PNNL-36824

The Design and Evaluation of Zero Trust Architecture for Electric Vehicle Charging Infrastructure

EVs @ Scale Series on EV Charging Station Cybersecurity

September 2024

Thomas E. Carroll
Laurence Chang
Cimone Wright-Hamor

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-36824

The Design and Evaluation of a Zero Trust Architecture for Electric Vehicle Charging Infrastructure

EVs @ Scale Series on EV Charging Station Cybersecurity

September 2024

Thomas E. Carroll
Laurence Chang
Cimone Wright-Hamor

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Acronyms and Abbreviations

ABAC	Attribute-Based Access Control
CSF	Cybersecurity Framework
CSMS	Charging Station Management System
DNS	Domain Name System
DoS	Denial of Service
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Station
EVSE	Electric Vehicle Supply Equipment
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCPP	Open Charge Point Protocol
OSI	Open Systems Interconnection
PVLAN	Private Virtual Local Area Network
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

Abstract

Implementing a zero trust architecture can significantly bolster the security of electric vehicle (EV) charging infrastructure. EV charging infrastructure includes numerous networked interfaces, each of which can present potential vulnerabilities. When these vulnerabilities are exploited, they can compromise the entire system, leading to severe operational and security risks.

Zero trust is a security model that operates on the principle of "never trust, always verify," which helps manage the attack surface and limit the scope of any potential compromises. Fundamentally, this model ensures that no entity, whether inside or outside the network, is trusted by default.

The design principles of zero trust include continuous verification, strict deny-by-default access controls, and micro-segmentation. Continuous verification ensures that every request is thoroughly checked, regardless of its origin. Strict access controls enforce the principle of least privilege, allowing users and devices only the minimum necessary access to perform their functions. Micro-segmentation involves dividing the network into smaller, isolated segments to prevent lateral movement in case of a breach.

In the context of EV charging infrastructure, zero trust can be implemented through various strategies. For example, multi-factor authentication (MFA) can be required for engineers to access the management interfaces and control systems of charging stations. Real-time monitoring and analysis of network traffic can help detect and respond to anomalies. Systems that do not need to communicate with each other can be micro-segmented to enhance security. All communications should adhere to predefined policies to be permitted. Additionally, encrypting communications can protect sensitive information exchanged between chargers and management systems.

This paper presents a zero trust architecture specifically designed for EV charging infrastructure. Implementing zero trust not only mitigates risks but also builds a resilient infrastructure capable of withstanding and quickly recovering from cyber threats. The architecture addresses six defined security objectives. A comprehensive test plan is developed to assess the architecture against these objectives, and the results of the evaluation are reported. This approach is essential for maintaining the reliability and integrity of EV charging services in an increasingly interconnected and vulnerable digital landscape.

This is the first in a planned series of papers exploring the implementation of zero trust in EV charging infrastructure. Each paper will delve into different aspects and applications of zero trust, highlighting how various work processes and requirements can lead to distinct architectural designs. These architectures will be tailored to address specific security challenges and operational needs within the EV charging ecosystem, ensuring a robust and adaptable security framework.

Acknowledgments

The authors thank Mr. Lee Slazek from the Vehicle Technologies Office (VTO), U.S. Department of Energy, for his support. The authors are deeply grateful for his involvement and the positive impact he has made on electrified transportation.

Contents

Figures

Tables

1.0 Introduction

Electric vehicle (EV) charging infrastructure continues to grow to keep pace with the increasing adoption of electric vehicles. Just between 2022 and 2023, the number of stations grew from 57,482 to 68,475, a 19.1 percent increase, and the number of charging ports rose from 151,273 to 184,098, an increase of 21.7 percent (Alternative Fuels Data Center 2024). This expansion is driven by initiatives such as the National Electric Vehicle Infrastructure program and state regulations, which provide funding and policy support to develop a robust and accessible charging network. These efforts aim to reduce range anxiety, promote sustainable transportation, and support the transition to a greener economy by ensuring that EV charging infrastructure keeps pace with the rising number of electric vehicles on the road.

Inadequate EV charging infrastructure cybersecurity is regarded as a significant barrier that is impeding broader adoption of EVs (Barney Carlson 2024). Various studies, such as (J. Johnson, Berg, et al. 2022a; Nasr et al. 2022; Barney Carlson 2024), have indicated that chargers and related infrastructure are vulnerable due to general insufficient cybersecurity measures, are in many cases internet accessible, and frequently lack strong access controls. Due to the chargers being interconnected with the electric grid, there is a concern that compromising a significant number of these chargers could adversely affect the grid's stability (J. Johnson, Anderson, et al. 2022; Maloney et al. 2023; Nasr et al. 2022; Carlson et al. 2023).

A zero trust strategy may more effectively mitigate the cybersecurity risks associated with EV charging infrastructure. Zero trust operates on the principle of "never trust, always verify," meaning that no entity, whether inside or outside the network perimeter, is automatically trusted. Instead, every access request is rigorously authenticated, authorized, and encrypted, regardless of its origin. By applying zero trust principles, such as least privilege access, micro-segmentation of networks, and real-time threat detection, the resilience of EV charging infrastructure against cyber and cyberphysical threats can be significantly bolstered.

The purpose of this document is to introduce and evaluate an EV zero trust architecture and design that integrates a Patero QoR quantum-safe overlay network; private virtual local area network (VLAN), Open Systems Interconnection (OSI) Layer 2 port isolation; and Duo, a multi-factor authentication gateway. The testbed was built at Idaho National Laboratory and tested against with the intention of validating the proposed security objectives and zero trust architecture.

This document will define the identified security objectives that should be met in zero trust architectures for EV charging infrastructures, define the tests to validate the objectives, demonstrate the test results, and identify the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 controls that support our defined objectives. The proposed architecture described in this paper is influenced by multiple cybersecurity and zero trust documents (Rose et al. 2020; Computer Security Division 2016; “NSA Releases Maturity Guidance for the Zero Trust Network and Environment Pillar,” n.d.; Nist 2023; Rose et al. 2020; Kerman et al., n.d.; Grayson 2023).

The authors suggest that multiple architectures could be designed to meet both security and operational objectives, with business goals guiding the selection of the appropriate design. Zero trust is typically viewed as a process of continuous improvement, not a single product solution.

Instead, it involves various products that fulfill different architectural and design elements. Integrating these products into a cohesive solution may require significant time and investment.

The focus of this work is on the relationships between chargers and infrastructure, and on enabling network resilience. Zero trust allows security technology to align with business goals and processes, while also ensuring compliance with data, assets, and infrastructure. Additionally, it can integrate security measures across primary EV digital layers and contain breaches without affecting reputation. The detailed insights about the infrastructure can be obtained about actions taken, ensuring alignment with business outcomes. Zero trust can be employed to manage the connection between the charger and the internet, thereby limiting negative impacts. The control of the EVSE (Electric Vehicle Supply Equipment) is limited, so it is not within the scope of this work.

2.0 Overview of EV Charging Infrastructure

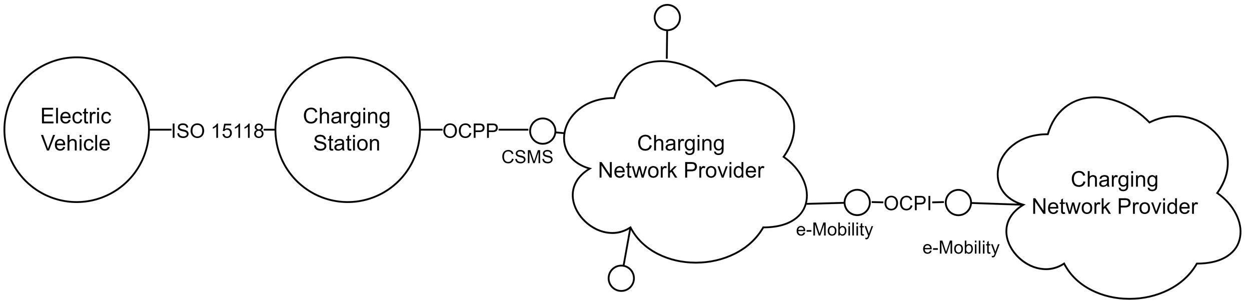


Figure 2.1 Logical representation of EV charging infrastructure.

EV charging infrastructure includes the charging stations and associated equipment needed to recharge EV batteries. For this paper, a simplified model is used to represent EV charging infrastructure, comprising just the charging station and the charging station management system (CSMS), illustrated in Figure 2.1. The EV charging station (EVCS), often referred to as the EVSE, is the device that transfers electricity from the local electrical supply to the EV. The CSMS, owned and operated by the charging network provider (CNP), is designed to centrally control and monitor a network of EVCSs. The CNP may also have an e-mobility interface to support roaming, which allows EV drivers to access and use charging stations that are operated by different charging network providers using a single account or access method. Roaming enables EV drivers to conveniently charge their vehicles at various charging stations across different networks without needing separate memberships or accounts for each provider.

The National Electric Vehicle Infrastructure Formula Program, detailed in 23 C.F.R Part 680, mandates support for three protocols: ISO 15118, the Open Charge Point Protocol (OCPP), and the Open Charge Point Interface (OCPI). ISO 15118 regulates the signals and communication between EV and EVCS. For communication between EVCS and CSMS, the OCPP is utilized. This widely accepted protocol allows for the remote oversight and management of charging stations. OCPP utilizes the WebSocket protocol for its core communication, which operates over a single Transmission Control Protocol/Internet Protocol (TCP/IP) connection initiated by an HTTP handshake to enable real-time, bidirectional message exchanges between charging stations and CSMS. Lastly, OCPI targets the interoperability across charging networks, standardizing the exchange of key data like station location, status, pricing, and the initiation and billing of charging sessions, thereby enhancing user experience. This protocol is a web API adhering to the RESTful architecture concepts.

Not explicitly shown in the diagram are the IEEE 2030.5 and OpenADR protocols, which play a crucial role in smart charge and smart grid management(Grayson 2023). These protocols facilitate advanced communication and interaction between charging stations and the broader energy grid, with aims to enhance the efficiency of the charging infrastructure, reduce costs, minimize the impact on the electrical grid, and maximize the use of renewable energy sources.

EV chargers and stations will need standard IP services such as the Domain Name System (DNS) for looking up service addresses and the Network Time Protocol (NTP) for time synchronization. Additionally, the EV charging infrastructure will employ additional interfaces and protocols to support its auxiliary or proprietary functions that are not mentioned in EV charging standards. For instance, charging stations are typically equipped with remotely accessible maintenance interfaces, which facilitate diagnostic and repair operations. These interfaces often rely on common protocols such as secure shell protocol for command-line she; access or the hypertext transfer protocol (HTTP) for web-based management tools.

Charging stations may include an integrated point-of-sale terminal designed to handle contactless payment cards. These terminals are essential for processing transactions and require secure, reliable communication channels to connect with payment processors or merchant banks. This involves the exchange of sensitive financial information, necessitating stringent security measures to protect against data breaches and ensure compliance with payment industry standards.

A charging depot might be equipped with a meter, a device for monitoring electricity consumption. The meter can communicate and relay its measurements through protocols such as Modbus-TCP or MQTT, both of which utilize the TCP/IP for reliable data transmission.

Charging network providers furnish a comprehensive set of interfaces, primarily access through the web, to support charging station operators and consumers. The charging station operator interfaces are designed for a range of critical tasks, such as performing operations over pools of chargers, establishing a pricing model, analyzing operational data, and performing diagnostic and security-related functions. For consumers, interfaces provide the ability to locate and reserve charging stations, monitor and manage their charging sessions, manage billing and payments, and review energy consumption and charging history.

For more information on the components in the EV charging infrastructure, the various industry players, or the applicable legislation, the reader is encouraged to review the following (J. Johnson, Berg, et al. 2022b; US EPA 2020; “EV201: How an Electric Vehicle Works! | EVgo,” n.d.; Sanghvi and Markel 2021).

