Open V2X Management Platform Cyber-Resilience and Data Privacy Mechanisms

Conference Paper · July 2024

DOI: 10.1145/3664476.3669917

2 authors, including:

Alexios Lekidis
University of Thessaly
59 PUBLICATIONS **553** CITATIONS

SEE PROFILE

Open V2X Management Platform Cyber-Resilience and Data Privacy Mechanisms

Alexios Lekidis
alekidis@uth.gr
University of Thessaly, Dpt. of Energy Systems
Gaiopolis Campus, 41500
Larissa, Greece

Hugo Morais
hugo.morais@tecnico.ulisboa.pt
INESC-ID, Instituto Superior Técnico—IST
Universidade de Lisboa, 1049-001
Lisboa, Portugal

ABSTRACT

Vehicle-to-Everything (V2X) technologies have been recently introduced to provide enhanced connectivity between the different smart grid segments as well as Electric Vehicles (EVs). The EVs draw power to the grid and may be used as an energy flexibility resource for households and buildings. The increased number of interconnections though, is augmenting substantially the cyber-security and data privacy threats that may occur in the V2X ecosystem. In this paper, such threats are categorized into cyber-attack classes which serve as a basis for deriving Tactics, Techniques, and Procedures (TTPs) for the V2X ecosystem. Additionally, the sensitive data that are exchanged in charging and discharging scenarios are reviewed. Then, an analysis of the existing cyber-security mechanisms is provided and further mechanisms/tools are proposed for detecting/preventing the categorized threats, which are being developed in an Open V2X Management Platform (O-V2X-MP) within the EV4EU project. These mechanisms will provide security-by-design in O-V2X-MP, as well as ensure protection in the V2X interactions.

KEYWORDS

Vehicle-to-Everything, Threat Landscape, Open V2X Platform, Cyber-resilience solutions

ACM Reference Format:
Alexios Lekidis and Hugo Morais. 2024. Open V2X Management Platform Cyber-Resilience and Data Privacy Mechanisms. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30-August 2, 2024, Vienna, Austria.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3664476.3669917

1 INTRODUCTION

Vehicle-to-Everything (V2X) incorporates solutions that are deploying electric vehicle battery storage to power households, buildings, grids, etc. According to the EV placement in the V2X ecosystem, different use cases are feasible based on the utilization of the discharged energy from EV batteries, such as Vehicle-to-Grid (V2G), Vehicle-to-Home (V2H), Vehicle-to-Building (V2B) and finally Vehicle-to-Vehicle (V2V). V2X implies a bidirectional energy transfer from the batteries to the grid (discharge) and from the grid to the batteries (charge).

The increasing electricity demands for power supply are constantly being augmented by the EV charging power [24]. Hence, V2G can be used as a power supply for the grid during periods of high demand [12], and absorb excess power during periods of low demand. Specifically, a V2G solution can be used as a buffer in the grid, reducing the power in peak periods and increasing the power in the valleys. This enables EV owners to reduce their energy bills just by leaving their EVs plugged in when they are not driving them. From the moment when the EV is connected to the power grid, via V2G, the system operator, and mainly the flexibility operators, would have the ability to control the EV battery's charging and discharging process. Moreover, through EV discharging, reliable energy capacity can be offered to energy markets [21].

Nevertheless, the abundance of interfaces and interactions in the V2X ecosystem increases exponentially the threat landscape [19]. To cope with such threats, encryption mechanisms are currently being introduced in the communication between the EV and the charging station. Nevertheless, such mechanisms are not adequate to protect the entire V2X ecosystem [2] and cyber-attacks are still prominent, as in a recent incident causing each EV user to be charged 2000 dollars on average[1]. However, to achieve cyber-resilience in the V2X ecosystem additional cyber-security mechanisms have to be developed to increase the system elasticity in cyber-attacks. In this paper, we provide a detailed overview of the V2X system cyber-threat landscape by organizing it in cyber-attack classes as an initial step towards deriving adversary TTPs for V2X systems. Specifically, the paper includes the following concrete contributions:

- Analysis of the V2X cyber-threat landscape, including the cyber-attack classes as well as data privacy challenges.
- Design and offered services for a newly introduced Open V2X Management Platform (O-V2X-MP) handling the interactions and communication protocols in the V2X ecosystem.
- Review of the existing V2X cyber-security mechanisms, mainly based on the ISO 15118 standard.
- Proposed mechanisms for ensuring security-by-design in the O-V2X-MP, as well as its interactions with further entities in the V2X ecosystem.

The rest of the paper is organized as follows. Section 2 presents an overview of EV communication architectures, V2X interactions, and the O-V2X-MP platform. Then, Section 3 provides an overview of the V2X-oriented cyber-security and data privacy threats. The existing security mechanisms are accordingly presented in Section

[1]https://medium.com/@ekarabatsakis/how-customers-helped-us-survive-a-cyber-attack-5ddd2729c3f3

ARES 2024, July 30-August 2, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07.
https://doi.org/10.1145/3664476.3669917

4 and right after Section 5 describes further mechanisms that can be developed for V2X systems. Finally, Section 6 provides conclusions and some perspectives for future work.

2 V2X ECOSYSTEM

This section provides an overview of the EV communication architecture, the V2X ecosystem as well as the O-V2X-MP that is introduced in the EV4EU project for handling the interactions within the V2X ecosystem.

