Funded by
the European Union

Horizon Europe

EUROPEAN COMMISSION

European Climate, Infrastructure and Environment Executive Agency (CINEA)

Grant agreement no. 101056765

Electric Vehicles Management for carbon neutrality in Europe

Deliverable D5.4
Cyber-security and Privacy analysis for V2X services

Document Details

Due date	31-05-2023
Actual delivery date	06-06-2023
Lead Contractor	Public Power Corporation (PPC)
Version	1.0
Prepared by	Alexios Lekidis (PPC), Christos Dalamagkas (PPC)
Reviewed by	António Grilo (INESC ID), Jesper Hyldig (BEOF)
Dissemination Level	Public

Project Contractual Details

Project Title	Electric Vehicles Management for carbon neutrality in Europe
Project Acronym	EV4EU
Grant Agreement No.	101056765
Project Start Date	01-06-2022
Project End Date	30-11-2025
Duration	42 months

Document History

Version	Date	Contributor(s)	Description
0.1	16/04/2023	PPC	Table of contents
0.2	23/05/2023	PPC	First version
0.3	30/05/2023	INESC ID, BEOF	Deliverable internal review
1.0	01/06/2023	PPC	Revised version based on review comments with additional improvements on the sections and in the images

Disclaimer

Acknowledgment

This document is a deliverable of EV4EU project. EV4EU has received funding from the European Union´s Horizon Europe programme under grant agreement no. 101056765.

Funded by
the European Union

[1] https://ev4eu.eu/

Executive Summary

The *Cyber-security and Privacy analysis for V2X services (Deliverable D5.4)* provides an overview of the cyber-security mechanisms that will be employed within the EV4EU project to ensure the cyber-resilience of the Open V2X Management Platform (O-V2X-MP) as well as the offered services. Initially, it presents background details as the high-level design of the O-V2X-MP platform as well as existing cyber-security mechanisms that are provisioned in existing Vehicle to Everything (V2X) standards for charging and discharging scenarios. Then, the cyber-security and data privacy threats that may occur in the V2X ecosystem are presented in terms of cyber-attack classes as well as sensitive data that are exchanged in charging and discharging scenarios in terms of General Data Protection Regulation (GDPR).

The V2X cyber threats are tackled using cyber-resilience mechanisms for the O-V2X-MP platform and its interactions with the external entities in the V2X ecosystem that are accordingly presented. The mechanisms that are chosen in the scope of the EV4EU project are based on *i)* authentication and authorization methods for ensuring trust in the V2X scenarios involving also the O-V2X-MP platform, *ii)* access control mechanisms for user protection in the O-V2X-MP, *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.

This deliverable also presents how the O-V2X-MP platform and the associated cyber-resilience mechanisms are currently used and integrated in a testbed that is available within the EV4EU project and will be also used in the first phases of the execution for the Greek pilot (including pilot planning). The testbed will be made available for all the pilots of the EV4EU project and it includes additional mechanisms for the protection against cyber-attacks in an Information Technology (IT) as well as an industrial infrastructure. These mechanisms are also applicable to the V2X ecosystem, including a firewall solution, security log collection and aggregation mechanisms, such as the Security Information and Event Management (SIEM) as well as Software Define Network (SDN) switches for controlling the network traffic and flows of the testbed and protecting the O-V2X-MP against cyber-attacks by blocking or isolating potential infected or malicious devices/systems.

The cyber-security mechanisms that are described in this deliverable will be used as a main reference point for the development of the O-V2X-MP platform, that will be reported on February 2024 as a part of deliverable D5.5 “Open V2X Management Platform”. Finally, the deliverable D5.4 has been prepared and edited by the leader of Work Package (WP) 5 – PPC.

Table of Contents

List of Figures

List of Tables

Acronyms

API	Application Programming Interface
BUC	Business Use Cases
CA	Certificate Authority
CDR	Charge Detail Record
CIA	Confidentiality, Integrity, and Availability
CPO	Charge Point Operator
CSMS	Charging Station Management System
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DoS	Denial of Service
DSO	Distribution System Operator
eMSP	emobility Managed Service Provider
EPES	Electrical Power and Energy Systems
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HIDS	Host-based IDS
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IOC	Indicators of Compromise
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MISP	The Open Source Threat Intelligence Sharing Platform
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
OCPP	Open Charge Point Protocol
OIDC	OpenID Connect
ORM	Object-Relational Mapper
O-V2X-MP	Open V2X Management Platform
PCAP	Packet Capture
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
ReDiS	Remote Dictionary Server
REST	REpresentational State Transfer
RFID	Radio-Frequency Identification
SASL	Simple Authentication and Security Layer
SCADA	Supervisory Control And Data Acquisition
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCP	Transmission Control Protocol
TLS	Transport Layer Security

URL	Uniform Resource Locator
V2G	Vehicle-to-Grid
V2X	Vehicle-to-Everything
VE	Virtual Environment
VPN	Virtual Private Network
VPP	Virtual Power Plants
VSFTPD	Very Secure FTP Daemon
WP	Work Package

1 Introduction

1.1 Scope and Objectives

This deliverable provides an overview for the design of security mechanisms to allow secure access to the O-V2X-MP platform that is described in D5.3 “High-Level Design of O-V2X-MP” [1]. The considered security mechanisms are as follows:

- Secure access to the platform with respect to Authentication and Authorization
- Trustful data exchange among platform components
- Data encryption
- Secure communication with V2X stations, Electric Vehicles (EVs) and systems operated by other players (System operators, Virtual Power Plants - VPPs, Markets, etc.), from the technology and functional standpoint

The final objective of the deliverable is to evaluate system resilience to cyber-attacks through the EV4EU project use-cases.

1.2 Structure

The current document is divided into six sections. Section 1 introduces and describes the D5.4. Section 2 provides a background on the high-level design of the O-V2X-MP platform as well as the provisioned security mechanisms that are already standardized for V2X communications. Then, Section 3 describes the threat landscape for V2X, including the relevant cyber-attack classes and the data privacy implications. Accordingly, Section 4 presents the security mechanisms that will be implemented within the O-V2X-MP platform to ensure its protection and the cyber-resilience of the EV4EU project entities it interacts with. Section 5 describes the integration of the O-V2X-MP platform and the relevant cyber-resilience mechanisms in the testbed where the O-V2X-MP is currently deployed. Finally, Section 6 presents overall conclusions and considerations about this deliverable.