3.0 Overview of Cybersecurity Threats

This section provides a brief overview of potential cybersecurity vulnerabilities experienced by EV charging infrastructure, citing actual examples where possible. While not exhaustive, it serves to motivate the objectives that the zero trust architecture aims to achieve. (J. Johnson, Berg, et al. 2022a) provides a comprehensive discussion of EV charging infrastructure vulnerabilities. The discussion focuses on EV charging infrastructure networks and communication interfaces, excluding the EVCS interface. This emphasis is due to the opportunities available for charging station operators and network providers to implement safeguards and countermeasures to address vulnerabilities. However, it is important to note that at least one example will be provided where an attack stage involves communication via the EV–EVCS interface.

EVCSs are networked systems, interfacing the power grid and the vehicle. This network posture presents a potential remotely exploitable attack surface. EVCSs are likely susceptible to common networked system vulnerabilities, such as buffer overflows, authentication bypasses, and crashes.

OCPP is a protocol standardizing the communication between EVCS and CSMS. Older versions, such as OCPP 1.6, have weak security foundations. Even though these deficiencies have been remedied in recent versions such as OCPP 2.0.1, OCPP 1.6 continues to be widely supported. Recent attacks on the protocol have targeted its weak identity and authentication mechanisms.

Due to the weak identity and authentication mechanisms in OCPP 1.6, an adversary could guess the charger ID, use brute force to discover IDs, or intercept unencrypted traffic between the EVCS and the CSMS. Once the charger ID is compromised, the adversary can disrupt the connection between the charger and the CSMS by initiating a new connection using the stolen ID. As a result, the CSMS will cease communications with the legitimate charger, effectively causing a denial of service (DoS) attack on the charger.

SaiFlow effectively exposed these vulnerabilities in (Lakshmanan 2023). Importantly, if the CSMS supports multiple versions of OCPP, a station operator using OCPP 2.0.1 may still be at risk of attack if an attacker can exploit the OCPP 1.6 interface.

When not operated with Transport Layer Security (TLS) or alternative communication security measures, OCPP is susceptible to off-path attacks, including Address Resolution Protocol poisoning. Off-path attacks allow malicious actors to intercept, alter, or forge communication between devices without being directly in the communication path. This is particularly concerning in the context of OCPP because these vulnerabilities can be exploited to disrupt operations or inject malicious commands (Zhdanova et al. 2022). Ensuring the implementation of TLS is crucial to mitigating these risks by encrypting communications and authenticating the parties involved.

The use of misconfigured OCPP messages between the EVSE and the CSMS may allow an adversary to conduct a remote attack that could jeopardize the availability of EVSE. Invalid OCPP messages could result in an unexpected system state, which may cause the EVSE to crash, consume available system resources, or result in unintended system behaviors. Instant unexpected load shed during peak demand of one EVSE may not drastically affect the grid and compromise regional grid stability. An example of this is the known Grizzl-E charger issue, which adequately handles OCPP formatting issues (hacsjalano 2023).

Idaho National Laboratory has proposed a scenario where an inattentive operator uses a CSMS to broadcast commands to a large number of chargers, causing them to nearly simultaneously cease power transfer (Carlson et al. 2023). This could lead to voltage transients, potentially destabilizing the electrical grid. This underscores the need for continuous monitoring and traffic shaping of messages to prevent such disruptions.

Malware will often require access to networks. For instance, a Log4j vulnerability was identified and demonstrated in the RiseV2G implementation of the ISO 15118 standard ("Examining Log4j Vulnerabilities in Connected Cars and Charging Stations" 2021). Interestingly, the first phase of the attack communicated the malicious string over the EV–EVCS interface. This vulnerability exposed the system to remote code execution, allowing attackers to execute arbitrary code. Such an exploit could lead to unauthorized access, manipulation of data, or disruption of services. A key aspect of the Log4j vulnerability was that it caused the charger to download the untrusted code from the network.

Implanting malicious software, such as cryptocurrency mining operations or botnet command and control mechanisms, typically requires network access and resources. Attackers often leverage network connectivity to download and install untrusted code, communicate with command-and-control servers, and exfiltrate data("Botnet Anatomy," n.d.). In the case of cryptocurrency mining, the malicious software would consume significant computational power and bandwidth, while continuously communicating with mining pools over the network. Similarly, botnet command and control systems rely on network resources to send instructions to compromised devices, orchestrate attacks, and receive stolen data.

Many chargers come with proprietary, often web-based, management interfaces. These interfaces allow administrators to configure settings, monitor operations, and manage updates remotely through a web browser. While convenient, these management interfaces can also introduce security vulnerabilities if not properly secured. Attackers have exploited default passwords, weak authentication parameters, outdated software, or unpatched vulnerabilities to gain unauthorized access (Böck 2023; "Alpitronic Hypercharger EV Charger | CISA" 2024; W. Johnson 2023).

There have been reported instances of defacement. Defacement often involves compromising an external service or performing a domain takeover. In such cases, attackers alter the content displayed on a website or web-based interface, often to display their own messages or malicious content. One common method for achieving this is through DNS poisoning, where attackers manipulate the DNS to redirect traffic from the legitimate site to a malicious one. This can lead to users unknowingly interacting with a compromised site, furthering the potential for data theft, malware distribution, or other malicious activities. Domain takeovers, where attackers gain control over a domain name, can have similar consequences, allowing them to intercept communications, alter web content, or impersonate the legitimate service.

Based on the vulnerabilities discussed above, the security objectives that a zero trust architecture should accomplish can be derived. This includes an analysis of how zero trust principles can mitigate these specific threats and those with similar characteristics, ultimately enhancing the overall security posture of EV charging infrastructure.

4.0 Security Objectives

This section outlines the security objectives that support the design and implementation of zero trust for EV charging infrastructure. These objectives are informed by the threat assessment and its characteristics discussed in the previous section, Section 3.0. The six security objectives are deny-by-default, least privilege access, authentication and authorization, secure communication, minimize network exposure, and minimize third-party dependencies. These objectives inform the development of the zero trust architecture described in Section 6.0.

4.1 Deny by Default

The security objective deny by default requires blocking all requests to network resources unless they are explicitly permitted by security policies. Strict rules and conditions define and regulate the permissions for each user, device, or application, ensuring that only verified entities gain access.

4.2 Least Privilege Access

The least privilege access security objective addresses minimizing the number of logical relationships that an identity (user, device, or resource) within the network can have to essential relationships required for the system to function. The access least principle is vital in EV charging due to the different scopes on which the infrastructure components may operate. The various roles and responsibilities may affect the management of the infrastructure, thus changing the access required for the systems to function. In the event of a compromised account, least privilege access limits the devices affected and the potential damage.

For example, chargers may operate in a scope local to that charging site but may need a route to a remote CSMS or other resources that may reside in the cloud. Charger-to-grid communications may also occur, representing yet another scope of operation. By applying the principle of least privilege access, the attack surface can be reduced by ensuring that entities in the system operate and abide by the network, user, and application restrictions they are assigned to.

4.3 Authentication and Authorization

The authentication and authorization security objective requires explicit verification of all entities by proving the identity and policy access to the requested resource. Identities may include humans and non-humans (i.e., users, devices, and services). Identities enrolled in the network go through a continual authentication and authorization, initiated with the enrollment of an identity to the network and the generation of its certificate.

Each access request must be authenticated with the network controller. This piece serves as the continual authentication of the model. Furthermore, authorization is determined in forms of policies, in which the default is deny everything. An explicit policy must be made to allow a given identity to reach a given service, thus providing the authorization piece.

4.4 Secure Communication

The secure communication security objective protects data in transit to prevent the loss of data integrity and confidentiality. EV chargers, CSMS, and back-office communications should be secured to protect the integrity and confidentiality of the data passed between the endpoints.

4.5 Minimize Network Exposure

The minimize network exposure security objective aims to restrict external network access of the charging infrastructure and establish isolated zones to aid in the protection of infrastructure assets and data.

Restricting external network access may be accomplished by using a policy to explicitly manage and enforce all external network connectivity. The primary functionality for an EVCS is to provide electrical power to plug-in electric vehicles, with the possible functionality of delivering power back to the grid. The charger is not intended to function as a general-purpose computing device. Therefore, the number of other network endpoints the charger may need to communicate with is limited and may include the CSMS, firmware server, and payment server.

Policies are created leveraging the known characteristics (i.e., primary functionality and connectivity) of the EV charging station and only permit network connectivity required for essential functions. These policies can minimize trivial adversarial tasks (e.g., standard reconnaissance and access resource), which can disrupt the chain of attacks (i.e., persistence, execution, etc.). Limiting charger access to only the explicitly defined external applications will prevent undefined communication from existing in the network—thus, lateral movement should be avoided. Network access should be restricted to authorized cloud-based CSMS or operators.

Isolated zones can be achieved by pervasive logical partitioning into subnets to restrict network access. Pervasive logical partitioning can be achieved by creating multiple network namespaces on edge routers. These treatments result in the micro-segmentation of network devices, restricting lateral communications even at a physically local site and controlling what external entities can communicate back with it. This security control aligns with the Networks pillar, enabling network security on a per-charger basis and preventing lateral movement attempts in the broader EV charging network and beyond.

4.6 Employ Trusted Network Infrastructure

The goal is to ensure that chargers and ancillary charging equipment are configured to use trusted network services and infrastructure controlled by the charging site operator, rather than relying on untrusted instances provided by the site host, internet service provider, or other third parties. This approach reduces the attack surface by minimizing common attack vectors and vulnerabilities when using third-party infrastructure while also supporting key security imperatives, such as reliable monitoring and logging. For example, using a trusted NTP instance ensures accurate time synchronization for precise logging. Similarly, relying on secure DNS services decreases the chance of disruptions or malicious interference.

The following section maps these security objectives to the NIST CSF.

5.0 Mapping Security Objectives to the NIST Cybersecurity Framework

The NIST CSF framework, developed by the National Institute of Standards and Technology, is a comprehensive guide designed to help organizations manage and reduce cybersecurity risks. It consists of five core functions—Identify, Protect, Detect, Respond, and Recover—that provide a strategic view of the life cycle of an organization's management of cybersecurity risk. The framework facilitates the alignment of cybersecurity activities with business requirements, risk tolerances, and resources, making it widely applicable across various sectors and industries.

The following table maps the following CSF controls that are met by the security controls described previously. The zero trust efforts are focused on a CSF core function called Protect (PR) and the following subtopics:

- (AA) Identity Management, Authentication, and Access Controls
- (DS) Data Security
- (PS) Platform Security
- (IR) Technology Infrastructure Resilience

Table 5.1. Mapping the defined security objectives to NIST CSF 2.0 Controls

Security Objective	Supporting NIST CSF 2.0 Controls
Deny by default	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
Least Privilege Access	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
Authentication and Authorization	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions PR.AA-03: Users, services, and hardware are authenticated PR.AA-04: Identity assertions are protected, conveyed, and verified
Secure Communication	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected
Minimize Network Exposure	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.AA-04: Identity assertions are protected, conveyed, and verified PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties PR.PS-01: Networks and environments are protected from unauthorized logical access and usage PR.IR-02: The organization's technology assets are protected from environmental threats
Employ Trusted Network Infrastructure	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.IR-02: The organization's technology assets are protected from environmental threats

5.1 Deny by Default

The deny by default security objective is mapped to PR.IR-01 and PR.AA-05 through the definition of explicitly prohibiting undefined traffic rules such that network and endpoints are protected from unauthorized access and that all relationships must be explicitly defined. By operating the network in a deny by default manner, we guarantee that only the traffic that has been defined and vetted are the only sources of communication allowed to propagate in the environment.

5.2 Least Privilege Access

5.2.1 Protect – Technology Infrastructure Resilience

The least privilege access can be mapped to the PR function and the IR category. PR.IR, an organization's risk strategy, dictates the security architecture, which establishes asset protection (i.e., confidentiality, integrity, availability, and resilience). PR.IR-01 helps protect networks and environments from unauthorized logical access and usage. The principle of least privileged access can be demonstrated by restricting the users' access rights to a minimal privileges required to perform their job. These restrictions reduce the risk of unauthorized access to sensitive systems and data, contributing to the goal of protecting networks and environments from unauthorized logical access and usage, as outlined in PR.IR-01.