2.1 EV communication architecture

The main entities that are involved in EV communication architectures are 1) the vehicle, 2) the charging station, and 3) the Charging Station Management System (CSMS). The CSMS is responsible for the remote control, monitoring, and maintenance of the charging stations as well as the resolution of faults or issues in them. Furthermore, it can also obtain remote diagnostics from the charging stations regarding their health status, real-time availability and audit logs. The EV charging architecture entities along with their

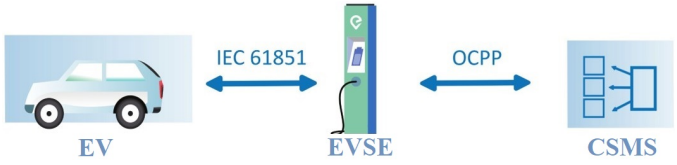

Figure 1: EV charging architecture entities

communication flows and the corresponding standards are illustrated in Figure 1. The figure presents the communication flows and the corresponding standards between 1) EVs, charging stations, and the CSMS system.

As depicted by Figure 1 each entity invokes a different communication channel through the use of standardized interfaces for data exchange. Specifically, the main standards that are currently used in EV charging infrastructures are the IEC 61851 [23] as well as Open Charge Point Protocol (OCPP) [16]. IEC 61851 provides the modes for EV charging and OCPP defines how the Electric Vehicle Supply Equipment (EVSE) and the CSMS exchange messages and commands between them as 1) the initialization of the charging sessions, 2) the termination of the sessions as well as 3) diagnostics as the overall energy consumed during a charging session or the operational status of the charging station. Moreover, it also provides reporting mechanisms and error messages while the station is idle or during a charging session.

2.2 V2X entities and corresponding interactions

The V2X ecosystem consists of different entities that are depicted in Figure 2. Initially, the EV is connected to an Alternate Current (AC) or Direct Current (DC) Charging Station through different standards such as ISO 15118-2/-20, IEC 61851, and CHAdeMO. Charging stations are controlled by the CSMS platform of the Charge Point Operator (CPO), or as often termed V2G Aggregator, using the OCPP communication protocol and its different versions, such as 1.6 for traditional EV charging and OCPP 2.0.1 for V2X scenarios. The CPO is responsible for ensuring that the EV charging network is operational, available, and stable. Furthermore, eMobility Service Providers (eMSPs) offer charging services to EV drivers by providing access to multiple charging points around a geographic area. Additionally, eMSPs offer Customer Relationship Management (CRM)/Enterprise Resource Planning (ERP) integration - Customer and invoicing integrations. Furthermore, eMSPs may use either the Open Charge Point Interface (OCPI)[2] or the Open Intercharge Protocol (OICP)[3] protocol to connect to CPO networks through the Roaming Platform (Clearing House). Finally, the House/Building Energy Management System (EMS) receives data from the CPOs and the eMSPs through the Open Automated Demand Response (OpenADR) [8] and the IEEE 2030.5 [6] protocols as well as can communicate with further EMS from other households.

2.3 Open V2X Management Platform

Within the EV4EU project a new backend EV charging platform, called Open V2X Management Platform (O-V2X-MP) is being developed to facilitate the implementation of the V2X scenarios as well as to integrate technical, social, and environmental aspects of the V2X ecosystem. The platform implements a CSMS system and offers both OCPP 1.6 and 2.0.1 versions for bidirectional charging[4]. Similar CSMS platforms are being implemented as the Mobility House project[5], nevertheless, the main differentiator of O-V2X-MP is its service-based architecture and the ability to be highly modular and extensible. Specifically, the O-V2X-MP service-based architecture is illustrated in Figure 3 and the offered services include:

(1) *CPO services* related to the charging station management, including diagnostics and operations to ensure their real-time availability.
(2) *eMSP services*, related to the provision of access to charging points as well as CRM, ERP, and invoicing integration for a specific area.
(3) *User Management services* related to the different user groups that are present in the platform, such as platform manager, CPO manager, Billing manager, eMSP manager as well as 1st and 2nd line support engineers.
(4) *API services* related to the Application Programming Interfaces (APIs) that the platform has, such as location API where charging stations may be retrieved, Charge Detail Record (CDR) API, based on which complete session details can be exported, the tariff API from which the Wholesale EV charging session costs are calculated and finally the CRM API which is used from the EV user enters his/her customer details and viewing the charging history.
(5) *Secure WebSocket layer* for the communication with the EV chargers using OCPP, which ensures the protection against cyber-attacks using Transport Layer Security (TLS) WebSocket connection [20] or a Virtual Private Network (VPN) IPsec tunnel [20].
(6) *Roaming services*, which offer transaction possibilities with Roaming partners throughout Europe, so that EV drivers can charge in the network of partners, but also the drivers

[2] https://evroaming.org/app/uploads/2020/06/OCPI-2.2-d2.pdf
[3] https://assets.website-files.com/602cf2b08109ccbc93d7f9ed/60534f2e20d0f87be17ba21b_oicp-cpo-2.2.pdf
[4] https://github.com/EV4EU/ov2xmp
[5] https://github.com/mobilityhouse/ocpp