1.3 Relationship with other deliverables

Deliverable D5.4 describes the security mechanisms that will be used to protect against cyber-security and data privacy threats in the O-V2X-MP. Since security aspects constitute a layer in the O-V2X-MP, this deliverable receives input from D5.3 “High-Level Design of O-V2X-MP” [1]. The considered security mechanisms that will be developed in the O-V2X-MP platform will be reported in D5.5 “Open V2X Management Platform” in terms of testing their performance and accuracy for the detection of cyber-threats. Such tests will be performed in relation to the Business Use Cases (BUCs) of the project that are defined in deliverable D1.5 “V2X Use-cases repository” [2].

2 Background

This section provides background on the high-level design of the O-V2X-MP platform that will be employed for the management of charging stations within the EV4EU project as well as the existing cyber-security mechanisms that are included in the design of the standards and protocols for V2X charging and discharging scenarios.

2.1 O-V2X-MP platform overview

The O-V2X-MP is used for implementing the Vehicle-to-Everything (V2X) scenarios within the project. The high-level design of the O-V2X-MP that is presented in deliverable D5.3 [1] is illustrated in Figure 1. This design also includes a security layer, which protects the platform as well as the EV users against both cyber and physical threats and attacks using cyber-security and data privacy mechanisms. The security layer uses all the applicable security mechanisms in the V2X ecosystem. These mechanisms relate to 1) the communication between the EV and the charging station as well as 2) the communication between the charging station and the O-V2X-MP for remote control, diagnostics and maintenance purposes.

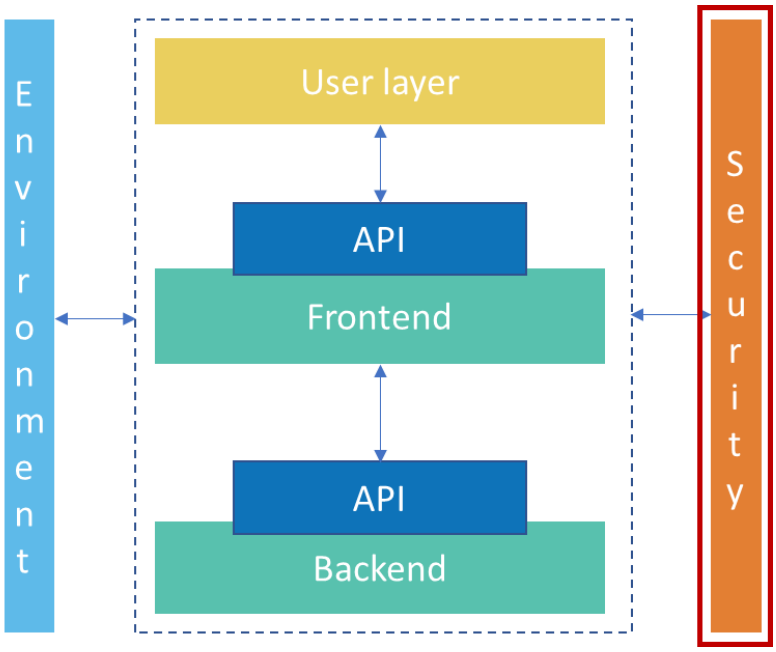

Figure 1 – Security layer in the O-V2X-MP platform design

The current implementation of the O-V2X-MP follows the Open Charge Point Protocol (OCPP) 1.6 for traditional charging scenarios as well as OCPP 2.0 [3] standards for V2X-based charging and discharging scenarios and the supported interactions in the V2X ecosystem. The O-V2X-MP development is based on the Django framework [4]. The reasons for choosing the Django framework are presented below:

1) It is based on the Python programming language, allowing to integrate a variety of libraries and additional functionalities. An example using Python concerns the development of custom decision-making logic and directly incorporate it into the O-V2X-MP backend.

2) It allows the development of scalable web applications, while it already implements essential functionalities and additionally it contains integration with cyber-security mechanisms, which are listed in Section 4 (for example, session management and user authentication).

3) It is a mature, open-source project, and is being continuously updated and maintained by an active community.
4) The "ocpp" Python library from mobilityhouse [5] supports the OCPP 2.0.1 protocol, which is an essential feature for implementing the Vehicle-to-Grid (V2G) functionalities of O-V2X-MP.
5) Continuous development, integration and testing features for the O-V2X-MP are ensured using Django.

Furthermore, the O-V2X-MP implementation is containerized using Docker [6]. By containerizing the platform, each individual component becomes isolated and encapsulated within its own container, ensuring consistency and reproducibility across different environments. Docker containers provide a lightweight and portable way to package and distribute applications, making it easier to deploy and manage complex software systems.

2.2 Existing V2X cyber-security mechanisms

The communication between the EV and the Electric Vehicle Supply Equipment (EVSE) is following the ISO 15118 standard [7]. In terms of security, ISO 15118 incorporates various measures to ensure the integrity, confidentiality, and authenticity of the exchanged information (Figure 2). 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 [8], 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 in Section 3.1 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.
- *Data Privacy*: guidelines for the protection of personal data and ensuring compliance with data protection regulations. It specifies how sensitive information, such as user credentials or vehicle identification data, should be handled and protected.