5.2.2 Protect – Identity Management, Authentication, and Access Control

Least privilege access can be mapped to the PR function and the AA category. PR.AA restricts the access of authorized users, services, and hardware to physical and logical assets. PR.AA-05 incorporates the principle of least privilege and separation of duties by managing, enforcing, and reviewing permissions, entitlements, and authorizations defined in a policy. The combination of identity verification and resource authorization creates access controls adhering to the principle of least privilege. Together, these policies restrict users' access rights to the lowest level necessary to perform their job functions. This directly supports defining and managing access permissions, ensuring access is granted based on specific needs and responsibilities and incorporating the principles of least privilege and separation of duties. Thus, implementing least privilege access helps enforce and uphold the principles outlined in PR.AA-05.

5.3 Authentication and Authorization

5.3.1 Protect – Identity Management, Authentication, and Access Control

Authentication and Authorization are directly related to the PR function and the AA category. PR.AA-02 is based on the core components of proofing and binding identities to credentials based on the context of interactions. By effectively implementing authentication and authorization mechanisms, organizations can ensure that identities are properly proofed and bound to credentials in accordance with the context of their interactions, thereby aligning with the requirements outlined in PR.AA-02.

PR.AA-03 requires that all users, services, and hardware be authenticated. Authentication involves verifying the identity of users, services, and hardware, ensuring that they are who or what they claim to be. Authorization, on the other hand, determines what actions and resources authenticated entities are allowed to access based on their verified identity. By implementing robust authentication and authorization mechanisms, organizations can fulfill the requirement of authenticating users, services, and hardware as specified in PR.AA-03, thereby ensuring the integrity and security of the systems and data.

PR.AA-04 focuses on the protection, conveyance, and verification of identity assertions. Through authentication, the process of verifying the identity of users, services, and hardware helps protect the integrity of identity assertions. Authorization complements this by conveying and verifying the rights and access associated with the verified identities. By effectively implementing authentication and authorization measures, organizations can ensure that identity assertions are safeguarded, accurately conveyed, and reliably verified, thus aligning with the requirements of PR.AA-04.

5.4 Secure Communications

5.4.1 Protect – Data Security

Secure communications directly relate to the PR function and the DS category. In PR.DS, an organization's risk strategy to protect the confidentiality, integrity, and availability of information dictates how data is managed. PR.DS-02s protect the confidentiality, integrity, and availability of data during transit. By implementing secure communication protocols such as encryption and digital signatures, organizations can safeguard data as it is transmitted across networks. Secure communications provide confidentiality, authentication, and integrity to prevent unauthorized individuals form accessing information between two nodes within a network. These measures ensure that data remains confidential, unaltered, and accessible only to authorized parties, thereby meeting the requirements outlined in PR.DS-02.

5.5 Minimize Network Exposure

5.5.1 Protect – Technology Infrastructure Resilience

Restricting network exposure directly aligns with the PR function and the IR category. PR.IR-01 plays a crucial role in protecting networks and environments from unauthorized logical access and usage. By implementing measures to limit network exposure, such as using firewalls, access controls, and network segmentation, organizations can effectively reduce the potential attack surface and minimize unauthorized access to their networks and environments. This directly supports the goal of protecting networks and environments from unauthorized logical access and aligns with the requirements outlined in PR.IR-01.

5.5.2 Protect – Identity Management, Authentication, and Access Control

Restricting network exposure is related to the PR function and AA category. By limiting network exposure, organizations can help protect the integrity and security of identity assertions as they are conveyed and verified across the network. This restriction reduces the potential attack surface for unauthorized entities seeking to manipulate or access identity assertions, thus aligning with the goal of protecting identity assertions as outlined in PR.AA-04.

By limiting network exposure, organizations can better control and manage access to network resources, thereby enforcing the defined policies and incorporating the principles of least privilege and separation of duties. This riction reduces the attack surface and helps ensure that access permissions are managed and enforced in line with the requirements outlined in PR.AA-05.

5.5.3 Protect – Platform Security

Restricting network exposure directly aligns with the PR function and the PS category. PR.PS states that an organization's risk strategy governs the protection of their confidentiality, integrity, and availability of hardware, software, and services of physical and virtual platforms. PR.PS-01 focuses on establishing configuration management practices and ensuring these practices are applied. By implementing access controls and network segmentation, organizations can effectively establish configuration management practices. Thus, providing the organization with confidentiality.

5.5.4 Protect – Technology Infrastructure Resilience

Restricting network exposure is related to the PR function and the IR category. PR.IR-02 focuses on protecting the organization's technology assets from environmental threats. By limiting network exposure, organizations can reduce the potential impact of environmental threats on their technology assets. This restriction helps safeguard the integrity and availability of technology assets by minimizing their exposure to external threats and vulnerabilities, consequentially aligning with the goal of protecting technology assets from environmental threats as outlined in PR.IR-02.

5.6 Employ Trusted Network Infrastructure

5.6.1 Protect – Technology Infrastructure Resilience

Restricting third-party dependencies is related to the PR function and the IR category. By carefully managing and restricting the dependencies on third-party systems or services, organizations can reduce the risk of unauthorized access and use of sensitive data and resources. This contributes to the overall goal of protecting networks and environments from unauthorized logical access as outlined in PR.IR-01, because it limits the potential attack surface and vulnerabilities that could be exploited by unauthorized parties.

By carefully managing and restricting dependencies on third-party systems or services, organizations can reduce the exposure of their technology assets to environmental threats. This ensures that the organization's core technology remains insulated from potential vulnerabilities introduced by third-party dependencies, aligning with the goal of protecting technology assets from environmental threats as outlined in PR.IR-02.

6.0 Architecture

This section describes the network architecture employed for testing purposes and maps the components to the security objectives. The design of this architecture considered the actors, roles, and processes involved in charging, as well as the specified security objectives outlined in Section 3.0. It presents three architecture variants, which, while similar, differ primarily in their network pathways to the CSMS and the component set up to manage these differences.

Exploring the distinct network pathways to the CSMS is crucial due to the possible differences in responsibilities between the charging station operator and the charging network operator. Typically, the network operator manages the charging network and operates the CSMS, allowing the station operator to choose which network to use. However, in many business models, the charging station operator and the charging network provider are the same entity.

Beyond the roles of the charging station operator and the charging network operator, there is a third key player: the site host. The site host owns or occupies the land where the EV charging equipment is installed. In this study, it is assumed the site host provides internet connectivity for the charging station and is responsible for Switch 2 and the firewall.[1] The charging station operator must request exceptions from the site host to ensure the firewall is appropriately configured to pass the EV charging infrastructure communications. This setup was implemented to test connectivity behind firewalls and represents a common deployment scenario.

Refocusing on the network pathway variations:

- Variant 1, illustrated in Figure 6.1, the charging station connects to the CSMS through a secure network that also ties in cloud services and the back office.
- Variant 2, depicted in Figure 6.2, involves the charging station directly connecting to the CSMS over the internet, using the local Internet Service Provider (ISP) for traffic routing.
- Variant 3, shown in Figure 6.3, charger communication is consolidated into one or more clouds and utilizes cloud-based routing to facilitate communication with the CSMS.

The key differences between the variants lie in the routing to the CSMS. In Variant 1, traffic is routed through the secure “dark” net, providing a high degree of communication security from the charger to the CSMS. In Variant 2, the CSMS is accessible from the global internet, leaving the CSMS at risk of a SaiFlow denial of service (DoS) attack (see Section 3 for a description of the attack). Variant 3 uses a cloud provider to route traffic to the CSMS. Communication security is ensured by CryptoQoR up to the cloud, and although the traffic is not protected by QoR, the risk is managed by operating over the cloud network backbone. Additionally, with concentrated communications, cloud-to-cloud network gateways can be employed to manage risk effectively. Apart from these attributes, the choice of variant will be further influenced by factors such as feasibility and cost.

[1] The site host uses a Palo Alto Networks Next-Generation Firewall, version 11.0.3h1. This firewall is configured to support widely used applications such as HTTPS, DNS, and NTP, and has been additionally tailored to facilitate communications from the Patero QoR.

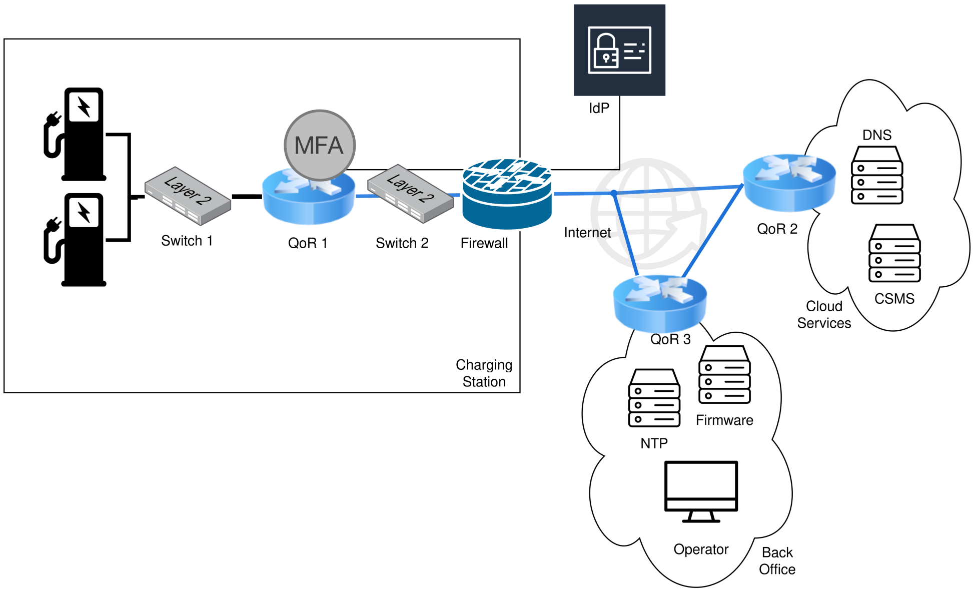


Figure 6.1. Variant 1: The charging station connects to the CSMS via a secure network overlay (expressed as solid blue lines) established by QoR1 and QoR2.

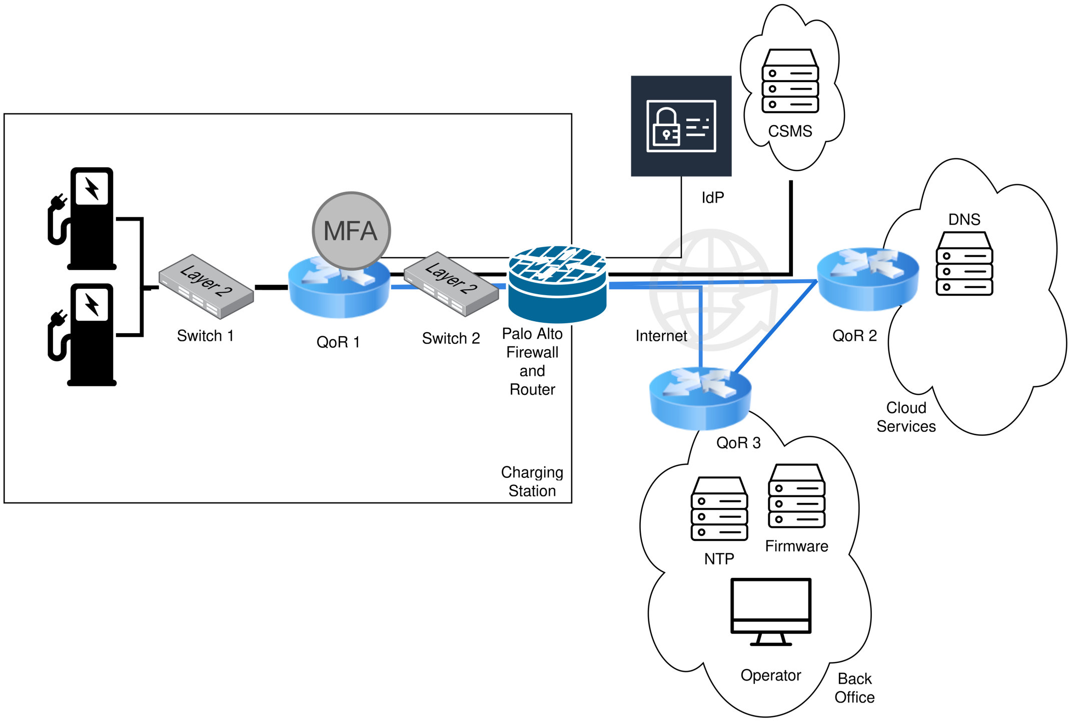


Figure 6.2. Variant 2: The CSMS is accessible via the internet, with QoR 1 routing the charger's OCPP communication to the service (illustrated by the bold black line). In this setup, the traffic is not secured by the QoR fabric.