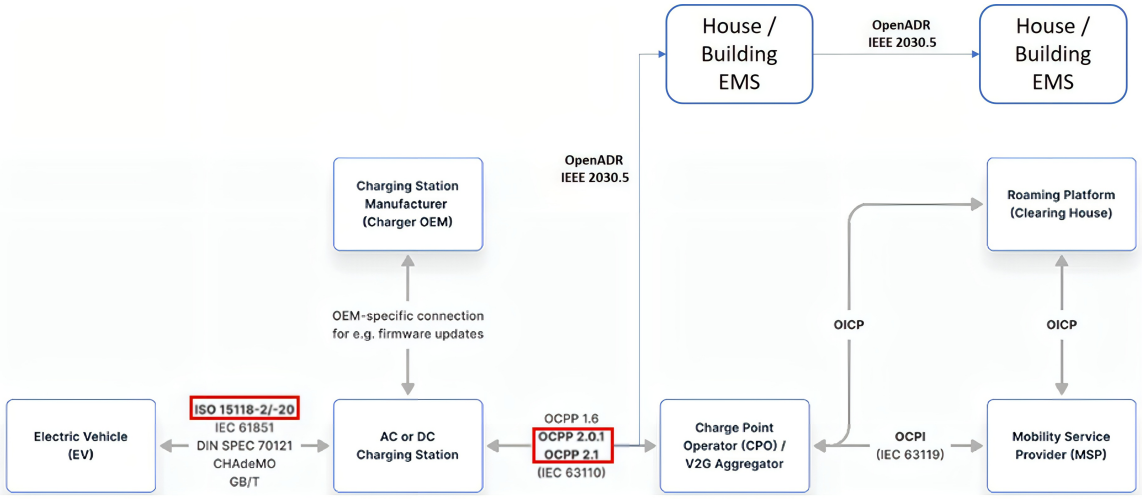

Figure 2: EV charging architecture entities

of other eMSPs to charge into the charging network. The integration with these services is based on the OICP or OCPI protocol, which allows the connection with roaming hubs as Hubject[6] and GIREVE[7] respectively.

3 V2X CYBER-SECURITY AND DATA PRIVACY THREATS

V2X cyber-security threats include disruption of the EV charging process, leading to potential harm to the electricity grid and connected vehicles. Additionally, data privacy threats relate to stealing personal information, such as bank (i.e., credit/debit) cards for payment as well as username and e-mail address.

The V2X cyber-security threats are based on the Confidentiality, Integrity, and Availability (CIA) triad. Confidentiality ensures that data is only readable by intended recipients (according to Figure 2 interactions), protecting it from unauthorized third parties. Integrity ensures that any modification can only be done by authorized entities in the V2X ecosystem. Availability ensures that the V2X charging and discharging services offered are available to the user within an expected time frame. Cyber-security events can target any or all of these areas, leading to different impact categories. The impact categories of V2X cyber-security incidents can be cyber-physical, data-driven, and reputational [10]. Cyber-physical impacts could include compromising EVs and putting the EV driver's life in danger. Data-driven impacts often aim to collect private data such as encryption private keys, bank cards, EV user credentials, and preferences. Reputational impacts aim to decrease the amount of trust among a company's actual or potential customers. Every impact category is considered by adversaries before executing TTPs to conduct cyber-attacks in V2X systems.

Given the potential threats and impacts, all entities in the V2X ecosystem must implement robust security measures to ensure business continuity in the e-mobility service. This also includes the presence of a continuous risk assessment process within the O-V2X-MP platform, which also considers EV user privacy. For instance, sharing users' or billing data could diminish the adoption of EV and V2X systems. Hence, techniques should be in place to ensure user anonymity and protect user data.

In the following section, an overview of the cyber-attack classes that are relevant to the V2X ecosystem is presented. Then, the focus is given to the data privacy threats, which arise in the exchange of information between the EV, the charging stations, and the CSMS platform as well as the interactions with external entities.

3.1 Cyber-attack classes

The identified attack classes along with the required mitigation actions to be implemented as counter-measures against them are illustrated in Table 1.

Denial of Service (DoS) attacks on the V2X scenarios aim at disrupting or disabling communication, potentially causing service disruptions or affecting the stability of the grid. A DoS attack on V2X aims at overwhelming the V2X communication channels with a flood of requests, exploiting vulnerabilities in the V2X implementation to crash or freeze systems, or intentionally manipulating data to cause errors or misbehavior in the V2X interactions. These attacks can disrupt the proper functioning of V2X services, hinder grid management, and impact the availability of EV charging or discharging capabilities. Distributed DoS (DDoS) attacks on V2X concern malicious attempts to disrupt the normal functioning of the charging station by overwhelming it with a flood of illegitimate requests or traffic. The objective of a DDoS attack is to exhaust the charging station processing power and memory, rendering it inaccessible to EV users.

Frame injection in V2X refers to a type of attack where an adversary injects or modifies V2X messages with malicious intent. Injection attacks may have various objectives, including:

(1) *Data manipulation*: An adversary may modify the V2X message content to manipulate the data exchanged between the EV and the grid. For example, charging or discharging