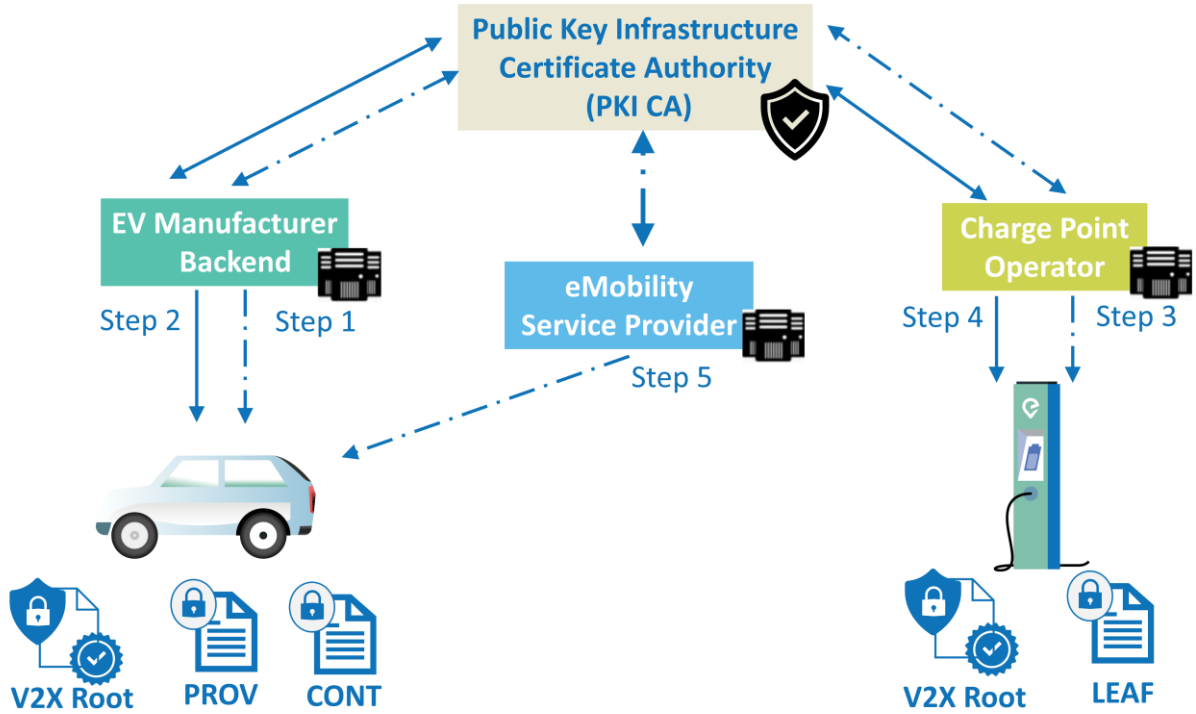

Figure 2 – ISO 15118 certificate exchange through a PKI (based on [9])

Figure 2 includes steps and entities involved in the charging/discharging process. Specifically, the entities that are involved are the EV, the EV manufacturer, the charging station, the Charge Point Operator (CPO), the emobility Managed Service Provider (eMSP) as well as the root PKI Certificate Authority (PKI CA). The EV manufacturer has a backend that manages all EV aspects, including security certificates authenticated by a PKI (either their own or third-party provider as shown in Figure 2).

The EV needs to have a provisioning certificate, marked as "PROV" in Figure 2, installed in the EV which is signed by its own or a third-party PKI (Step 1 in Figure 2). Then, the EV must have an ISO 15118 compliant V2X root certificate installed in the vehicle's communication controller (Step 2 in Figure 2). The charging station that is connected to a Charge Point Operator's platform, needs to have a digital certificate, marked as "LEAF" in Figure 2, signed by a third-party V2X root CA PKI to authenticate itself during the charging session (Step 3 in Figure 2).

In a similar manner with the EV, the charging station also needs to have the V2X root certificate installed in its communication controller (Step 4 in Figure 2). 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 charges and costs from a charging session can be processed. The eMSP stores this information and generates a digital contract certificate, marked as "CONT" in Figure 2, 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 (in Step 5 of Figure 2) 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 Plug & Charge session can be initiated.

3 V2X cyber-security and data privacy threats

Cyber-security threats to V2X can manifest in various forms, including unauthorized access to information, information theft, cyber warfare, or organized crime. Examples of such threats could include unauthorized access to the EV charging process including personal information, such as bank cards for payment as well as username and e-mail address. Additionally, the tampering of data or control systems could lead to disruption in energy distribution or potential harm to the electricity grid and connected vehicles.

The threats to cybersecurity can be categorized based on the impact they have on the Confidentiality, Integrity, and Availability (CIA) of exchanged data and systems - often referred to as the CIA triad. Confidentiality ensures that information is only readable by intended recipients, protecting it from unauthorized third parties. Integrity ensures that any modification can only be done by authorized agents. Availability ensures that the services offered by the system respond to the queries of the user within an expected time frame. Cyber-security events can target any or all of these areas, leading to a range of potential impacts.

The impact of cyber-security incidents can be physical, social, and cyber. Physical impacts could include compromising devices through physical access, breaking the hardware of devices, or provoking hazards that put the health or life of users in danger. Cyber impacts often aim to collect private data like encryption private keys, bank account numbers, contact lists, profile credentials, and preferences as well as to interrupt the system's normal operation by conducting V2X cyber-attack scenarios [10]. Social impacts can aim to slander or expose the private life of victims or decrease the amount of trust among a company's actual or potential customers.

Given the potential threats and impacts, it is crucial that all entities involved in the V2X ecosystem as well as the BUCs of the EV4EU project, should implement robust security measures to protect the connected systems as well as the data they handle. This includes cyber-security risk assessment, ensuring the security of connected devices and entities involved, and considering the privacy of users. For instance, sharing users' data by default, without their knowledge or consent, could lead to resistance to using such systems. Techniques and processes should be in place to ensure user anonymity and protect user data.

In the following part of this section we present an overview of the cyber-attack classes that are relevant for the V2X ecosystem and applicable to the EV4EU project. Then, focus is given to the data privacy threats, which arise from the use of the O-V2X-MP platform as well as its interactions with external entities that are applicable for the BUCs of the EV4EU project and which are part of the V2X ecosystem.

3.1 Cyber-attack classes

The attack classes based on the classification of [10] along with the required mitigation actions to be implemented as counter-measures against them are illustrated in Table 1.

Table 1 – V2X attack classes

Attack class	Description	Mitigation actions
Denial of Service (DoS)	Network flooding with empty OCPP packets	Authentication, encryption, access controls, and anomaly detection

Distributed Denial of Service (DDoS)	Massive flooding with empty OCPP packets on charging stations that would lead to service unavailability	Anomaly detection, Access controls and authentication
Frame injection	Inject false messages in EV charging and discharging scenarios	Authentication and authorization, encryption, Intrusion detection and monitoring
Replay attack	Intercepting and 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 for either 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 Public-Key Infrastructure (PKI)

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 electricity grid. A DoS attack on V2X can take various forms, such as 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 electric vehicle charging or discharging capabilities.

Distributed Denial of Service (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 communication frames with malicious intent. V2X communication frames are the units of data transmitted between the EV and the charging infrastructure. Such injection attacks can have various objectives, including:

1) *Data manipulation*: An adversary may modify the content of V2X frames to manipulate the data exchanged between the EV and the grid. For example, they could alter charging or discharging instructions, energy meter readings, or authentication credentials, 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, with the intention of manipulating or disrupting 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 Charging Station Management System (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. By doing so, 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*: in this scenario, 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 to 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 (i.e., credit/debit) card number, 4) Radio-Frequency Identification (RFID) card number (refered in OCPP as ID Tag) as well as 5) mobile phone number. This is enforced by GDPR legislations. An example of test ID Tag information from a CSMS platform that is deployed in the testbed that is described in Section 5, is illustrated in Figure 3. The tag is anonymized and given a random ID to comply with GDPR regulations. The actual ID tag can be only accessible by authorized personnel that have administrative or eMSP role in the CSMS platform (described in [1]).

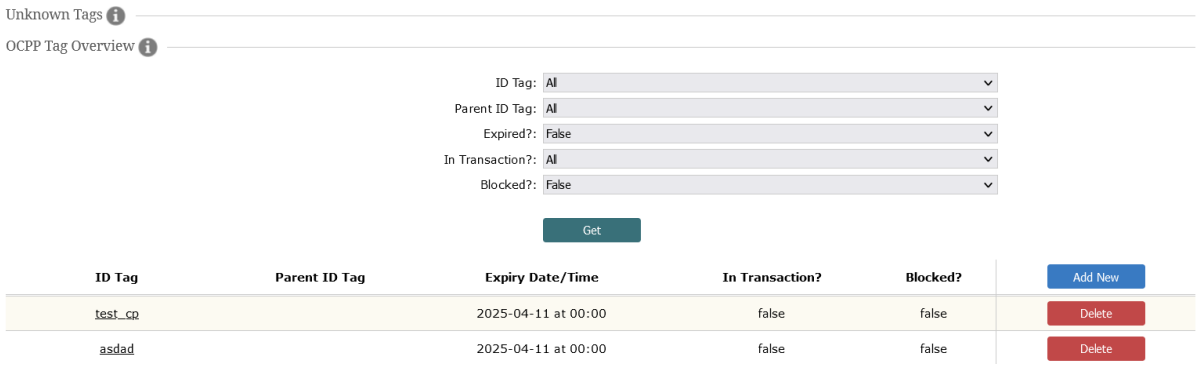

Figure 3 – OCPP ID Tag information from a CSMS platform

Additionally, OCPP 2.0.1 has recently added functionality to enable charging stations and CSMS systems to comply with the GDPR regulations [3]. This functionality allows storing, requesting and removing personal data from charging stations. In order to enable GDPR compatibility, OCA suggests that TLS is used (profile 2 and 3 from the chapter Security in OCPP 2.0.1 [3]). 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 CSMS's to make sure that their specific functionality complies to the GDPR regulations.

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:

- *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 compliancy 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, helps ensure that privacy is embedded into the architecture and operations of the system.

4 Proposed V2X cyber-resilience mechanisms

In deliverable D5.3 [1] a functional view of the services that are employed by O-V2X-MP was provided, hence in this section we describe the proposed tools and mechanisms of the O-V2X-MP architecture, which also include the cyber-security mechanisms. These tools and mechanisms are illustrated in Figure 4.

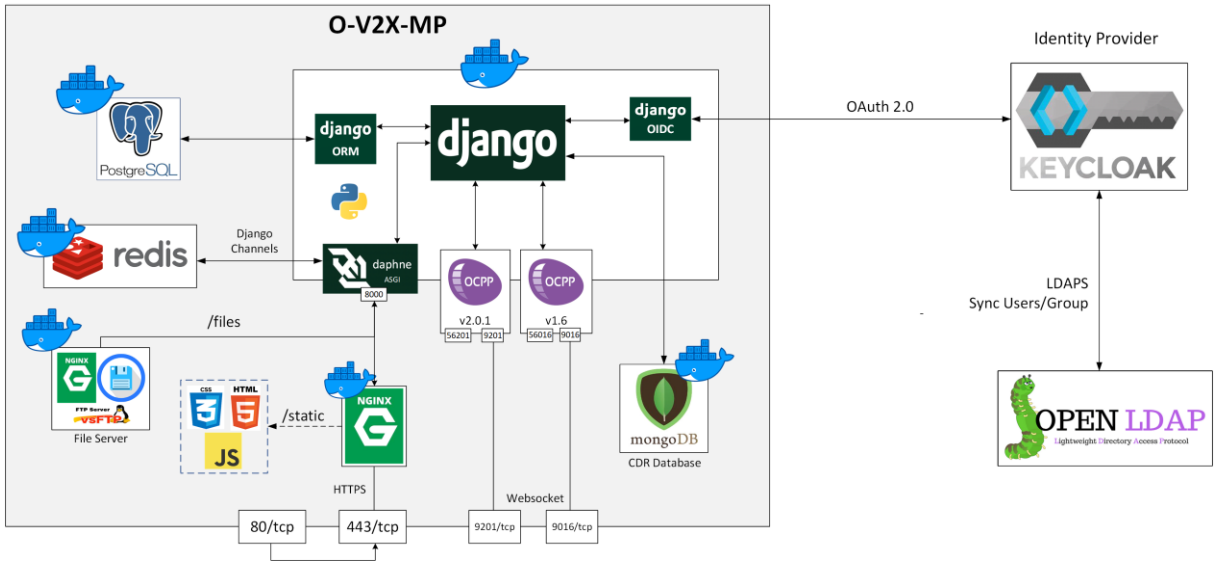

Figure 4 – O-V2X-MP architecture with cyber-security mechanisms

The components that are marked with the Docker logo (blue whale) in the figure are based on dockerized containers. Furthermore, communication between Django and the O-V2X-MP is handled through using a dedicated interprocess communication method. The proposed integration that is considered is through a REpresentational State Transfer (REST) API, which will be available through Flask [11]. This REST API will be used by Django to send OCPP requests and receive responses.

The Django channels are implemented using the Remote Dictionary Server (ReDiS) library [12]. This is easy to implement and can be done immediately. ReDiS is an open-source, in-memory data structure store that can be used as a database, cache, and message broker. ReDiS is known for its speed, flexibility, and versatility, making it a popular choice for various applications that require fast data access and high-performance caching. Furthermore, the current implementation also includes the Django Object-Relational Mapper (ORM) [13], which enables the interaction with the Structured Query Language (SQL) databases including queries, and database manipulation. Specifically, the main goal of ORM is to enable data exchange between a database and models in an application. Hence, it maps a relation between the database and a model. So, ORM maps object attributes to fields of a table. The main advantage of using ORM is that it makes the entire development process fast and error-free, while eliminating the need to write SQL code. The database that was selected for such interactions was PostgreSQL [14].

Four categories of mechanisms were considered applicable and most prominent for the cyber-attack detection and prevention in the O-V2X-PM platform. Additional categories, such as the Trusted Execution Environments [15], were also marked as applicable, but their protection scheme was considered as complementary to the four identified categories. The four categories are:

1) *Authentication and authorization methods* that are described in Section 4.1.
2) *Access control mechanisms* that are described in Section 4.2.

3) Message and data privacy, message integrity, non-repudiation, data loss prevention using *data encryption* mechanisms, further described in Section 4.3.
4) *Network security* mechanisms such as behavioral analytics and Intrusion Detection Systems (IDS) that are described in Section 4.4.

4.1 Authentication and authorization methods

Authorization is performed using OAuth 2.0 [16]. OAuth 2.0 is an open standard protocol that allows users to grant limited access to their resources across websites without sharing their credentials. It is commonly used for authentication and authorization in web and mobile applications. OAuth 2.0 provides a framework for secure and controlled access to Application Programming Interfaces (APIs) by enabling the use of access tokens. 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 O-V2X-MP platform is based on Keycloak [17]. 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. Keycloak offers a wide range of capabilities, including user management, role-based access control, social logins, multi-factor 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. Keycloak is highly customizable and extensible, making it a popular choice for managing user identities and securing applications.

Keycloak interacts with the O-V2X-MP platform through the Django OIDC module [18] illustrated in Figure 4.

4.2 Access control mechanisms

The user groups of the O-V2X-MP platform were detailed in deliverable D5.3 [1]. The access for the different user groups on the O-V2X-MP platform will be based on a Lightweight Directory Access Protocol (LDAP) mechanism [19]. OpenLDAP [20] is an open-source implementation of the LDAP protocol, which is a widely used industry standard for accessing and managing directory information. OpenLDAP provides a server that stores and organizes directory data, allowing clients to perform operations such as searching, adding, modifying, and deleting entries in the directory.

OpenLDAP is designed to be scalable, reliable, and efficient, making it suitable for managing large-scale directory services. It supports various authentication mechanisms, including simple password-based authentication and more secure methods, as the Simple Authentication and Security Layer (SASL). OpenLDAP also supports encryption and secure communication through the TLS protocol. Furthermore, OpenLDAP can be integrated with other systems and applications through its APIs and protocols, making it a flexible and versatile solution for directory services.

Finally, access control policies are implemented to allow only specific groups to have access on a File Server (illustrated in Figure 4), from where diagnostic logs of the stations can be downloaded. The File Server is based on Hypertext Transfer Protocol (HTTP) requests and mounted using nginx [21] as well as Very Secure FTP Daemon (vsftpd) [22]. Nginx is an open-source web server and reverse proxy server. It is known for its high performance, stability, and scalability, making it widely used for serving web content, handling HTTP requests, and acting as a load balancer or reverse proxy. In the O-V2X-MP architecture it is used as a web server, where it can serve static and dynamic web content, including HyperText Markup Language (HTML) files, images, Cascading Style Sheets (CSS) stylesheets, and

JavaScript files. Furthermore, it supports essential web server functionalities like virtual hosting, Secure Sockets Layer (SSL)/TLS termination, Uniform Resource Locator (URL) rewriting, and access control.

Moreover, vsftpd is an open-source File Transfer Protocol (FTP) server software designed for Unix-like systems, including Linux. It aims to be lightweight, secure, and efficient, providing a reliable platform for FTP file transfers. Additionally, vsftpd is commonly used in scenarios where a reliable and secure FTP server is required, such as file sharing, website maintenance, software distribution, or automated file transfers. It is popular among system administrators and hosting providers due to its security features, performance, and ease of configuration.

4.3 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 [23] protocols or enabling firewall rules, for instance to discard V2X packets from blacklisted IPs. These mechanisms are not only implemented in the O-V2X-MP platform, but also in its interactions with the external entities in the V2X ecosystem. Furthermore, these mechanisms are also part of the testbed where the O-V2X-MP is currently integrated and hence are depicted in detail in Section 5.

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 2. However, the OCPP 2.0 protocol also requires the implementation of security mechanisms to protect the communication between CSMS as the O-V2X-MP platform and the charging stations [24]. During the EV4EU project we will also investigate the implementation of these mechanisms in order to protect the sensitive data that are exchanged with the O-V2X-MP platform but also with external entities as system operators or VPPs.

4.4 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. According to the National Institute of Standards and Technology (NIST), Intrusion Detection can be defined as “the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents” [25].

In the V2X context, incidents relate to any events compromising the CIA triad of EV charging and discharging scenarios or any attempts to bypass its security mechanisms [26]. This monitoring process can be automated by using an IDS which identifies eventual incidents. Upon detection, the system will generate a response, which can be categorized as passive or active response [26].

An active response will try to mitigate the incident, for example by collecting additional information about the attacks, deterring the intruder by terminating her connection and reconfiguring the other network and security devices (e.g., router and firewall) to block further packets originating from the malicious source IP address. An IDS responding in a passive manner will solely report the offense, by simply notifying the system administrator or the incident response team with, for instance, a pop up on their operations center dashboard or the SIEM system [27]. This leaves the next actions to be taken up to them. Generally, the IDS imply passive response, while the term Intrusion Prevention System (IPS) has been coined to differentiate systems supporting active response.

Based on [25], the IDS are distinguished in Host-based IDS (HIDS) and Network-based IDS (NIDS) approaches. These approaches mainly differ in the data source they monitor and analyze. A HIDS

collects information and monitors events occurring within a single system. By analyzing the diverse data gathered such as system logs or file accesses and modifications, it can identify precisely the ongoing activities on that host and determine the user(s) and process(es) involved in an attack on the system [25]. A NIDS monitors network packets for a specific part of the network [26]. Moreover, it protects endpoints by analyzing the network traffic going to and coming from them. In general, an IDS architecture contains several sensors deployed at strategic points on the network, where they monitor analyze traffic as well as report attacks to a central management console [25].

The NIDS that will be used within the EV4EU project for V2X charging and discharging scenarios includes the following modules:

1) *Real-time (RT) parser*: Enables the real-time network monitoring for exchanged packets in the in-vehicle network.
2) *Offline parser*: Enables data analysis for the network activity that is logged into dedicated network traffic files (i.e. Packet Captures - PCAPs).
3) *Detection algorithms*: Is applying customized heuristics for detection of security threats/operational hazards according to the OCPP protocol or even for lower-layer protocol as the Transmission Control Protocol (TCP), in which OCPP is based on.
4) *Events Database (EventDB)*: Temporary storage for events/alerts before forwarding to a security event collection system, such as the SIEM.

The interactions between the modules are depicted in Figure 5. Specifically, these interactions concern the gathering of network traffic data and their transmission towards the detection module of the V2X NIDS, which executes the underlying algorithms to detect anomalies in the data. Then, through a dedicated interface it stores any detected events/alerts, which will be afterwards transmitted to a SIEM system. Accordingly, the SIEM will trigger the necessary actions for restoring the V2X system to its normal operation (further described in Section 5).

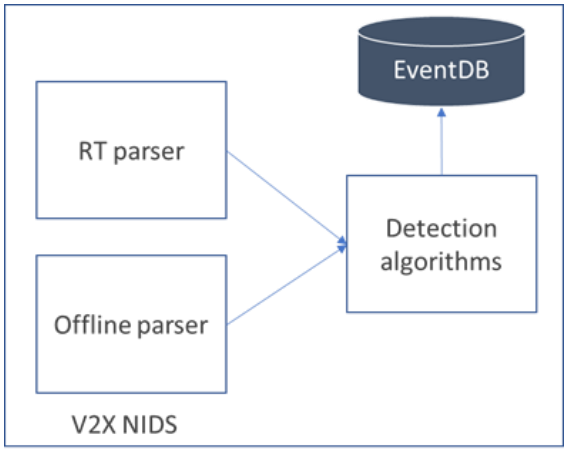

Figure 5 – V2X NIDS functional modules

The implementation of the V2X NIDS will be mainly based on the Zeek [28] 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, 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 custom scripts that extract specific information from V2X protocols, such as OCPP 1.6 and OCPP 2.0.1 [3], or define customized detection rules to protect the O-V2X-PM interactions in the network level. This allows to detect unknown (i.e., zero-day) threats by performing

knowledge- and behaviour-based intrusion detection. Moreover, Zeek supports the integration with a security analytics dashboard based on Kibana [29] that is illustrated in Figure 6.

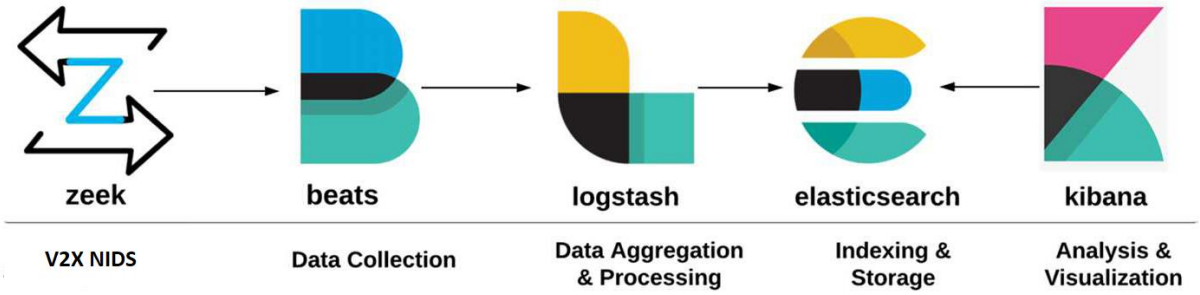

Figure 6 – V2X NIDS integration support based on the use of Zeek

The V2X NIDS may also use signature-based detection that is based on Suricata [30], an open-source software allowing to integrate with threat intelligence sources, such as IP reputation lists, blacklists, and emerging threat feeds. These sources are afterwards blacklisted to ensure protection against know threats. Specifically, such integration enhances the detection capabilities by incorporating information about known malicious IP addresses, domains, or Indicators of Compromise (IOCs) in the V2X ecosystem. Suricata has a dedicated rule-based language, called Suricata Rule Language [31], for defining detection and prevention rules. Furthermore, the rules can be customized based on the specific environment in which the software is deployed. Within EV4EU, Suricata will be employed to enhance the detection accuracy against known threats and will be coupled with the MISP threat intelligence sharing platform [32] for gathering threat feeds and IOCs related to potential cyber-attacks, vulnerabilities or exploits.

5 Integration of O-V2X-MP along with the cyber-resilience mechanisms

The high-level overview of the testbed where the O-V2X-MP is currently deployed is illustrated in Figure 7. Specifically, the infrastructure is segmented to enforce a Demilitarized Zone (DMZ) between the IT part and the critical Electrical Power and Energy Systems (EPES) devices of the Supervisory Control and Data Acquisition (SCADA) network (e.g. Programmable Logic Controllers - PLCs, Power generator). Hence, the testbed is split into different network segments (Virtual LAN networks) to enforce an airgap between the critical devices and the Information Technology (IT) systems. This is illustrated in Figure 7 in the interactions between the IoT Laboratory and the Main Control Room, where the former contains the IT systems and the latter the critical devices of the SCADA network.

Communication is handled through Aruba switches which include Software Defined Networking (SDN) technologies i.e., controller software and dashboard for altering and visualizing the network traffic flows (Figure 7). The infrastructure also includes containerized processes and applications (through docker images) by using Virtual Environment (VE) computing nodes and Type-1 hypervisor, which is based on a Proxmox installation [33]. Access to the infrastructure and the individual segments is restricted through a Virtual Private Network (VPN).

Additionally, the software tools are installed on a server that resides in the IT part of the infrastructure but collects network data, logs and electrical measurements from the EPES devices. Furthermore, penetration testing is periodically performed, and vulnerabilities have been identified and a mitigation plan was carried out both on SCADA and substation network.

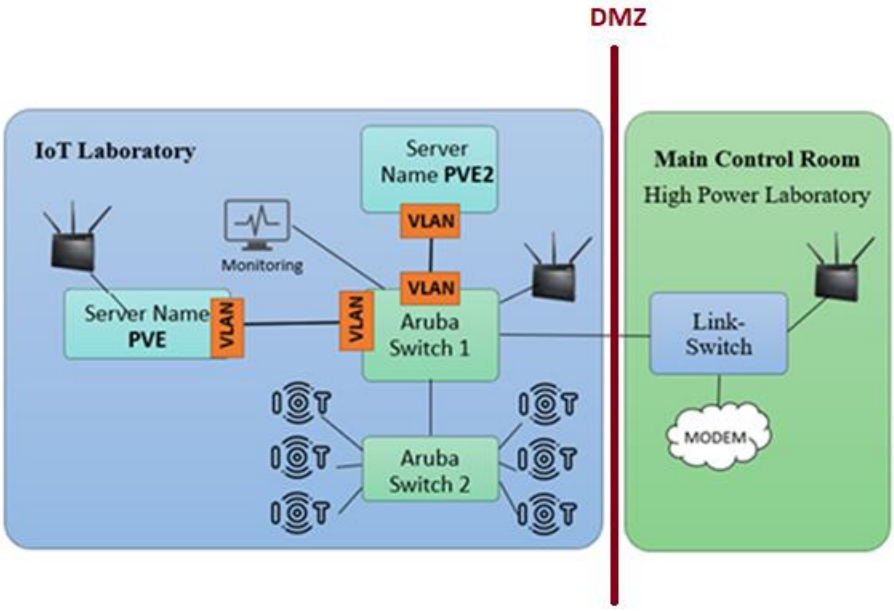

Figure 7 – Testbed architecture that will be used for the O-V2X-MP deployment

The O-V2X-MP installation resides in an infrastructure server, where the Proxmox VE is deployed, hosting virtual machines for all the components of O-V2X-MP. The testbed where O-V2X-MP is currently deployed is additionally protected by firewall mechanisms. Such mechanisms are used to block unauthorized and malicious access using the pfSense software [33]. pfSense is a free and open-source firewall and router distribution based on FreeBSD license. It is designed to be used as a network security appliance and provides a wide range of features for managing and securing computer networks.

Furthermore, a Graylog server installation [35] is used to collect and analyse the firewall logs. Graylog is an open-source log management and analysis platform that allows organizations to collect, store, and analyse log data from various sources in a centralized location and it is mainly used as a SIEM solution. Graylog is composed of different components, with Graylog Server being the core component responsible for processing and indexing logs. This component can also receive input from the NIDS presented in Section 4.4. A view of the Graylog Server logs is illustrated in Figure 8.

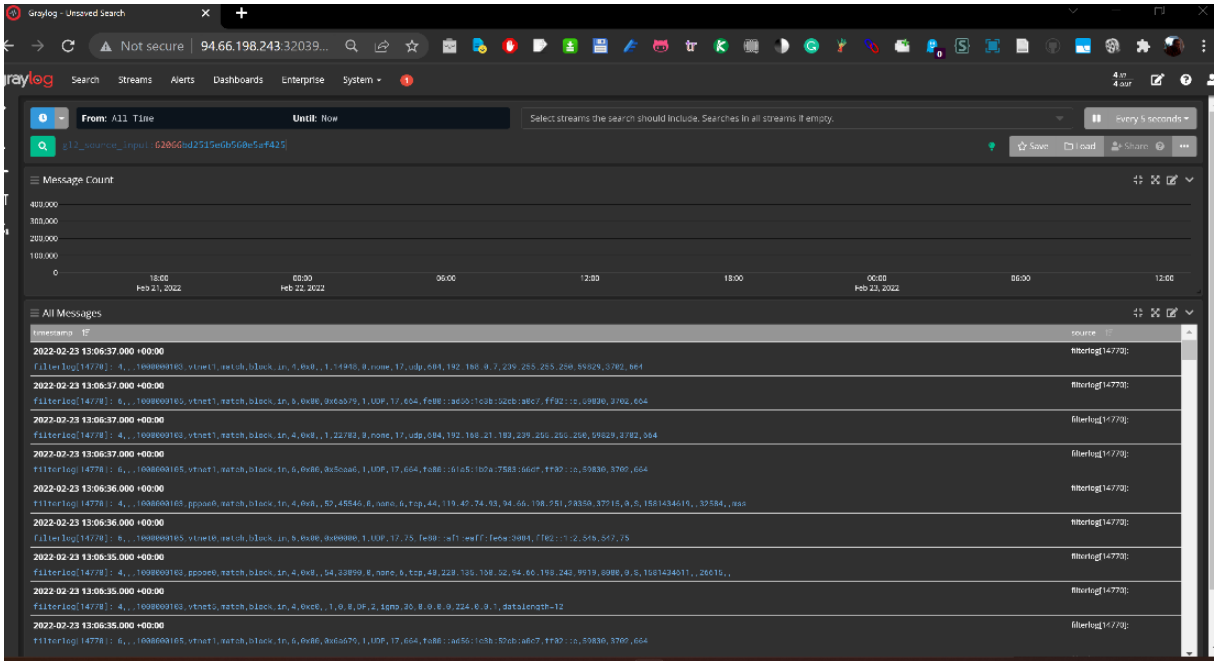

Figure 8 - Graylog server with pfSense firewall logs

6 Conclusions

This deliverable provides an overview of the cyber-security and data privacy mechanisms that will be employed to ensure cyber-resilience of the O-V2X-MP platform. Initially it reflects upon the design of the O-V2X-MP platform as well as existing cyber-security mechanisms that are provisioned in the V2X ecosystem for charging and discharging scenarios. Then, it provides a list of cyber-security and data privacy threats that are applicable in V2X charging and discharging scenarios. The list is defined in terms of cyber-attack classes and data privacy threats. To cope with the V2X threats, dedicated V2X detection and prevention mechanisms are accordingly presented in order to ensure cyber-resilience for the O-V2X-MP platform as well as the interactions will all the other entities, such as system operators, VPPs, Markets within the scope of the EV4EU project.