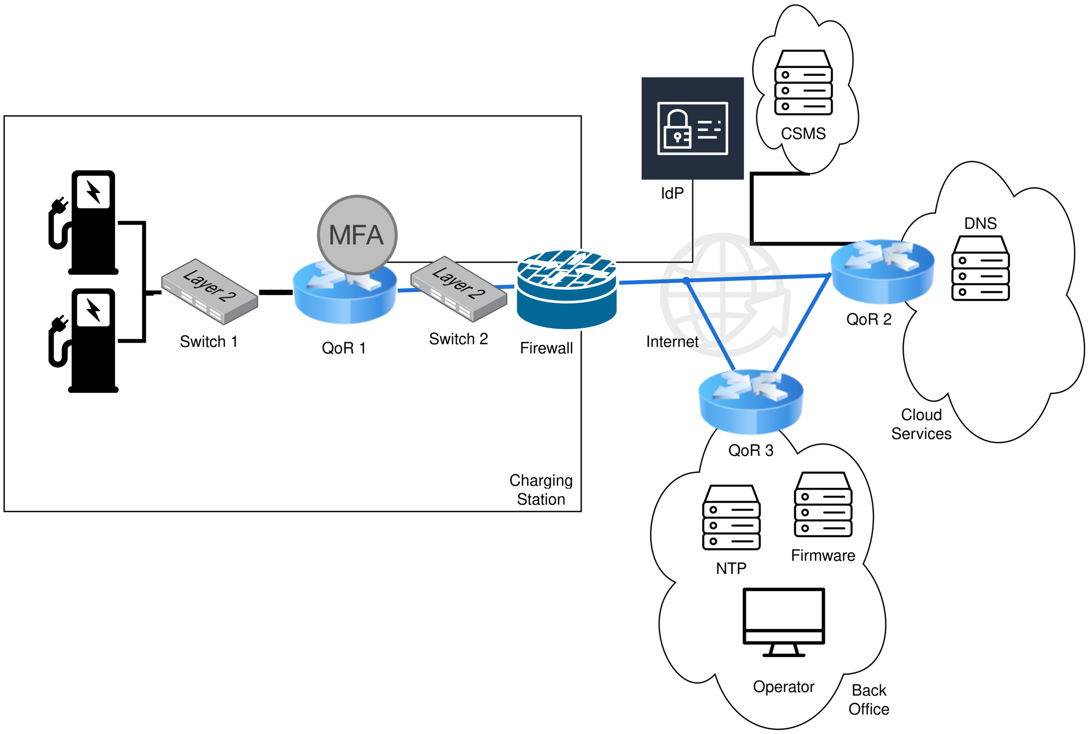


Figure 6.3. Variant 3: QoR2 routes the communication to the internet-accessible CSMS, with cloud routing facilitating the connection between QoR2 and the service. In this setup, the QoR fabric secures the communication up to the cloud, while cloud-to-cloud routing is used to reach the CSMS.

The secure network safeguards communication between the chargers and cloud routers, with the cloud routers providing greater routing security compared to local ISPs. During testing, the STeVe management system[1] is employed, which implements OCPP 1.6. The security provided by the overlay network is particularly advantageous because OCPP 1.6[2] lacks fundamental security measures such as TLS to secure the protocol and passwords to authenticate the charger to the CSMS service.

In the architecture, the QoR gateway routers, operating on Ubuntu Jammy and Patero CryptoQoR 0.5.1 (0-4-0-psk), establish a secure network overlay. CryptoQoR employs a modern, high-performance VPN protocol that utilizes hybrid post-quantum cryptography, safeguarding against both conventional and quantum computing threats. Each of the three QoR gateways maintains a direct, point-to-point connection to the others. The linked communications that are protected by QoR are illustrated as the solid blue lines in Figure 6.1, Figure 6.2, and Figure 6.3. This overlay ensures the confidentiality and integrity of end-system communication over the internet by encapsulating traffic. The gateways enforce policies based on OSI model[3]

[1] https://github.com/steve-community/steve
[2] Both OCPP 2.0.1 and OCPP 1.6 security, an extension to OCPP 1.6, feature enhanced security measures to protect the protocol, including TLS for communication security.
[3] The Open Systems Interconnection (OSI) model is a conceptual framework used to understand network interactions in seven layers. Each layer serves a specific function and communicates with the layers

layers 2 (data link layer), 3 (network layer), and 4 (transport layer) properties. These policies would be established by the network and security architects. The orchestration of the Patero QoR, Duo Network Gateway, and private VLAN establishes and enforces a deny-by-default posture, resulting in explicit policy-based permissions being required for all communications. Management interfaces, which will be discussed later, undergo special treatment, necessitating additional authentication and authorization processes. Systems and services behind the gateways are inaccessible directly from the internet; instead, they must be accessed strictly through the overlay network. Charge Station Operator (CSO)-operated instances of DNS and NTP are integrated into the zero trust network architecture to minimize dependency on third-party resources and limit the chargers' need for internet access.

In future work, the QoR would be the place to investigate communication resilience. One particularly effective method is Wide Area Network (WAN) bonding, which aggregates multiple independent internet connections into a single logical channel. A key benefit of this approach is hot failover, which ensures service continuity by seamlessly switching between channels while persisting network sessions.

Additional work can consider the CSMS as a proper cloud service, where a network security policy controls both inbound and outbound traffic to and from the CSMS. This policy should include stringent measures such as firewall configurations, traffic filtering, and monitoring to ensure that only authorized data flows are allowed, thereby safeguarding the system against potential cyber threats and unauthorized access.

Switch 1 is configured for private VLAN, a networking feature that partitions a single VLAN into multiple isolated sub-VLANs, enabling finer control over network traffic and enhancing security by restricting communication between devices within the same VLAN. In effect, this approach isolates devices at OSI Layer 2 and affects every layer above it. When private VLAN is active, the top charger shown in the architecture cannot communicate with the bottom charger. QoR 1 is configured to enforce the policy that inbound network interface must be different from the outbound network interface—otherwise, traffic must be dropped.

Switch 1 has been further configured to enhance security. All unused ports are administratively disabled to prevent unauthorized access. Additionally, the switch actively monitors and reports changes in Media Access Control (MAC) addresses, the association of MAC addresses with physical interfaces, and link states, ensuring comprehensive oversight and security management.

The Duo Network Gateway, version 3.0.0, serves as the authentication and authorization mechanism for traffic accessing the charger and charging station device management interfaces. This can be considered an example of a resource-based portal. Whenever an engineer or operator attempts to access these resources, they are required to provide not only a password but also undergo a secondary verification process via their phone. This two-factor authentication enhances the security posture by adding an extra layer of protection, ensuring that only authorized personnel can gain access to these critical components of the network infrastructure.

directly above and below it. A comprehensive description of the OSI model is The OSI (Open Systems Interconnection) model, a conceptual framework used to understand network interactions in seven layers. Each layer serves a specific function and communicates with the layers directly above and below it.

Because the Duo Network Gateway is integrated with an attribute-based access control (ABAC) system for identity and access management, it can be configured to ensure that only engineers who have the necessary qualifications and training are granted access to specific equipment they are trained to operate. ABAC operates on the principle of evaluating various attributes associated with users, resources, and the environment to make access control decisions. In this context, attributes such as job role, certification status, and training records can be considered when determining whether an engineer is authorized to interact with particular equipment. By leveraging ABAC, organizations can enforce granular access policies that align with their security requirements and regulatory compliance mandates, thereby reducing the risk of unauthorized access and ensuring that only qualified personnel can perform critical tasks.

The implementation aimed to validate the compatibility of QoR with firewall environments. Configuration of the firewall prioritized the allowance of essential protocols such as HTTPS, DNS, and NTP. Additionally, it was crucial to configure the firewall to facilitate the transmission of CryptoQoR traffic, ensuring the seamless integration and functionality of QoR systems within the network architecture.

From the perspective of the charging station operator, the correlation between specific security key components and their role in respective security objectives is detailed in Table 6.1.

Table 6.1 Coverage of Security Objectives per technical security component.

Security Objectives	Technical Security Components			
	Patero QoR	Duo Network Gateway	Switch 1	DNS/NTP
Deny-by-Default Policy Enforcement	X		X	
Least Privilege Access	X			
Authentication and Authorization	X			X
Secure Communication	X			
Minimize Charging Infrastructure Network Exposure		X	X	
Minimize Third-Party Dependencies				

To rigorously evaluate the effectiveness of the zero trust architecture described, we establish specific test objectives designed to challenge and assess the robustness of the security measures we've set in place. In this configuration, it is expected that traffic will only flow according to the strict policies set in place and defined by the team.

It is understood that today's chargers that are currently deployed and in production may not have some of the utilities or tools needed for some of the testing to be performed. As a compromise, we substitute the compromised charger for a given host running Linux that enables us to use common networking tools such as Netcat or Telnet, among others. Using a Linux host also enables us to use other downloaded tools such as Nmap or Zmap for validating tests that require the ability to scan large numbers of hosts on the internet.

7.0 Test Plan

The following section details the definitions of test objectives, aligns them with the security objectives presented in Section 3.0, and explain the procedures for evaluating if security components have effectively addressed the cyber threats. Real-world operational configurations and cyber threats have been used to help create a series of scenarios. The procedures in this section will outline the process and steps involved in evaluating specific use cases and sub-cases. The goal is to demonstrate and assess how the attack surface changes in response to the features of the zero trust architecture. Network architecture is decomposed and isolated to verify the impact of security controls on the testbed.

7.1 Test Objectives

Table 7.1 Coverage of Security Objectives per test objectives.

Security Objectives	Test Objectives			
	Validate Testbed	Mitigate MiTM Attacks Against EVSE/CSMS	Minimizing Charge Attack Surface	Mitigating Local DNS Poisoning Attack
Deny-by-Default Policy Enforcement		X		
Least Privilege Access		X		
Authentication and Authorization		X		
Secure Communication				X
Minimize Charging Infrastructure Network Exposure		X	X	X
Minimize Third-Party Dependencies			X	X

The primary concerns of the test objectives are to exercise the capability to dictate EV charger communications and mitigate malicious traffic occurring in the system in the event of an internet-based threat compromising a charger or the CSMS. Communications between an EV charger and the other components of an EV charging infrastructure may vary depending on the current needs and operations of the charger. For purposes of describing the testbed, three primary domains are defined:

1. Charging Station: This domain comprises one EVSE or more where the EVs would connect to for charging purposes.
2. Back office: This domain comprises ancillary Charging Station Operator services. Services may include a local CSMS, local file servers, web servers, NTP, and others.
3. Cloud Server: This domain comprises services residing on the internet that the charging station may need to connect to for administrative or operational purposes. Examples include payment gateways, external CSMS, web servers, patch servers, and others.

Test procedures will focus on the EV charging infrastructure and its environment after it has been integrated with the security measures described in previous sections.

7.2 Validate Testbed

The testbed was designed to quickly and flexibly switch between the architecture variants outlined in Section 6.0. Before each evaluation, a validation process was conducted to ensure that essential communication functions operated as expected, maintaining functionality comparable to a conventional network without the added componentry.

In cases where the charger host is a real-world charging system, a charging session is initiated to further validate the setup.

Please refer to Table 7.2 for the procedure.

Table 7.2. Procedure to validate testbed.

Procedural Step	Procedural Action	Validation Notes
1	On charger host: verify OCPP connection is established with the CSMS	Validation of reachability indicates router is routing OCPP application traffic properly to the CSMS host(s) after passing through Patero CryptoQoR gateways and the Palo Alto firewall.
2	On charger host: verify HTTP/HTTPS connection is established with the back-office firmware server	Verification of an established HTTP/HTTPS connection indicates that HTTP/HTTPS application data is properly transmitted and received on the HTTP/HTTPS application port after traffic passes through Patero CryptoQoR gateways and the Palo Alto firewall.
3	Initiate charging session	Power transfer occurs; charging host continuously reports charging transaction to the CSMS.