[6]https://www.hubject.com/
[7]https://www.gireve.com/

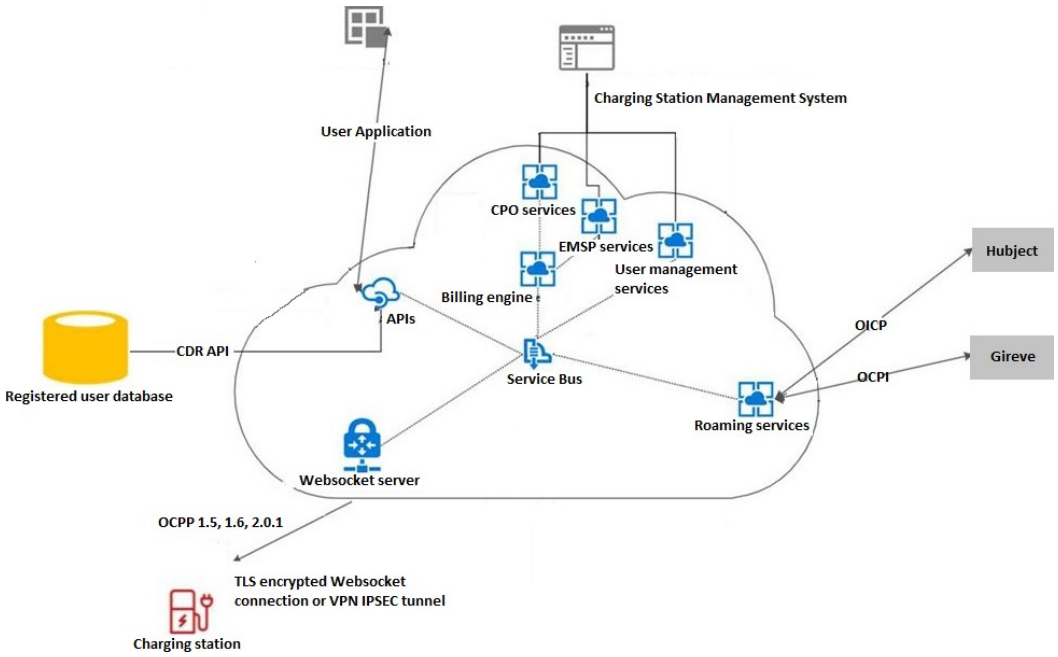

Figure 3: Service-based architecture of the O-V2X-MP platform

Attack class	Description	Applicable mitigation actions
Denial of Service (DoS)	Network flooding with empty OCPP packets	Authentication, encryption, access controls, and anomaly detection
Frame injection	Inject false messages in EV charging and discharging scenarios	Authentication and authorization, encryption, Intrusion detection and monitoring
Replay attack	Intercepting/replaying communication between an EV and a charging station to manipulate the charging/discharging process	Message Authentication, Secure Key Exchange, Accurate timestamping, Session unique sequence numbers
Impersonation	Stealing energy from either EV or charging station directions	Robust authentication mechanisms (e.g., secure credentials ' certificates, or cryptographic keys to verify the identity of the EV)
Sybil attack	Copy ID tokens to multiply energy charge for free	Anomaly detection, Authorization through a PKI

Table 1: V2X attack classes

instructions, energy meter readings, or authentication credentials can be altered, leading to unauthorized access, inaccurate billing, or even disruptions in the electricity grid management.

(2) *Service disruption*: By injecting specially crafted frames, an adversary can attempt to disrupt the V2X communication between the EV and the electricity grid. This disruption can cause service interruptions, delays, or malfunctions in charging or the electricity grid stabilization processes.

(3) *Spoofing or impersonation*: Frame injection can be used to impersonate legitimate entities in the V2X ecosystem. By injecting forged frames with spoofed identities or credentials, an adversary could attempt to gain unauthorized access, deceive the system, or manipulate data for malicious purposes.

In V2X Replay attacks, an adversary intercepts and replays communication between an EV and a charging station, to manipulate or disrupt the charging process or gaining unauthorized access to the V2X system. In a normal V2X scenario, the EV and the charging station communicate with each other to negotiate the charging parameters, such as the charging rate and duration, authentication credentials, and other control signals. A replay attack occurs when an adversary captures these communication packets and later replays them, potentially tricking the charging station into performing unauthorized actions.

A V2X impersonation attack can occur when an adversary attempts to masquerade as a legitimate entity (such as an EV, a charging station, or a CSMS) to gain unauthorized access, manipulate data, or disrupt the V2X system. The main impersonation attacks are as follows:

- *EV Impersonation*: an adversary could impersonate a legitimate EV by generating false EV identification information. Hence, the adversary may gain unauthorized access to the charging station or manipulate charging parameters, such as charging rates or durations. This could lead to unauthorized charging or even damage to the charging infrastructure.
- *Charging Station Impersonation*: an adversary could impersonate a valid charging station to gain control over EVs or deceive them into performing unauthorized actions. This

could involve manipulating charging rates, stealing sensitive information from EVs, or causing electricity grid disruptions.
- *CSMS Impersonation*: impersonation of a legitimate CSMS by sending forged or spoofed messages or commands to the charging stations or EVs. This may lead to unauthorized control over the charging process, manipulation of charging parameters, or even the injection of malicious firmware into the charging station.

Sybil attack in V2X refers to a type of cyber-security attack where an adversary creates multiple fake identities or virtual entities to gain an unfair advantage or disrupt the V2X system.

3.2 Data privacy and GDPR

Data privacy in the context of V2X refers to protecting the confidentiality and appropriate handling of sensitive information generated and exchanged during V2X communications. V2X involves the transmission of data related to energy consumption, charging schedules, user preferences, and potentially personal or vehicle identification information.

EV user privacy protection is an important requirement for V2X communications. Privacy protection technologies aim to prevent attacks or confuse adversaries who attempt to track vehicles by intercepting communications or tracing V2X interactions. A range of privacy protection strategies have already been developed and partially standardized. It is important to ensure that these privacy-preserving approaches do not impede safety functions.

