Flexible energy systems Leveraging the Optimal integration of EVs deployment Wave

Grant Agreement Nº: 101056730

Deliverable 3.2

Schemes and solutions to guarantee data Privacy and Cyber Security for EV charging

Author(s):
Roberta Terruggia, Elisa Albanese, Luca Zuanazzi (RSE)
Bettina Kämpfe (TUC)

Funded by the European Union

Website FLOW

Document information Table

Project Data			
Project Acronym	FLOW		
Project Title	Flexible energy system Leveraging the Optimal integration of EVs deployment Wave		
Grant Agreement n.	101056730		
Topic identifier	HORIZON-CL5-2021-D5-01-03		
Funding Scheme	RIA		
Project duration	48 months		
Coordinator	Catalonia Institute for Energy Research		
Website	https://www.theflowproject.eu/		
Deliverable Document Sheet			
Deliverable No.	3.2		
Deliverable title	Schemes and solutions to guarantee data Privacy and Cyber Security for EV charging		
Description	Description of cyber security threats for EVs and identification of the most effective measures and procedures to prevent t hem		
WP No.	3		
Related task	3.2		
Lead beneficiary	RSE		
Author(s)	RSE, TUC		
Contributor(s)	RSE, TUC		
Type	Report (R)		
Dissemination L.	Public (PU)		
Due Date	30/06/2023	Submission Date	3/07/2023

Version	Date	Author(s)	Organisation(s)	Comments
V0.1	26/04/2023	Roberta Terruggia, Elisa Albanese, Luca Zuanazzi	RSE	Document draft
V0.2	23/05/2023	Bettina Kämpfe	TUC	Chapter 6: Privacy and security user perception
V0.3	09/06/2023	Roberta Terruggia, Elisa Albanese, Luca Zuanazzi	RSE	Final report before internal review
V1.0	30/06/2023	Roberta Terruggia, Elisa Albanese, Luca Zuanazzi	RSE	Version for submission

DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

This document and all information contained here is in the sole property of the FLOW Consortium. It may contain information subject to Intellectual Property Rights. No Intellectual Property Rights are granted by the delivery of this document or the disclosure of its content. Reproduction or circulation of this document to any third party is prohibited without the written consent of the author(s). The dissemination and confidentiality rules as defined in the Consortium agreement apply to this document. All rights reserved.

Table of contents

Funded by the European Union

Funded by
the European Union

List of Acronyms

Acronym	Meaning
AC	Alternate Current
CIR	Controllore Infrastruttura di Ricarica (Charging Infrastructure Controller)
CPO	Charging Point Operator
CS	Charging Station
CSMS	Charging Station Management System
DC	Direct Current
DDOS	Distributed Denial Of Service
DSO	Distribution System Operator
EMSP	Electric Mobility Service Provider
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
ICT	Information and Communications Technology
M	Month
MITM	Man In The Middle
OCPP	Open Charge Point Protocol
RO	Remote Operator
TLS	Transport Layer Security
V2G	Vehicle To Grid
WP	Work Package

Executive Summary

The deliverable addresses the cyber security and data privacy of Electric Vehicle charging infrastructure to provide requirements and best practices to FLOW architecture development. Ensuring the cybersecurity of electric vehicle (EV) recharge infrastructure is crucial to maintain the integrity, availability, and reliability of charging services. We provide an overview of security threats on EV charging infrastructures focusing on three main architectures: public EV charging, semi-public EV charging and private EV charging.

This document explores the importance of cybersecurity in EV charging infrastructure and highlights key considerations for safeguarding its integrity. We will delve into the measures that can be taken to mitigate cybersecurity risks, including secure communication protocols, access control mechanisms, regular updates, physical security measures, intrusion detection systems, and employee training.

Possible consequences of threats to the EV charging infrastructure can impact different aspects as power grid disturbances, financial and energy loss, information disclosure and loss of privacy or impacts to the mobility sector in terms of uncharged or damaged EVs.

The security by design principle can be guaranteed following security requirements and best practices and applying the cyber security measures provided by the communication protocols and standards.

The experimental evaluation highlights the importance of the implementation of preventive and defensive measures. In particular, it is crucial to monitor the system status to evaluate the security of the EV charging infrastructure and detect anomalies.

Funded by
the European Union

1. Introduction

With the rapid growth of electric vehicles (EVs) around the world, the need for a robust and secure charging infrastructure is paramount. As EVs become more prevalent, ensuring the cybersecurity of EV charging infrastructure is crucial to maintain the integrity, reliability, and trust in this critical component of the electric transportation ecosystem.

Cybersecurity threats pose significant risks to EV charging infrastructure, including potential unauthorized access, data breaches, system tampering, and service disruptions. As charging stations are increasingly interconnected and rely on various communication protocols, protecting them from cyber-attacks is essential to maintain the safety and functionality of the charging network.

By understanding the challenges and implementing robust cybersecurity practices, stakeholders in the EV industry can ensure the availability, reliability, and security of charging services for electric vehicles.

As the EV market continues to grow and EV charging infrastructure expands, it is crucial to address cybersecurity as an integral part of the overall design, deployment, and operation of charging networks. By doing so, we can build a resilient and secure charging infrastructure that promotes the widespread adoption of electric vehicles and facilitates a sustainable and clean transportation future.

This report describes the cyber security threats for EVs and identifies the most effective measures and procedures to prevent them. The document is structured as follow: chapter 2 provides an overview of security threats and their consequences on EV Charging infrastructure, then chapter 3 addresses the main requirements and best practices to guarantee cyber security. Chapter 4 highlights the security aspects of more used communication protocols and standards. An experimental security evaluation referring a company fleet EV infrastructure is presented in chapter 5 and privacy and security user perception are introduced in chapter 6. Finally, chapter 7 provides some conclusions.

2. Overview of security threats on EV charging infrastructure

In this chapter we first describe a generic architecture of the EV charging infrastructure, introducing the main devices, interfaces and networks, and then we make an overview of security threats and their potential impacts on such infrastructure.

2.1. EV charging infrastructure architecture

In order to study the cyber security aspects, it is important to focus on possible EV charging infrastructures and their ICT architecture.

Among the multiple different EV charging infrastructure implementations, in this section we give a generic description of the three major types of architecture: i.e. public, semi-public and private charging. As this is an extremely fast pace evolving sector, there are often different names used for the same concept in the literature; we will try to use the most common acronyms and definitions, for example, following the ones given by the Open Charge Point Protocol (OCPP) [1] and Broek et al. [2].

2.1.1. Public charging

By public charging we mean an EV charging infrastructure that is publicly accessible by all EV drivers. These Charging Stations (CSs) can be located along the streets or on sites of major interest, like commercial centres, train stations, airports or tourist attractions.

The simplest infrastructure that one can think of is simply an EV connected to a CS. The control of such CS is delegated to the so called Charging Point Operator (CPO), sometimes also called Charging Station Operator (CSO), which is responsible for managing the network of CSs, setting up the charging prices, enabling the EV driver to charge and gathering the information of the charging cycles measured by the CSs. These operations are performed through a set of remote tools called Charging Station Management System (CSMS), which have the purposes of:

- communicating with the CSs;
- defining and sending to the CS the charging parameters, basing on the driver's input, the EV and the status of the power grid;
- gathering and storing the charging cycles information received from the CSs.

Since by CS we actually mean a physical system that can charge multiple EV at a time, there is also a name for the part of the CS that delivers energy to a single EV, namely Electric Vehicle Supply Equipment (EVSE). A CS can thus host multiple EVSEs. Sometimes EVSEs are also called Charging Points (CPs) with the same meaning of different physical outputs that can work in parallel.

What we have described so far is just the simplest possible version of an EV charging infrastructure. However, there are several other components and actors that may appear and play an important role, here we will describe only the most relevant ones for a generic public infrastructure.

Notice that the CPO may not be the physical owner of the CSs but only its operator, therefore there may be an additional actor in the EV infrastructure responsible for the maintenance or upgrade of the CSs, like the manufacturer or a specialized company that performed the installation.

The Electric Mobility Service Provider (EMSP) is an actor that offers electricity to EV drivers setting up contracts that may also provide fixed/discounted rates or a seamless user experience when charging with CSs of different brands or belonging to different CPOs. The EMSP is an optional actor and its role may also be fulfilled by either the CPO or the Distribution System Operator (DSO).

The communication between the CSs and the CPO can be facilitated with the installation of a Local Proxy or a Local Controller. The former being simply a unit close to one or more CSs that routes the communication from the CSMS to the corresponding CS and vice versa. A local proxy is very useful, for example, in the common situation in which CSs do not have access to the network, due to their location like in an underground parking garage. A local controller, instead, is not just a router but can also send messages to its CSs independently of the CSMS, for example for smart charging purposes.

Funded by the European Union

Another important actor in the EV charging infrastructure is called Remote Operator (RO), an external entity that communicates with the CSs for smart charging purposes that was recently introduced by CEI, the Italian standardization body [3]. For example, the RO gathers information about the loads and green energy production and sends messages to modulate the charging power in order to avoid peaks in energy demand and reduce carbon emissions. Notice that the official document defining the role of the RO, CEI PAS 57-127 [3], refers to a semi-public or private architecture, explicitly leaving the public one out of the scope. One of the reasons for this choice is that smart charging is believed to become more effective in charging infrastructures where the EV is parked for several hours, like at workplace or home, compared to a public CS where the driver may prefer the maximum charging speed for a shorter parking time. In the literature, analogous roles are already mentioned, just with different names. For example, the OCPP states that the CPO receives the information about the status of the power grid communicating with the Distribution System Operator (DSO) relative to the grid to which the CSs are connected. This situation, however, poses the problem of a conflict of interest for the DSO, hence the need for an intermediary role like the RO, which would be able to directly communicate with the back end of both the CPO and the EMSP.

In the following Figure 1, we present a diagram of a simple public charging infrastructure.

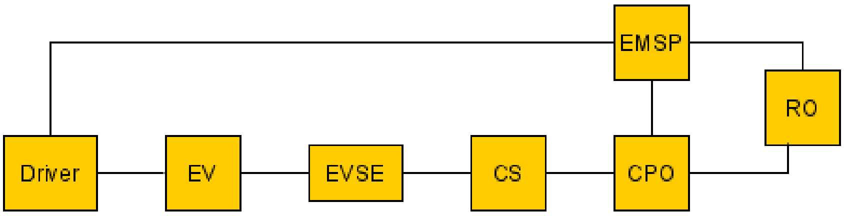


Figure 1. Public infrastructure diagram.

2.1.2. Semi-public charging

By semi-public (or workplace) charging we mean an infrastructure that is accessible to a restricted number of EV drivers, like in a company car park but also like in a condominium or hotel.

In this infrastructure the role of the CPO is generally fulfilled by the authority offering the charging service, that is the company or condominium and so on and so forth. In some cases, however, some services can be outsourced to the CSs supplier who then acts as the CPO.

The role of EMSP is not present in this infrastructure, however, the administrator of the CSs should offer an analogous service of simple and common way to authenticate and enable charging, for example through a mobile application, RFID technology or supporting Plug&Charge. Again, exceptions always exist; sometimes a charging infrastructure can be both private and public depending on the time schedule set by the company/condominium. When CSs are in public mode, any driver can negotiate a charging session with the CPO or through any else EMSPs.

To perform congestion management, the DSO asks for flexibility services to the RO, which in turn communicates with the CPOs. This communication is mediated by a device called CIR (from italian meaning Controllore Infrastruttura di Ricarica), that can be installed directly in each CS or in the CPO central system, that is the CSMS.

Sometimes the role of the RO is substituted by a so called Energy Management System (EMS) which has the similar role of modulating the charging power but is generally intended to operate more on a local scale, like inside the company micro-grid, for example to avoid overload and tripping the breaker.

In the following Figure 2, we present a diagram of a simple semi-public charging infrastructure.

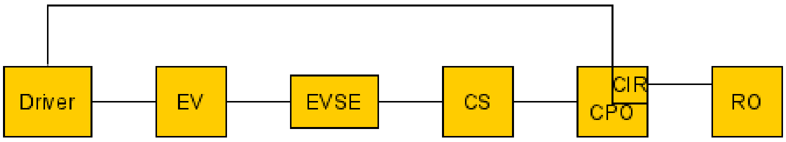


Figure 2. Semi-public infrastructure diagram.

2.1.3. Private charging

By private (or domestic) charging we mean an infrastructure of private use like the one at home or in a private garage. In this situation the CS is typically a wallbox, while the role of the CPO is fulfilled by the house owner, which also corresponds to the EV driver. The communication between the owner and the wallbox, for example for configuration purposes, is generally handled through a mobile application. Obviously, in this infrastructure there is no EMSP.

Analogously to the semi-public charging, also in this case it is important to mention the role of the RO, which modulates the charging power to offer smart charging services. The communication between the RO and the wallbox is again mediated by the CIR, which can either be a constituent component of the wallbox or a separate device that communicates with it. Furthermore, the CIR communicates also with the smart electric meter, or with a separate smart meter if the electric meter is an older generation model. Notice that CIR is a specifically Italian technology and not all member states of the European Union allow for a direct communication between the CS and the smart meter.

In the following **Figure 2. Semi-public infrastructure diagram.**Figure 3, we present a diagram of a simple private charging infrastructure.

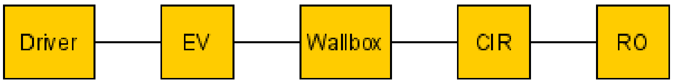


Figure 3. Private infrastructure diagram.

2.2. EV charging infrastructure threats

In this section we make a review of the threats relative to the EV charging infrastructure and their potential impacts on the different architectures previously described. A threat should be defined as

Funded by the European Union

something that may lead to a violation in any way of the requirements of a specific infrastructure. In the next chapter we will give a more detailed description of the security requirements for the EV infrastructure. For now, it is sufficient to say that, in general, a threat may compromise the properties of integrity, availability, confidentiality, authenticity, authorization and non-repudiation relative to the ICT infrastructure with potential consequences even on the electric grid.

2.2.1. Driver's authentication

The authentication of the EV driver at the CS can happen in different ways: with an application on the driver's smartphone, communicating via Bluetooth or NFC technology, or with an RFID card. Extensive researches have shown concerns about these authentication methods [4].

For example, only the static ID of the RFID card is used for authentication which is transmitted in plain text through the air and therefore can easily be spoofed to create a clone of the card. If one has access to the card or can get to a range of about 10 cm, the ID can be eavesdropped with a simple NFC equipped smartphone. Otherwise, an attacker can stick a simple eavesdropping device on the CS or, with more sophisticated electronic equipment, can even spoof the ID at a distance of several meters [5]. Alternatively, an attacker can try out random card IDs, guessing the domain range that the CS accepts from a few spoofed IDs.

The same considerations hold for a driver authenticating with a smartphone via NFC, which can act both as a card and as a reader. The only difference is that the ID can be spoofed only for the short period of time when the communication is enabled through the application for the authentication.

A cloned card can be used for free charging, billing the victim driver instead, or to release and steal the expensive charging cables. This threat is obviously more concerning in the case of public charging infrastructure, because the CSs are accessible to anyone, and thus an attacker can easily spoof the ID, and there is a broad network of CSs, allowing an attacker to use the cloned card in different places. However, this threat is concerning also in the case of semi-public charging, even if the attacker would have a higher risk of being caught, being the number of drivers with access to the CSs reduced.

2.2.2. EV to CS communication

According to the most common protocols, the communication between the EV and the CS can be carried through Power Line Communication (PLC). Such technology uses power line for data transmission and is known to be easily subjected to spoofing, due to leaks of signal through the charging cable, and to external electromagnetic interference [6]. This means that this communication is particularly prone to side-channel attacks. Furthermore, there is also the risk of so called ARP spoofing and Man In The Middle (MITM) attacks, for example by using a modified charging cable or a fake CS [7].

The consequences of these threats have been extensively studied. Köhler et al. [8] demonstrated that a charging session can be wirelessly aborted interfering with the PLC communication in an attack they called *Brokenwire*. Other studies have shown the possibility to falsify meter measurements and sniff personal data like billing related information or credentials of the EV or the driver [9]. It is then possible to freely charge at the expense of a victim driver in several ways [10]:

- performing a packet replay attack: after having obtained a genuine communication, the attacker repeats it playing the role of the victim driver charging its EV instead;
- performing a MITM attack: through a modified charging cable or a fake CS the attacker can position itself between the victim driver and the EVSE, spoofing the communication to later perform a packet replay attack, or simply forwarding the communication to a real CS while intercepting the energy to charge its EV in real-time;
- similarly to the MITM attack, the attacker can wait for the victim to initiate an authenticated charging session. Once the charging is complete, the adversary pauses the session, making it seems to the victim that the process has ended, and then resumes it once the victim has departed.

It is also possible to use the sniffed personal information to perform user tracking, for example using the MAC address. If the infrastructure supports V2G (Vehicle 2 Grid) technology, an attacker could also masquerade as a supply equipment to extract energy from the battery of a victim's EV. Furthermore, there have been reports indicating the potential risk of EVs transmitting viruses to CSs, which could subsequently facilitate the further propagation of the malware. Finally, due to the large number of parties involved, there is also the threat of billing repudiation from a driver, since the trust of the authenticity and integrity of a communication can be compromised by the aforementioned attacks [7].

Potential impacts do not stop at the communication level, with loss of confidentiality or financial integrity, but also involve a reduction of the service performance with consequences on battery health and wiring integrity due to alterations in the charging power.

As for the previous case, also this type of threats mainly concerns a publicly accessible EV charging infrastructure. However, proper security analysis should be carried out also for semi-public and private infrastructures, since in such cases security recommendations are less frequently implemented.

2.2.3. EVSE, CS and CSMS vulnerabilities

Extensive studies have investigated the vulnerabilities of the different EVSE's interfaces, for example, a comprehensive review has been written by Johnson et al. [4]. Depending on the manufacturer and the intended architecture, there is a wide range of EVSEs available, each offering distinct functionalities and different security features. In general, an EVSE has two types of interfaces: one exposed to the internet or to the local area network for configuration and sharing information on the charging sessions, and one locally accessible for maintenance purposes. Numerous vulnerabilities have been identified concerning these interfaces, primarily resulting from inadequate selection of authentication mechanisms, software implementations, and susceptibility to physical tampering.

CSs often are accessible through interfaces like web services, exposed locally or even to the internet, for CS configuration and monitoring of the charging sessions. For example, in a private or semi-public infrastructure, an EVSE is typically accessible from the local network by a smartphone or personal computer via Wi-Fi. Extensive studies reported several vulnerabilities relative to these interfaces for different brands of EVSEs, here we summarize just a few representative mentions:

Funded by the European Union

- insecure direct object references in web API and other API vulnerabilities may allow for account hijacking, changing configuration data without authentication and firmware updates that would give access to the local network [11];
- insecure firmware packages, mobile applications and web applications may allow for Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF) and JavaScript information exposure. The impacts of these threats may affect charging processes, user and billing information and also the status of the power grid [12];
- vulnerabilities in Common Gateway Interface (CGI) binaries and stack buffer overflow of a CS's website may allow an attacker inside the target's Wi-Fi network to gain control of the device, stopping charging sessions at any time or increasing the maximum charging current causing a black-out or overheating the wiring with risk of fire [13];
- application used by drivers to authenticate and manage their charging session sometimes can be reverse engineered to reveal weaknesses relative to the CS and cloud interfaces. Furthermore, services exposed to the internet may allow for location with network discovery tools like Shodan and Nmap. Once these services are reachable, they can be attacked exploiting vulnerabilities like the lack of brute force protection and the usage of unsecure cryptographic algorithms. The impacts ranges from data disclosure to disruption of the service: it has been reported also the possibility to remotely lock and unlock the CS. Such attack, when coordinated, can lead to a simultaneous stop of multiple charging sessions, with potential failure of the power grid [14];
- especially in the case of the public architecture, the CS communicates with a backend which can be hosted in the private infrastructure of the CPO or on a public cloud. Several studies have investigated the vulnerabilities of this communication, reporting unsecure authentication methods and applications susceptible to SQL injection attacks. Furthermore, MITM attacks with the purpose of data exfiltration can also be performed [15];
- lastly, since the owner, the installer and the manufacturer of the CSs can theoretically be three different actors, there is the threat that one of these actors may keep a backdoor for remote access. A recent example of the potential consequence occurred in the recent Russian invasion of Ukraine: a Russian CPO had outsourced some components to a Ukranian company, which kept and exploited a backdoor to remotely change settings in the CSs and display anti-Putin and pro-Ukraine messages [16].

CSs typically have also a maintenance interface by means of a serial or ethernet port, Bluetooth, or via a front display. Extensive researches have shown several vulnerabilities, for example:

- the INL (Idaho National Laboratory) found outdated Linux kernels with unnecessary services, processes running as root, weak password hashing, lack of secure boot, unsigned firmware, exposed ports, direct processor control via JTAG interfaces, bypassable tamper-detection tools, and other insecure coding practices [14];
- multiple wallbox devices are made by cheap single-board computers, like a Raspberry Pi, that do not include the appropriate secure functionality, like the secure bootloader. This is a threat for personal information, passwords and credentials that can be obtained simply pulling out the flash memory [11];

Funded by
the European Union

- being these communications only locally accessible, they are often implemented without the necessary careful analysis of the security practices. For instance, a specific brand of wallbox recently demonstrated vulnerabilities in its low energy Bluetooth communication interface, including the potential for authentication bypass and plaintext communication exploitation [17];
- it was reported a successful factory reset of a CS triggered through a particular blinking pattern that was picked up by a photodiode on the device [13].

All of these vulnerabilities represent a considerable threat to the EV infrastructure, independently of the architecture, that can be exploited by an attacker in order to obtain a wide range of impacts. A very well-done summary of the possible consequences is given by [18]:

- financial or energy loss;
- information disclosure or loss of privacy;
- power grid disturbances such as voltage and frequency variations;
- impacts to the mobility sector due to uncharged or damaged EVs;
- computational resources of the charging infrastructure employed for unintended use like mining of cryptocurrencies or executing DDoS attacks.

The magnitude of these impacts varies accordingly to the number of devices involved in the different attacks; therefore, it is of paramount importance to perform security assessments and verify the compliance with the best practices, especially in the case of the public infrastructure where a large number of devices can be simultaneously compromised.

3. Security requirements and best practices

The security requirements of an EV charging infrastructure are extremely relevant in ensuring the safety and reliability of the system. As the adoption of electric vehicles continues to rise [19] , the need for a robust and secure charging network becomes increasingly vital. The security considerations encompass various aspects, including protection against cyber threats, prevention of unauthorized access to charging stations, secure data transmission, and the overall integrity of the charging infrastructure. Implementing stringent security measures is crucial to instill confidence in EV users, foster trust in the charging ecosystem, and safeguard the entire energy grid against potential vulnerabilities.

In this chapter, our focus is on providing a comprehensive description of the security requirements applicable to the different types of charging infrastructure. Subsequently, we present an overview of the best practices that can be implemented on an EV charging infrastructure. The aim is to effectively address the security threats detailed in the preceding chapter. By following these best practices, stakeholders can enhance the security measures employed in their EV charging infrastructure and mitigate potential vulnerabilities.

Funded by the European Union

3.1. Security requirements

The security requirements for the EV charging service involve all the users and components of the different possible architectures. In this section we describe the security requirements classifying them in the perspective of the main actors, namely EV's driver, CPO, EMSP and DSO. This description is done summarizing various sources from the literature, the most relevant being [2] [10] [20].

Notice that by requirements we mean the high-level goals of the different actors. Since this description can be quite abstract, in the next section we give a more concrete translation in terms of the best practices to follow in order to comply with these requirements.

3.1.1. EV's driver

The EV and its driver communicate, through a series of devices and networks, with the CPO and the EMSP exchanging personal and charging information.

Personal information includes, for example, geolocation at a given time of the EV, and thus of its associated driver, therefore must be secure in order to comply with the privacy regulations. Another example could be on the charging status information of the EV, which over time can lead to an indication of the average distance travelled. More sensitive information is obviously related to the billing process, like the driver's payment method which must be kept confidential.

Furthermore, information disclosure does not lead only to loss of privacy or confidentiality but can also affect the trust in the EV charging infrastructure due to the threats of masquerading attacks. The driver wants to ensure that he is not billed in place of another malicious driver and that the energy he pays for is not skimmed but goes entirely and directly into his EV. For these reasons, a requirement is that all billing messages and notifications corresponding to every service cycle must be sent and received by the proper recipient.

Regarding the availability of the charging infrastructure, it is essential for drivers to have the capability to fully charge their EVs without any risk of an attacker compromising their mobility. Therefore, it should not be possible to limit or abort the charging session, neither to make any damage to the EV or harm the driver's safety.

Finally, the EV's driver wants to ensure that the tariff it negotiates with the EMSP it has a contract with and receives from the CPO can be trusted; that is the CPO must forward the complete and integer tariff table of the different charging speeds without changing it to its advantage.

3.1.2. Charging Point Operator

The CPO needs to secure the communications with all the other actors present in the EV charging infrastructure.

The security requirements, from the perspective of the CPO, clearly begins from the physical security of its own devices, like CSs and EVSEs, which are subject to an elevated risk of tampering being publicly accessible. The goal of the CPO is to minimize the downtime of its infrastructure preventing any permanent or temporary damage. It is important to note that both cyber attacks and physical

Funded by the European Union

tampering can result in the malfunctioning of a CS, necessitating the need to secure the publicly accessible interfaces from both a physical and cyber perspective.

Even though in this case there are not personal information subjected to privacy regulations, also the CPO wants to secure its communications in order to protect data that could be business confidential. For example, the CPO does not want its competitors to know how busy its charging points are, or how fast EVs typically charge. The security of communications is also important to instill confidence in EV's drivers and avoid the risk of charging sessions repudiation.

Furthermore, the CPO sends to the EMSP data on the concluded charging sessions, for billing purposes, in the form of so called Charge Detail Records (CDRs). This information must satisfy the requirements of confidentiality, integrity and authenticity; for example, a CPO wants to ensure an EMSP cannot falsify or repudiate CDRs.

3.1.3. E-Mobility Service Provider

First of all, the EMSP wants to ensure that its EV charging services are correctly available to the customers. By this we mean that the direct communication between the EMSP and EV's driver should work properly and securely, but also that the CSs of the CPOs an EMSP has a contract with are functioning and allowing a secure communication with the drivers.

The charging and billing information an EMSP exchanges with the drivers must be secure in order to ensure that all service cycles are correctly paid by the proper users. Furthermore, an EMSP wants to ensure that only CPOs it has contracts with can push data to its systems, and those data must be non-falsifiable and non-repudiable.

Finally, also the data relative to the EMSP are business confidential, and thus, for example, an EMSP does not want to show the actual tariff it negotiates with the EV to the CPO because he could then sell this information to the EMSP competitors. In other words, an EMSP would like to have a communication with the EV's driver that is secure at the end-to-end level.

3.1.4. Distribution System Operator

The foremost requirement is clearly the availability of electricity. By this we mean the availability at the CS and even more importantly in the whole power grid to which the CS is connected. The DSO, but also all the other actors in the EV charging infrastructure, want to ensure that a malfunctioning CS or one that receives incorrect information does not affect the electricity supply of the entire grid.

Secondly, the DSO exchanges confidential information with the CPO, which are sensible both for business matters but also because a poorly secure communication would consequently compromise the security of the DSO's system leading to vulnerabilities of the power grid infrastructure.

Furthermore, the DSO (or the Remote Operator or Energy Management System if present) wants to ensure that the power limits negotiated with the CPO are respected and not exceeded.

Funded by
the European Union

3.2. Best practices

In this section we describe the best practices the various actors of the EV charging infrastructure should employ as a consequence of the security requirements we have just listed. The technological and economic feasibility of these solutions depends on the type of architecture and on the specific situation considered.

3.2.1. EV's driver authentication

This paragraph covers the threats relative to the EV's driver authentication mechanism to a CS.

First of all, the usage of a cloned RFID card is mainly mitigated by the high risk of the attacker to be caught in the act since charging EVs still takes a considerable amount of time, enough for an authority to intervene. In order to detect a suspicious usage of an RFID card, the entity responsible for the card proper functionalities should implement monitoring techniques taking into account, for example, location, time span and amount of consumed energy [21].

An opposite but also complementary point of view is to improve the authentication mechanism in order to reduce the feasibility of a masquerading attack. Many of the most common protocols are tackling this threat introducing a challenge-response authentication mechanism based on asymmetric cryptography. The two major types of solutions are the following [20]:

- Substitute the RFID cards, which nowadays are mainly MIFARE Classic cards, with more advanced cards, capable of stronger cryptographic operations. For example, contactless banking cards, which are based on the EMV standard, solved the same user authentication problem in the banking sector. Equivalently, current RFID cards can be substituted with NFC equipped smartphones running an application that performs the same cryptographic of the aforementioned more advanced cards. In addition to substituting the current cards, this solution requires the physical upgrade of the card readers in the CSs;
- Implementing a protocol that allows the EV to autonomously identifying and authenticating itself to the CS. For example, the Plug&Charge technology is introduced by the ISO 15118; further details are given in the protocols dedicated chapter. This solution would have specific requirements for both the EVs and the CSs, therefore the older EV models may not have the necessary capabilities to support this technology. On the CS side, existing stations would need an upgrade that may involve installing new hardware components or updating the firmware of the charging station.

  Notice that this solution, in addition to the security features, has the advantage to simplify the charging experience from the EV's driver perspective.

3.2.2. Communication security

In this paragraph we aim to secure the communications between the different devices of the EV charging infrastructure against attacks that violate the confidentiality, integrity and authenticity of the messages, like MITM attacks or ARP spoofing.

Funded by the European Union

In order to secure the communication between the numerous actors of the EV charging infrastructure, newer versions of the most common protocols impose the implementation of Transport Layer Security (TLS) technology, while in older versions it was only a suggestion. Notice, however, that not all CPOs may follow this suggestion or use the latest version of the protocols. One of the reasons for this choice lies in the fact that the overhead introduced by TLS increases the messages size, which is in general quite small. Since the communication between CSs and CPO is often carried over cellular network, where the transmission has bandwidth restrictions and is charged per byte, the introduction of such overhead may become extra costly [2]. Furthermore, TLS implementation not only requires CSs to have a more performing, and more expensive, hardware, but also assigns to the CPO the responsibility to correctly manage digital certificates.

TLS technology ensures the confidentiality, integrity, and authenticity of data transmitted between two parties and can be implemented in two modes:

- **one-way TLS:** One-way TLS is the most common implementation of TLS. In this mode, only the server is required to authenticate itself to the client. The server presents its digital certificate to the client during the TLS handshake process, which contains the server's public key. The client verifies the authenticity of the certificate by checking its digital signature against a trusted certificate authority (CA). Once the certificate is validated, the client generates a session key to encrypt and decrypt the data exchanged between the client and server. This ensures that the communication between the client and server is secure and protected against eavesdropping and MITM attacks;
- **mutual TLS (also known as two-way TLS):** Mutual TLS goes a step further by requiring both the server and the client to authenticate themselves to each other. In addition to the server's certificate presented during the handshake, the client also presents its own digital certificate to the server. This certificate includes the client's public key. The server verifies the client's certificate in the same way the client verifies the server's certificate. Both parties can independently validate the certificates using trusted CAs. Once the certificates are authenticated, both the client and server can securely communicate and exchange data using a session key generated during the handshake.

Nowadays, the most common protocols typically require the implementation of one-way TLS, performing the authentication of the client to the server on the application layer with static credentials. Some studies suggest the implementation of mutual TLS, replacing these static credentials with TLS client certificates in order to mitigate the risk of password leaks and subsequent masquerading attacks. Furthermore, only new versions of some of these common protocols indicate which version of TLS should be implemented leading to different cipher suites being used in different communication links. The standardization of TLS requirements, together with a unified Public Key Infrastructure (PKI), would simplify the ecosystem, reduce the risk of interoperability bugs and make it easier to update the implementation if vulnerabilities are found [20].

3.2.3. End-to-end security

Even when all the communication links are secure, end-to-end security is not guaranteed due to the large number of actors involved. The fundamental idea behind end-to-end security is to secure the data at its source and maintain that security throughout the entire communication process, regardless of the intermediate infrastructure or entities involved. It means that the data is encrypted and decrypted only by the sender and recipient, and no intermediate parties (including service providers or network infrastructure) have access to the plaintext data.

In the EV charging infrastructure, all actors must trust each other in that once a message exits a TLS tunnel, its integrity and confidentiality are maintained. Several solutions are proposed in the literature to overcome this problem:

- in addition to TLS, some authors suggest the implementation of security at the level of application layer, in order to provide end-to-end confidentiality and non-repudiability. For example, a novel approach in compliance with General Data Protection Regulation (GDPR) is given by [22], while a solution for EVs and CSs not adopting the latest protocols can be found in [20];
- other studies, like [2], have shown the possibility to use a so called publish/subscribe architecture, which would be particularly beneficial also in terms of flexibility and scalability, given the large number of different parties involved in the infrastructure.
  In this architecture, there are three main entities: publishers, subscribers, and a message broker. Publishers are responsible for generating and publishing messages to specific topics or channels without having any knowledge of who or how many subscribers there are. They produce messages containing relevant data or events that need to be communicated to interested parties. Subscribers, on the other hand, express their interest in specific topics or channels and receive relevant messages whenever they are published. Subscribers can dynamically subscribe or unsubscribe to topics based on their needs. They are typically decoupled from the publishers and do not have any direct knowledge of their existence. The message broker acts as an intermediary between publishers and subscribers. It receives published messages and routes them to the appropriate subscribers based on their subscriptions. The broker ensures that messages are delivered only to interested subscribers, allowing for efficient and targeted communication. It also manages the complexities of message distribution, such as handling multiple subscribers, scalability, and fault tolerance.

3.2.4. Physical security

Another important aspect to consider when securing the EV charging infrastructure is obviously the physical access to the CSs, especially in the public architecture. In this paragraph we tackle the attack phase in which physical access is involved to gain control of a device, acquire its confidential information or alter its performances.

To enhance the security of the CSs enclosure, various measures can be implemented [18] [23]:

- firstly, the physical security can be improved by incorporating a robust locking mechanism, sensors, and tamper-evident seals. This ensures that access to the interior components is prevented or detected;
- to protect sensitive information, it is essential to avoid posting login credentials or any other confidential data inside the CS. Additionally, encryption should be applied to internal storage

devices, such as hard drives, to safeguard data at rest. This ensures that even if the storage medium is compromised, the information remains protected;

- to prevent unauthorized bypassing of drive encryption, a password-protected BIOS and secure boot process can be employed in the internal systems of the CS. This ensures that the encryption measures are not easily bypassed;
- to maintain the integrity of the firmware, a bootloader can be utilized that verifies digital signatures on all firmware updates and supports secure boot operations. This ensures that only authorized and verified firmware updates are installed;
- debug ports and local wireless interfaces should be disabled, configured to prevent the display of sensitive information, or require authentication. This prevents unauthorized access and exposure of sensitive data through these ports;
- furthermore, any unused services on the internal EVSE systems should be disabled to minimize potential vulnerabilities. By disabling unnecessary services, the attack surface is reduced, enhancing overall security. Running services instead should follow the principle of least privilege;
- devices, especially CSs, should be designed in order to support the requirements of future updates of protocols. CSs are meant to be operative for decades and, since this a fast pace evolving sector, hardware should be redundant to support future innovations and regulations without necessitating of expensive upgrades. At the same time, it should be possible to remotely update the firmware and configuration settings of the devices. This operation must be secure, with ensured firmware images, and possibly not needing a reboot to minimize the downtime and communication loss.

3.2.5. Monitoring security

Even when all the mitigation techniques are being implemented the risk of an attack will only be reduced but never be completely zero. For this reason, and also in the eventuality of some prescribed practices not being followed, the relevant actors in the EV charging infrastructure should implement monitoring mechanisms, in order to detect and promptly stop any eventual attacks, together with periodic functionalities and security assessments.

In order to facilitate the detection and response to security incidents, it is necessary for the CS to record relevant security events and enable their collection for analysis. As the security logs play a crucial role in maintaining security, they must also be safeguarded themselves. This information should be accessible both locally, using standard maintenance tools, and remotely, allowing the CSs to transmit all the logs to a centralized system [24].

Additional information can be gathered from intrusion detection systems, firewalls as well as cyber deception technology. It is important for devices to have sufficient storage capacity to retain these logs in case the system encounters malfunctions or experiences a disruption in communication with the central system. Moreover, all the gathered information should be accompanied by a synchronized timestamp indicating the occurrence of the respective event [25].

All these data should be sent and processed by a Security Information and Event Management (SIEM) platform, which is a centralized system that enables organizations to collect, analyse, and manage security event and log data from various sources within their network infrastructure. SIEM platforms provide real-time monitoring, threat detection, and incident response capabilities. The main functions of a SIEM platform include:

- **log collection:** SIEM platforms gather log data from diverse sources such as servers, network devices, applications, databases, and security appliances. These logs contain valuable information about security events, system activities, and user actions;
- **event correlation:** SIEM platforms analyse and correlate the collected log data to identify patterns, anomalies, and potential security incidents. By correlating events from multiple sources, the platform can provide a holistic view of the organization's security posture;
- **threat detection:** SIEM platforms employ various techniques, such as signature-based detection, anomaly detection, and behaviour profiling, to identify potential security threats and attacks. They compare incoming events against known attack patterns and security policies to generate alerts for suspicious activities;
- **incident response:** SIEM platforms facilitate incident response by providing automated workflows and response playbooks. When a security incident is detected, the platform can trigger predefined actions, such as sending notifications, blocking malicious IP addresses, or initiating forensic investigations;
- **compliance reporting:** SIEM platforms help organizations meet regulatory and compliance requirements by generating reports and audit logs. They provide insights into security events, user activities, and policy violations, which can be crucial for demonstrating compliance to auditors and regulatory bodies;
- **log storage and retention:** SIEM platforms typically include storage capabilities to retain log data for a specified period. This enables forensic analysis, historical investigations, and compliance audits.

4. Existing communication protocols and standards in terms of security solutions

In the rapidly expanding landscape of EV charging infrastructure [19], various protocols play a crucial role in enabling efficient and standardized charging solutions. With the aim of providing charging compatibility across different EV models and facilitating seamless charging experiences, multiple protocols have emerged. These protocols encompass aspects such as physical connectors, electrical characteristics, and communication standards. Understanding the diverse array of protocols employed in EV charging infrastructure is essential for creating interoperable and efficient charging networks on a global scale.

As protocols for EV charging infrastructure have evolved over time, there has been a growing emphasis on incorporating robust security features. This shift has been prompted by the identification and publication of vulnerabilities in the literature, prompting protocol developers to address potential risks and enhance the security measures. As a result, many of the widely adopted protocols have undergone

Funded by the European Union

updates and revisions to strengthen their security capabilities, ensuring a safer and more resilient charging ecosystem for EV owners and charging infrastructure operators.

In this chapter we present a brief overview on the most common protocols used in the different communication links, focusing on the security features they provide. Moreover, in **Figure 4** we show the protocols that will be mentioned and the corresponding communication channels. Notice that this is not an architecture depiction but only a diagram of the potential entities, communication links and protocols, some of which are mutually exclusive.

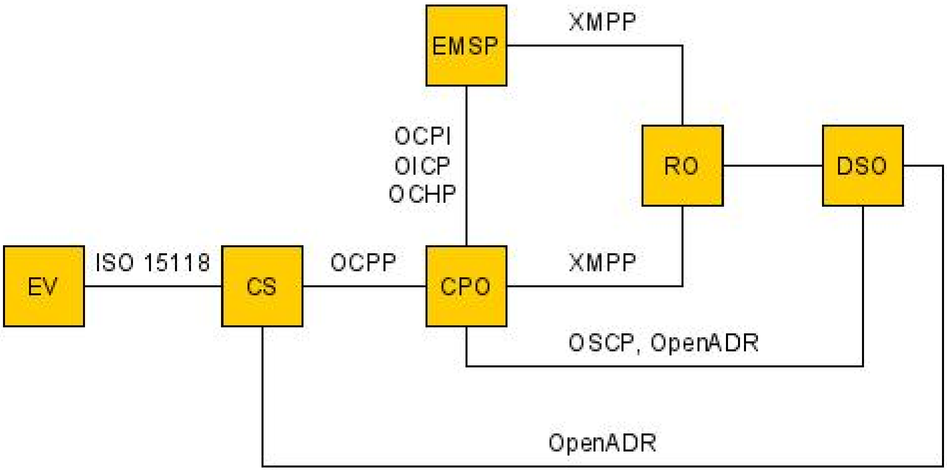


Figure 4. Infographic summary of the protocols and the corresponding communication links. Bear in mind that not all communications are present at the same time.

4.1. EV to CS communication

The communication between the EV and the CS is described by several standards and protocols. This complexity arises primarily because the communication between the two relies on a novel physical connector, which is responsible for the power delivery. This connector has been evolving to accommodate technological advancements.

Some connectors have become standard de facto of specific regions of the world, like the CHAdeMO connector in Japan, the SAE J1772, also known as the "Type 1" connector, in North America, the GB/T in China and the Combined Charging System (CCS) in Europe [26]. There exist also proprietary standards like the Tesla Supercharger. It's worth noting that interoperability between different protocols is becoming more common as EV charging infrastructure evolves. Some CSs now feature multiple connectors, allowing different EV models to utilize the same station regardless of the protocol they support.

ISO 15118 is the widely adopted standard for communication between EVs and CSs, particularly in Europe. This standard supports various physical connectors such as CCS and GB/T. In addition to the usual charging parameter negotiation, ISO 15118 enables new functionalities like Plug&Charge, which

Funded by the European Union

allows for seamless authentication and charging without the need for manual intervention, and V2G (Vehicle 2 Grid), enabling EVs to contribute power back to the grid when needed.

ISO 15118 covers multiple layers of the OSI (Open Systems Interconnection) reference model, namely [7]:

- **physical layer:** in this layer fall the physical specifications of the connector used, like pin assignments and electrical properties. ISO 15118 is actually an extension of the IEC 61851 standard, from which is based the low-level communication over the Control Pilot Pin of the charging cable;
- **data link layer:** the standard also specifies the procedures for a reliable and secure communication, these include error detection, error correction, data framing, and flow control mechanisms. Power Line Communication (PLC) is used for high-level communication, this layer is based on the HomePlug Green PHY protocol;
- **network layer:** network addressing and routing are tackled using IPv6 and other protocols on the network layer, like StateLess Address Auto-Configuration (SLAAC) and SECC Discovery Protocol (SDP);
- **transport layer:** the standard classifies different deployment scenarios in *private*, *trusted* and *public environments*, analogously to our private, semi-public and public architectures. Depending on the classification, some security features can be omitted in favor of an easier and cheaper installation. For example, the use of plain TCP is allowed in private and trusted environments, while, in the public scenario, the use of Transport Layer Security (TLS) is mandatory;
- **session and presentation layers:** ISO 15118 does not cover these layers comprehensively, messages between an EV and a CS follow the XML-EXI format;
- **application layer:** this layer includes data format used to perform authentication, authorization, charging parameter negotiation, and other higher-level functions required for effective communication.

Overall, the standard ISO 15118 includes several security mechanisms which, however, are not mandatory in all the deployment environments. Furthermore, it introduces the more secure authentication mechanism Plug&Charge, while still supporting external means of identification like RFID cards.

4.2. CS to CSMS communication

The Open Charge Point Protocol (OCPP) [1] has emerged as the dominant communication standard for establishing seamless connectivity between charging stations (CSs) and their corresponding back-end systems, also known as the Charging Station Management Systems (CSMS). What sets OCPP apart from other protocols is its open and free nature, making it widely accessible to the industry. One of its key advantages is its ability to facilitate cross-vendor operability, enabling charging stations from different manufacturers to effectively communicate and cooperate. Supported by the Open Charge Alliance (OCA), OCPP has seen the release of four versions to date, reflecting the continuous evolution of the charging infrastructure [27]:

Funded by the European Union

- OCPP 1.2 released in 2011;
- OCPP 1.5 released in 2012;
- OCPP 1.6 released in 2015;
- OCPP 2.0.1 released in 2018.

OCPP is demand-response protocol of the application layer and its latest version is compliant with the standard ISO 15118 previously described [28]. Protocols used in the other OSI layers are described in parts 2 and 3 of ISO 15118. Typically, OCPP messages are built upon HTTP(S) or WebSocket(S), and they can further utilize either the Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML), referred to as OCPP-S, or the JavaScript Object Notation (JSON), known as OCPP-J, which is the most widely adopted version of the protocol.

Note that only the latest version 2.0.1 has security built in with the objective of providing a secure communication in terms of integrity, confidentiality and mutual authenticity. Furthermore, the protocol defines secure procedures for firmware update and events logging, as well as allowed algorithms and cypher suites. Three security profiles are supported by OCPP 2.0.1:

- **Unsecured Transport with Basic Authentication Profile:** only the CS authenticates itself via HTTP and the communication is not secured
- **TLS with Basic Authentication:** the CS authenticates itself via HTTP and the CSMS authenticates itself via TLS, the communication is then secured by TLS
- **TLS with Client Side Certificates:** CS and CSMS authentication is given by mutual TLS, the communication is then secured by TLS

The unsecure profile is only allowed in trusted networks, like when there is a VPN connection between the CS and the CSMS. However, as many studies have pointed out, this poses the problem of the CPO responsibly and correctly evaluating the trustiness of the environment. This concern may be underestimated, especially in private and semi-public architectures.

Even though a correct implementation of the latest OCPP version may fulfill many of the best practices suggested in the previous chapter, in reality the version 1.6 of OCPP is still the most widely adopted, and such version does not have explicit security features defined within the protocol itself [10]. Only in a later publication of 2018, a white paper titled “Improved security for OCPP 1.6-J” describes how the security enhancements, introduced in OCPP 2.0, can be used, on top of OCPP 1.6-J, in a standardized way.

4.3. CPO to EMSP communication

The communication between a CPO and an EMSP can follow a protocol like OCPI (Open Charge Point Interface), OICP (Open InterCharge Protocol), or OCHP (Open Clearing House Protocol) [20].

OCPI, maintained by the EVRoaming Foundation [29], is the most commonly used, the current version is OCPI 2.2.1 and was released in 2021. It is an open and standardized protocol that enables communication and interoperability between different EV charging infrastructure networks and service providers. OCPI defines a set of APIs (Application Programming Interfaces) and data formats

Funded by the European Union

that facilitate various charging-related operations, such as charging station discovery, session management, pricing information, and payment transactions.

The primary goal of OCPI is to create a common framework that allows EV drivers to easily access and use charging stations from different networks using a single user interface or mobile application. It promotes an open and transparent ecosystem by providing a standardized way for charging infrastructure operators and service providers to exchange information and interact with each other.

OCPI is designed to be technology-agnostic and supports different communication protocols, including HTTP/RESTful APIs and WebSocket. It focuses on providing a consistent and seamless charging experience for EV drivers, regardless of the charging network they are using.

OCPI does not explicitly define security features within its protocol specification, the implementation of security measures, like traffic encryption, is the responsibility of the system and service providers. The documentation [30] just briefly says that security is given on the HTTP transport level with SSL, requiring a certificate from the server and static credentials from the client. Notice that this means that OCPI explicitly advises against mutual TLS and instead refers to SSL (Secure Socket Layer), which is considered outdated and insecure.

4.4. CPO to RO communication

In order to maintain grid stability in the presence of high-capacity charging points, it is essential for the Distribution System Operator (DSO) to have the capability to communicate with the Charge Point Operator (CPO) regarding the current capacity and supply-demand status. An analogous communication must take place between the CPO and the Energy Management System (EMS), if present. Mainly two protocols are used for this purpose [20]:

- **Open Smart Charging Protocol (OSCP):** supported by the Open Charge Alliance [31], the current release is OSCP 2.0. It facilitates communication and negotiation between a DSO and a CPO. The DSO generates a forecast of supply and demand in 15-minute intervals and shares with the CPO the assigned and the available spare capacity. The CPO can then negotiate for a higher or lower capacity allocation. Subsequently, the CPO develops a charging plan for the CSs, specifying the power limits they can provide per time slot, and communicates this information to the CSs using protocols such as the OCPP. Notice that OSCP does not include security features, just like the OCPI it simply says that the HTTP interfaces are protected with SSL and static credentials.
- **OpenADR (Open Automated Demand Response):** supported by the OpenADR Alliance [32], the current release is OpenADR 2.0. It provides similar features to the OSCP, with the difference that it gives more control to the DSO which, for example, is allowed to directly turn off CSs in case of peak demand. Furthermore, OpenADR comes with security built-in: it has two security profiles, both with some mandatory security measures. It also specifies which cipher suites and TLS version to implement.

In the presence of a Remote Operator (RO) in private infrastructures, as we recall from the architecture section, the communication between him and the CSs is mediated through a device called CIR [3]. Such communication follows the Extensible Messaging and Presence Protocol (XMPP) in a publish/subscribe

Funded by the European Union

paradigm. The reference documentation includes detailed security requirements and guides for a secure implementation. For example, it mandates the use of mutual TLS and SASL (Simple Authentication and Security Layer) security, in order to provide authenticity and an encrypted communication channel. Cipher suites and TLS version are specified, together with a description of the required Public Key Infrastructure (PKI) for managing digital certificates.

5. Testing and evaluation of secure EV charging infrastructures

Implementing preventive and defensive security measures in EV charging infrastructure is crucial. The de-facto protocol used to manage communications between charging stations and back-end systems of charge point operators or charging station management systems is the Open Charge Point Protocol (OCPP) [27]. As previously mentioned, the OCPP protocol is an open standard with no cost or licensing barriers for adoption developed by the Open Charge Alliance (OCA) since 2009. The most recently developed version is OCPP version 1.6 [33] and version 2.0.1 [1], which has been released but hasn't been widely adopted yet. The protocol uses HTTP(S) and WebSocket. The OCPP messages are structured based on the Simple Object Access Protocol (SOAP)/Extensible Markup Language (XML) which is denoted as OCPP-S or on the JavaScript Object Notation (JSON) standard which is marked as OCPP-J and is the most adopted version. OCPP v1.6 messages are grouped into six profiles: Core, which includes all messages required for the basic functionality of the OCPP; Firmware Management, about updating the firmware of the Charging Station (CS) and getting logs when required; Local Authentication List Management, messages containing configurations and features to reduce the traffic between the CS and back-end and to operate when its network connection is lost; Remote Trigger, trigger messages sent by the CS; Reservation, messages sent to reserve a connector of the CS and Smart Charging, messages to control the power consumption by limiting charging parameters. The OCPP version 1.6 does not include security requirements. These were added later and published with the OCPP1.6 Security Whitepaper "Improved Security for OCPP1.6-J" in three different editions, the last one in 2022 [34]. Three different security profile and their requirements are described in the OCPP1.6 Security White Paper:

1. Unsecured Transport with Basic Authentication, which uses HTTP Basic Authentication for the Charging Station.
2. TLS with Basic Authentication, which uses HTTP Basic Authentication, and TLS Authentication using Certificates for the Central System.
3. TLS with Client-Side Certificates, which uses TLS Authentication and Certificates for both Charging Station and Central System.

Using OCPP v1.6-J without security profiles can be insecure, as recently reported in [35] by researchers Saposnik *et al.* of the SaiFlow Team. The Team recently discovered an attack method that combines two new vulnerabilities found in the OCPP 1.6-J standard: mishandling of multiple chargers' connections and weak authentication policy. Cyber attackers could disrupt the original connection

Funded by the European Union

between the CS and the backend by opening an additional connection to the backend on behalf of the CS. This action could lead to Denial of Service (DoS) attacks, and data/energy theft. The SaiFlow Team suggests mitigating these attacks by monitoring anomalies of Charging Stations and checking for multiple connections that use the same identity. The Team also stresses adding at least a basic authentication mechanism to Charging Stations or preferably mutual TLS authentication. If using basic authentication, it is crucial to use customized passwords for each CS and avoid using the default password provided by the Charging Stations' manufacturers. By enforcing this policy, it will be harder for attackers to spoof the charger's identity, making the multiple charger connections attack method obsolete.

Regarding the vulnerabilities highlighted by the SaiFlow Team, the OCA, as reported in [36], stresses that it is essential to implement the additions from the Security Whitepaper "Improved security for OCPP 1.6-J" for OCPP 1.6-J implementation or to use OCPP 2.0.1 instead, which has security built in.

This is an example of how crucial it is to adopt strong security measures when implementing a communication protocol in EV Charging Infrastructure. Furthermore, the case highlights the importance of monitoring and situational awareness systems. For this reason, implementing a platform that can collect and analyze traffic features in real-time has been considered a necessary step to evaluate the security of an EV charging infrastructure and detect anomalies.

5.1. RSE EV Charging Infrastructure

RSE is a medium-sized company located in Italy, with about 350 employees divided into two offices about 100 km apart. As shown in **Figure 5**, the recharging infrastructure is located in Milan and comprises 12 Charging Stations with two connectors, each with a rated output of 22 kW AC. The Charging Stations are OCPP v1.6-J compliant and were bought from five manufacturers (Calbatt/Gewiss, BeCharge, Fimer, SCAME, and S&H) to test interoperability.

From the electrical point of view, the Charging Stations are installed in a dedicated sub-portion of the company's electrical grid, and an independent power quality analyzer, Janitza UMG 512, located in the cabinet, measures the relevant electrical information such as total active/reactive energy, voltage fluctuations, and currents.

From the IT point of view, six CSs are connected through ethernet cables and optical fibers using a Virtual Local Area Network (VLAN) to an OCPP v1.6-J Controller written in Python3.8 running on a Virtual Machine on the RSE's Private Cloud based on OpenStack [37]. Three CSs are connected to two CSs each through an RS485 standard serial connector (master-slave scheme). The remaining three CSs are IoT-enabled and connected to the OCPP controller through the Public Internet. The charging infrastructure also contains a firewall to monitor and control accesses. The power quality analyzer sends measurements to an application running on a Virtual Machine on RSE Private Cloud over Ethernet using Modbus protocol. The OCPP Controller communicates with the CSs using the OCPP-J/WebSocket protocol and with an Application Programming Interface (API) to manage business parameters and electrical parameters from the Low Voltage Microgrid of the RSE Test Facility. The OCPP controller also interacts with a database service SQL where all the data exchanged between the OCPP Controller and the CSs are stored, and with an Optimizer of the charging process. The company's

Funded by the European Union

badge has an RFID code used by the Charging Stations for authentication and billing. The company fleet comprises four fully electric vehicles (Renault Zoe, 52 kWh battery) and three Plug-in Hybrid EVs (Renault Megane, 9.8 kWh battery). For the employees, there are around 15 regular users of the infrastructure, which have both fully electric and plug-in hybrid vehicles. An overview of RSE's EV Charging Infrastructure is shown in **Figure 6**.

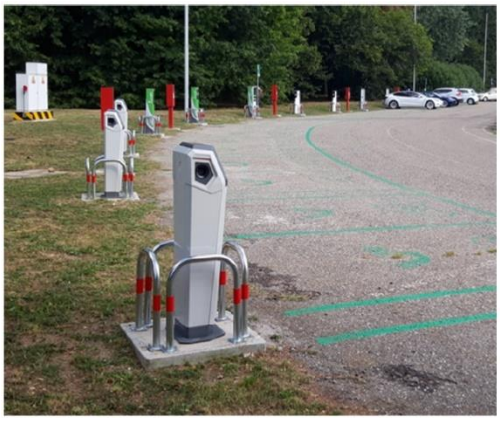


Figure 5. Overview of RSE's EV Charging Infrastructure.

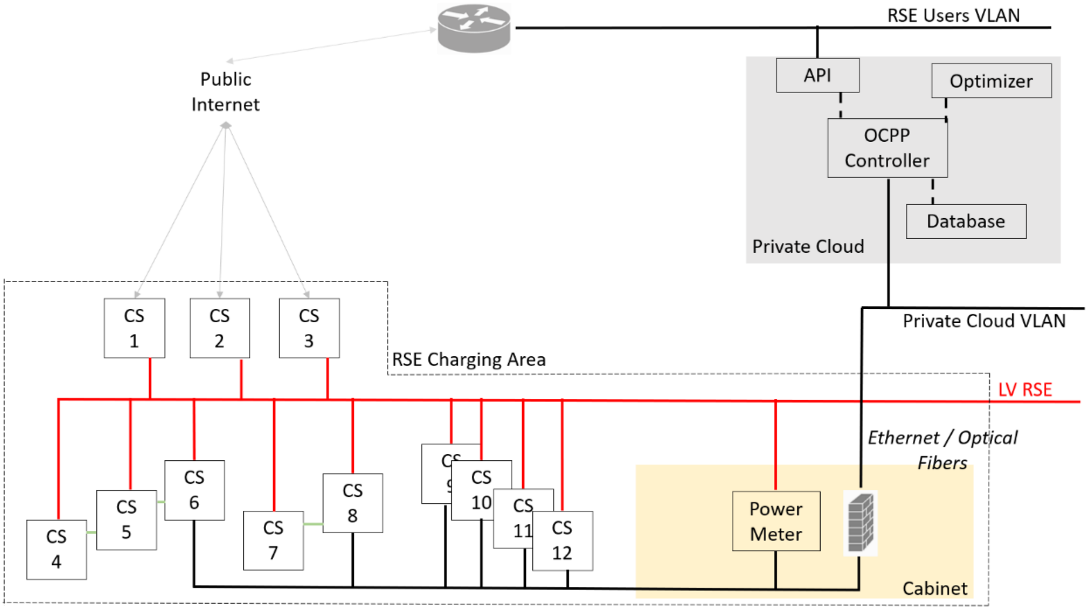


Figure 6. RSE's EV Charging Infrastructure Schema.

5.2. Packet Analyzer Platform

Pursuing the security-by-design principle, a platform has been implemented to extract network-based information from the communications between the CSs and the OCPP controller. The ethernet switch located on the VLAN that connects CSs and the OCPP Controller is configured to replicate the traffic on a port which is in turn connected to a server (Dell Power Edge T640 with Ubuntu 20.04.1 LTS operating system) located in RSE's IoT and BigData Laboratory, as shown in **Figure 7**. Two different applications are combined to extract and analyze traffic features: TShark and Elastic Stack.

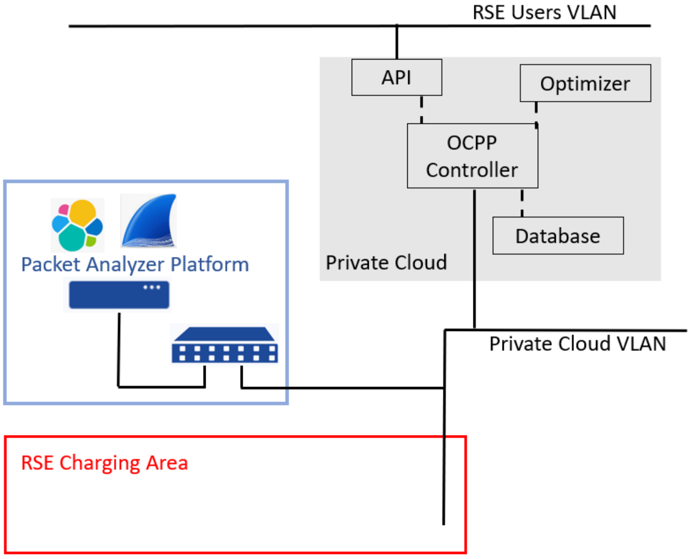


Figure 7. RSE's EV Charging Infrastructure and Packet Analyzer Platform Schema.

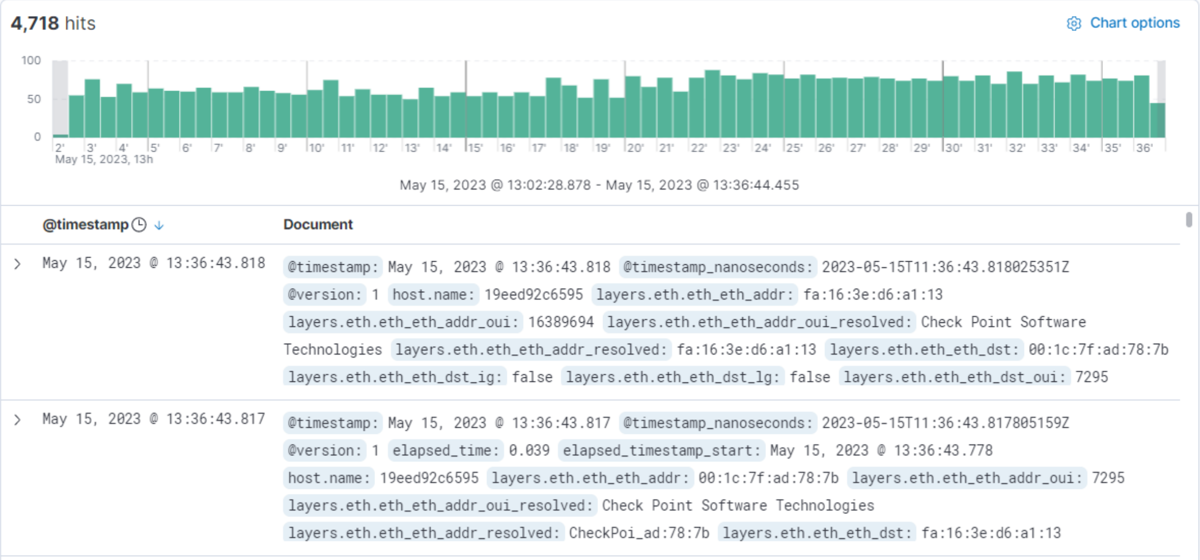
Tshark [38] is a command line version of Wireshark [39], an application that captures packet data from a network and prints a decoded form of those packets to file. The software is free and open source and is the most used worldwide for analyzing network packets. The tool is primarily used to troubleshoot network issues, investigate security issues, test network applications, and fix protocol implementations. Its main features are the ability to capture in real-time packets from network interfaces, to read and import packets from files of different formats, to display packets with detailed protocol information, to save captured data and export them in other formats (for example pcap file format) and to filter and select packet according to different criteria. In this case, version 3.2.3 of the TShark application is installed on the previously mentioned server located in the RSE IoT and Big Data Laboratory.

The Elastic Stack [40] comprises three open-source projects: Elasticsearch, Kibana, and integrations, of which the most used are Logstash and Beats [40]. Elasticsearch is a distributed search and analytics engine based on Apache Lucene. Kibana is a data visualization and exploration tool, and Logstash is a data import tool that allows one to collect data from various sources, transform it and send it to the desired destination. The three open-source projects interact with each other: Logstash aggregates,

Funded by the European Union

processes, and imports data from various sources and sends it in real-time to Elasticsearch. Elasticsearch indexes the data and enables users to perform complex queries on their data and use aggregations. Kibana allows users to create powerful visualizations of their data, share dashboards, and manage the stack. The strengths of the Elastic Stack are speed, scalability, and the ability to work with data of different formats. For the project, the version used of the ELK Stack is 7.7.0. In addition, the stack was installed as a cluster consisting of three Elasticsearch nodes, a Logstash node, and a Kibana node. The five nodes were installed respectively on five Docker containers [41] located on the server of the IoT and BigData Lab of RSE.

The TShark tool and the Elastic Stack were combined to build a Packet Analyzer Platform. For this purpose, a custom bash script is written to capture packets with TShark from the server's interface and to print it to a file in JSON format. Then, a Logstash pipeline is configured to correctly parse the packets in the file and send it to the Elasticsearch engine in real time. The possibility to filter and parse messages using Logstash means that this platform can be used and configured to elaborate messages of any protocol, making it a highly interoperable tool. The Kibana open-source tool is used to query and analyze the data and to create dashboards and charts to visualize metrics. These components form a real-time situational awareness system based on evaluating selected features directly extracted from the communication network. This information is crucial to promptly detect anomalies and outages in the network and assess the system's resilience. As visible in **Figure 8**, the platform processes about 8000 packets per hour in real-time for the entire recharge infrastructure; it is essential to highlight that the performances of the Packet Analyzer Platform are highly scalable.



```
May 15, 2023 @ 13:36:43.818   @timestamp: May 15, 2023 @ 13:36:43.818 @timestamp_nanoseconds: 2023-05-15T11:36:43.818025351Z
                              @version: 1 host.name: 19eed92c6595 layers.eth.eth_eth_addr: fa:16:3e:d6:a1:13
                              layers.eth.eth_eth_addr_oui: 16389694 layers.eth.eth_eth_addr_oui_resolved: Check Point Software
                              Technologies layers.eth.eth_eth_addr_resolved: fa:16:3e:d6:a1:13 layers.eth.eth_eth_dst: 00:1c:7f:ad:78:7b
                              layers.eth.eth_eth_dst_ig: false layers.eth.eth_eth_dst_lg: false layers.eth.eth_eth_dst_oui: 7295

May 15, 2023 @ 13:36:43.817   @timestamp: May 15, 2023 @ 13:36:43.817 @timestamp_nanoseconds: 2023-05-15T11:36:43.817805159Z
                              @version: 1 elapsed_time: 0.039 elapsed_timestamp_start: May 15, 2023 @ 13:36:43.778
                              host.name: 19eed92c6595 layers.eth.eth_eth_addr: 00:1c:7f:ad:78:7b layers.eth.eth_eth_addr_oui: 7295
                              layers.eth.eth_eth_addr_oui_resolved: Check Point Software Technologies
                              layers.eth.eth_eth_addr_resolved: CheckPoi_ad:78:7b layers.eth.eth_eth_dst: fa:16:3e:d6:a1:13
```

Figure 8. Snapshot of Logstash pipeline, the bar plot corresponds to the count rate of captured packets from the network, below part of the content of selected packets is shown.

Funded by
the European Union

5.3. Analysis of network traffic of RSE EV Charging Infrastructure

In a connection between a Charging Station and a Controller using OCPP-J, the Controller acts as a WebSocket server and the CS acts as a WebSocket client. As reported in **Figure 9**, three different kinds of packets are sent in a WebSocket connection: TCP (SYN, SYN/ACK, ACK, FIN) packets, HTTP Request and Response, WebSocket Ping, Pong, and OCPP-J over WebSocket.

Analyzing the traffic through the Packet Analyzer Platform, we see that for a selected CS, it is possible to filter the packets related to different protocols, as visible in **Figure 10**.

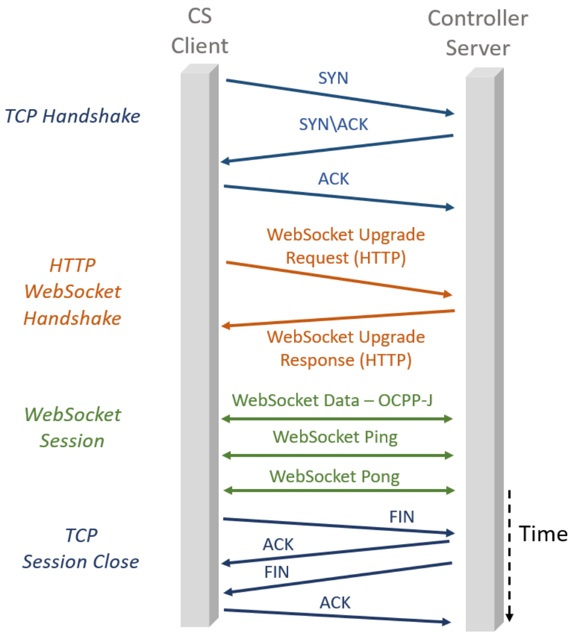


Figure 9. A diagram describing the connection between a CS and a Controller using OCPP-J/WebSocket

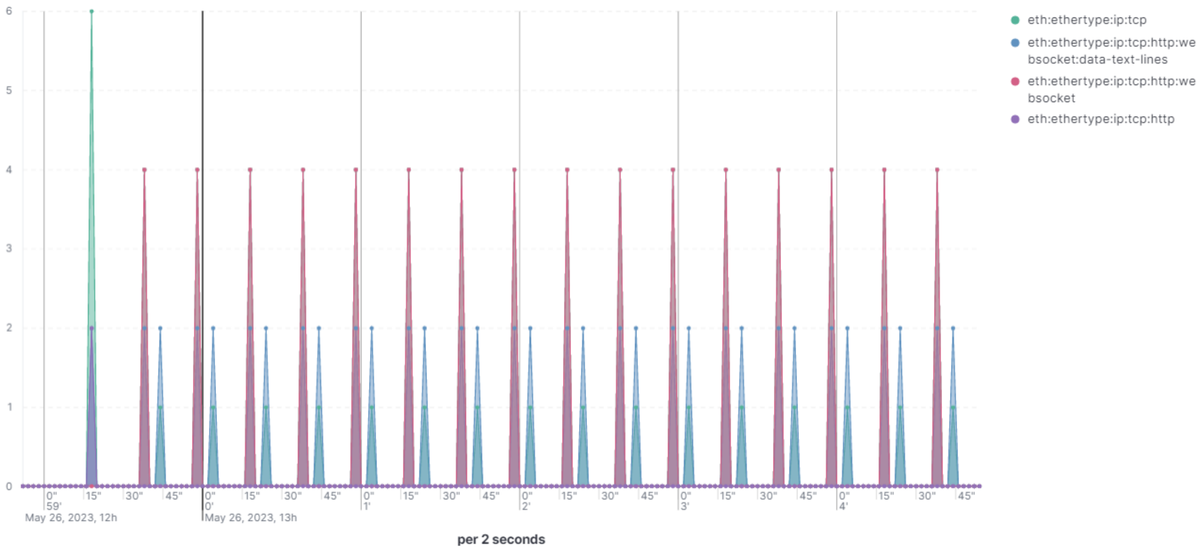


Figure 10. Count rate of packets (count per 2 seconds), colors correspond to different type of packets sent in the communication between particular a CS and the Controller.

By selecting a particular CS and filtering for different TCP flags present in the TCP packets, it is possible to verify if there are anomalies in the sequence of the TCP handshake. The count rate of TCP packets exchanged between the CS and the Controller filtered for different TCP flags is shown in **Figure 11**. It is essential to note that the software implemented on the selected CS automatically disconnects and reconnects the CS to the Controller about one time per day. The CS remains disconnected for about 10 seconds during this procedure, as visible in **Figure 11**. In this time window, a malicious entity can connect to the controller on behalf of the actual CS. This attack could lead to a potential Denial-of-Service of the original CS and energy/data theft.

Funded by the European Union

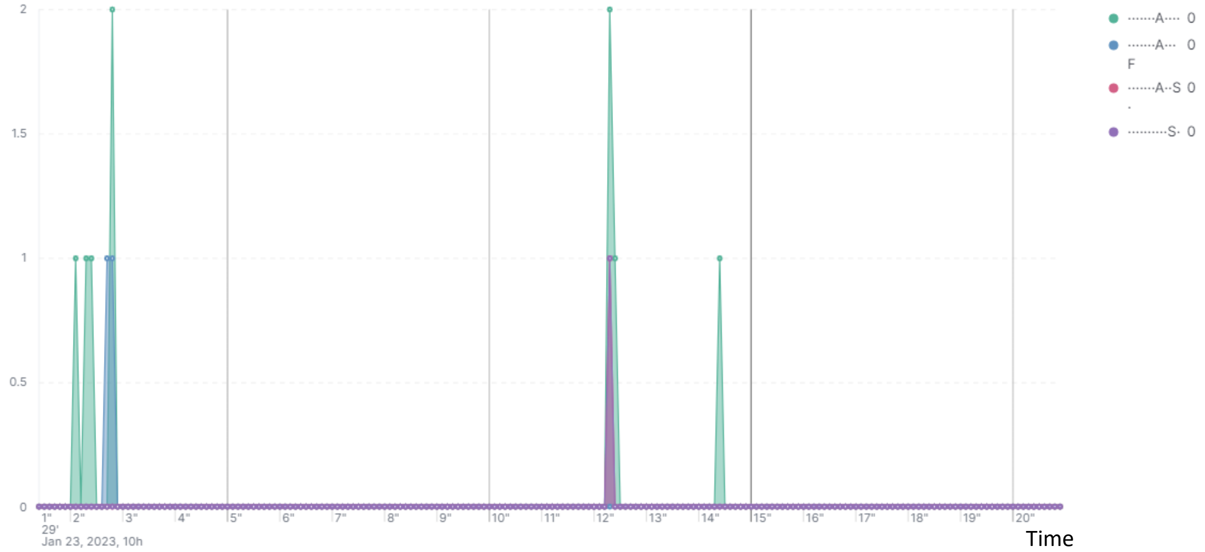


Figure 11. Count rate of TCP packets (counts/s) exchanged between a selected CS and Controller during the end of a connection and the start of a new one; colors correspond to different TCP flags.