7.3 Use Case 1 – Mitigating DoS Attacks

The procedures outlined in Table 7.3 utilizes the SaiFlow DoS vulnerability that is described in 3.0. The essential condition is that the CSMS is *publicly accessible from the global internet*, allowing an attacker to connect remotely from anywhere on the global internet. With respect to this attack, it is immaterial if the charger is directly connected to the internet or not. Mitigation techniques and mappings will then be discussed in the next section after demonstrating the outcome.

The legitimate charger will be dropped from the connection in what is effectively a DoS on the charger. The impersonating actor will then have established a communication with the CSMS, which from its perspective still believes the connection to be legitimate. To validate the OCPP connection between an EV charger and CSMS, a `ClearChargingProfile` command is issued to the charger and a response is captured over the wire.

Table 7.3. Procedure to validate use case 2.

Procedural Step	Procedural Action	Validation Notes
1	On CSMS: Issue a `ClearChargingProfile` command to the charger host	Validation of this step indicates that the legitimate charger has maintained a connection to the CSMS up to this step, as the charger would have sent a message response to the `ClearChargingProfile` command.

2	On an adversary machine, attempt to connect to the CSMS host using the legitimate charger host's identity name	
3	Verify OCPP communication is established between the impersonating charger and the CSMS by issuing a `SetChargingProfile` command	Validation of this step indicates that the OCPP connection has been taken over by the impersonating charger. The actor will have received the `SetChargingProfile` command instead of the legitimate charger receiving it.

7.4 Use Case 2 – Minimizing Charger Attack Surface

7.4.1 Authorized Charger Communication Validation

The use case of validating the authorized charger communications seeks to demonstrate how least privilege can be applied and enforced to the charger component of the EV charging infrastructure. Through enforcement of least privilege communications, the surface area of attacks stemming from the charger, which is arguably the component that will have the most day-to-day user interaction, can be diminished greatly.

Table 7.4. Procedure to validate authorized EVSE communication.

Procedural Step	Procedural Action	Validation Notes
1	On the charger host: attempt host discovery by using the `ping` command against another charger on the same network	The expected outcome of this test step is that the Internet Control Message Protocol (ICMP) request from the compromised charger host would be blocked, rejected, or dropped by the Patero security device. Additional traffic types may also be tested to ensure that unexpected traffic is blocked across all protocols.
2	On the charger host: attempt host discovery by using `ping` against another charger on a different network	The expected outcome of this test step is that the ICMP request from the compromised charger host would be blocked, rejected, or dropped by the Patero security device, preventing the request from propagating past the first network.

7.4.2 Validating Charger to Internet Communication Restrictions

This test showed how private VLANs (PVLANs) can be used to prevent communication between two chargers while still allowing CSMS communication to both chargers. This demonstrates the ability to restrict the types of communication a charger can have within the same VLAN.

Table 7.5. Procedure to validate Charger to internet communication.

Procedural Step	Procedural Action	Validation Notes
1	On the charger host: verify unauthorized external host reachability is prohibited	Verify blocked unauthorized internal-to-external pings to demonstrate an example of an unauthorized outbound connection being dropped by the firewall

2	On the external host: verify unauthorized internal host connectivity is prohibited	Verify that unauthorized external-to-internal pings are blocked to demonstrate an example of an unauthorized outbound connection being dropped by the firewall

7.5 Use Case 3 – Mitigating DNS Poisoning Attacks

In the scenario where an adversary can compromise a DNS server that the chargers are directed to use for resolution (local or at the ISP level), the adversary is then able to sit in the middle between the communications of the charger and whatever resource the charger needs to use for its operations. By moving the DNS to a private cloud Virtual Private Cloud or using an overlay-only DNS, cache poisoning can be mitigated because the adversary would need a direct entry into the cloud or overlay resource to compromise the DNS.

In this functional test, it is demonstrated that external network entities attempting to access nodes in the network will be blocked from propagating inside the network. The following figure shows host connection attempts via ICMP requests but is blocked at the gateway 100.64.0.10. The DNS resolution for a CSMS on the internet and not part of the network is demonstrated. Two treatments are considered—the first treatment includes on-network nodes that use on-network DNS for host resolution, and the second treatment includes on-network nodes that require host resolution via a DNS server outside the network (i.e., ISP or public DNS).

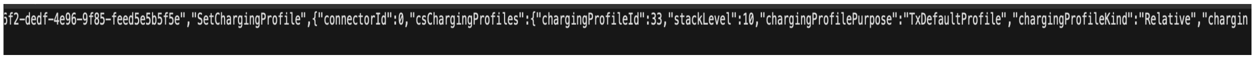
8.0 Results

This section demonstrates the relationship between the use cases, test plan, and results.

8.1 Validate Testbed

8.1.1 CSMS Reachability and OCPP Connectivity

In this test, it was confirmed that the EV charger located in VLAN 101 at 192.168.2.100 can route through QoR1 and QoR2 to reach the on-network CSMS located in VLAN 100 at 192.168.0.250. The traffic is captured at both QoR1 and QoR2 to demonstrate that both security gateways receive the OCPP WebSocket traffic. OCPP connectivity is also demonstrated to be established by the SetChargeProfile command being sent by CSMS and received by the EV charger. This SetChargeProfile message is shown as a packet capture in Figure 8.1.



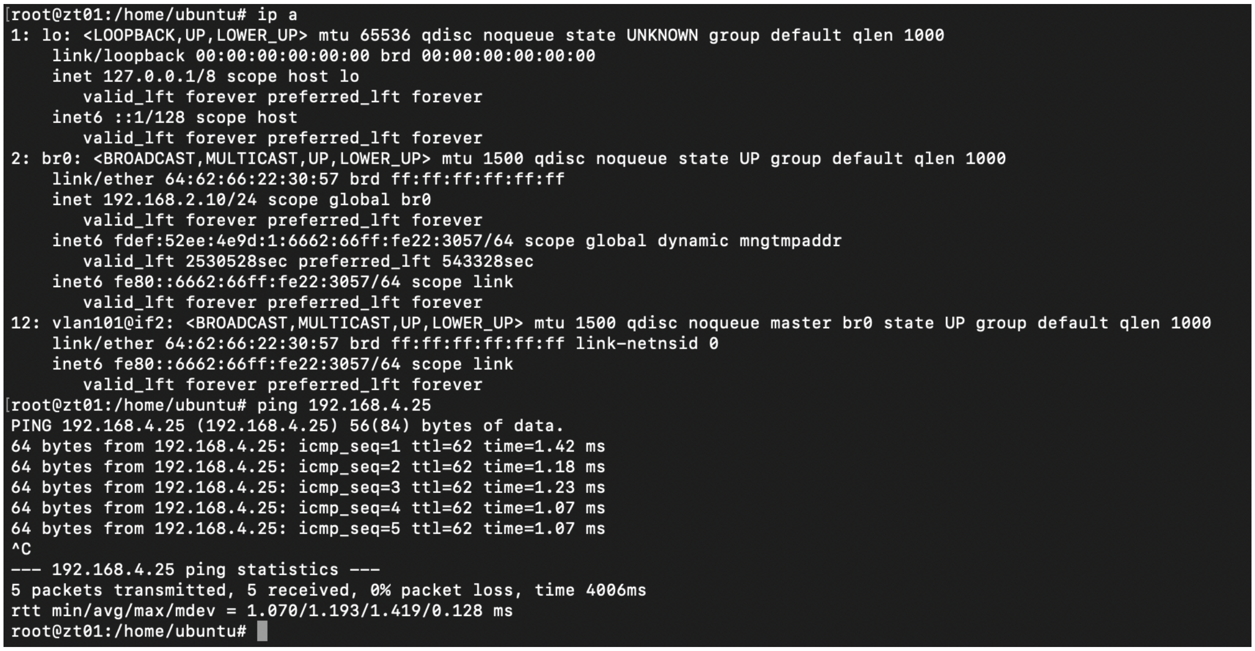
```
5f2-dedf-4e96-9f85-feed5e5b5f5e","SetChargingProfile",{"connectorId":0,"csChargingProfiles":{"chargingProfileId":33,"stackLevel":10,"chargingProfilePurpose":"TxDefaultProfile","chargingProfileKind":"Relative","chargin
```

Figure 8.1. JSON result from a successful TCP connection between CSMS and an EV charger.

8.1.2 HTTP Reachability (Firmware Server)

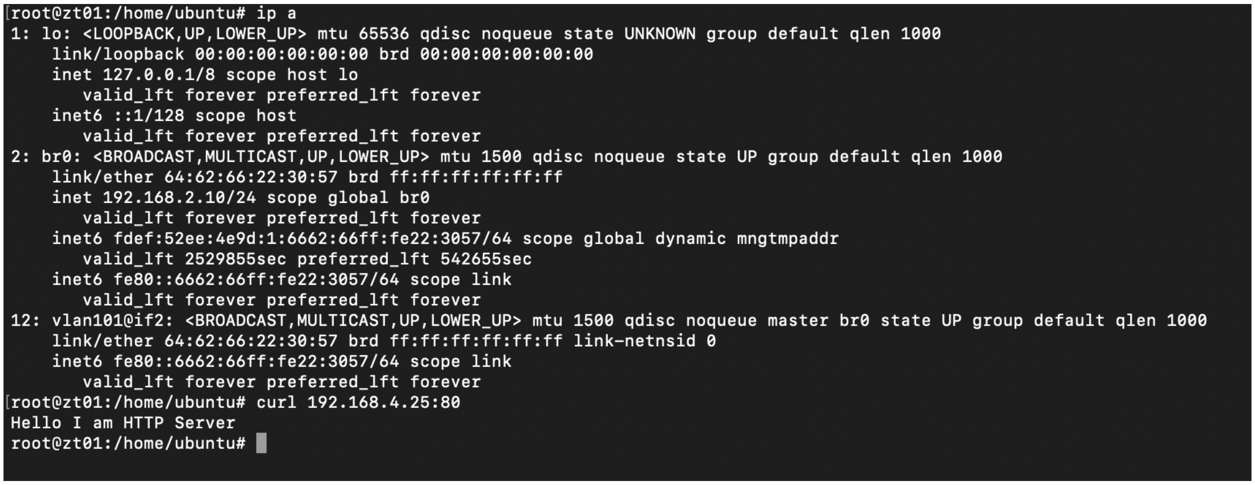
In this functional test, the use case of an EV charger requiring a firmware update and needing to establish an HTTP(S) connection with a back-office firmware server is demonstrated.