The sensitive data that need to be protected in the V2X ecosystem mainly include EV user information such as 1) username, 2) user e-mail address, 3) bank card number, 4) Radio-Frequency Identification (RFID) card number as well as 5) mobile phone number. Protection is enforced by General Data Protection Regulation (GDPR) legislation. The RFID tag shall be anonymized and given a random ID to comply with GDPR. The actual ID tag can be only accessible by authorized personnel that have administrative or eMSP roles in the CSMS platform [9]. An example of ID Tag information from the O-V2X-MP platform is illustrated in Figure 4. The tag is anonymized and given a random ID to comply with GDPR. The actual ID tag can be only accessible by authorized personnel who have administrative or eMSP roles in the CSMS.

Additionally, OCPP 2.0.1 has recently added functionality to enable charging stations and CSMS systems to comply with the GDPR regulations[8]. This functionality allows storing, requesting, and removing personal data from charging stations. To enable GDPR compatibility, OCA suggests that TLS is used (profiles 2 and 3 from the chapter Security in OCPP 2.0.1). Nevertheless, the data exchange functionality is vendor-specific, so it cannot be considered in OCA's standards. Hence, it is up to vendors of Charging Stations and CSMSs to make sure that their specific functionality complies with the GDPR. Moreover, due to the lack of production-ready OCPP 2.0.1 implementations for both charging stations and CSMS systems, such mechanisms are still being investigated and will be accordingly developed. Hence, to address data privacy and GDPR concerns in V2X, the following measures should be prioritized in the implementation:

[8]https://www.openchargealliance.org/protocols/ocpp-201/

- *Data anonymization*: personal and sensitive information can be anonymized or pseudonymized to remove or obscure direct identifiers. This helps protect the privacy of individuals by reducing the risk of re-identification, as well as ensures compliance with GDPR legislations.
- *Secure data transmission*: encrypting V2X communications using secure protocols (e.g., TLS) helps protect data from unauthorized interception or tampering while in transit.
- *Secure storage and access controls*: applying appropriate security measures to store V2X data, such as encryption at rest, access controls, and robust authentication mechanisms, helps protect data from unauthorized access or breaches.
- *Privacy by design*: incorporating privacy considerations into the design and development of V2X systems, such as privacy impact assessments, privacy-enhancing technologies, and privacy-conscious default settings, to ensure that privacy is embedded into the architecture and operations of the system.

4 EXISTING V2X CYBER-SECURITY MECHANISMS

In comparison to the traditional EV charging scenario, communication between the EV and the EVSE in V2X ecosystems follows the ISO 15118 standard [13]. ISO 15118 incorporates various security measures to ensure the integrity, confidentiality, and authenticity of the exchanged information. Key security aspects addressed by ISO 15118 are:

- *Authentication and Authorization*: defines authentication mechanisms to verify the identities of the charging station and the vehicle. This includes the use of digital certificates and Public Key Infrastructure (PKI) to establish trust between the entities involved in the communication. Mutual authentication ensures that both the charging station and the vehicle can verify each other's identities before establishing a secure communication channel.
- *Secure Communication for Data Exchange Protection*: includes the support of the Transport Layer Security (TLS) protocol to secure the communication between the charging station and the vehicle. TLS ensures that the data transmitted between the entities is encrypted, preventing unauthorized access or eavesdropping. Additionally, encryption algorithms are employed to protect the integrity of messages and prevent tampering or data manipulation during data exchange.
- *Secure Key Exchange*: specifies secure key exchange mechanisms, such as the Diffie-Hellman key exchange [14], to establish a shared secret key between the charging station and the vehicle. This enables encrypted communication and protects against unauthorized access.
- *Protection against Replay Attacks*: measures to prevent replay attacks (see Table 1 for more details) by incorporating timestamping and message sequencing. Timestamps allow the validation of message freshness, while sequencing ensures that messages are processed in the correct order and duplicates are detected.

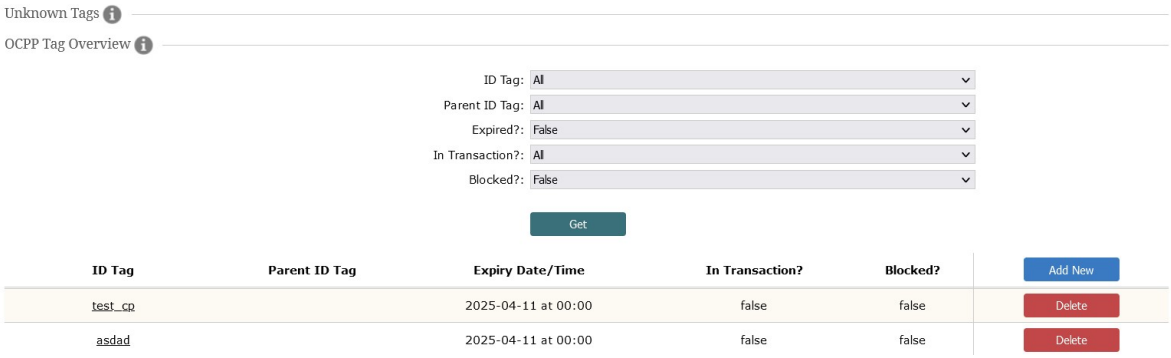

Figure 4: OCPP ID Tag information from the O-V2X-MP platform

- *Data Privacy*: guidelines for the personal data protection of and ensuring compliance with relevant regulations. It specifies how sensitive information, such as user credentials or vehicle identification data, should be handled and protected.

Figure 5 includes steps and entities involved in the charging or discharging process. Specifically, the entities that are involved are the EV, the EV manufacturer, the charging station, the CPO, the eMSP as well as the root PKI Certificate Authority (PKI CA). The EV manufacturer has a backend that manages security certificates authenticated by a PKI (either their own or a third-party provider). The EV needs to have a provisioning certificate, marked as "PROV" in Figure 5, installed in the EV which is signed by its own or a third-party PKI (Step 1). Then, the EV must have an ISO 15118-compliant V2X root certificate installed in the vehicle's communication controller (Step 2). The charging station that is connected to a CPO platform, needs to have a digital certificate, marked as "LEAF" in Figure 5, signed by a third-party V2X root CA PKI to authenticate itself during the charging session (Step 3).

As with the EV, the charging station also needs to have the V2X root certificate installed in its communication controller (Step 4). The EV user can sign up for charging services with the eMSP. The EV owner shares payment details (e.g., credit card, debit card, bank account) with the eMSP so that costs from a charging session can be processed. The eMSP stores this information and generates a digital contract certificate, marked as "CONT" in Figure 5, that needs to be signed by the V2X root PKI to authenticate the identity of the EV owner during a charging session. This contract certificate can be installed in the EV directly or via the charging station (Step 5) it is being installed directly in the EV. Given that all these steps are performed, and all the digital certificates are in place, the ISO 15118 authorization is correctly performed, and the charging session can be initiated. Apart from existing mechanisms though, the next section proposes further V2X mechanisms to ensure cyber-resilience.

5 PROPOSED O-V2X-MP CYBER-RESILIENCE MECHANISMS

Four categories of mechanisms were considered applicable and most prominent for cyber-attack detection and prevention in the O-V2X-MP platform and its interactions in the V2X ecosystem. Additional categories, such as the Trusted Execution Environments [22], were also marked as applicable, but their protection scheme was considered complementary to the four identified categories. The four categories are:

(1) Authentication/authorization methods (Section 5.1).
(2) Access control mechanisms (Section 5.2).
(3) Data privacy, integrity, non-repudiation using encryption mechanisms as well as loss prevention (Section 5.3).
(4) Network security mechanisms such as behavioral analytics and Intrusion Detection Systems (IDS) (Section 5.4).

5.1 Authentication and authorization methods

Initially, authorization is performed using OAuth 2.0 [7]. OAuth 2.0 is an open standard protocol that allows to grant limited access to controlled resources. It provides a framework for secure access to APIs by enabling the use of access tokens. Specifically, it separates the roles of the resource owner (user), the client application (third-party application), and the resource server (API provider), and uses authorization codes, access tokens, and refresh tokens for secure communication and token management.

The identity management system that is prominent for the interactions between O-V2X-MP and further V2X ecosystem entities is based on Keycloak [4]. Keycloak is an open-source identity and access management solution that provides features for authentication, Single Sign-On (SSO), and authorization. It is based on industry standards such as OAuth 2.0 and OpenID Connect (OIDC), making it suitable for securing web and mobile applications. Moreover, it offers user management, role-based access control, social logins, multifactor authentication, and integration with external identity providers. It can be used as a standalone server or embedded into existing applications, providing centralized authentication and authorization services.

5.2 Access control mechanisms

Access for different user groups in the O-V2X-MP is based on the Lightweight Directory Access Protocol (LDAP) mechanism [17]. Specifically, OpenLDAP [3] is an open-source implementation of LDAP and is widely used for accessing and managing directory information. Furthermore, OpenLDAP provides a server that stores and organizes directory data, allowing one to search, add, modify, and delete directory entries. Moreover, it is designed to be scalable

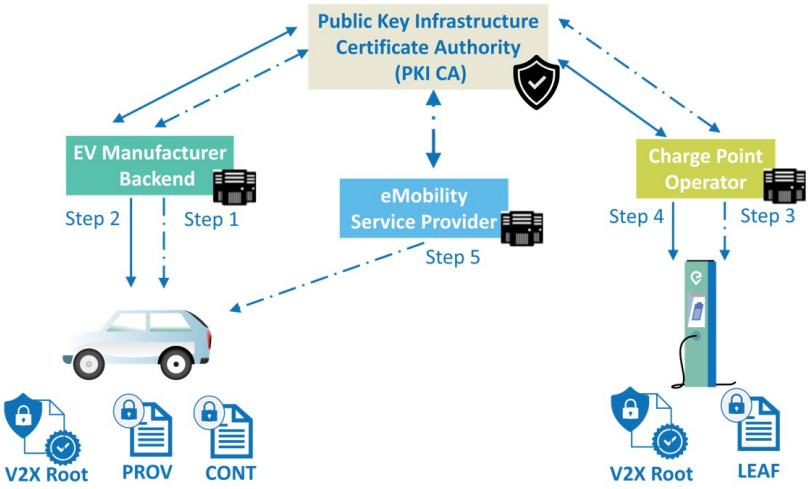

Figure 5: ISO 15118 certificate exchange through a PKI

and reliable, making it suitable for managing large-scale directory services. It supports various authentication mechanisms, including simple password-based authentication and more secure methods, such as the Simple Authentication and Security Layer. Encryption and secure communication through TLS is also supported.

Finally, access control policies are being implemented to allow only specific groups to have access to file servers from where diagnostic logs of the stations can be downloaded.

5.3 Data encryption

To ensure a higher level of end-to-end security, additional mechanisms are considered, such as encryption on the exchanged V2X packets through TLS or IPsec [5] protocols or enabling firewall rules, for instance, to discard V2X packets from blacklisted IPs.

Encryption mechanisms are used to protect the data exchanged between the EV and the charging stations through the ISO 15118 protocol, as depicted in Section 4. However, the OCPP 2.0.1 protocol also requires the implementation of security mechanisms to protect the communication between CSMS and the charging stations [1]. Within EV4EU, we will also investigate the implementation of these mechanisms to protect the sensitive data that are exchanged between the EV, the charging station the CSMS as well as further entities of the V2X ecosystem, such as the EMS and the users.

5.4 Network security mechanisms

Multiple network security mechanisms exist in the cyber-security domain. Those that are applicable for the V2X charging and discharging scenarios as well as coping with the threats mentioned in Section 3 are, to the best of our knowledge, based on IDS systems since V2X are cyber-physical systems. Moreover, the abundance of interactions/protocols in Section 2 necessitates the use of a NIDS.

In detail, V2X incidents aim at compromising the CIA triad of EV charging and discharging scenarios or any attempts to bypass existing security mechanisms [15]. Monitoring processes can be used by IDS to identify eventual incidents. When linked to monitoring the network, a Network-based IDS (NIDS) is used, whereas when linked to the individual applications a Host-based (HIDS).

Upon detection, a response is generated, which can be categorized as a passive or active response [15]. An IDS responding passively will solely report the offense, and the next actions shall be taken by the incident response team. Instead, an active response will try to mitigate the incident through Intrusion Prevention Systems (IPS). Mitigation includes collecting additional information about the attacks, deterring the intruder by terminating the connection, and reconfiguring network and security devices (e.g., router and firewall) to block further packets originating from the malicious source IP address.

The implementation of the V2X NIDS is mainly based on the Zeek [11] open-source software enhanced with the support of V2X protocols as well as detection algorithms. Specifically, Zeek passively monitors network traffic by capturing packets, network flows, and communication patterns as well as analyzes the data in real-time. It also provides detailed logs and metadata about various network events, such as network connections, protocols, traffic volumes, and content analysis. Additionally, the detection algorithms are based on custom scripts that extract specific information from V2X protocols, such as OCPP 1.6 and OCPP 2.0.1 or define customized detection rules to protect the interactions at the network level. This allows the detection of unknown (i.e., zero-day) threats by performing knowledge- and behavior-based intrusion detection.

Moreover, Zeek supports the integration with a security analytics dashboard based on Kibana [18]. The integration allows gathering O-V2X-MP logs in Elasticsearch, as depicted in Figure 6. Additionally, through a dedicated interface, such integration stores any detected events/alerts, which will be afterward transmitted to a Security Information and Event Management (SIEM) system [11]. Accordingly, the SIEM will trigger the necessary actions for restoring the V2X system to its normal operation.

6 CONCLUSION

This paper provides an overview of the V2X cyber threats, as well as the cyber-security and data privacy mechanisms that shall be employed to ensure cyber-resilience in the V2X ecosystem. Initially,