Filtering for the HTTP messages, it is possible to examine the content of the HTTP WebSocket request sent by the client CS which is of the form:

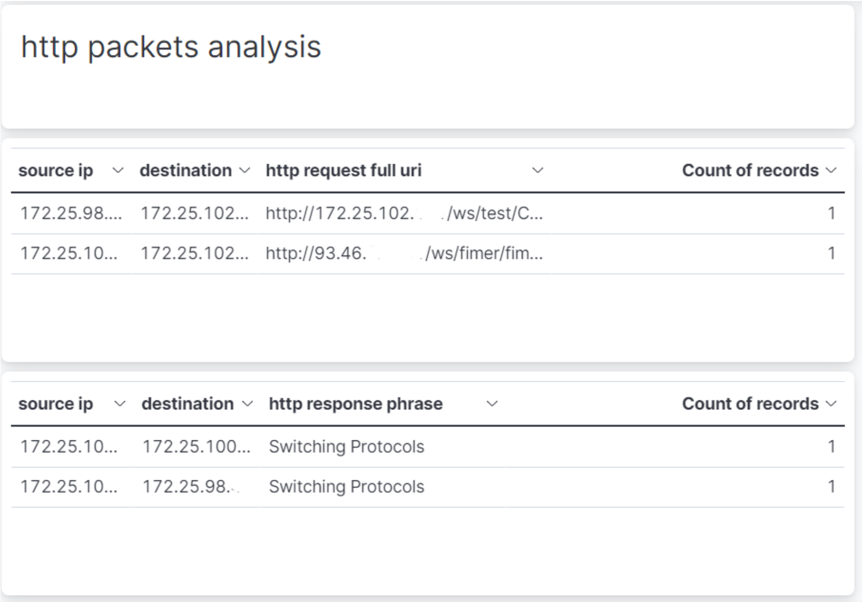
```
GET /ws/CS_test HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: …
Sec-WebSocket-Protocol: …
Sec-WebSocket-Version: 13
Origin: http://example.com
```

And the HTTP response of the server is of the form:

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: …
Sec-WebSocket-Protocol: …
```

As shown in Figure 12, the content of HTTP requests and responses can be aggregated and inspected to verify the presence of multiple connections or IP spoofing.

Funded by
the European Union



http packets analysis

source ip	destination	http request full uri	Count of records
172.25.98....	172.25.102...	http://172.25.102. /ws/test/C...	1
172.25.10...	172.25.102...	http://93.46. /ws/fimer/fim...	1

source ip	destination	http response phrase	Count of records
172.25.10...	172.25.100...	Switching Protocols	1
172.25.10...	172.25.98.	Switching Protocols	1

Figure 12. Snapshot of the Kibana dashboard created to display information regarding HTTP WebSocket request and response.

The WebSocket protocol specifies Ping and Pong messages that check if the remote client is still responsive. It is interesting to monitor the WebSocket Ping-Pong exchange to see if there are any anomalies. **Figure 13** shows the count rate of Ping messages the selected CS sends to the controller; the Ping interval is fixed at 20 seconds.

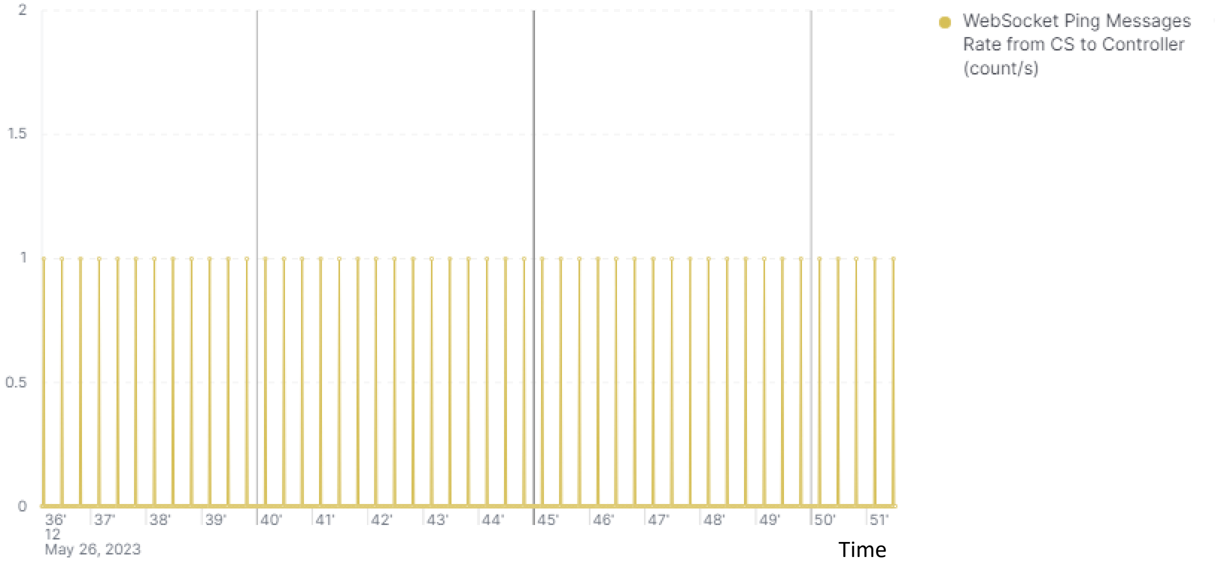


Figure 13. Count rate (count/s) of WebSocket Ping Messages from CS to Controller.

Funded by the European Union

So far, the variables analyzed are extracted directly from the parsed content of packets. It is also possible to calculate additional metrics from the network traffic using the Packet Analyzer Platform. This can be useful to understand patterns that characterize the network traffic and to detect anomalies. An example is the calculation of delays between request and response packets. Measuring latency between request and response messages can help detect DoS attacks which usually generate network congestion, and to detect the presence of a third malicious entity, for example, in Man-In-The-Middle attacks. For this reason, an elapsed time script is implemented in the Logstash pipeline to calculate the time difference between a Ping and a Pong in WebSocket communication. Ping and Pong are identified with an unambiguous Unique ID. **Figure 14** shows the elapsed time between Ping and Pong for all the CSs involved. Furthermore, the count rate of the Unique IDs was measured to prevent Message Replay attacks. It may hint at this attack if more than two Unique IDs are discovered.

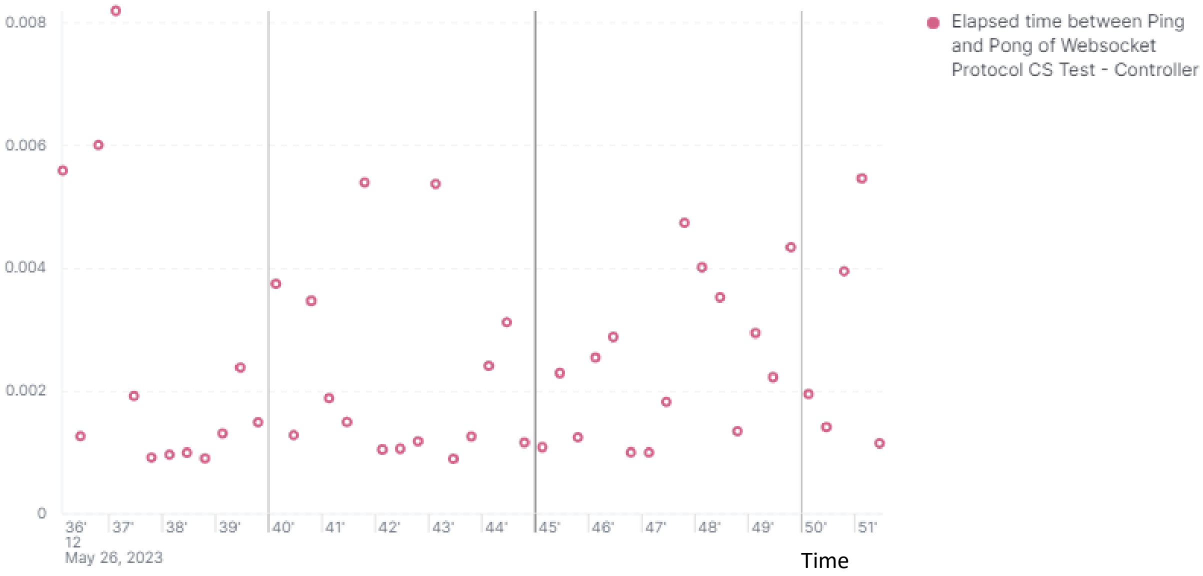


Figure 14. Elapsed time (seconds) between Ping and Pong of WebSocket communication between CS and Controller

The WebSocket Data layer contains OCPP-J messages. Using the Packet Analyzer Platform, it was possible to create a script that parses various messages required by the OCPP-J protocol. Most of the Security Information and Event Management platforms available on the market are usually focused on the analysis of logs and protocols typical of Information Technology systems, the added value of the Packet Analyzer Platform, which is proposed here, is the possibility to address and configure real-time packet analysis of protocols that are specific of the EV sector. Parsing the OCPP-J messages allows for verifying the correct sequence of request and response OCPP messages. For example, any OCPP-J message exchanged between a Controller and a CS is matched by an unambiguous Unique ID that can be checked to avoid packet replay and Man-in-the-Middle attacks. Also, it is possible to calculate additional time-related metrics in the present case. In the Logstash pipeline, the difference in time between a Heartbeat request and a response is calculated. The **Figure 15** shows the elapsed time between the OCPP Heartbeat request and response, which does not cross the threshold of 0.1 seconds in a typical network condition.

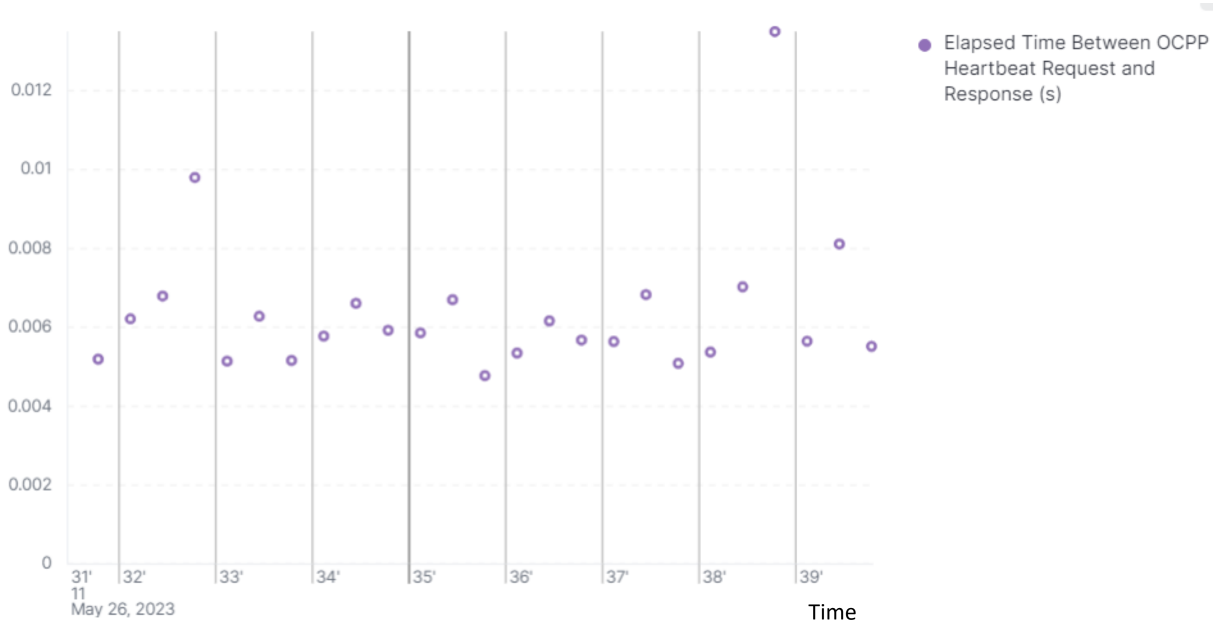


Figure 15. Elapsed time (seconds) between request and response of Heartbeat messages of OCPP-J over WebSocket protocol.

5.4. Vulnerability testing and Denial-of-Service attack

The experimental evaluation of the security of RSE EV Charging Infrastructure has been carried out in two stages: testing the vulnerability highlighted by the SaiFlow Team [35] and performing a DoS attack on a virtual CS connected to RSE EV Charging Infrastructure to test the anomaly detection capabilities of the Packet Analyzer Platform.

Considering the vulnerabilities exposed at the beginning of Chapter 5, an experimental setup was prepared to test the possibility of a connection to the Controller from a malicious entity on behalf of an original CS already connected. For this purpose, a fictitious Charging Station was created using a Python code installed on a single-board computer Raspberry PI 4, connected to the VLAN of the RSE EV Charge Infrastructure. The code simulates the behaviour of a CS that implements the OCPP-J v1.6 protocol to communicate with the controller. The first goal was to test if it is possible to enable a new connection on behalf of the CS already connected and, consequently, turn off communication between the original CS and the Controller. Using the simulated CS, we tried to connect to the Controller using the same id as the original CS. For this purpose, an HTTP WebSocket upgrade request has been sent to the Controller. We see that the malicious connection has been opened from the Controller and then immediately closed. The original CS continues to communicate without any interruption.

Funded by the European Union

```
2023-05-30 15:32:47,507 - APP Logger - WARNING - The requested websocket connection
is already active for CS: test_CS_1
INFO:     ('172.25.xxx.xxx', 58634) - "WebSocket /ws/test/CS_1" [accepted]
INFO:     connection open
INFO:     connection close
```

As highlighted in Section 5.3, most of the CS installed in the RSE EV Charging Infrastructure disconnects from the Controller for about 10 seconds daily. In this short period, a malicious entity could connect to the Controller and act on behalf of the original CS. In this case, the Controller wouldn't notice any change. As a defensive measure, the Packet Analyzer Platform can check for the authenticity of new connections, verify the source IP addresses, and see changes in the latency of messages due to, for example, a different location of the fictitious CS. Alerts can also be configured on the Packet Analyzer Platform to account for anomalies. To prevent this kind of intrusion, it is crucial to adopt the measures stated in the OCPP1.6 Security Whitepaper [34] or to implement the OCPP 2.1 version with built-in security features [1].

To study the effects of a DoS attack on a Charging Station of the RSE EV Charging Infrastructure, we consider the scenario in which an attacker, which has gained access to the network, disrupts the CS service. The attacker could have gained access to the network connecting to the controller on behalf of an original CS, which is the scenario previously mentioned. The intent of an attacker who uses the DoS technique is to make a machine or network resource unavailable to its users by temporarily or indefinitely disrupting the services of a host connected to the network. A DoS attack is usually accomplished by flooding the targeted machine with superfluous requests to overload systems and prevent or delay legitimate requests from being fulfilled. The experimental setup is composed of a virtual CS, installed on a Raspberry PI 4, connected through Ethernet to the private VLAN of the RSE EV Charging Infrastructure and a server (Dell Power Edge T640 with Ubuntu 20.04.1 LTS operating system) connected to the same VLAN which acts as the attacker. The tool used to attack the virtual CS is hping3 [42], an open-source tool that sends custom ICMP/UDP/TCP packets and analyzes the TCP/IP protocol. Hping3 is one of the de-facto tools for security auditing and testing of networks and firewalls. The experimental setup is represented in **Figure 16**.

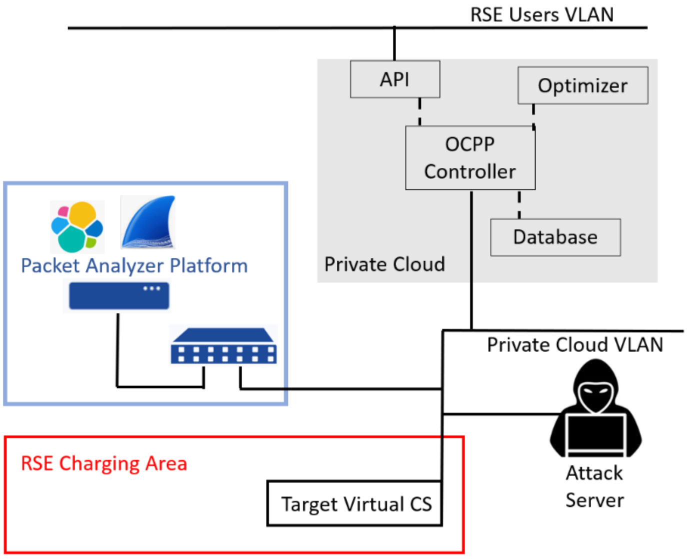


Figure 16. Experimental setup of the Denial-of-Service attack procedure.

An ssh connection was established with the virtual CS to monitor the attack procedure, and the tool bmon [43] was used to monitor network statistics of the interface of the single board computer on which the virtual CS is installed. In a typical service condition, the virtual CS receives a maximum of 1.58 KiBs per second, and a maximum of 3.76 KiBs per second are transmitted to the Controller. The attack has been launched towards the virtual CS using its IP address and overloading the target with TCP SYN packets. The source IP address was randomized to prevent replies from the attacked target.

During the attack, the number of received Byte/s increases towards almost 100 MiB until the virtual CS, due to the network congestion, cannot respond to the Controller anymore and remains disconnected. Analyzing the traffic between the attacker and the target would result in many TCP SYN messages sent to the virtual CS. However, collecting the traffic between the attacker and the target is only sometimes possible. It is, therefore, interesting to reveal the effects of network congestion on the connection between the CS and the Controller. Analyzing the network traffic between the virtual CS and the OCPP Controller, signs of network congestion are visible during the attack phase. As can be seen in the Figure 17 during the attack, the count rate of packets divided by protocol type changes significantly. In particular, the number of TCP packets exchanged in the communication increases, and the time interval is stretched. Analyzing the time difference between a TCP packet and the previous one, it is visible that multiple TCP packets are sent quickly (see **Figure 18**).

Funded by the European Union

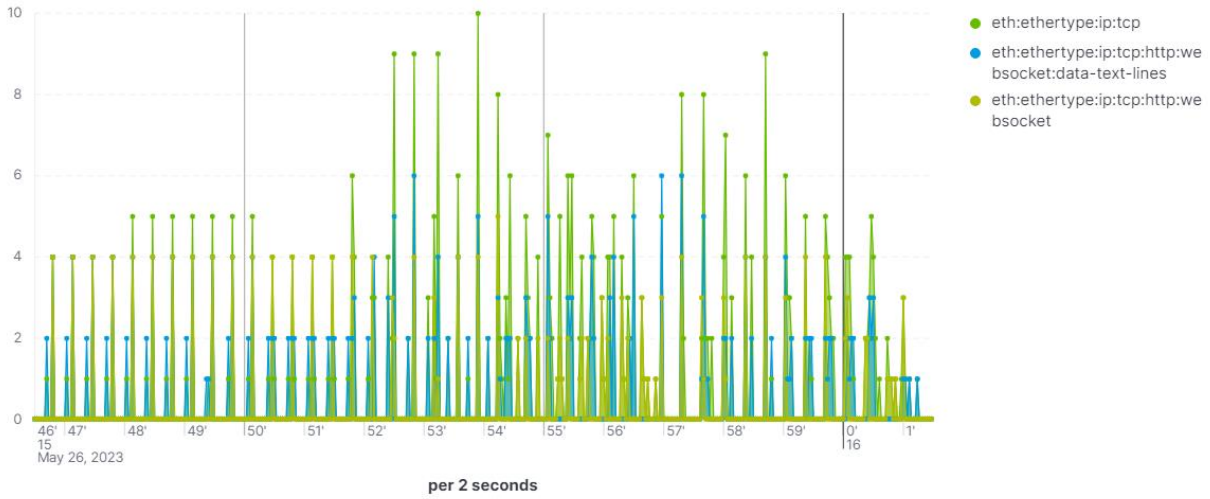


Figure 17: Count rate of packets exchanged between the CS and the Controller during the attack phase; colors correspond to different types of packets.

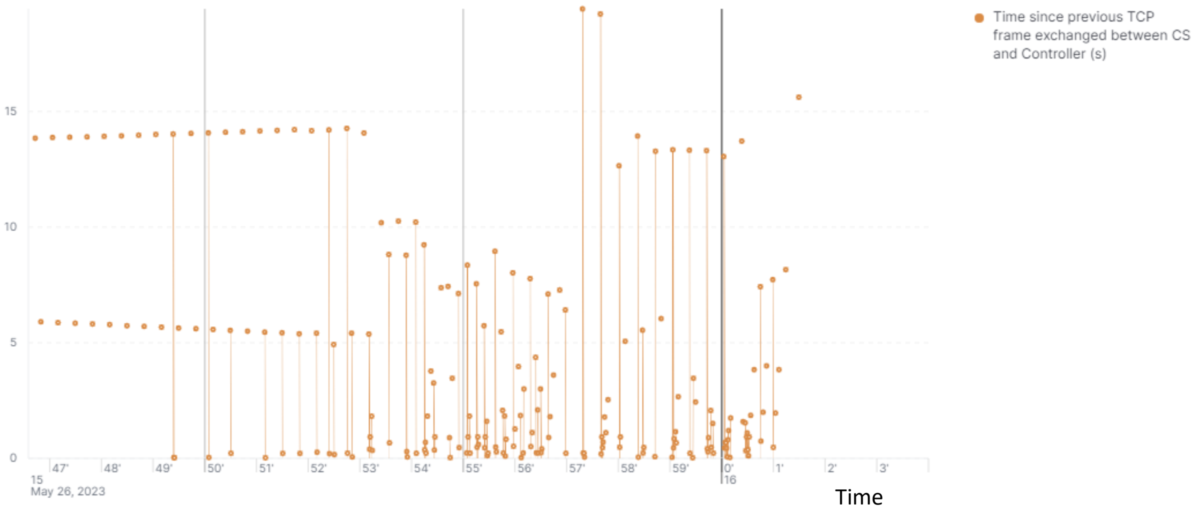


Figure 18. Time in seconds since previous frame of TCP packets exchanged between the CS and the Controller during the attack phase.

The high measured count rate of TCP packets is due to retransmission. Retransmission is the re-sending of packets that have been damaged or lost during their initial transmission. Packet retransmission is possible because the original sender retains a copy of the data sent until receipt of data is confirmed. In some cases, the sender will automatically initiate retransmission of data using the retained copy. Reasons for packet retransmission are the lack of an acknowledgment that data has been received

Funded by the European Union

within a reasonable time, the receiver notifying the sender that expected data hasn't been received or is damaged, and the sender discovering that transmission was unsuccessful, usually through out-of-band means. The presence of retransmission packets is a clear signal of a DoS attack. Using the Packet Analyzer Platform, it is possible to enable in the TShark tool the Expert Info functionality. This tool shows unusual behaviour or anomaly situations on the network, such as retransmissions or fragmentation of packets. As shown in **Figure 19**, TCP retransmission packets are present during the attack phase.

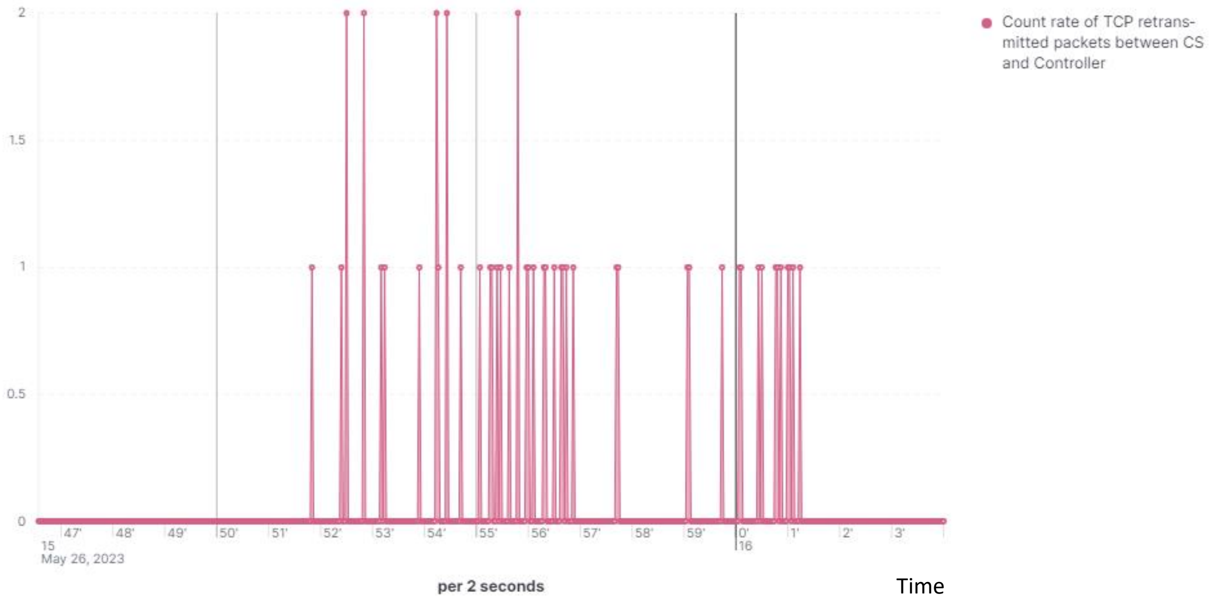


Figure 19. Count rate (counts/ 2 seconds) of TCP retransmitted packets in the connection between CS and Controller during the attack phase.

The count rate of WebSocket messages also presents anomalies that are network congestion symptoms. In **Figure 20**, the count rate of Pong Messages sent by the CS to the Controller during the attack is shown.

Funded by the European Union

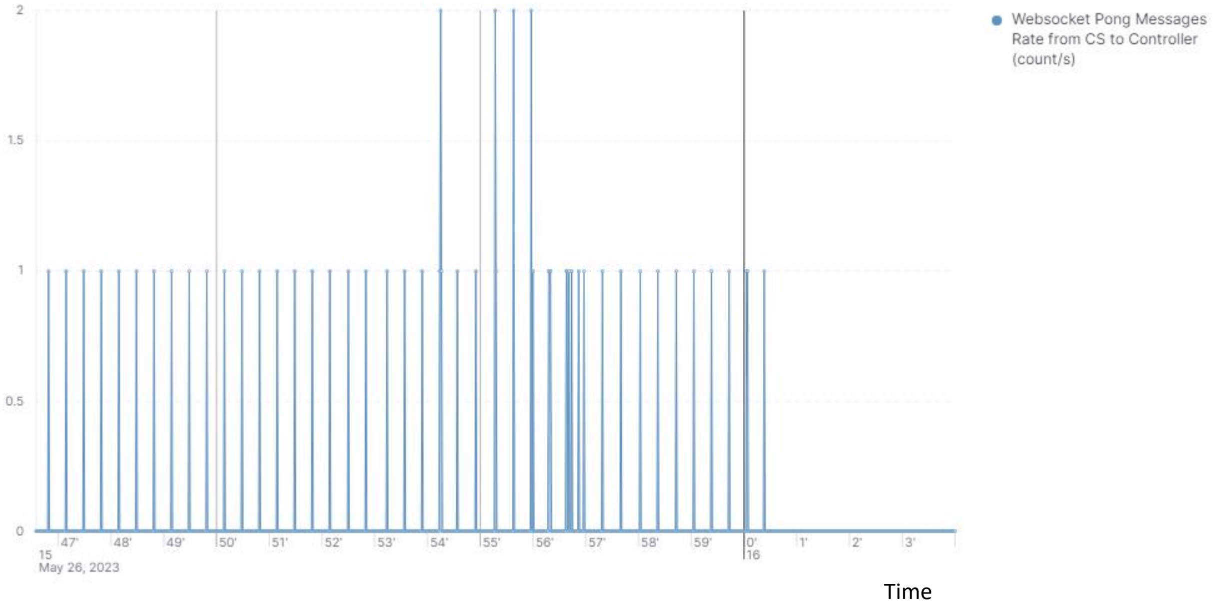


Figure 20. Count rate (count/s) of WebSocket Pong sent by CS to the Controller during the attack phase.

Figure 21 shows that the time difference between the WebSocket Ping and Pong between the CS and the Controller increases during the attack phases. Messages experience an increasing delay as network congestion increases, crossing the threshold of 0.1 seconds, which states a typical network behavior.

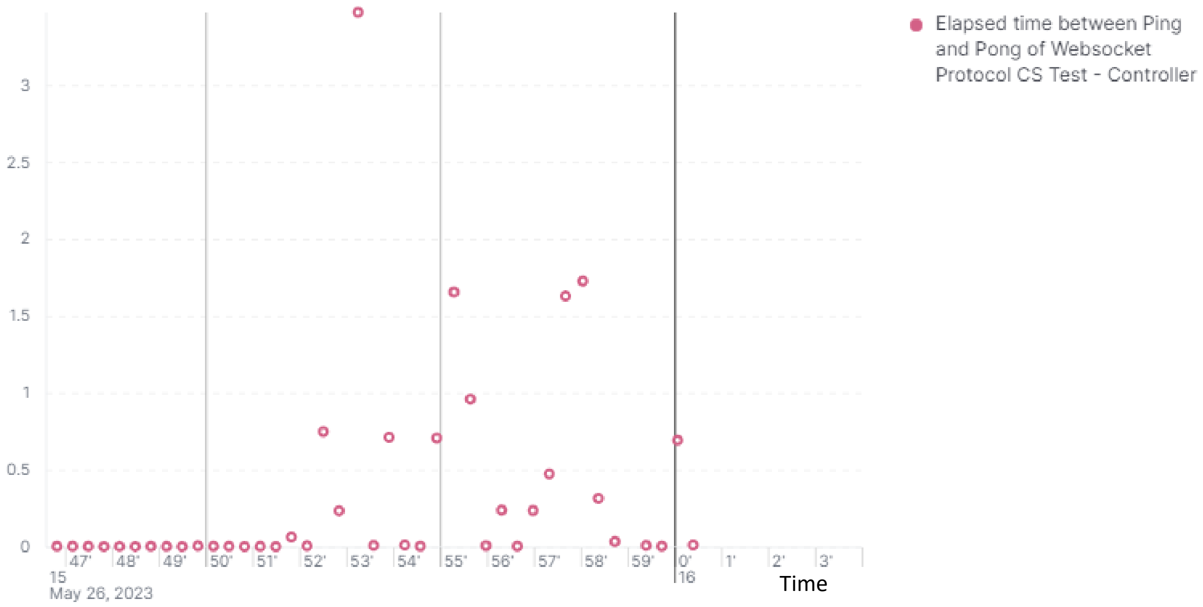


Figure 21. Elapsed time (s) between Ping and Pong of the WebSocket communication between the CS and the Controller during the attack phase.

In conclusion, the importance of implementing preventive measures such as authentication and mutual TLS, as suggested by the main guidelines for OCPP implementations, was demonstrated. Furthermore, the importance of defensive measures for anomaly detection has been stressed. In this regard, collecting information from network traffic has been revealed to be an essential aspect. Network packet capture and analysis can increase the situational awareness of the system. Furthermore, datasets constructed capturing packets from real EV charging infrastructure networks, currently lacking, can be created to train and test machine learning models designed for anomaly detection capability in the specific context of the electric mobility sector.

6. Privacy and security user perception

6.1. User Research on Data Privacy in Smart Charging

User research showed that privacy concerns could be a barrier to smart charging participation [44]. This may be because smart charging requires granular information about the consumption needs of BEV users. In addition, detailed consumption data is collected. Smart data processing makes it possible to identify precise indicators of activity patterns, ranging from energy consumption and charging information to movement profiles and daily routines.

A questionnaire study [45] revealed that the willingness to share information about smart charging varies depending on the degree of data aggregation: While consumers would certainly provide information that is generated and processed in a smart charging scenario (level 1 information = raw data, which is processed in the backend system and level 2 information = already processed data aggregated to long-term data), the willingness to share information that contains a threat potential is significantly lower (level 3 information deduced from level 1 and 2, focusing on possible threats of long-term generated and processed data) and consumers are not willing to give this kind of information.

Similar results emerged from a highly naturalistic five-month smart charging field trial in Germany [46]. Again, participants were least likely to provide personal information at level 3 (e.g. "Whether my household is unattended when I leave the house") compared to information at level 2 (e.g. "Rating the amount of energy I charge per week") and level 1 (e.g. "Location of the charging station where I charge"). The overall pattern in terms of serious concerns about derived information remained stable over time and was rarely influenced by real-world experience. Preferred data recipients and trust in them were also constant. As level 1 and 2 information is considered less critical, it may be readily made available to all stakeholders. In contrast, level 3 information should not be shared with any stakeholder. But participants' willingness to share personal information can be significantly increased if trust in the involved stakeholders grows. That the recipient of the data plays an important role for customers was also shown by research in the smart home context [47].

6.2. Conclusion and Recommendations from the Literature

Besides the technical feasibility of smart charging systems, the inclusion of the user perspective regarding data protection is essential to achieve active consumer participation [48], especially in the initial phase. This will encourage consumer trust and thus participation in the smart grid. However, the strong and stable rejection of sharing level 3 information indicates that regardless of their experience, users perceive a long-term risk potential for their privacy in the context of smart charging. Therefore, when developing smart charging systems, privacy should be embedded top-down from the beginning [46], e.g. by:

(1) Applying of a holistic approach, such as Privacy by Design [49]

(2) Integrating automated mechanisms for data encryption, anonymisation, decentralised data storage, etc. into the design of the ICT architecture for smart charging to protect user privacy by default Heuer (2013)

(3) Incorporating data minimisation and avoidance principles [50] to reduce the threat potential of smart systems per se

Then, from the bottom up, users must be able to decide to what extent (1) they want to be informed, (2) they want to control the sharing of data with trusted actors. Thereby, it is important to ensure that the involved stakeholders and all processes are presented in a transparent manner. In addition, the possibility of personal customer support fosters trust building.

6.3. Ongoing and Further Research within FLOW

As data protection and privacy are crucial for smart charging, the topic is investigated in WP2 T2.2.2. A questionnaire study on the willingness to share smart charging data in different charging scenarios is currently being conducted by TUC. In June 2023, data from N = 103 German respondents with and without EV experience are available. This dataset will be expanded to include respondents from the countries where the demos are placed. Results will be reported within WP2 (D2.2: Factors influencing user acceptance of smart charging and V2X concepts) and submitted to WP3.

7. Conclusions

The document presents some key considerations for EV charging infrastructure cybersecurity and describes the experimental setup where, by means of an advanced ICT monitoring platform, some evaluations on RSE EV charging infrastructure are carried out. Finally, some considerations on privacy and security user perception are presented.

In conclusion, ensuring the cybersecurity of electric vehicle (EV) charging infrastructure is of paramount importance to maintain the integrity, availability, and reliability of charging services. With the increasing adoption of EVs, it is crucial to implement robust security measures to safeguard charging infrastructure from potential cyber threats.

As highlighted in the reported analysis, key considerations for EV charging infrastructure cybersecurity include secure communication protocols, strong access control and authentication mechanisms, regular firmware and software updates, physical security measures, intrusion detection and monitoring systems and secure backend systems.

By implementing these measures, EV charging infrastructure can mitigate the risk of unauthorized access, data breaches, tampering, and other cybersecurity incidents. Timely security updates, monitoring for suspicious activities, and promoting cybersecurity awareness among stakeholders are essential to ensure the ongoing protection of charging infrastructure.

The experimental analysis demonstrates the importance to implement preventive security measures on the entire charging infrastructure, in particular applying the security recommendations of the communication protocols and standards. Moreover, it is essential to include defensive measures specialised for the EV context in terms of monitoring and anomaly detection systems. The evaluation of protocol specific indicators extracted from traffic analysis allows to detect possible malicious activities and stop the attacker actions.

A comprehensive approach to cybersecurity is necessary to address the evolving threat landscape and stay ahead of potential risks. Collaboration among charging infrastructure providers, electric vehicle manufacturers, cybersecurity experts, and regulatory bodies is vital to establish industry-wide best practices and standards for EV charging infrastructure cybersecurity.

Funded by
the European Union

8. References

[1] F. Buve, P. Klapwijk e R. de Leeuw, *Open Charge Point Protocol 2.0.1,* Open Charge Alliance, 2020.

[2] F. van den Broek, E. Poll e B. Vieira, «Securing the information infrastructure for EV charging,» *International Conference on Wireless and Satellite Systems,* July 2015.

[3] CEI, *PAS 57-127, Charging Infrastructure Controller (CIR) for electric vehicles,* 2023.

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

[5] M. Engelhardt, F. Pfeiffer, K. Finkenzeller e E. Biebl, «Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics,» *Smart SysTech 2013; European Conference on Smart Objects, Systems and Technologies,* 2013.

[6] R. Baker e I. Martinovic, «Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging,» *28th USENIX Security Symposium,* pp. 407-424, August 2019.

[7] K. Bao, H. Valev, M. Wagner e H. Schmeck, «A threat analysis of the vehicle-to-grid charging protocol ISO 15118,» *Computer Science - Research and Development,* September 2017.

[8] S. Kohler, R. Baker, M. Strohmeier e I. Martinovic, «BROKENWIRE: Wireless Disruption of CCS Electric Vehicle Charging,» *Network and Distributed System Security (NDSS) Symposium,* 2023.

[9] S. Lee, Y. Park, H. Lim e T. Shon, «Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 based Electric Vehicle Charging Technology,» *Proceedings of the 2014 International Conference on IT Convergence and Security,* October 2014.

[10] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis e 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, n. 3, pp. 1504-1533, 2022.

[11] Pen Test Partners, «Smart Car Chargers. Plug-n-Play for Hackers?,» July 2021. [Online]. Available: www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers. [Consultato il giorno 24 May 2023].

[12] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha e C. Assi, «Power jacking your station: In-depth security analysis of electric vehicle charging station management systems,» *Computers & Security,* vol. 112, 2022.

[13] Kaspersky, «Remotely controlled EV home chargers - the threats and vulnerabilities,» December 2018. [Online]. Available: securelist.com/remotely-controlled-ev-home-chargers-the-threats-and-vulnerabilities/89251. [Consultato il giorno 24 May 2023].

Funded by
the European Union

[14] Idaho National Laboratory, *Cyber Security Research and Development: Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment,* 2018.

[15] J. E. Rubio, C. Alcaraz e J. Lopez, «Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks,» *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* pp. 1-5, 2018.

[16] C. Jewers, «Russian Motorway's Electric Vehicle Chargers Are Hacked to Display Message Supporting Ukraine,» Daily Mail, 2022. [Online]. Available: www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html. [Consultato il giorno 24 May 2023].

[17] L. R. Saposnik, «May 2023 Security Advisory for ABB Terra AC Charging Station,» May 2023. [Online]. Available: www.saiflow.com/abb-terra-ac-charging-stations-vulnerabilities-may-2023. [Consultato il giorno 24 May 2023].

[18] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan e M. Kunz, «Cybersecurity for Electric Vehicle Charging Infrastructure,» *Sandia Technical Report,* pp. 18-21, July 2022.

[19] European Commission, «European Alternative Fuels Observatory,» [Online]. Available: https://alternative-fuels-observatory.ec.europa.eu/general-information/about-european-alternative-fuels-observatory.

[20] P. van Aubel e E. Poll, «Security of EV-Charging Protocols,» *ArXiv,* n. 2202.04631, February 2022.

[21] M. van Eekelen, E. Poll, E. Hubbers, B. Vieira e F. van den Broek, «An end-to-end security design for smart EV-charging for Enexis and ElaadNL,» *ElaadNL Technical Report,* December 2014.

[22] P. van Aubel, E. Poll e J. Rijneveld, «Non-Repudiation and End-to-End Security for Electric-Vehicle Charging,» *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe),* 2019.

[23] European Network for Cyber Security, *EV Charging Systems Security Requirements,* Commissioned by ElaadNL, 2017.

[24] European Network for Cyber Security, *EV-301-2019, Security requirements for procuring EV charging stations,* Commissioned by ElaadNL, 2019.

[25] R. Metere, M. Neaimeh, C. Morisset, C. Maple, X. Bellekens e R. M. Czekster, «Securing the Electric Vehicle Charging Infrastructure,» *ArXiv,* n. 2105.02905, April 2021.

[26] K. Riya, R. Gupta, S. Agrawal, S. Tanwar, R. Sharma, A. Alkhayyat, B.-C. Neagu e M. S. Raboaca, «A Review on Standardizing Electric Vehicles Community Charging Service Operator Infrastructure,» *Applied Sciences,* vol. 12, n. 12096, 2022.

Funded by the European Union

[27] Open Charge Alliance, «OPEN CHARGE POINT PROTOCOL 2.0.1,» 2020. [Online]. Available: www.openchargealliance.org/protocols/ocpp-201/.

[28] International Organization for Standardization, «Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements,» [Online]. Available: www.iso.org/obp/ui/#iso:std:iso:15118:-2:ed-1:v1:en.

[29] EVRoaming Foundation, «OCPI Background,» 2021. [Online]. Available: evroaming.org/ocpi-background/.

[30] R. de Leeuw e R. Lamers, «OCPI 2.2.1 Open Charge Point Interface,» *EVRoaming Foundation,* 2021.

[31] Open Charge Alliance, «OPEN SMART CHARGING PROTOCOL 2.0,» 2020. [Online]. Available: www.openchargealliance.org/protocols/oscp-20/.

[32] OpenADR Alliance, «OpenADR 2.0 Specifications,» [Online]. Available: www.openadr.org/specification.

[33] R. de Leeuw, R. Lamers, B. McMahon, L. Muhlenberg, P. Rademakers, S. Tcaciuc e K. van Zuuren, Open Charge Point Protocol 1.6, Open Charge Alliance , 2015.

[34] F. Buve e P. Klapwijk, Improved security for OCPP 1.6-J., Open Charge Alliance, 2022.

[35] L. Saposnik e D. Porat, «Hijacking EV Charge Points to Cause DoS,» SAIFLOW, 1 February 2023. [Online]. Available: https://www.saiflow.com/hijacking-chargers-identifier-to-cause-dos/.

[36] Open Charge Alliance, «RECENT QUESTIONS ABOUT OCPP & SECURITY,» OCA, 16 March 2023. [Online]. Available: https://www.openchargealliance.org/news/recent-questions-about-ocpp-en-security/.

[37] «openstack,» [Online]. Available: https://www.openstack.org/.

[38] «tshark - manual page,» [Online]. Available: https://www.wireshark.org/docs/man-pages/tshark.html.

[39] «Wireshark,» [Online]. Available: https://www.wireshark.org/.

[40] «Elastic Stack,» [Online]. Available: https://www.elastic.co/elastic-stack/.

[41] «Docker,» [Online]. Available: https://www.docker.com/.

[42] S. Sanfilippo, «Hping3,» 5 August 2022. [Online]. Available: https://www.kali.org/tools/hping3/.

[43] T. Graf, «bmon(1) - Linux man page,» [Online]. Available: https://linux.die.net/man/1/bmon.

Funded by
the European Union

[44] B. Kämpfe, Zimmermann, J., M. Dreisbusch, Grimm, A. L., J. H. Schumann, Naujoks, F., A. Keinath e J. Krems, «Preferences and perceptions of bidirectional charging from a customer's perspective–a literature review and qualitative approach,» in *Electrified Mobility 2019: Including Grid Integration of Electric Mobility*, 2022.

[45] S. Döbelt, B. Kämpfe e J. Krems, «Smart Grid, Smart Charging, Smart Privacy? An Empirical Investigation of Consumers' Willingness to Provide Smart Charging Information,» in *Tagungsband ComForEn 2014*, 2014.

[46] S. Döbelt, M. Günther, B. Kämpfe e J. Krems, «Examining BEV Drivers' Willingness to Share Personal Information in the Context of Smart Charging: Results of a Five-Month BEV Field Trail,» in *8th International Electric Vehicle Conference (EVC 2023)*, 2023.

[47] H. Yang, H. Lee e H. Zo, «User acceptance of smart home services: an extension of the theory of planned behavior,» in *Industrial Management & Data Systems*, 2017, pp. 68-69.

[48] H. T. Haider, O. H. See e W. Elmenreich, «A review of residential demand response of smart grid. Renewable and Sustainable Energy Reviews,» in *Forschung und Entwicklung zu Assistenzsystemen und Big Data – Vorsprung durch Datensparsamkeit. Tagungsband Fachkongress „Social Business" Mittelstand Digital*, 2016.

[49] A. Cavoukian, J. Polonetsky e C. Wolf, «Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation.,» in *Identity in the Information Society*, 2010, pp. 275-294.

[50] O. Raabe, M. Lorenz, F. Pallas, E. Weis e I. Jahr, «Datenschutz im Smart Grid und in der Elektromobilität,» Karlsruher Institut für Technologie, 2011.

[51] S. Döbelt e M. Günther, «Two Values Work Alike: Linking Proenvironmental and Privacy Preserving Behavior.,» in *63th Conference of Experimental Psychologists*, 2021.

[52] Open Charge Alliance, «OPEN CHARGE POINT PROTOCOL 1.6,» 2015. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-16/.

Funded by
the European Union