Host Connectivity Test result shown in Figure 8.2 validates that the Firmware Server in VLAN 103 at 192.168.4.25 can reach the host on VLAN 101.



```
[root@zt01:/home/ubuntu# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.10/24 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fdef:52ee:4e9d:1:6662:66ff:fe22:3057/64 scope global dynamic mngtmpaddr
       valid_lft 2530528sec preferred_lft 543328sec
    inet6 fe80::6662:66ff:fe22:3057/64 scope link
       valid_lft forever preferred_lft forever
12: vlan101@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
    link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::6662:66ff:fe22:3057/64 scope link
       valid_lft forever preferred_lft forever
[root@zt01:/home/ubuntu# ping 192.168.4.25
PING 192.168.4.25 (192.168.4.25) 56(84) bytes of data.
64 bytes from 192.168.4.25: icmp_seq=1 ttl=62 time=1.42 ms
64 bytes from 192.168.4.25: icmp_seq=2 ttl=62 time=1.18 ms
64 bytes from 192.168.4.25: icmp_seq=3 ttl=62 time=1.23 ms
64 bytes from 192.168.4.25: icmp_seq=4 ttl=62 time=1.07 ms
64 bytes from 192.168.4.25: icmp_seq=5 ttl=62 time=1.07 ms
^C
--- 192.168.4.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.070/1.193/1.419/0.128 ms
root@zt01:/home/ubuntu# 
```

Figure 8.2. Test to demonstrate that the firmware server (192.168.4.25) was reachable from the EV charger (192.168.2.10).



```
root@zt01:/home/ubuntu# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.10/24 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fdef:52ee:4e9d:1:6662:66ff:fe22:3057/64 scope global dynamic mngtmpaddr
       valid_lft 2529855sec preferred_lft 542655sec
    inet6 fe80::6662:66ff:fe22:3057/64 scope link
       valid_lft forever preferred_lft forever
12: vlan101@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
    link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::6662:66ff:fe22:3057/64 scope link
       valid_lft forever preferred_lft forever
root@zt01:/home/ubuntu# curl 192.168.4.25:80
Hello I am HTTP Server
root@zt01:/home/ubuntu#
```

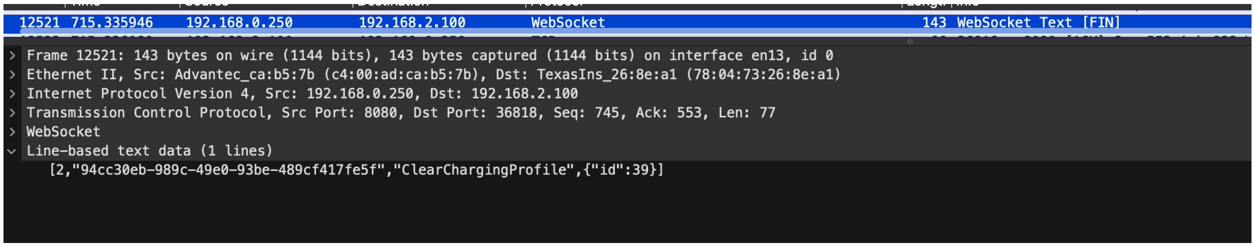
Figure 8.3. Demonstrate route to back office with firmware server.

8.2 Use Case 1: DoS Attack

8.2.1 SaiFlow DoS Attack Demonstration

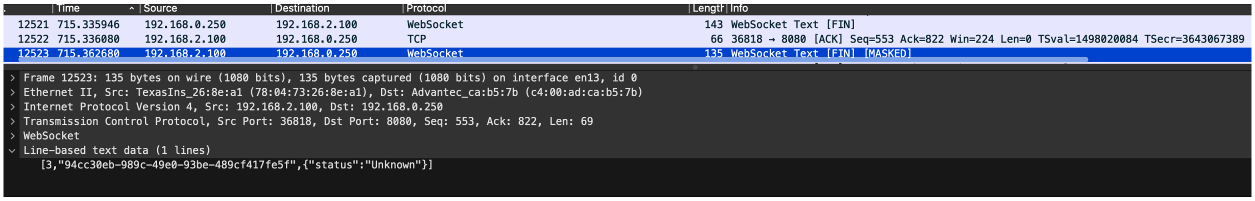
This evaluation is performed in an environment where there are no zero-trust fabric or enforcement policies deployed, the SaiFlow DoS attack can be exercised such that an actor can connect and deny availability to an existing charger to CSMS connection by spoofing the charger's identity. The legitimate charger will be dropped from the connection in what is effectively a DoS on the charger. The impersonating actor will then have established communication with the CSMS, which from its perspective still believes the connection to be legitimate.

In this setup, an EV charger is set up in VLAN 101 with IP address 192.168.2.100 and a CSMS with an interface listening on 192.168.0.250. To validate the OCPP connection between the EV charger and CSMS, a `ClearChargingProfile` command is issued to the charger and a response is captured over the wire.



```
12521 715.335946    192.168.0.250     192.168.2.100     WebSocket                                    143 WebSocket Text [FIN]
> Frame 12521: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface en13, id 0
> Ethernet II, Src: Advantec_ca:b5:7b (c4:00:ad:ca:b5:7b), Dst: TexasIns_26:8e:a1 (78:04:73:26:8e:a1)
> Internet Protocol Version 4, Src: 192.168.0.250, Dst: 192.168.2.100
> Transmission Control Protocol, Src Port: 8080, Dst Port: 36818, Seq: 745, Ack: 553, Len: 77
> WebSocket
v Line-based text data (1 lines)
    [2,"94cc30eb-989c-49e0-93be-489cf417fe5f","ClearChargingProfile",{"id":39}]
```

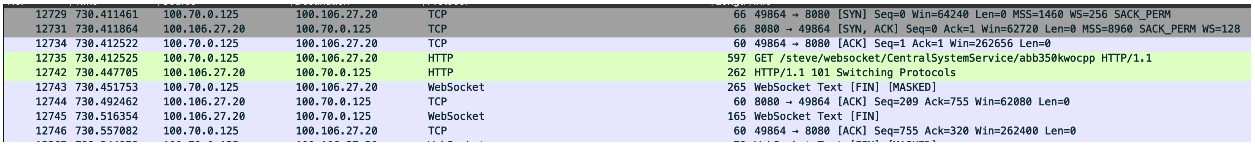
Figure 8.4. A ClearChargeProfile command sent from CSMS to a charger.



```
.     |Time        ^ |Source          |Destination     |Protocol                        |Lengtl|Info
12521 715.335946    192.168.0.250    192.168.2.100    WebSocket                          143 WebSocket Text [FIN]
12522 715.336080    192.168.2.100    192.168.0.250    TCP                                 66 36818 → 8080 [ACK] Seq=553 Ack=822 Win=224 Len=0 TSval=1498020084 TSecr=3643067389
12523 715.362680    192.168.2.100    192.168.0.250    WebSocket                          135 WebSocket Text [FIN] [MASKED]
> Frame 12523: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface en13, id 0
> Ethernet II, Src: TexasIns_26:8e:a1 (78:04:73:26:8e:a1), Dst: Advantec_ca:b5:7b (c4:00:ad:ca:b5:7b)
> Internet Protocol Version 4, Src: 192.168.2.100, Dst: 192.168.0.250
> Transmission Control Protocol, Src Port: 36818, Dst Port: 8080, Seq: 553, Ack: 822, Len: 69
> WebSocket
v Line-based text data (1 lines)
    [3,"94cc30eb-989c-49e0-93be-489cf417fe5f",{"status":"Unknown"}]
```

Figure 8.5. ClearChargeProfile response sent from a charger to CSMS.

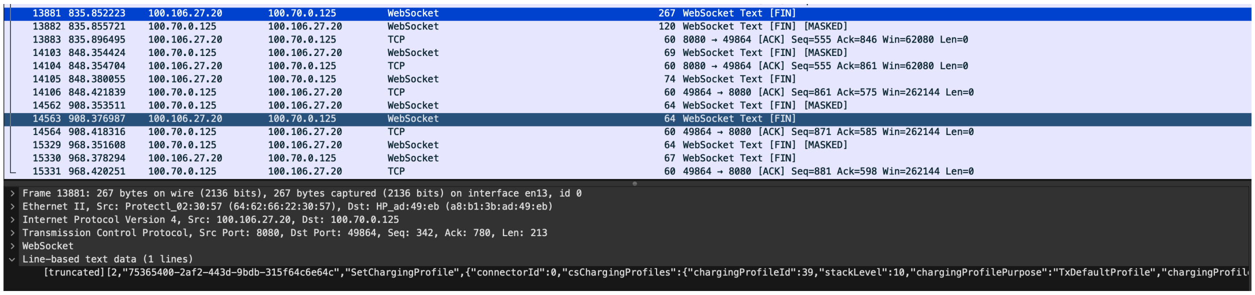
At this point, the actor with an IP address of 100.70.0.25 attempts to take over control of communications from the legitimate charger by establishing a connection to the CSMS on its internet-facing interface of 100.106.27.20 using the charger's profile ID of abb350kwocpp. OCPP has no specification on multiple connections, so the CSMS will accept the most recent connection from any IP because these values are not validated by the CSMS.



```
12729 730.411461   100.70.0.125     100.106.27.20    TCP          66  49864 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12731 730.411864   100.106.27.20    100.70.0.125     TCP          66  8080 → 49864 [SYN, ACK] Seq=0 Ack=1 Win=62720 Len=0 MSS=8960 SACK_PERM WS=128
12734 730.412522   100.70.0.125     100.106.27.20    TCP          60  49864 → 8080 [ACK] Seq=1 Ack=1 Win=262656 Len=0
12735 730.412525   100.70.0.125     100.106.27.20    HTTP        597  GET /steve/websocket/CentralSystemService/abb350kwocpp HTTP/1.1
12742 730.447705   100.106.27.20    100.70.0.125     HTTP        262  HTTP/1.1 101 Switching Protocols
12743 730.451753   100.70.0.125     100.106.27.20    WebSocket   265  WebSocket Text [FIN] [MASKED]
12744 730.492462   100.106.27.20    100.70.0.125     TCP          60  8080 → 49864 [ACK] Seq=209 Ack=755 Win=62080 Len=0
12745 730.516354   100.106.27.20    100.70.0.125     WebSocket   165  WebSocket Text [FIN]
12746 730.557082   100.70.0.125     100.106.27.20    TCP          60  49864 → 8080 [ACK] Seq=755 Ack=320 Win=262400 Len=0
```

Figure 8.6. Spoofed "charger" establishing OCPP connection with the CSMS.

At 835.852223 seconds, the CSMS issues a SetChargingProfile command to 100.70.0.125. Meanwhile, the legitimate charger never receives this command, as seen by the time gap of about 13 seconds in charger traffic 2.



```
13881 835.852223   100.106.27.20    100.70.0.125     WebSocket   267  WebSocket Text [FIN]
13882 835.855721   100.70.0.125     100.106.27.20    WebSocket   120  WebSocket Text [FIN] [MASKED]
13883 835.896495   100.106.27.20    100.70.0.125     TCP          60  8080 → 49864 [ACK] Seq=555 Ack=846 Win=62080 Len=0
14103 848.354424   100.70.0.125     100.106.27.20    WebSocket    69  WebSocket Text [FIN] [MASKED]
14104 848.354704   100.106.27.20    100.70.0.125     TCP          60  8080 → 49864 [ACK] Seq=555 Ack=861 Win=62080 Len=0
14105 848.380055   100.106.27.20    100.70.0.125     WebSocket    74  WebSocket Text [FIN]
14106 848.421839   100.70.0.125     100.106.27.20    TCP          60  49864 → 8080 [ACK] Seq=861 Ack=575 Win=262144 Len=0
14562 908.353511   100.70.0.125     100.106.27.20    WebSocket    64  WebSocket Text [FIN] [MASKED]
14563 908.376987   100.106.27.20    100.70.0.125     WebSocket    64  WebSocket Text [FIN]
14564 908.418316   100.70.0.125     100.106.27.20    TCP          60  49864 → 8080 [ACK] Seq=871 Ack=585 Win=262144 Len=0
15329 968.351608   100.70.0.125     100.106.27.20    WebSocket    64  WebSocket Text [FIN] [MASKED]
15330 968.378294   100.106.27.20    100.70.0.125     WebSocket    67  WebSocket Text [FIN]
15331 968.420251   100.70.0.125     100.106.27.20    TCP          60  49864 → 8080 [ACK] Seq=881 Ack=598 Win=262144 Len=0

> Frame 13881: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface en13, id 0
> Ethernet II, Src: Protectl_02:30:57 (64:62:66:22:30:57), Dst: HP_ad:49:eb (a8:b1:3b:ad:49:eb)
> Internet Protocol Version 4, Src: 100.106.27.20, Dst: 100.70.0.125
> Transmission Control Protocol, Src Port: 8080, Dst Port: 49864, Seq: 342, Ack: 780, Len: 213
> WebSocket
v Line-based text data (1 lines)
    [truncated][2,"75365400-2af2-443d-9bdb-315f64c6e64c","SetChargingProfile",{"connectorId":0,"csChargingProfiles":{"chargingProfileId":39,"stackLevel":10,"chargingProfilePurpose":"TxDefaultProfile","chargingProfil
```

Figure 8.7. Spoofed "charger" responding to the SetChargingProfile command from CSMS.