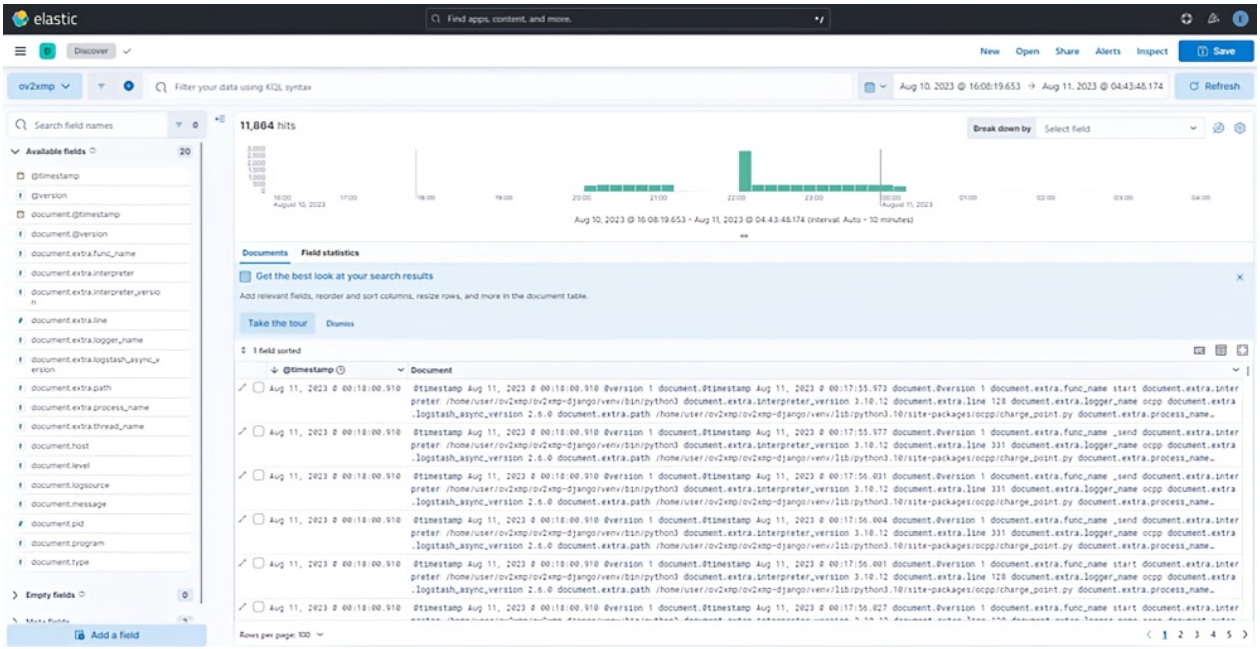

Figure 6: O-V2X-MP log integration in Elasticsearch

the attack classes are identified which is the initial step towards deriving the V2X adversary TTPs and then an overview of the existing security mechanisms for V2X systems follows. Then, four further categories of mechanisms to provide cyber-resilience are proposed including i) authentication and authorization methods for ensuring trust in the V2X scenarios, ii) access control mechanisms for user protection, iii) data encryption mechanisms for the protection of sensitive data exchanged in the charging and discharging scenarios and finally iv) network security mechanisms for the detection of anomalies in the V2X communications.

In terms of next steps, the proposed mechanisms are developed/integrated into the O-V2X-MP within EV4EU. The mechanisms will be validated against a real attack set based on the presented attack classes, detection accuracy metrics, and mitigation/threat eradication actions following the conducted attacks.

ACKNOWLEDGMENTS

This work has been funded by the European Union's Horizon Research and Innovation Programme under grant agreement no. 101056765 (EV4EU). H.M was supported by Portuguese national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020.

REFERENCES

[1] Alcaraz, Cristina et. al. 2023. OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security* (2023), 1–27.
[2] Kaibin Bao, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. 2018. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science-Research and Development* 33, 1-2 (2018), 3–12.
[3] Matt Butcher. 2007. *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services.* Packt Publishing Ltd.
[4] Chatterjee, Ayan et. al. 2022. Applying spring security framework with keycloak-based oauth2 to protect microservice architecture apis: A case study. *Sensors* (2022).
[5] Naganand Doraswamy and Dan Harkins. 2003. *IPSec: the new security standard for the Internet, intranets, and virtual private networks.* Prentice Hall Professional.
[6] Ghalib, Marwan et. al. 2018. Implementation of a smart grid communication system compliant with IEEE 2030.5. In *2018 IEEE ICC Workshops*. IEEE.
[7] Dick Hardt. 2012. *The OAuth 2.0 authorization framework.* Technical Report.
[8] Herberg, Ulrich et. al. 2014. OpenADR 2.0 deployment architectures: Options and implications. In *2014 IEEE SmartGridComm*. IEEE, 782–787.
[9] Kamal, Naheel Faisal et. al. 2023. Light-weight Communication Fault Tolerant OCPP-based EV Supply Equipment. In *2023 IEEE CPE-POWERENG*. IEEE, 1–6.
[10] Metere, Roberto et. al. 2021. Securing the electric vehicle charging infrastructure. *arXiv preprint arXiv:2105.02905* (2021).
[11] Muhammad, Adabi Raihan et. al. 2023. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science* 217 (2023), 1406–1415.
[12] Mullan, Jonathan et. al. 2012. The technical, economic and commercial viability of the vehicle-to-grid concept. *Energy Policy* 48 (2012), 394–406.
[13] Marc Mültin. 2018. ISO 15118 as the Enabler of Vehicle-to-Grid Applications. In *International conf. of electrical and electronic technologies for automotive*. IEEE.
[14] Eric Rescorla. 1999. *Diffie-hellman key agreement method.* Technical Report.
[15] Scarfone, Karen et. al. 2007. Guide to intrusion detection and prevention systems (idps). *NIST special publication* 800 (2007), 94.
[16] Schmutzler, Jens et. al. 2013. Evaluation of OCPP and IEC 61850 for smart charging electric vehicles. *World Electric Vehicle Journal* 6, 4 (2013), 863–874.
[17] J Sermersheim. 2006. Rfc 4511: Lightweight directory access protocol (ldap): The protocol.
[18] Shah, Neel et. al. 2022. A framework for social media data analytics using Elasticsearch and Kibana. *Wireless networks* (2022), 1–9.
[19] Skarga-Bandurova et. al. 2022. Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations. In *2022 IEEE Big Data*. IEEE.
[20] Jon C Snader. 2015. *VPNs Illustrated: Tunnels, VPNs, and IPsec: Tunnels, VPNs, and IPsec.* Addison-Wesley Professional.
[21] Darlene M Steward. 2017. *Critical elements of vehicle-to-grid (v2g) economics.* Technical Report. National Renewable Energy Lab.(NREL), Golden, CO.
[22] Valero, José María Jorquera et. al. 2022. Trusted Execution Environment-enabled platform for 5G security and privacy enhancement. *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions* (2022).
[23] Peter Van Den Bossche. 2010. IEC 61851-1: Electric vehicle conductive charging system-Part 1: General requirements. In *2*. Iec, 1–99.
[24] Vopava, Julia et. al. 2019. Investigating the impact of E-mobility on the electrical power grid using a simplified grid modelling approach. *Energies* 13, 1 (2019), 39.