During the development of the O-V2X-MP platform we will consider the inclusion of additional mechanisms on the categories that were presented in this deliverable, based on the tests that will be conducted on the O-V2X-MP through the BUCs. The initial experiments and developments of the cyber-security mechanisms for the O-V2X-MP and its external interactions to entities in the V2X ecosystem will be part of a report that will be also part of the open-source software tool and both will form deliverable D5.5 “Open V2X Management Platform”.

References

[1] A. Lekidis, “Deliverable 5.3: High-level design of O-V2X-MP”, Electric Vehicles Management for carbon neutrality in Europe (EV4EU) Horizon Europe funded project, grant agreement 101056765 (submitted), 2023

[2] H. Morais et al., “D1.5, V2X Use-Cases Repository", Electric Vehicles Management for carbon neutrality in Europe (EV4EU) Horizon Europe funded project, grant agreement 101056765 (submitted), 2023

[3] Open Charge Alliance, “OPEN CHARGE POINT PROTOCOL 2.0.1”, [Online]: https://www.openchargealliance.org/protocols/ocpp-201/

[4] Django framework, [Online] : https://www.djangoproject.com/

[5] Mobilityhouse, “ocpp library”, [Online]: https://github.com/mobilityhouse/ocpp

[6] Docker, [Online]: https://www.docker.com/

[7] M. Mültin, "ISO 15118 as the Enabler of Vehicle-to-Grid Applications." International Conference of Electrical and Electronic Technologies for Automotive. IEEE, 2018.

[8] E. Rescorla, Diffie-hellman key agreement method. No. rfc2631. Network Working Group, 1999.

[9] Electric Vehicle Charging Open Payment Framework with ISO 15118, [Online]: https://www.securetechalliance.org/wp-content/uploads/EV-Charging-Open-Pmt-Framework-WP-FINAL2-Feb-2021.pdf

[10] R. Metere, M. Neaimeh, C. Morisset, C. Maple, X. Bellekens and R.M. Czekster, “Securing the electric vehicle charging infrastructure. State-of-the-art review and recommendations with a focus on smart charging and vehicle-to-grid”, 2021. [Online]: https://publications.aston.ac.uk/id/eprint/43411/1/2105.02905v1.pdf

[11] Flask tutorial, [Online]: https://flask.palletsprojects.com/en/2.3.x/

[12] M.D. Da Silva and H.L. Tavares, Redis Essentials. Packt Publishing Ltd., 2015. [Online]: https://www.packtpub.com/product/redis-essentials/9781784392451

[13] Django ORM, [Online]: https://docs.djangoproject.com/en/4.2/topics/db/queries/

[14] PostgreSQL, [Online]: https://www.postgresql.org/

[15] J.M.J. Valero, P.M.S. Sánchez, A. Lekidis, P. Martins, P. Diogo, M.G. Pérez, A.H. Celdrán, and G.M. Pérez, 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, pp.203-223, 2022.

[16] D. Hardt, The OAuth 2.0 authorization framework (No. rfc6749). Internet Engineering Task Force (IETF). 2012

[17] A. Chatterjee, and A. Prinz, Applying spring security framework with KeyCloak-based OAuth2 to protect microservice architecture APIs: a case study. Sensors, 22(5), p.1703, 2022.

[18] Django OIDC, [Online]: https://django-oidc-provider.readthedocs.io/en/latest/

[19] J. Sermersheim, Lightweight directory access protocol (LDAP): The protocol (No. rfc4511), Network Working Group, 2006.

[20] M. Butcher, Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services. Packt Publishing Ltd., 2007. [Online]: https://www.packtpub.com/product/mastering-openldap-configuring-securing-and-integrating-directory-services/9781847191021

[21] Nginx, [Online]: https://www.nginx.com/

[22] Very Secure FTP Daemon, [Online]: https://security.appspot.com/vsftpd.html
[23] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.
[24] C. Alcaraz, J. Cumplido and A. Trivino. "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0." International Journal of Information Security, 1-27, 2023.
[25] K. Scarfone, P. Mell: Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) Recommendations of the National Institute of Standards and Technology. In: Nist Special Publication 800-94 (2007), [Online]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
[26] R. Bace, P. Mell: Intrusion Detection Systems. In: Special Publication (NIST SP) - 800-31, 2001.
[27] R. Leszczyna, and M. R. Wróbel. "Evaluation of open source SIEM for situation awareness platform in the smart grid environment." 2015 IEEE World Conference on Factory Communication Systems (WFCS). IEEE, 2015.
[28] Zeek Network Security Monitoring Tool, [Online]: https://zeek.org/
[29] N. Shah, D. Willick, V. Mago: A framework for social media data analytics using Elasticsearch and Kibana. Wireless Networks. pp. 1–9, 2018.
[30] Suricata threat detection, [Online]: https://suricata.io/
[31] Suricata Rules Format, [Online]: https://docs.suricata.io/en/latest/rules/intro.html
[32] MISP Threat Intelligence Sharing Platform, [Online]: https://www.misp-project.org/
[33] R. Goldman, Learning Proxmox VE. Packt Publishing Ltd., 2016. [Online]: https://www.packtpub.com/product/learning-proxmox-ve/9781783981786
[34] pfSense firewall, [Online]: https://www.pfsense.org/
[35] Graylog server, [Online]: https://www.graylog.org/