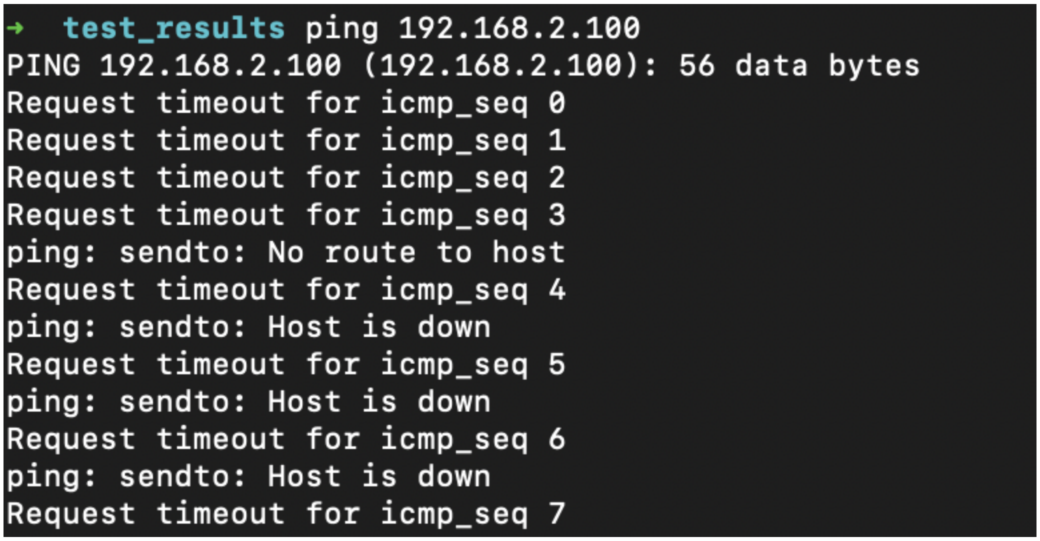
This attack is mitigated within the proposed zero trust architecture variant 1, which uses the Patero CryptoQoR to isolate the chargers and the CSMS within a secure virtual network that is distinct from the internet. Once enabled, neither the chargers nor the CSMS are accessible from the global internet. This inability to connect was verified during the construction of the testbed. The attacker would need to compromise the internal network or gain physical access to the infrastructure, significantly raising the difficulty and complexity of any potential attack.

Variant 3 offers a partial mitigation if the secure cloud-to-cloud communication is employed.

8.3 Use Case 2: Minimized Charger Attack Surface

8.3.1 Charger-to-Charger Communication Blocked with PVLAN Treatment

This test demonstrated the use of PVLANs to block the communications between two chargers. When viewed in conjunction with the subsequent testing results in this section, it can be seen that while charger-to-charger communications are blocked, service to the CSMS for both chargers is still enabled. By establishing that charger-to-charger communication in the same VLAN should be blocked, we limit the types of communication that the charger can establish.

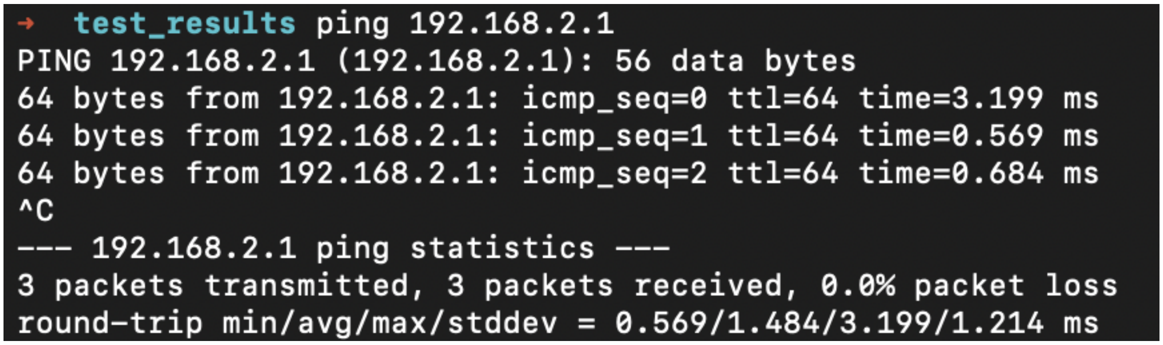


```
➜  test_results ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
ping: sendto: No route to host
Request timeout for icmp_seq 4
ping: sendto: Host is down
Request timeout for icmp_seq 5
ping: sendto: Host is down
Request timeout for icmp_seq 6
ping: sendto: Host is down
Request timeout for icmp_seq 7
```

Figure 8.8. Demonstrate that a charger is unable to communicate to another charger by pinging another charger at 192.168.2.100.

8.3.2 Charger to Gateway Connectivity Enabled with PVLAN Treatment

Using the PVLAN treatment, we demonstrate that hosts can still be allowed to talk with certain services on the network such as the default gateway.

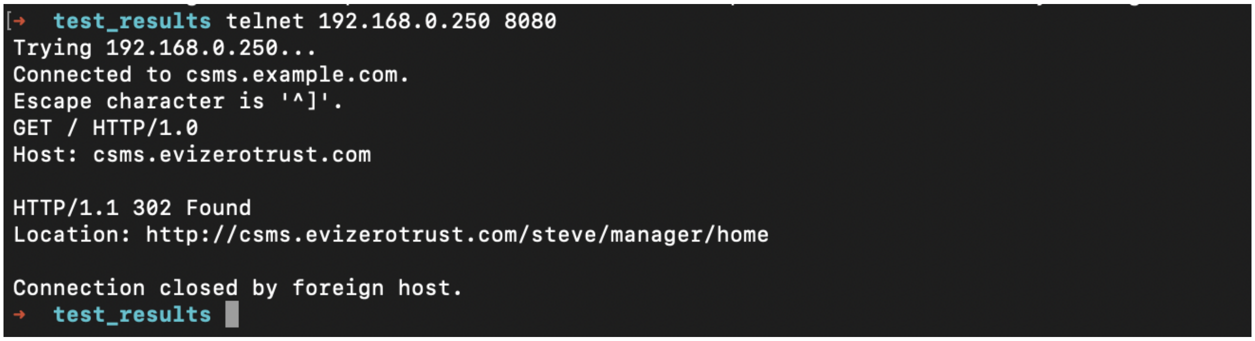


```
➜  test_results ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=0 ttl=64 time=3.199 ms
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.569 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.684 ms
^C
--- 192.168.2.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.569/1.484/3.199/1.214 ms
```

Figure 8.9. Charger can reach the gateway (192.168.2.1) via ping.

8.3.3 Charger to CSMS Communication Enabled with PVLAN Treatment

With the same treatment, it is demonstrated that communication with the CSMS is still enabled.

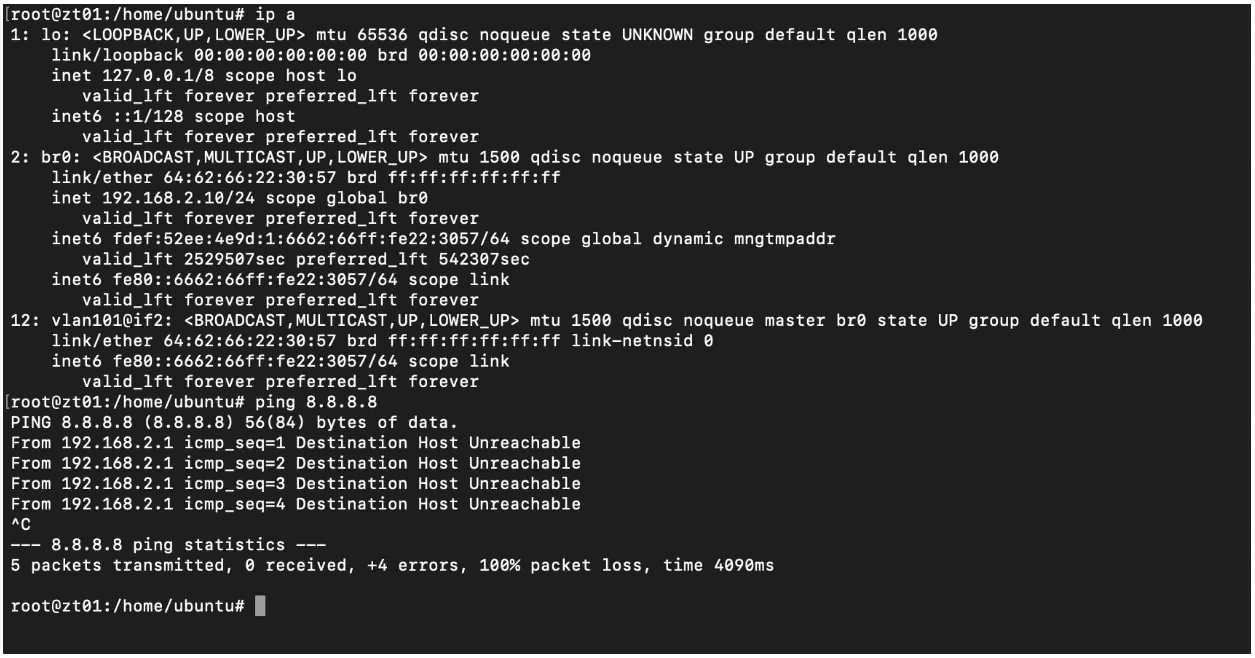


```
[→  test_results telnet 192.168.0.250 8080
Trying 192.168.0.250...
Connected to csms.example.com.
Escape character is '^]'.
GET / HTTP/1.0
Host: csms.evizerotrust.com

HTTP/1.1 302 Found
Location: http://csms.evizerotrust.com/steve/manager/home

Connection closed by foreign host.
→  test_results
```

Figure 8.10. Successful connection request from the charger to CSMS.

8.3.4 Restricted Charger Network Exposure

In this functional test, unauthorized external access from VLAN 101 is attempted. It is demonstrated that within the network, this traffic is blocked and prevented from accessing entities on the internet that are not defined and authorized by policy.

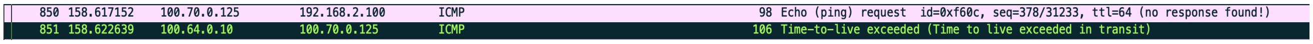


```
[root@zt01:/home/ubuntu# ip a
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
     inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
     inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
 2: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
     link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff
     inet 192.168.2.10/24 scope global br0
        valid_lft forever preferred_lft forever
     inet6 fdef:52ee:4e9d:1:6662:66ff:fe22:3057/64 scope global dynamic mngtmpaddr
        valid_lft 2529507sec preferred_lft 542307sec
     inet6 fe80::6662:66ff:fe22:3057/64 scope link
        valid_lft forever preferred_lft forever
 12: vlan101@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br0 state UP group default qlen 1000
     link/ether 64:62:66:22:30:57 brd ff:ff:ff:ff:ff:ff link-netnsid 0
     inet6 fe80::6662:66ff:fe22:3057/64 scope link
        valid_lft forever preferred_lft forever
[root@zt01:/home/ubuntu# ping 8.8.8.8
 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
 From 192.168.2.1 icmp_seq=1 Destination Host Unreachable
 From 192.168.2.1 icmp_seq=2 Destination Host Unreachable
 From 192.168.2.1 icmp_seq=3 Destination Host Unreachable
 From 192.168.2.1 icmp_seq=4 Destination Host Unreachable
 ^C
 --- 8.8.8.8 ping statistics ---
 5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4090ms

 root@zt01:/home/ubuntu#
```

Figure 8.11. Internal device attempting to reach the internet.

