaces to this domain, threatening the security of the vehicle, the charging station, and potentially the grid. The rapid deployment of electric vehicle charging stations (EVCSs) has contributed to the electric vehicle (EV) ecosystem's lack of proper security measures. Evidence of cyberattacks at EV charging stations illustrates increasing cybersecurity risks for critical energy and transportation infrastructures. For example, there are reports that some charging stations in Russia were hacked[1], and electric vehicle users in the U.K. reported seeing videos with inappropriate content playing on public charging stations[2]. The electric vehicle charging infrastructure is an important part of the smart

* Supported by Vinnova through the project Sustainable Energy with Adaptive Security(2021-01683) and RICS Centre on Resilient Information and Control Systems financed by Swedish Civil Contingencies Agency(MSB)

[1] https://www.utilitydive.com/news/putin-hacks-of-ev-electric-vehicle-charging-stations-cybersecurity-preparations/634547/

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

grid, so such cyberattacks could potentially impact the electrical grid, ranging from localized, relatively minor effects to long-term national disruption [6].

Previous research [21] has shown that several Electric Vehicle Charging Management Systems (EVCMSs) exhibit internet-facing ports and assets with exploitable vulnerabilities. However, we are not aware of any studies that have focused on the internet-facing charging stations (EVCSs) themselves. Since both the management systems and the charging stations are connected to the internet, they are likely to be targeted by an adversary to gain access to the system. Thus, there is a need to complement existing research on the security posture of electric vehicle management systems based on insights on the state of security of the charging stations. While the management system can operate in a cloud environment with associated security protection mechanisms, the charging stations are essentially IoT devices with limited capacity and lack of security monitoring services. Moreover, the potential impact of a security breach at the charging station is high since it might negatively affect the vehicle and even the electrical grid if coordinated with other compromised charging stations [17].

In this work, we investigate the current security state for the electric vehicle charging ecosystem. This ecosystem consists of electric vehicles, mobile applications accessed by the EV user, charging stations, charging management systems, and web applications. Our focus is on the internet-connected EV charging stations (EVCSs) and charging management systems (CMS), whereas the vehicle's connection to the CS using protocols such as ISO 15118 is outside our scope. We analyze the relevant components to identify protocols, services, and vendor-specific information. We then use existing cybersecurity search engines to collect information about internet-connected charging stations and discover which ports, services, and technologies are provided by the hosts. We perform a vulnerability assessment using standard vulnerability databases based on this public information. Moreover, for each found vulnerability we classify it according to Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat model to better understand the security property that might be violated if the vulnerabilities were to be exploited. Finally, we perform an initial assessment of the potential impact of such attacks if performed against the EV charging components.

Our results show that many analyzed hosts expose relatively complex software services like the Apache web server and interactive web applications. We identify a total of 78 vulnerabilities in 8 charging stations and 3 vulnerabilities for 3 charging management systems. We disclose the identified issues by making responsible disclosures and discussing vendor responses. Our threat analysis of these vulnerabilities reveals that most are related to information disclosure, but other threats exist, such as spoofing and denial of service.

To summarize, our contributions in this paper are as follows.

- Identify and analyze 81 vulnerabilities in internet-facing electric vehicle charging stations and charging management systems. Identifying these vulnerabilities seems to indicate that the security level of the vehicle charging infrastructure is still relatively weak.

– Threat classification and initial impact analysis according to the STRIDE model for EV charging infrastructure attacks potentially possible given the identified vulnerabilities.

In the rest of this paper, we first introduce the charging infrastructure components and technologies to visualize and clarify the focus of our work. We also briefly discuss the security aspects of each component, its limitations, and the threats they may face. In section 3, we describe the application of the vulnerability analysis method for detecting and analyzing vulnerabilities in EV charging systems and the results. Section 4 classifies the observed vulnerabilities according to the STRIDE model and details some of the most interesting aspects of the vulnerabilities. In addition, we discuss the impacts of the threats being exploited, identifying the potential risks that may affect the components of the EV charging ecosystem. Section 5 discusses the identified issues by making responsible disclosures and discussing vendor responses. Section 6 presents the related work in this domain, and section 7 concludes the paper.

2 Charging infrastructure components

This section deals with the shortcomings of security in the EV charging ecosystem. As shown in Figure 1 the charging ecosystem's architecture and common components. Earlier papers have presented similar architectures [6]. It presents the information flow marked with blue arrows and the power flow marked with red arrows. Attacker pathways to the charging stations are not limited to physical attacks but also include web-based attack vectors. If these succeed, attackers can change the operation of devices, switch on or off the charging sessions, and so on. Assuming that attackers may have access to a large number of charging stations, one can imagine them simultaneously triggering the termination of all active charging sessions, potentially causing harm to energy utilities and damage to equipment due to the sudden change in electrical load [31].

The Open Charge Point Protocol (OCPP) supports communication between the charging stations and the management systems. This protocol has adapted to the changing security requirements due to earlier concerns with weak authentication, end-to-end security, non-repudiation, and weak encryption. However, securing OCPP itself does not resolve all security problems in these systems. Physical security of the CSs, EV charging applications, hardware, and software-related security also need better understanding. In the remainder of this section, we discuss each of the architecture's main components and security issues related to these components.

Electric vehicle (EV) Electric vehicles are what motivates the existence of the charging infrastructure. Data exchange across the EV charging infrastructure is enabled through various communication protocols. The communication between the EV and EVCS is mainly provisioned through the following standards:

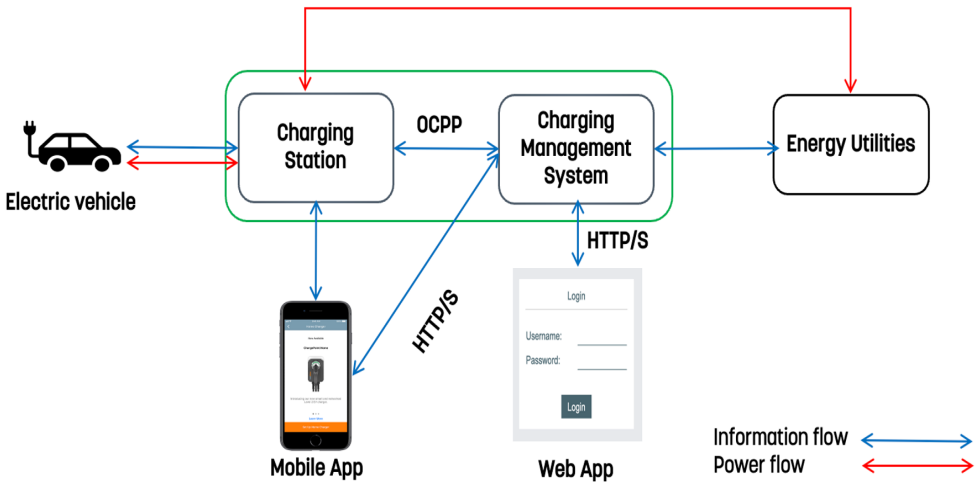

Fig. 1. EV charging ecosystem

- International Electromechanical Commission (IEC): IEC defines multiple standards that address different aspects of EV charging, including IEC 62169 and 61851.
- International Standardization ISO (ISO): ISO 15118 details the communication infrastructure within the charging environment and supports power flow from EVs.

Our work does not investigate the security posture of the communication between the EV and EVCS, focusing rather on the EVCS and CMS components.

Charging Station Charging stations act as an interface or a high-wattage access point between the EV and the power grid. CSs are IoT devices running firmware and are located in close vicinity of the charging site. Charging stations can provide authentication based on RFID access tags and, in some cases, exhibit a payment terminal for credit card payments. CSs are controlled by the Charging Management System (CMS), which creates the messages that declare the power limits and the operational state of the CS. The CS can be compromised directly via on-site interactions or remotely through communication interfaces. An attacker who controls many CSs and EVs can, for instance, attempt to disrupt the power grid with synchronized charging loads. Notably, control over a large enough number of CPs and EVs would be gained via remotely exploitable vulnerabilities. Charging stations typically have internal charger ports, external maintenance ports, and wired ports. Physical ports are available for CS vendors to debug the equipment; however, these ports are often left open in production equipment, which may allow adversaries to monitor or disrupt equipment oper-

ations. Charging stations commonly host Telnet, SSH, or local website services, allowing the owner to configure the device or collect/maintain data [14].

EVCS-CMS The Open Charge Point Protocol leads the effort towards a standardized communication protocol for this domain. OCPP facilitates the exchange of data between the CS and CMS, and it is used to manage the schedule of charging EVs, secure the logs of EV users and their charging, and maintain the status of the EVCS itself. Different versions of this protocol have been developed, starting from version OCPP 1.2, followed by 1.5, 1.6, and up to the latest OCPP 2.0. Attackers may undesirably exploit the compromised EVCS station to jeopardize the supply-demand balance of a grid by remotely controlling the charging behaviors of the station through a large-scale compromise. Each EV generates critical info (location, charging time, and average power consumption per hour) at the charging station, which can be subject to misuse. Attackers can cause a sustained, significant spike in demand, resulting in cascading disconnection of power supply from the grid and abnormal operation performance (load shedding). As a consequence of these attacks, the power plants would be forced into restart conditions, causing widespread brownouts or blackouts and grid instability. This situation can threaten the security and stable operation of the power systems. Identifying and securing the entry points that the threat actors can exploit is critical to controlling unintended access to the CS infrastructure. Therefore, cyber-physical security concerns of the EV charging ecosystem and the possible detection and mitigation measures must be addressed to ensure safe, secure, and resilient charging.

Charging Management System CMSs typically are hosted on a cloud server and manage all operations of the public CSs. This system directs users to the available CS, schedules and manages charging sessions, and logs EVCS utilization data. The CS management system can send the CS-specific control signals related to the duration of the charging session, charging rate, beginning and termination commands, etc. CMS's main tasks are to communicate with the CS, to define the service parameters taking into account the user input, and the EV and the power grid status, to collect and store the charging system data, to host the user application, and to maintain a booking registry for the service. OCPP protocol bears a major responsibility in the communication processes between the CSMs and CSs. OCPP supports smart-charging policies and allows the CMS to implement customized profiles for the charging processes. OCPP allows open communication between an internet-connected charging station and the cloud-based backend, where the operators can easily manage accessibility, remotely upgrade firmware, monitor stations, bill users, optimize charging, and other extended functions.

The CMS can provide discrete grid services (peak shaving, voltage control, demand-side management, demand charge reduction, and emergency demand response). It receives charging requests from EVs/CSs and various grid service requests from utility control centers. It is used to provide common access to

CSs from different vendors over OCPP with the goal of open and interoperable EV charging. Charging management systems consist of the aggregator server, the monitoring clients, and the personal computer, which can be used for information exchange, e.g., battery status and charging information.

Mobile and web applications These are web or smartphone applications through which users can interact with the management system over the internet (in case of a public EVCS) or directly to the charger over a LAN (in case of a private EVCS). These services allow users to reserve and control charging sessions, pay for public charging, control charging rates, start/terminate charging sessions, and monitor the status of the EV. The user's actions, the user device's vulnerabilities, and the user's application add data and parameters to the service, indirectly affecting the charging operations and security.

Energy utilities EVCSs are typically connected to the power grid and, as such, can greatly impact the grid's security and stability. The distribution system operator (DSO) is the organization responsible for distributing electricity to the end-users. The DSO allows or prohibits the power flow to the charging site and, based on the EV's data feedback, ensures balance and decongestion in the grid [24].

3 Vulnerability identification in the EV charging ecosystem

Our goal is to identify vulnerabilities in electric vehicle charging stations and electric vehicle charging management systems accessible from the internet to demonstrate the potential risks facing the EV charging ecosystem. In this section, first, we describe the method we used to identify and assess vulnerabilities, and then we discuss the results.

3.1 Vulnerability analysis method

Figure 2 shows an overview of our method. Each step in the process is described below.

Search engine selection We start with the engine selection in order to reuse known data on internet-facing devices. A survey done in 2020 on cyberspace engines [3] shows that Shodan, Censys, BinaryEdge, ZoomEye, and Fofa are leading regarding the number of detectable devices and services. We use Shodan, Censys, and BinaryEdge in this step of our analysis. ZoomEye and Fofa are used in a later stage.

Keyword selection We need to know what to search for to focus on relevant protocols, components, vendors, and services related to charging stations and charging management systems. To collect instances of potentially vulnerable internet-facing EV services, we select 35 relevant keywords, including "OCPP",

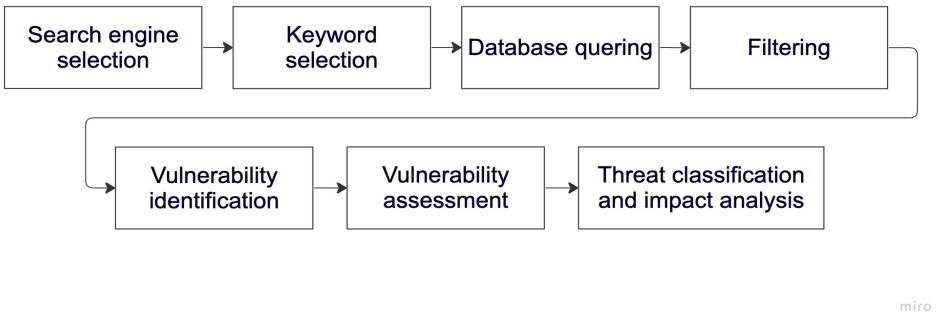

Fig. 2. Overview of vulnerability analysis method

"Charging Interface", "Charging station", "EV charging", "OCPP interface", and several vendor names.

Database querying and search refinement Using the keywords and the selected databases, we discover hundreds of IP addresses, some of which are deemed irrelevant. Combining several keywords helps to restrict the search results. As a result, we narrow down to 35 IP addresses with a relevant technology running behind. For each IP address we collect information such as the server type, location, port, network equipment information (i.e., router or switch), and protocol used.

Filtering We further filter the selected services to exclude non-interactive web pages. This leaves us with web management interfaces that are used for configuring and maintaining CSs and CMSs. As a result, we decrease the number of IP addresses to 11.

Vulnerability identification We leverage search engines ZoomEye and Fofa to passively collect security-related information about the selected IP addresses. As a result, we get security status records, such as vulnerabilities in the form of Common Vulnerability Exposures identities (CVE-ID) and exploitation information.

Vulnerability assessment There are cases when the CVE-ID is missing for an output from the engines. Therefore, we search for more information in the National Vulnerability Database (NVD), which provides the CVE as well as Common Vulnerability Scoring System (CVSS) information. We also use other databases such as Tenable and CVE details database, that combine NVD data with information from other sources, such as the Exploit database.

Threat classification and impact analysis To evaluate the impact of each vulnerability, we consider the security properties that are violated according to the STRIDE threat model. The security properties we consider are authentication, integrity, non-repudiation, confidentiality, availability, and authorization. We analyze the vulnerabilities individually by considering the possible impact on the electric vehicle charging ecosystem, including the affected component.

3.2 Results of vulnerability analysis

Table 1 shows the number of vulnerabilities detected for each charging station interface and OCPP management system used by the named vendors. We identify the vendors based on the information in the web service interface found through the cybersecurity search engines. In total, we identified 81 reported vulnerabilities. 63 vulnerabilities were detected on charging stations and 25 on management systems. The vendors KeContact P30 Wallbox, EVBOX, EVSE, ENSTO Chago EVF200, Mennekes, Teltonika, EVTEC, and ETREL are charging station interfaces connected to the internet. SECWIN, CIRCONTROL, and CIRCUTOR are OCPP management systems deployed on cloud computing technology. Besides, we represent the total number of vulnerabilities and their risk level referring to the CVSS v3.1. These results reveal that the system identified by our method as being connected to KeContact30 P30 Wallbox contains the most significant vulnerabilities.

Note that we have not verified that the vulnerable instances are really running legitimate and updated software versions from the charging station vendors. We perform the analysis based on the information gathered by public sources and any errors or misattributions in those sources would also be reflected in our results. Methodologically, it is difficult to assess this information as there are potential legal and ethical obstacles with digging too deep into the services linked from cybersecurity search engines (as these services might not be meant for public access).

Table 2 shows the number of vulnerabilities detected on each technology. Our vulnerability analysis approach identified ten vulnerable technologies listed under the Product column. In the second column of this table, we list the vulnerabilities detected in each technology, which comprise eighty-one vulnerabilities. With technologies relying on the Apache server, we identified sixteen vulnerabilities making this technology the most vulnerable and exposed on our list.

4 Threat classification and impact analysis

In the previous section we discussed a number of vulnerabilities seemingly present in connected EV charging systems. However, the criticality assessments of these vulnerabilities as retrieved from vulnerability databases are not necessarily made in connection to EV charging systems. Many of the vulnerabilities are in fact related to web services, and therefore the criticality is typically determined based

Table 1. The number of vulnerabilities detected for each type of charging station interface and OCPP management system

Charging station interface/OCPP MS	Critical	High	Medium	Total
KeContact P30 Wallbox	-	11	4	15
EVBOX	2	6	2	10
EVSE	-	6	1	7
ENSTO Chago EVF200	-	5	6	11
Mennekes	-	6	-	6
Teltonika	-	10	1	11
EVTEC	-	4	-	4
ETREL	-	14	-	14
SECWIN	-	1	-	1
CIRCONTROL	1	-	-	1
CIRCUTOR	-	1	-	1

Table 2. The vendors and vulnerabilities detected on each technology

Product	Count of Vulnerability
Apache server	31
DNS server	5
Dropbear server	2
Gateway	4
GoAhead webserver	2
gSOAP toolkit	3
Microsoft IIS httpd	13
OpenSSH server	11
OpenWrt httpd	1
nginx	1
PHP server	8

on a generic system model. In this section, we take a closer look at the vulnerabilities to classify them in relation to what the attacker can accomplish if the vulnerability is exploited. Moreover, we discuss how these attacks could impact the EV charging ecosystem. There are several threat modelling frameworks [25] such as PASTA [30], OCTAVE [15], and LINDDUN [29]. In this work, we use the STRIDE methodology developed by Microsoft. STRIDE is one of the most mature threat modeling approaches that can help evaluate and identify system threats.

To accomplish our goal, we evaluate the information provided by the vulnerability databases such as CVE details[3], and NVD[4]. We aim to identify which security property of the assets is threatened by which threat. Finally, we map the impact information to the violated security property. The mapping is done as follows: threats that violate the authentication property expose the technology

[3] `https://www.cvedetails.com/`
[4] `https://nvd.nist.gov/`

discovered to spoofing attacks; the threats that violate integrity reveal tampering attacks; non-repudiation-related threats expose to repudiation; confidentiality-related threats expose to information disclosure; availability-related threats expose to denial of service, and authorization related threats expose to the elevation of privilege attacks. The chart in Figure 3 presents our findings using the STRIDE model. We proceed by selecting and describing some of the more interesting vulnerabilities in each category.

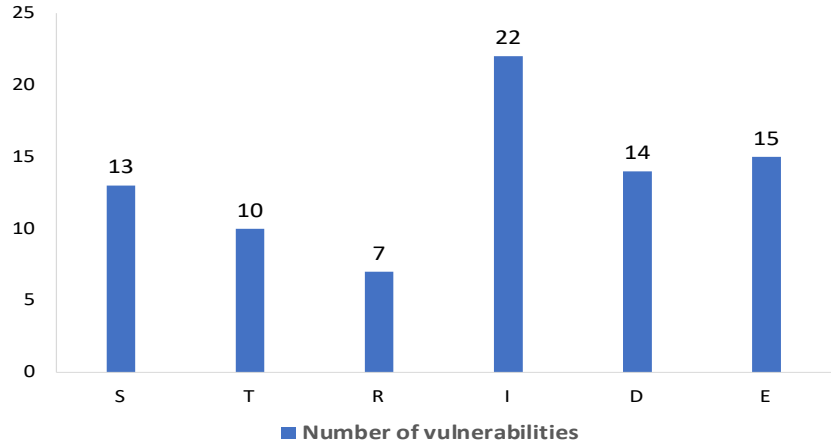

Fig. 3. Threat classification according to the STRIDE model. The characters in the x-axis stand for Spoofing (S), Tampering (T), Repudiation (R), Information disclosure (I), Denial of Service (D), and Elevation of Privilege (E)

Spoofing As mentioned above in STRIDE, the authentication violation may lead to spoofing attack scenarios. There are 13 vulnerabilities with spoofing affecting authentication. One of the services exhibits a FreeSSHd Authentication Bypass vulnerability, which allows remote attackers to bypass authentication via a crafted session (CVE-2012-6066). When an actor claims to have a given identity, the software does not ensure the claim is correct. Concerning our EV charging ecosystem architecture, an attacker may masquerade as a legitimate user and compromise the user's identity, potentially leading to energy theft and privacy violation. Similar attacks have been discussed by Gottumakkala et al. [10].

Tampering Integrity is the security property that is threatened by tampering attacks. There are 10 vulnerabilities with tampering affecting integrity. Among these, we can mention an "HTTP verb tampering" vulnerability, in which an

attacker modifies the HTTP method to bypass access restrictions. This allows the attacker to access data that should otherwise be protected. The vulnerability may affect the OCPP communication messages in the CSs and CMSs. Another possible threat can be tampering with the configuration values. This can happen if an attacker gains access to the CS or CMS and alters the credentials, installs malware within the updates, deletes logs, and tampers with charging time to desynchronize the energy monitoring [2]. Even worse, Nasr et al. setup and conduct simulation experiments to illustrate the feasibility of leveraging a botnet of exploited EVCS to carry out frequency instability attacks against the power grid and its operations [22].

Repudiation Repudiation is the user's ability to reject or deny the claims against them for performing something, and the victim cannot verify the truth of the claim. Threats to non-repudiation are due to the absence of system or application logs. There are 7 vulnerabilities affecting repudiation. Among these, a vulnerability PEPPERL+FUCHS WirelessHART-Gateway (CVE-2021-34559) may allow remote attackers to rewrite links and URLs in cached pages to arbitrary strings. Exploiting this vulnerability can propagate with an HTTP Cross-Site Request Forgery attack that forces users to execute unwanted actions on a web application they're currently authenticated to use. In older versions of OCPP, where digital signatures are not forced, repudiation attacks may arise (as well as tampering). If messages between CM and CMS are not properly audited, the system may not determine the responsible entity when an error occurs [2].

Information disclosure Confidentiality is the security property threatened by information disclosure. In our analysis, 22 vulnerabilities affect confidentiality. We observed several OpenSSH vulnerabilities, such as (CVE-2020-15778), (CVE-2018-15473), and (CVE-2023-25136) in different vendor products. Successful exploitation of these could allow a remote attacker to disclose sensitive information (or modify files). Leaking sensitive information may affect the reputation of the vendor. In addition, attackers can potentially extract internal IP addresses, back-end office URLs, security credentials, telemetry data, energy consumption, charging status of CSs, and software versions used. A cybersecurity report by Sandia National Laboratories [13] mentions a scenario where a threat actor illicitly may remotely exploit the vulnerabilities and cause information disclosure and loss of privacy.

Denial of Service Denial of service attacks threaten the availability of CSs and CMSs. If threat actors exploit certain vulnerabilities, they can disrupt service communication with the authentication server, interrupting the real energy charge in EVs requested by the EV users. We found 14 vulnerabilities that potentially lead to a DoS attack. One vulnerability (CVE-2023-25136) allows an attacker to cause a denial of service through excessive CPU utilization in

the server. Also, we observed presence of CVE-2017-9765, which allows remote attackers to execute arbitrary code, which may lead to DoS after tampering. Other DoS variants discussed in literature [11] are UDP or TCP/IP flood, low-rate DOS, ping flood, or ICMP flood. These attacks can take down a charging station or other nodes in the charging station ecosystem. In these attacks, an adversary targets the CMS or associated components to overload the network, preventing it from providing services to legitimate users. Such an attack can have severe consequences, affecting grid stability.

Elevation of Privilege To gain unauthorized access to CS, CMS, and other components, attackers start by finding weak points through which they may first penetrate the network. They then attempt to escalate privileges to gain further permissions or access other sensitive subsystems [2]. The security property threatened by the elevation of privilege attacks is the authorization property. We noted 15 vulnerabilities that threaten authorization, e.g., a root privilege escalation vulnerability (CVE-2019-0211) that with a successful exploit provides access to the server. We observed another vulnerability (CVE-2022-31793), which if successful, enables an attacker to access the device's configuration, including access to passwords. A third vulnerability (CVE-2023-28231), if successfully exploited, could result in the execution of arbitrary code with administrative privileges.

Summary From Figure 3, it is obvious that threats relevant to information disclosure and privilege escalation are more prevalent, and threats of repudiation are seen to a lesser extent in this ecosystem. The most alarming observations are the instances of elevation of privilege. The massive use of such threats can enable actions that can further impact the other components of the ecosystem, including the grid operations. The absence of non-repudiation is also alarming. However, even from an individual perspective, the disclosure of information may be as relevant. Also, spoofing and tampering can lead to more serious instances like the elevation of privilege.

5 Responsible disclosure

We performed responsible disclosure of our findings for all 11 vendors and their associated vulnerabilities. While all vulnerabilities were previously known, these still show up in search engine databases. We reported our findings via the official email addresses and contact forms of the vendors. Two vendors responded. One vendor stated that:

> "Fortunately for KEBA charging stations, all of the CVE entries can be considered as "false-positives". Most of the mentioned software solutions are not in use for charging stations and the related infrastructure components. Of course, it could be possible that a customer uses the mentioned software solutions for managing/accessing our products. But this scenario is out of scope for our risk assessment."

Another vendor (Mennekes) stated:

> "The interface behind the mentioned IP address indeed seems to show one of our products. ... However, besides the fact that these systems should not be connected to the public internet, the system uses a very old software version (v4.61).
> We had a comprehensive security audit and penetration test in the meanwhile. ... Finally, the CVEs mentioned still do not really match the software used in these products, no matter which version is used."

Based on the vendor response regarding the false positive CVE entries, additional verification of cybersecurity search engine data seems to be a relevant direction for future work. It is possible that they report inaccurate information regarding the software running on the detected devices, as well as regarding the vulnerabilities present. We are not aware of any existing independent assessment of the quality of the data provided by these search engines. Another possibility suggested by both vendors is that a customer uses software solutions for managing/accessing their product that were not intended or foreseen by the vendors. Such unforeseen usage of the products by the customers may indicate that the identified vulnerabilities do exist for some EV charging components "in the wild", and that they are thus not being covered by security updates and audits by the vendors.

The services running on the IP addresses we analyzed are web management portals using CSs and CMSs software. From the outside, it is difficult to determine which entities that are responsible for taking care of identified vulnerabilities in these services. It can be argued that there is a shared responsibility between the EV charging component vendors, the software vendors that create the underlying technologies (e.g., web servers) and the owners and operators of the equipment. Upcoming regulations such as the European Cyber Resilience Act (CRA) are likely to increase the responsibility of the vendors to ensure that their products are secure throughout the entire lifecycle.

Given the second vendor's response that the system should not be connected to the public internet and the use of outdated software we see two possible explanations. Either the owners of the EV charging components have intentionally or unintentionally (e.g., through misconfiguration) connected these products to the public internet in a way that was not intended, or we may be dealing with honeypots and not with real systems.

6 Related work

We divide the description of related work into two parts. First, we discuss threat modeling and risk analysis techniques related to EV charging systems, and then we survey other works that assess the security posture of the EV charging infrastructure.

6.1 Threat modeling and risk analysis in EV charging systems

Casola et al. [5] propose an approach to support the security analysis of an IoT system using an almost entirely automated process for threat modeling and risk assessment, which also helps to identify the security controls to mitigate existing security risks. Baggot et al. [4] review the literature and present a risk-based framework in which they underscore the need for a coordinated U.S. cybersecurity effort toward formulating strategies and responses to protect the nation against attacks on the electric power grid. Shevchenko et al. [25], discuss twelve threat modeling methods from various sources and target different parts of the process. They do not recommend a threat modeling method over another; the decision of which method(s) to use should be based on the needs of the system and its specific concerns. Müller et al. [20], systematically formulate threat scenarios for the Cyber-Physical Systems (CPS) within Flexibility Markets (FM), revealing remaining security challenges across all domains. Based on threat scenarios, unresolved monitoring requirements for the secure participation of distribution system operators in FM are identified, eliciting future works that address these gaps. Granadilla et al. [9] propose a dynamic risk management response system consisting of proactive and reactive management software aiming at evaluating threat scenarios in an automated manner and anticipating the occurrence of potential attacks. They apply their system to a real case study of a critical infrastructure with multiple threat scenarios. We note that a systematic vulnerability-attack-impact analysis e.g. through the STRIDE classification that we adopt here would be useful.

Shrestha et al. [26] propose a methodology called Smart Grid Security Classification which aims to assign a system to a security class based on scores given to the various exposure aspects of the system and the respective protection mechanisms implemented without considering attackers. Kure et al. [18] present an integrated cybersecurity risk management framework to assess and manage the risks. Their approach enables the identification of critical CPS assets and assesses the impact of vulnerabilities that affect assets. Heiding et al. [12], investigate the cybersecurity of devices commonly located in connected homes: smart door locks, smart cameras, smart car adapters/garages, smart appliances, and miscellaneous smart home devices. They discover vulnerabilities that could lead to severe consequences for residents, such as an attacker gaining physical access to the house. Heading et al. [28] provides a four-stage IoT vulnerability research methodology built on top of four key elements: logical attack surface decomposition, a compilation of the top 100 weaknesses, lightweight risk scoring, and step-by-step penetration testing guidelines. Other works describe research about modeling and risk analysis techniques meant for EV charging systems. Lee et al. [19] analyze the security vulnerabilities of ISO/IEC 15118 and propose countermeasures to safely communicate between electric vehicles and power charging infrastructure. Gottumukkala et al. [10] present EVSE (electric vehicle supply equipment) as a cyber-physical system, then discuss and summarize cybersecurity-based vulnerabilities, threats, and consequences. In addition, they

present methods and future research directions to improve the CPS security of charging stations. These works are all in other CPS domains, and our work complements these for the EVCS domain.

6.2 Security posture on EV charging infrastructure

Zhdanova et al. [31] analyze conditions under which Vehicle to Grid (V2G) insecurity can lead to grid collapse. They use quantitative analysis and dynamic simulations of a typical European suburban grid to determine the scope and impact of EV charging manipulation. They review shortcomings of existing V2G protocols, analyze attack strategies able to cause overloads and validate known attacks based on experiments with off-the-shelf products. Lastly, they show that it is critical to consider the impact of known and unknown attacks and possible mitigations and fallback positions. Johnson et al. [14] survey publicly disclosed electric vehicle supply equipment vulnerabilities, the impact of EV charger cyberattacks, and proposed security protections for EV charging technologies. Bandurova et al. [27] analyze cyber security challenges of smart cities with a particular focus on the intelligent integrated and interconnected EV charging infrastructure. The analysis indicates that not all solutions have adequate cybersecurity protection. It is intended to lay a foundation for securing EV charging infrastructure by analyzing the problem context and the data to be protected, presenting some attack surfaces, cybersecurity threats, and vulnerabilities in the EV ecosystem. Our work confirms the lack of security protection and identifies individual components and vendor equipment in the current EV ecosystem.

Kern et al. [16] propose a framework for simulating and analyzing the impact of e-mobility-based attacks on grid resilience. They derive e-mobility-specific attacks based on the analysis of adversaries and threats and combine these attacks in their framework with models for grid and e-mobility to perform simulation-based outage analysis. The results show the scope of increased vulnerability during peak load hours, enabling attacks even with a small number of attacks in progress. They further discuss potential protection mechanisms for different resilience objectives, including detection, prevention, and response approaches. Nasr et al. [21] propose a novel multi-stage framework, ChargePrint, to discover Internet-connected EV charging management systems (EVCMS) and investigate their security posture. This framework leverages identifiers of EVCMSs to extend the capabilities of device search engines through iterative fingerprinting and a combination of classification and clustering approaches. Their security analysis highlights the insecurity of the deployed EVCMS by uncovering 120 0-day vulnerabilities. This sheds light on the feasibility of cyber attacks against the EVCS, its users, and the connected power grid. Their main focus is on the EVCSMS and the paper does not detail any EVCS-related vulnerabilities which is the focus of our work.

Ghafari et al. [8] investigate whether the abundance of Electric Vehicles can be exploited to target the stability of the power grid. They present a realistic coordinated switching attack that initiates interred oscillations between areas of

the power grid. The threat model is formulated to illustrate the possible consequences of the attack. Finally, to protect the grid from this attack, a framework is proposed to detect and prevent this attack even before being executed. Gautam et al. [7], describe the concept of Smart Charging Management System (SCMS) and provide a comprehensive review of cybersecurity issues of EVSEs and SCMSs with their possible impacts on the power grid. Some insights on research gaps and vulnerabilities associated with currently commercially available SCMS technologies are also provided. Acharya et al. [1] describe and analyse cyber vulnerabilities and point to the current and emerging gaps in the security of the EV charging ecosystem. They list and characterize all backdoors that can be exploited to seriously harm either EV and EVCS equipment or the power grid. Our work makes the causal chain between the vulnerabilities, attacks, and security violations concrete in the EVCS context.

Sayed et al. [24] examine the EV ecosystem from vulnerability to attacks and solutions. They suggest several patches for the existing vulnerabilities but their focus is on methods to detect EV attacks. Sarieddine et al. [23] study the security posture of the EV charging ecosystem against a new type of remote access that exploits vulnerabilities in the EV charging mobile application as an attack surface. They leverage static and dynamic analysis techniques to analyze the security of widely used EV charging mobile applications. Their focus is user/vehicle verification and improper authorization for critical functions, which allow adversaries to remotely hijack charging sessions and launch attacks against the connected critical infrastructure. Nasr et al. [22]devise a system lookup and collection approach to obtain a representative sample of widely deployed EVCSMS; they leverage reverse engineering and penetration testing techniques to perform a comprehensive security and vulnerability analysis of the identified EVCSMS and their software/firmware implementations. They simulate the impact of practical cyber attack scenarios against the power grid, which result in possible service disruption and failure in the grid. Our work is similar to this but studies the vulnerability-attack chain from the EV charging station perspective.

7 Conclusions

As a part of the smart grid, the EV charging ecosystem is also connected to the internet, potentially making it vulnerable to cyber-attacks. In this paper, we investigate parts of the EV charging infrastructure through a vulnerability analysis method based on penetration testing techniques. We classify the potential security issues using the STRIDE threat modeling approach and trace 81 vulnerabilities to systems that appear to be running several popular charging station products. Although we cannot for sure know how many of these vulnerabilities exist in current commercial deployments, we believe that these results motivate further investigation into how such vulnerabilities can potentially affect end-users and the electrical grid (assuming large-scale attacks). We perform an initial analysis of potential impact by relating to the EV charging ecosystem and

also discuss the identified vulnerabilities in the context of the STRIDE classification. Information disclosure is one of the more common vulnerability types, which can lead to loss of privacy and business-sensitive information. However, privilege escalation is one of the major categories that enables an attacker to gain control of the charging stations and traverse the network. These types of attacks can potentially cause substantial damage to the target system unless discovered in time.

Our work indicates that there are plenty of opportunities for attackers to utilize this new kind of infrastructure for malicious purposes. While awareness-raising efforts are an obvious step after the discovery of threat vectors, future research must also identify the defense-in-depth approaches to this new infrastructure and create means to protect the systems. At the same time, the vendor responses points to some threats to data validity. The first threat we identified is that we base our results on the outcome of search databases at face value. Some potential errors in vulnerability databases may not have been updated with the latest changes, and some of the systems we analyzed could even be security honeypots.

To improve the security of the EV charging infrastructure, future research should develop better tools and techniques to analyze and strengthen the security of the smart grid. This approach will help to expand the scope and depth of EV charging ecosystem security, and further explore the impacts of potential attacks.

References

1. Acharya, S., Dvorkin, Y., Pandžić, H., Karri, R.: Cybersecurity of smart electric vehicle charging: A power grid perspective. IEEE Access **8**, 214434–214453 (2020)
2. Alcaraz, C., Cumplido, J., Trivino, A.: Ocpp in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. International Journal of Information Security pp. 1–27 (2023)
3. Ashley, T., Gourisetti, S.N.G., Brown, N., Bonebrake, C.: Aggregate attack surface management for network discovery of operational technology. Computers & Security **123**, 102939 (2022)
4. Baggott, S.S., Santos, J.R.: A risk analysis framework for cyber security and critical infrastructure protection of the us electric power grid. Risk analysis **40**(9), 1744–1761 (2020)
5. Casola, V., De Benedictis, A., Rak, M., Villano, U.: Toward the automation of threat modeling and risk assessment in iot systems. Internet of Things **7**, 100056 (2019)
6. ElHussini, H., Assi, C., Moussa, B., Atallah, R., Ghrayeb, A.: A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid. ACM Trans. Internet Things **2**(2) (mar 2021). https://doi.org/10.1145/3437258, `https://doi.org/10.1145/3437258`
7. Gautam, M., Bhusal, N., Benidris, M.: Concept of smart charging management system and its consensus on cybersecurity (2020)
8. Ghafouri, M., Kabir, E., Moussa, B., Assi, C.: Coordinated charging and discharging of electric vehicles: A new class of switching attacks. ACM Transactions on Cyber-Physical Systems (TCPS) **6**(3), 1–26 (2022)

9. Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., Papillon, S., Debar, H.: Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems **83**, 535–552 (2018)
10. Gottumukkala, R., Merchant, R., Tauzin, A., Leon, K., Roche, A., Darby, P.: Cyber-physical system security of vehicle charging stations. In: 2019 IEEE Green Technologies Conference (GreenTech). pp. 1–5. IEEE (2019)
11. Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D., Lloret, J.: Cybersecurity risk analysis of electric vehicles charging stations. Sensors **23**(15), 6716 (2023)
12. Heiding, F., Süren, E., Olegård, J., Lagerström, R.: Penetration testing of connected households. Computers & Security **126**, 103067 (2023)
13. Johnson, J., Anderson, B., Wright, B., Quiroz, J., Berg, T., Graves, R., Daley, J., Phan, K., Kunz, M., Pratt, R., et al.: Cybersecurity for electric vehicle charging infrastructure. Tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States) (2022)
14. Johnson, J., Berg, T., Anderson, B., Wright, B.: Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies **15**(11), 3931 (2022)
15. Katsikas, S., Cuppens, E., Kalloniatis, C., Mylopoulos, J., Pallas, F., Pohle, J., Sasse, M.A., Abie, H., Ranise, S., Verderame, L.: A hybrid dynamic risk analysis methodology for cyber-physical systems. In: Computer Security. ESORICS 2022 International Workshops, vol. 13785. Springer International Publishing AG, Switzerland (2023)
16. Kern, D., Krauß, C.: Analysis of e-mobility-based threats to power grid resilience. In: Proceedings of the 5th ACM Computer Science in Cars Symposium. pp. 1–12 (2021)
17. Kern, D., Krauß, C.: Detection of e-mobility-based attacks on the power grid. In: 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). pp. 352–365 (2023). https://doi.org/10.1109/DSN58367.2023.00042
18. Kure, H.I., Islam, S., Razzaque, M.A.: An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences **8**(6), 898 (2018)
19. Lee, S., Park, Y., Lim, H., Shon, T.: Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology. In: 2014 International conference on IT convergence and security (ICITCS). pp. 1–4. IEEE (2014)
20. Müller, N., Heussen, K., Afzal, Z., Ekstedt, M., Eliasson, P.: Threat scenarios and monitoring requirements for cyber-physical systems of flexibility markets. In: 2022 IEEE PES Generation, Transmission and Distribution Conference and Exposition–Latin America. pp. 1–6. IEEE (2022)
21. Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., Assi, C.: Chargeprint: A framework for internet-scale discovery and security analysis of EV charging management systems
22. Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., Assi, C.: Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. Computers & Security **112**, 102511 (2022)
23. Sarieddine, K., Sayed, M., Torabi, S., Atallah, R., Assi, C.: Investigating the security of EV charging mobile applications as an attack surface. https://dl.acm.org/doi/10.1145/3609508 (2022)

24. Sayed, M.A., Atallah, R., Assi, C., Debbabi, M.: Electric vehicle attack impact on power grid operation. International Journal of Electrical Power & Energy Systems **137**, 107784 (2022)
25. Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., Woody, C.: Threat modeling: a summary of available methods. Tech. rep., Carnegie Mellon University Software Engineering Institute (2018)
26. Shrestha, M., Johansen, C., Noll, J., Roverso, D.: A methodology for security classification applied to smart grid infrastructures. International Journal of Critical Infrastructure Protection **28**, 100342 (2020)
27. Skarga-Bandurova, I., Kotsiuba, I., Biloborodova, T.: Cyber security of electric vehicle charging infrastructure: Open issues and recommendations. In: 2022 IEEE International Conference on Big Data (Big Data). pp. 3099–3106. IEEE (2022)
28. Süren, E., Heiding, F., Olegård, J., Lagerström, R.: Patriot: practical and agile threat research for IoT. International Journal of Information Security **22**(1), 213–233 (2023)
29. Tuma, K., Scandariato, R.: Two architectural threat analysis techniques compared. In: Software Architecture: 12th European Conference on Software Architecture, ECSA 2018, Madrid, Spain, September 24–28, 2018, Proceedings 12. pp. 347–363. Springer (2018)
30. UcedaVelez, T., Morana, M.M.: Risk Centric Threat Modeling: process for attack simulation and threat analysis. John Wiley and Sons, Inc, Chicester, 1st ed. edn. (2015)
31. Zhdanova, M., Urbansky, J., Hagemeier, A., Zelle, D., Herrmann, I., Höffner, D.: Local power grids at risk–an experimental and simulation-based analysis of attacks on vehicle-to-grid communication. In: Proceedings of the 38th Annual Computer Security Applications Conference. pp. 42–55 (2022)