8.3.5 Restricted Internal Network Connection from External Hosts

In this functional test, it is demonstrated that external network entities attempting to access nodes in the network will be blocked from propagating inside the network. The following figure shows host connection attempts via ICMP requests but is blocked at the gateway 100.64.0.10.



```
850 158.617152   100.70.0.125     192.168.2.100    ICMP                                         98 Echo (ping) request  id=0xf60c, seq=378/31233, ttl=64 (no response found!)
851 158.622639   100.64.0.10      100.70.0.125     ICMP                                        106 Time-to-live exceeded (Time to live exceeded in transit)
```

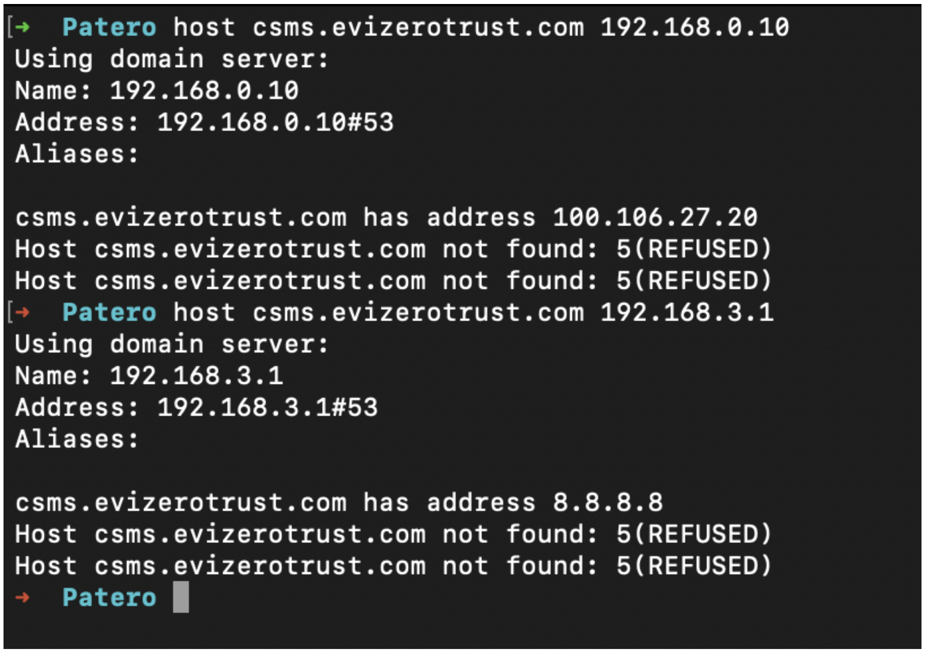
Figure 8.12. Line 850 demonstrates an external unauthorized device (100.70.0.125) attempting to access a device (EV charger at 192.168.2.100) within the zero-trust network.

8.4 Use Case 3: Mitigated External DNS-Cache Poisoning through Exclusive On-Network DNS Resolution

In this functional test, unauthorized external access from VLAN 101 is attempted. It is demonstrated that within the network, this traffic is blocked and prevented from accessing entities on the internet that are not defined and authorized by policy.

The DNS resolution for a CSMS on the internet that is not part of the network is demonstrated. Two treatments are considered; the first treatment includes on-network nodes that use an on-network DNS for host resolution, and the second treatment includes on-network nodes that require host resolution via a DNS server outside of the network (i.e., ISP or public DNS).

In Figure 8.13, the first DNS request using the on-network DNS server at 192.168.0.10 returns the right address of the “public” CSMS. The second query using an off-network server 192.168.3.1 demonstrates how the default server can be poisoned and return an incorrect/malicious IP address tied to the same hostname.



```
[→  Patero host csms.evizerotrust.com 192.168.0.10
Using domain server:
Name: 192.168.0.10
Address: 192.168.0.10#53
Aliases:

csms.evizerotrust.com has address 100.106.27.20
Host csms.evizerotrust.com not found: 5(REFUSED)
Host csms.evizerotrust.com not found: 5(REFUSED)
[→  Patero host csms.evizerotrust.com 192.168.3.1
Using domain server:
Name: 192.168.3.1
Address: 192.168.3.1#53
Aliases:

csms.evizerotrust.com has address 8.8.8.8
Host csms.evizerotrust.com not found: 5(REFUSED)
Host csms.evizerotrust.com not found: 5(REFUSED)
→  Patero
```

Figure 8.13. DNS resolution using on-network servers 192.168.0.10 demonstrates correct resolution of the CSMS server address, while using an external DNS server on 192.168.3.1 demonstrates how DNS can be poisoned with a false address (in this example, 8.8.8.8)

9.0 Conclusion

In this paper, the authors have presented a zero trust architecture designed to bolster the cybersecurity of the EV charging infrastructure. Six security objectives were identified to meet the deny by default, least privilege access, authentication and authorization, secure communications, minimize network exposure, and minimize dependencies on third-party resources and services objectives.

Seven security objectives identified informed the design, providing a robust framework tailored to the unique needs of this essential service. The assessment confirmed that the proposed design effectively meets these objectives, offering a secure foundation for the deployment and management of EV charging stations.

It is important to recognize that adopting a zero trust architecture is not the final goal but rather a pathway toward achieving greater security. Incremental continuous improvements are essential for adapting to evolving threats and technological advancements. This ongoing process underscores the dynamic nature of cybersecurity in the context of emerging technologies like EV charging infrastructure.

As EV chargers become more deeply integrated with smart charge management systems and increasingly responsive to grid event requests, the need for a more robust security posture becomes critical.

Further enhancements to the architecture can be made. For instance, continuous monitoring and analysis of data enables detection of potential security threats in real time. This involves comprehensive surveillance of network activity, which is further enhanced by monitoring physical parameters and leveraging real-time analytics. By correlating data from these various sources, zero trust systems can detect and mitigate potential threats early, before they have a chance to compromise the system. This proactive approach also enables timely responses to minimize exposure and damage when a compromise does occur.

The evaluation reviewed data produced by the system to assess its effectiveness. However, additional work is required to fully understand the properties and effectiveness of the monitoring processes. This includes exploring the integration of advanced analytics, refining detection algorithms, and ensuring that the monitoring infrastructure is capable of scaling with evolving threats and expanding system complexities.

Another enhancement is communication resilience. Adopting zero trust offers additional benefits, one of which is potentially enhanced communication resilience. Zero trust technologies often incorporate strategies that ensure highly available communication channels by integrating multiple communication mediums and providers. This redundancy allows for highly available and reliable communication, even in the event of network failures or physical disruptions.

As EV charging infrastructure evolves to support smart charge management and grid services, communication resilience will become increasingly vital. Reliable communication is essential for managing the complex interactions between EV charging stations and the power grid. This facilitates real-time energy management and response capabilities, enhancing both the stability and efficiency of grid operations as they integrate more dynamic and distributed energy resources.

Although the importance of communication resilience is recognized, it has not yet been fully incorporated into the architecture or assessed through rigorous testing.

Additionally, the development of the secure OCPP gateway by Pacific Northwest National Laboratory was not evaluated in this context but plays a crucial role (Carroll, Edwards, and Chang 2024). This gateway ensures that only authorized OCPP messages are allowed to traverse the network, effectively blocking any unauthorized communications. It addresses the disconnected network operator proposed by Idaho National Laboratory, where an operator inadvertently terminates multiple charging sessions, causing message overloading that is commonly encountered.

10.0 References

"Alpitronic Hypercharger EV Charger | CISA." 2024. May 9, 2024. https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-02.

Alternative Fuels Data Center. 2024. "Alternative Fuels Data Center: Maps and Data - U.S. Public and Private Electric Vehicle Charging Infrastructure." March 2024. https://afdc.energy.gov/data/10964.

Barney Carlson. 2024. "Cyber-Physical Security Pillar." Golden, CO, February 29.

Böck, Hanno. 2023. "Insecure Password Allowed Administrative Access to Electric Vehicle Chargers." December 4, 2023. https://industrydecarbonization.com/news/insecure-password-allowed-administrative-access-to-electric-vehicle-chargers.html.

"Botnet Anatomy." n.d. Cyren. Accessed January 26, 2024. https://www.cyren.com/tl_files/downloads/Botnet_Anatomy_Infographic.pdf.

Carlson, Barney, Kenneth Rohde, Matthew Crepeau, Sean Salinas, Anudeep Medam, and Stacey Cook. 2023. "Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure." Technical Paper 2023-01–0047. SAE.

Carroll, Thomas, Brian Edwards, and Laurence Chang. 2024. "Motivation and Design of the OCPP Security Service." PNNL--35706, 2332876. https://doi.org/10.2172/2332876.

Computer Security Division, Information Technology Laboratory. 2016. "CSF Filters - Cybersecurity Framework | CSRC | CSRC." CSRC | NIST. May 24, 2016. https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters.

"EV201: How an Electric Vehicle Works! | EVgo." n.d. Accessed August 23, 2024. https://www.evgo.com/ev-drivers/charging-basics/how-an-ev-works/.

"Examining Log4j Vulnerabilities in Connected Cars and Charging Stations." 2021. Trend Micro. December 23, 2021. https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html.

Grayson, Nakia R. 2023. "NIST IR 8473 Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure." NIST IR 8473. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8473.

hacsjalano. 2023. "Grizzl-E Smart Firmware V05.621 #442." Open Source. GitHub. March 15, 2023. https://github.com/lbbrhzn/ocpp/issues/442.

Johnson, Jay, Benjamin Anderson, Brian Wright, Jimmy Quiroz, Timothy Berg, Russell Graves, Josh Daley, et al. 2022. "Cybersecurity for Electric Vehicle Charging Infrastructure." SAND2022-9315. Sandia National Lab. (SNL-NM), Albuquerque, NM (United States). https://doi.org/10.2172/1877784.

Johnson, Jay, Timothy Berg, Benjamin Anderson, and Brian Wright. 2022a. "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses." *Energies* 15 (11): 3931. https://doi.org/10.3390/en15113931.

———. 2022b. "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses." *Energies* 15 (11): 3931. https://doi.org/10.3390/en15113931.

Johnson, William. 2023. "Electrify America Bug Opens Hacking Vulnerability Concerns [Updated]." *TESLARATI* (blog). January 30, 2023. https://www.teslarati.com/electrify-america-chargers-hacking-vulnerability-bug/.

Kerman, Alper, Murugiah Souppaya, Parisa Grayeli, Susan Symington, Karen Scarfone, William Barker, Peter Gallagher, et al. n.d. "NIST 1800-35E Implementing a Zero Trust Architecture."

Lakshmanan, Ravie. 2023. "Is Your EV Charging Station Safe? New Security Vulnerabilities Uncovered." The Hackernews. February 3, 2023. https://thehackernews.com/2023/02/is-your-ev-charging-station-safe-new.html.

Maloney, Patrick R., James O'Brien, Thomas E. Carroll, Richard M. Pratt, Lori Ross O'Neil, and Gregory B. Dindlebeck. 2023. "Electric Vehicle Infrastructure Consequence Assessment." PNNL-34072. Pacific Northwest National Laboratory (PNNL), Richland, WA (United States). https://doi.org/10.2172/1989051.

Nasr, Tony, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, and Chadi Assi. 2022. "Power Jacking Your Station: In-Depth Security Analysis of Electric Vehicle Charging Station Management Systems." *Computers & Security* 112 (January):102511. https://doi.org/10.1016/j.cose.2021.102511.

Nist, Gaithersburg Md. 2023. "The NIST Cybersecurity Framework 2.0." NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.

"NSA Releases Maturity Guidance for the Zero Trust Network and Environment Pillar." n.d. National Security Agency/Central Security Service. Accessed July 16, 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3695223/nsa-releases-maturity-guidance-for-the-zero-trust-network-and-environment-pillar/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3695223%2Fnsa-releases-maturity-guidance-for-the-zero-trust-network-and-environment-pillar%2F.

Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. "NIST 800-207 Zero Trust Architecture." National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.

Sanghvi, Anuj, and Tony Markel. 2021. "Cybersecurity for Electric Vehicle Fast-Charging Infrastructure." In *2021 IEEE Transportation Electrification Conference & Expo (ITEC)*, 573–76. Chicago, IL, USA: IEEE. https://doi.org/10.1109/ITEC51675.2021.9490069.

US EPA, OAR. 2020. "Plug-in Electric Vehicle Charging: The Basics." Other Policies and Guidance. September 16, 2020. https://www.epa.gov/greenvehicles/plug-electric-vehicle-charging-basics.

Zhdanova, Maria, Julian Urbansky, Anne Hagemeier, Daniel Zelle, Isabelle Herrmann, and Dorian Höffner. 2022. "Local Power Grids at Risk – An Experimental and Simulation-Based Analysis of Attacks on Vehicle-To-Grid Communication." In *Proceedings of the 38th Annual Computer Security Applications Conference*, 42–55. ACSAC '22. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3564625.3568136.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov