PNNL-35706

Motivation and Design of the OCPP Security Service

March 2024

Thomas E. Carroll
Brian Edwards
Laurence Chang

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-35706

Motivation and Design of the OCPP Security Service

March 2024

Thomas E. Carroll
Brian Edwards
Laurence Chang

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

Pacific Northwest National Laboratory is conducting in-depth research aimed at exploring how zero trust security principles can be effectively applied to electric vehicle charging infrastructure. This investigation seeks to enhance the resilience and reliability of these systems against cyber threats, ensuring secure and uninterrupted access to charging services for electric vehicle users and electric supply.

Zero trust is a security concept centered on the belief that system operators should not automatically trust users or systems based on their location, whether inside or outside the organization, but instead must verify everything trying to connect to their systems before granting access. A key aspect of the project is to demonstrate and validate zero trust approaches targeted to electric vehicle (EV) charging infrastructure. It has been observed that both open-source and commercial solutions often overlook the specific protocols employed in managing EV charging stations and proceeded with a general, protocol-agnostic approach. While these strategies effectively block non-authorized routes to the charging infrastructure, they do not tackle the situations where attackers may exploit legitimate access channels, such as the inattentive operator model posited by the Idaho National Laboratory.

To address this gap, this paper proposes and discusses a new security service targeted to the Open Charge Point Protocol (OCPP), which is the de facto protocol for the management of charging stations and serves a critical role in the broader adoption of electric vehicles. The design and architecture of the proposed OCPP security service are discussed in detail, outlining how it aims to safeguard charging station management system (CSMS) functions. The service is particularly important in scenarios where the charging station operator (CSO), responsible for the maintenance and operation of charging stations, and the charging network provider (CNP), which manages the charging network's accessibility and billing, are separate entities. This distinction is crucial because CSOs and CNPs often have different priorities, objectives, and operational responsibilities, which may not always align perfectly. For instance, a CSO might prioritize uptime and customer satisfaction, while a CNP might focus on maximizing revenue and network utilization. Such misalignment can create security vulnerabilities, as each entity might implement different policies and standards, potentially leaving gaps in the overall security posture.

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.

Acronyms and Abbreviations

CNP	charging network provider
CSMS	charging station management system
CSO	charging station operator
EV	electric vehicle
INL	Idaho National Laboratory
JSON	JavaScript Object Notation
JWS	JSON Web Signature
NEVI	National EV Infrastructure
OCPP	Open Charge Point Protocol
PNNL	Pacific Northwest National Laboratory

Contents

Figures

Tables

1.0 Introduction

Electric vehicle (EV) owners, prospective buyers, and industry experts all share concerns over the adequacy of the EV charging infrastructure. The Bipartisan Infrastructure Law, authorized on November 15th, 2021, marks a transformative step in the acceleration of EV charging infrastructure across the United States. The legislation earmarks a total of $7.5 billion specifically for the development of EV charging stations, allocating $5 billion of this fund to support the National Electric Vehicle Infrastructure (NEVI) program. This pivotal move is expected to catalyze a nationwide buildout, significantly enhancing the accessibility and convenience of EV charging, thereby facilitating a smoother transition for Americans toward cleaner mobility and addressing a significant barrier for EV adoption.

The widespread electrification of transportation systems will markedly increase electricity demand, forging a significant link between the previously distinct sectors of electric supply and transportation. This integration will broaden the scope and amplify the risks of cyberattacks. The concern is that rapid expansion of infrastructure, spurred by the rapid adoption of EVs and funding from the Bipartisan Infrastructure Law, without sufficient care, may introduce pervasive vulnerabilities, heightening the potential of cyberattacks that could disrupt both the electric supply and transportation networks. It is imperative that joint resilience strategies are adopted, treating the components as a single, integrated ecosystem, to avoid cascading effects that could disrupt essential services and economic activities.

To bolster the cybersecurity stature of EV charging infrastructure, Pacific Northwest National Laboratory is currently conducting in-depth research aimed at exploring how zero trust security principles can be effectively applied to electric vehicle charging infrastructure. This investigation seeks to enhance the resilience and reliability of these systems against cyber threats, assuring secure and uninterrupted access to charging services for electric vehicle users and electric supply. Stated simply, *zero trust* is a security concept that assumes no entity, inside or outside the network, should be automatically trusted (referred to as *implicit trust*). A key aspect of the project is to demonstrate and validate zero trust approaches targeted to EV charging infrastructure. It has been noted that both open-source and commercial solutions often overlooked the specific protocols employed in managing EV charging stations and proceeded with a general, protocol-agnostic approach. While these strategies effectively block non-authorized paths to the charging infrastructure, they do not tackle the situations where attackers may exploit legitimate access channels. One such a scenario is Idaho National Laboratory’s inattentive charging station operator (CSO) model, where a CSO employee absent-mindedly terminates charging at several charging stations [4]. The loss of load triggers a voltage transient, where the initial rapid rise in voltage may cause other protective devices to trip, disrupting power for consumers sharing the feeder.

To address this gap in protocol-agnostic zero trust, this paper proposes and discusses a security service targeted to the Open Charge Point Protocol (OCPP), which is the de facto protocol for the management of charging stations and serves a critical role in the broader adoption of electric vehicles. The design and architecture of the proposed OCPP security service, which sits inline in the communication between the charging station and charging station management system (CSMS), are discussed in detail, outlining how it aims to safeguard management, monitoring, and control functions. The service is specifically designed to address the particularly important scenarios where the CSO, responsible for the maintenance and operation of charging stations, and the charging network provider (CNP), which manages the charging network's accessibility and billing, are separate entities. This distinction is crucial because CSOs and CNPs often have different priorities, objectives, and operational responsibilities, which may not always align perfectly. For instance, a CSO might prioritize uptime and customer satisfaction, while a CNP might focus on maximizing revenue and network utilization. Such misalignment can create security vulnerabilities, as each entity might implement different policies and standards, potentially leaving gaps in the overall security posture.

2.0 Motivation

Pacific Northwest National Laboratory's efforts to secure EV charging infrastructure with zero trust has resulted in the demonstration of a variety of designs, approaches, and benefits that increase the cybersecurity posture of such environments. Beyond security, the project also considers how zero trust can be used to also support business objectives, such as access to a remote population of operators. At the core of zero trust is the least privilege principle, an information security concept that suggests individuals and systems granted the necessary minimum level of access or permission to perform their designated tasks. The use of least privilege policies governs charger networks accesses such that they allow for operational continuity while preventing chargers from reaching unauthorized hosts and services, whether operating locally or externally. Use of software-defined wide area network technologies and secure tunnelling also allow for the critical infrastructure resources to be accessed and operated over public networks, but not exposed to direct attacker threats. Infrastructure owners and operators can reach such “dark” services over private DNS, which then provide an end-to-end access to said resources, given the condition that they are authorized to do so using mechanisms that can be enforced by multi-factor authentication approaches, such as time-based one-time password.

Despite the promise of project results, there remains gaps in how existing open-source and commercial zero-trust products handle the OCPP and the distinct organizations involved in charging. The OCPP, a communication protocol that is used in EV charging stations to enable communication between charging stations and a CSMS, allows for the monitoring, control, and management of EV charging stations. Importantly, a CSO, the entity that owns and operates the chargers and supporting equipment, may be distinct from the CNP, the entity that operates the charging network. The technologies described above enforce authorized traffic types allowed on the network, meaning that any paths undefined by policies are unavailable for communication. Attackers will evolve to identify and employ these authorized paths. A key finding of the analysis of these technologies, is that they do not enforce the allowed data types that are authorized to be transmitted or received. There also exist certain high consequence events [4], in which excessive load shed during extreme fast charging of EVs results in power outages and grid degradation, a characteristic that is not addressed by OCPP or the grid network as they are deployed today. The ability to not only authenticate these per-request communications, but also authorize their message types is crucial to protecting the integrity of the actions EV charging stations and CSMS are attempting to perform and enforce only those actions that are necessary for the operational use cases. While OCPP may be the only allowed protocol to be sent and received in a network, malicious actors may piggyback on the lack of authorization within the protocol to exploit vulnerabilities of EV charging stations, which can be executed when a malicious actor spoofs the charger ID of an existing charge customer, causing the CSMS break in handling multiple connections and ultimately resulting in a loss of service to the CSMS [1].

PNNL has proposed developing an OCPP security service to fill these gaps. The security service would sit between the charger and the CSMS, where it may intercept, analyze, and process OCPP packets as they flow through the network, forwarding those that are authorized as defined by the security service policies, or deny them if they do not adhere to policy. This approach covers both the transport and data security in EV charging networks.

3.0 Background

As electric vehicles become more widely used, the demand for electric vehicle charging infrastructure increases. To efficiently and cost effectively manage and operate larger networks of charging stations that are deployed on a site, as well as orchestrate the communications and operations between chargers and cars, a charging station management system, or CSMS, is deployed to control which specific charger can connect to an EV purchasing a battery charge. The CSMS may either be located locally at the charging site or may be operated remotely in a cloud data center. The charger and the CSMS communicate using Open Charge Point Protocol (Figure 1).

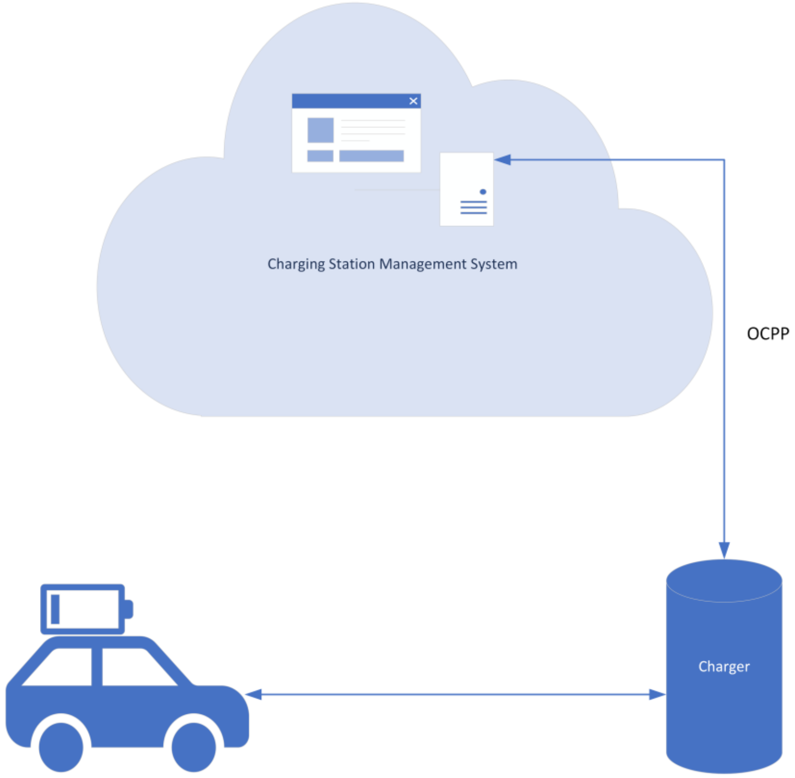

Figure 1 The charging station communicates with the CSMS using OCPP

OCPP plays a crucial role in ensuring the efficient and standardized operation of electric vehicle charging infrastructure, contributing to the growth and adoption of electric mobility. The current version of OCPP is 2.0.1, released March 31, 2020. A second edition was released December 12th, 2022. While the prior version of OCPP (OCPP 1.6J) continues to be extensively used, it lacks the advanced security measures found in the latest version, making it less secure by comparison.

OCPP has become the *de facto* protocol for charging station monitoring, control, and management. Key features of OCPP include:

- Standardized Communication: OCPP provides a standardized way for charging stations and central management systems to communicate with each other. This standardization promotes interoperability among different manufacturers' charging infrastructure and charge network providers.

- Remote Management: OCPP allows for comprehensive remote management of charging stations, including functionalities such as starting or stopping a charging session, retrieving charging station status, configuring charging station functions, and updating firmware.

- Real-time Data: The protocol supports real-time data exchange, enabling monitoring of charging station status, energy consumption, and other relevant information.

OCPP is characterized by its bidirectional request-response nature. The charging station establishes the connection to the CSMS, which is either on-site or operating remotely in a cloud. Requests can be initiated by either the charging station or the CSMS. OCPP messages are encoded in JavaScript Object Notation (JSON), a lightweight data-interchange format that is easy for humans to read and write, and easy for machines to parse and generate. At the lower protocol levels, OCPP operates over WebSocket, which is a protocol that provides simultaneous two-way communication channels over a single TCP/IP or TLS connection.

Certain requests to OCPP originating from a CSMS may trigger the charger to access remote network resources. For instances, a firmware update request contains a URL of the network path to the firmware file. As part of the firmware update process, the charging station would download the file from the specified path.

4.0 Architecture and Design

The OCPP security service is designed to ensure that all communications between the charging station and the Charging Station Management System requirements established by the CSO. This dual assurance safeguards the integrity of OCPP operations, guaranteeing that each action and command is both technically sound and strategically aligned. It effectively bridges the gap inherent in protocol-agnostic zero trust approaches; namely, the potential for attackers to exploit authorized pathways for malicious purposes. It enhances security by intercepting and validating OCPP messages against established contextual business rules and the system's current state, thereby safeguarding against malicious threats and minimizing the risk of significant incidents. Figure 2 depicts where the OCPP security service is positioned within the charging station-CSMS communication pathway. Incoming OCPP messages (versions 1.6 and 2.0.1 are supported) need to be inspected and pass a rule criterion enforced by the OCPP security service before being accepted, and then being routed to its destination. The criteria that the security service validates to assess whether a message should be passed are illustrated in Figure 3. Besides validating incoming messages through a rule criterion, the security service is also in charge of deciding at what point in time a rule-passed message can be routed to its destination through use of charger-state querying. The security service inserts notes about the ongoing charger-CSMS conversation into its internal database to increase visibility of the charger and CSMS state. This information collected allows the security service to know when to send out a certain message in a given moment. Bringing it all together, the security service fits into the zero trust architecture as it verifies the behavior of the charger and the CSMS, and complements protocol-agnostic zero trust network approaches. As part of this objective, the security service verifies all incoming OCPP messages to assure the messages conform with OCPP standards and best OCPP security practices. Even if the message source is seen as trusted on a network level, it still could become compromised and be allowed to send any OCPP messages, including ones that trigger a high-consequence event.

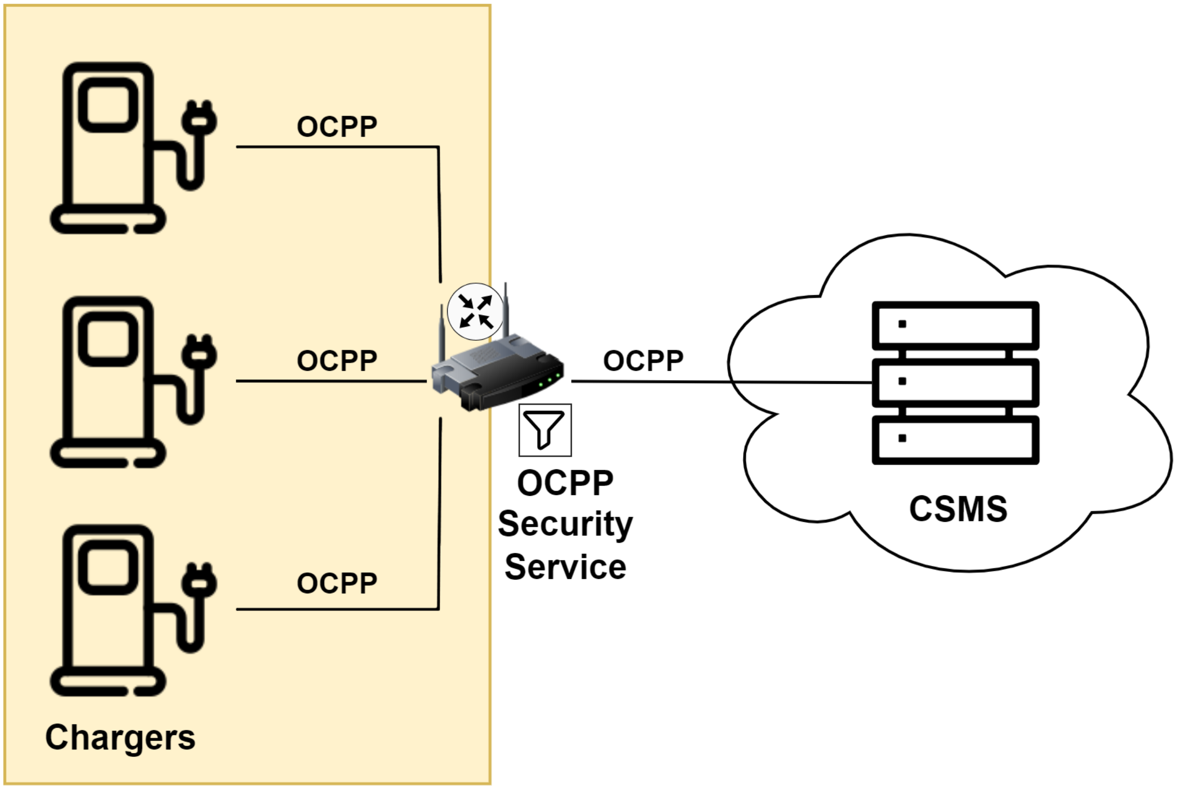

Figure 2 Communication flow between a charging station and CSMS

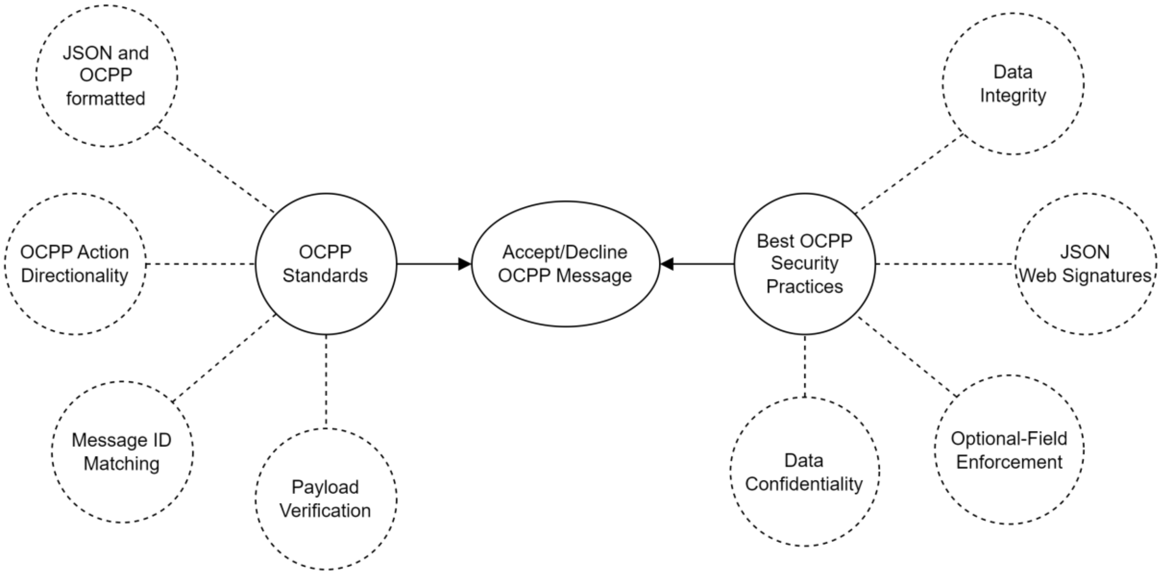

Figure 3 Security service message acceptance decision factors

Component Description

The main components of the security service are the message rules, special case message handler, message queue, charger information database, and aggregated charger message handler (which are all architecturally visualized in Figure 4). The message rules are responsible for deciding whether an incoming OCPP message should be accepted or declined based on format and structural rules. The special case message handler processes messages based on the message's action on a single charger level. The message queue holds rule-passed OCPP messages and routes them to their destination when specified, either implicitly or explicitly, by the rules. The charger info database holds information about chargers, such as their states and their current and past sessions and transactions. Finally, the aggregated charger message handler processes messages based on the message's action on a multiple charger level.

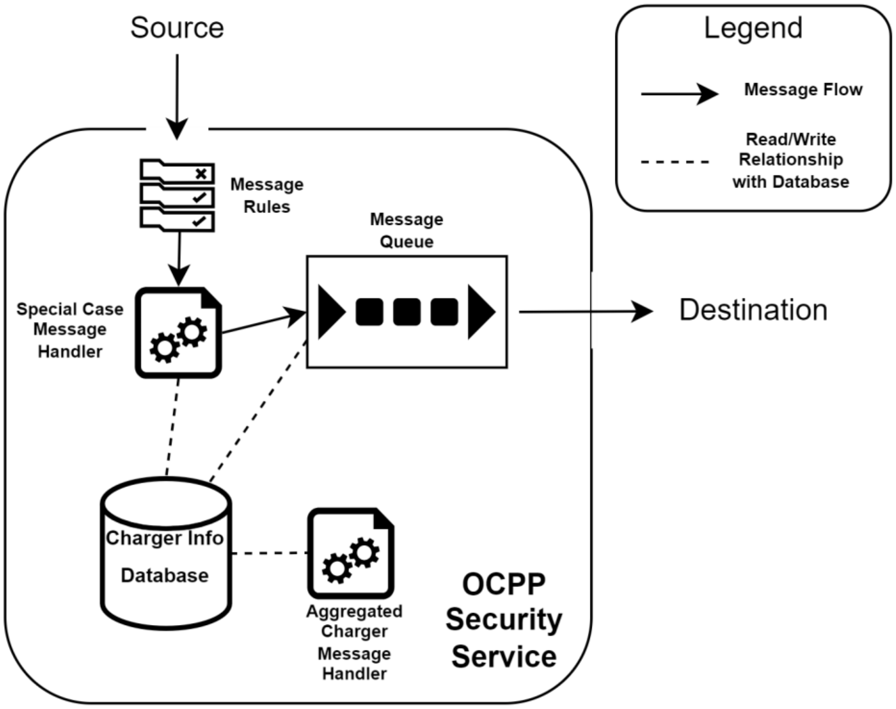

Figure 4 OCPP security service architecture

Detailed Description

When a charger initiates a connection to the CSMS, it does so by first connecting, knowingly or unknowingly, to the OCPP security service. There are two general approaches to connect to the OCPP security service: (i) the charger can be configured to directly connect to the OCPP security service, or (ii) the zero trust network can be configured to transparently route the relevant communications to the OCPP security service, meaning that the charging station is unaware of the existence of the security service. The OCPP security service can be operated as: (i) a cloud-based service or (ii) a directly integrated, locally deployed router or gateway, which is positioned near the charging station to facilitate communications.

When the OCPP security service receives a connection request from the charging station, the OCPP security service will handle that connection in a network namespace that is isolated from the other connections, as illustrated in Figure 5. By utilizing isolation, charger network access is explicitly managed, limiting communication access to other chargers or network resources. By keeping a potential threat contained to one charger, it removes a multitude of risks associated with inter-charger communication, such as denial of service attacks to knock other chargers offline. Figure 6 provides a visualization of this attack prevention.

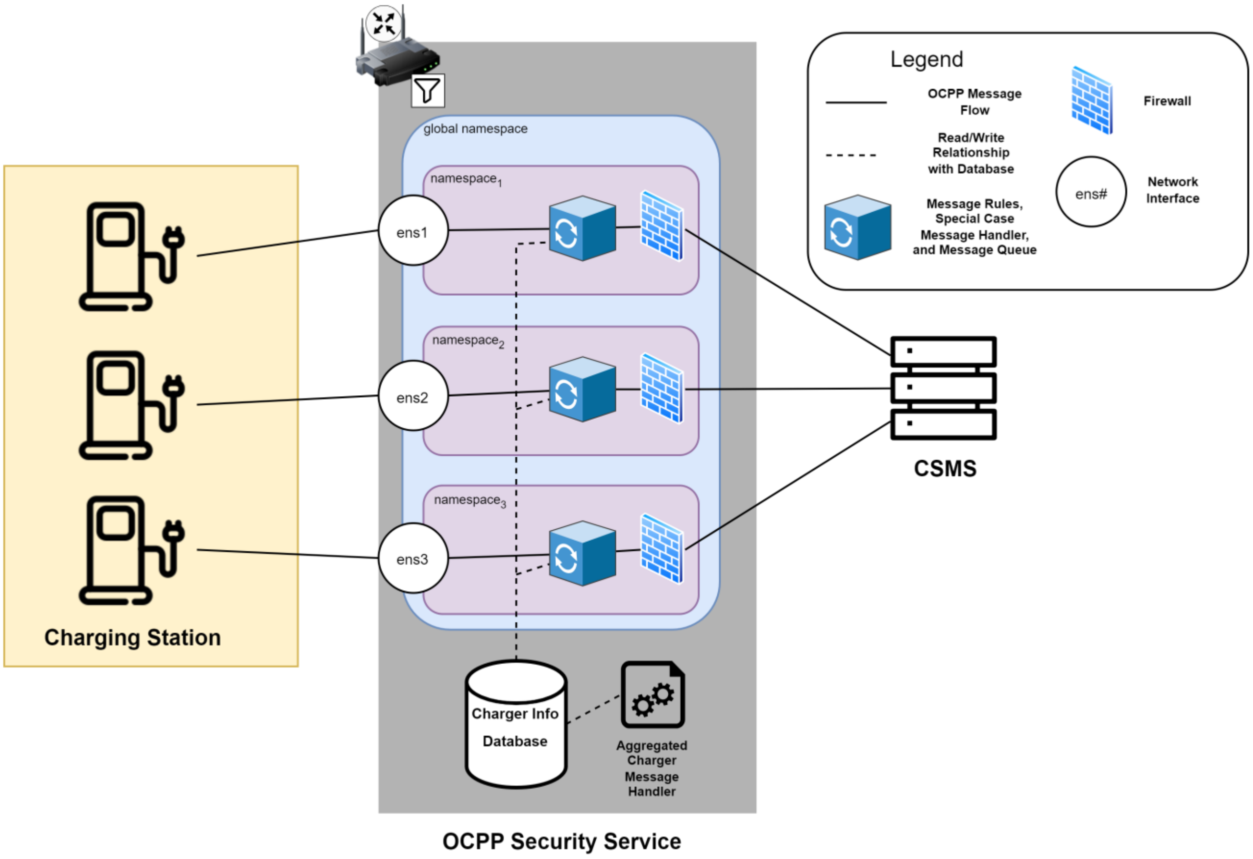

Figure 5 OCPP security service namespace architecture and message flow

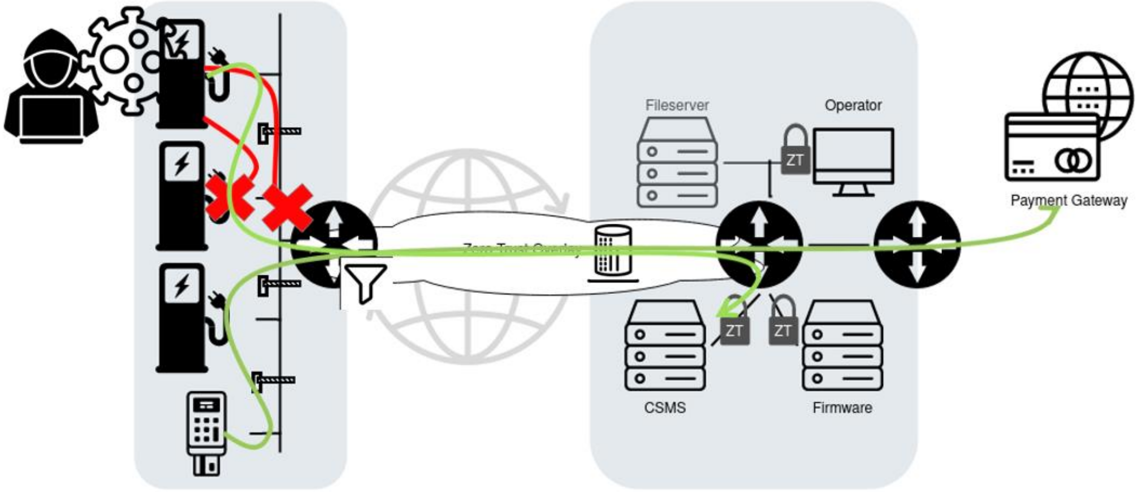

Figure 6 An attacker on one of the chargers is not allowed to make new connections or talk to other chargers

If the charger is connecting for the first time, the security service verifies with the charger information database whether the charger's identifier is already considered active. If the charger is not considered already active, the security service begins a corresponding connection to the CSMS, to allow the charger to communicate to the CSMS. If the charger is considered already active, the security service disconnects this new connection. This measure partially reduces the risk posed by spoofed charger identifiers, which can lead to confusion at the CSMS. Such confusion may result in messages being incorrectly routed to an attacker or the legitimate charger being disconnected, ultimately leading to a denial-of-service attack against the legitimate charger [1], also visualized in Figure 6.

For every OCPP message that comes through, whether it comes from the charger or the CSMS, it will first go through the security service’s OCPP message format and structure rules. If any of the rules fail on a message, the security service will either: return an OCPP error message back to the source, drop the message, or close the connection. The decision is chosen based on severity of the rule that failed and whether it can send an OCPP message back or not (only Call messages must have their messages returned, not Call Results or Call Errors [2]). The message rules, the action the security service takes when the rule fails, and the mitigated risk(s) are defined in order in Table 1.

Table 1 OCPP security service message format and structure rules

ID Number	Message Rule	Action when Rule Fails	Mitigated Risk(s)	Figure 2 Factor
0	Message is JWS[1] decodable (only applies for CSMS originated messages)	Close connection	Non-CSMS originated message attacks	JSON Web Signatures
1	Message is JSON[2] and OCPP formatted	Close connection	Non-JSON/non-OCPP formatted message attacks	JSON and OCPP formatted
2	Message action is legitimate and is allowed to be sent from the source (e.g., a charger should not send an "UpdateFirmware" message) [2]	Reply with Call Error	Denial of Service if destination can't handle irregular message action	OCPP Action Directionality
3	Call Result/Call Error message ID has a corresponding Call message ID	Drop message	Denial of Service by sending many Call Result/Call Errors	Message ID Matching
4	Message payload follows OCPP standards	Reply with Call Error (for Call) or Drop Message (for Call Result)	Denial of Service if destination can't handle irregular message payload	Payload Verification
5	"UpdateFirmware" message includes the optional ([2]) "signingCertificate" key value pair	Reply with Call Error	Malicious (defined by a virus or a downgrade) firmware installation	Optional Field Enforcement

Notes: [1]JWS – JSON Web Signature; [2]JSON - JavaScript Object Notation

After passing the rules, the message is a step closer to being put into queue. Now, the special case message handlers are triggered based on the message action. The current implementation tends to only "RemoteStartTransaction" and "RemoteStopTransaction" (OCPP 1.6) and "RequestStartTransaction" and "RequestStopTransaction" (OCPP 2.0.1). These are messages that relate to voltage modification and can be abused if many of these messages are sent at the same time to different chargers and lead to HCE #1[3], a voltage transient. The electrical demand could lead to overvoltage or undervoltage consequence events. To prevent such a consequence event, the special case handler will store the matched message in the charger info database (instead of allowing the message to be immediately sent to the charger), and then it will instead reply back to the CSMS with a CallResult of the successful action. Using information from the charger information database, the aggregated charger message handler (Figure 4) holds on to the voltage modification messages from all chargers and, based on a timer, it will send the messages to their corresponding message queues in intervals; e.g. two messages every 10 seconds. Future implementations will add more measures to other message actions in both the special case message handler and aggregated charger message handler.

At this point, the message is inserted into the message queue. The message queue is a priority queue that is ordered based on message arrival timestamp. The queue policy ensures that earlier messages are sent before later received messages. Call messages are sent out when no other Call message is in the conversation flow at the time, which is known via the charger information database, as only one Call message at a time is allowed in an OCPP connection [2]. However, all Call Result and Call Error messages are sent out without any requirements, even if they are behind a Call message in the queue.

5.0 Future Work

Besides the OCPP-focused security features addressed in the paper and implemented in the gateway, other OCPP-related security measures are planned. Future work will address additional security weaknesses associated with the OCPP 2.0.1 protocol [4], such as preventing the CSMS from changing the charging profile on the charger to any (potentially malicious) charging profile (via “SetChargingProfile”). Each of those security measures will also be applied to OCPP 1.6, when possible. Additionally, a local firmware server within the security service is planned. The purpose of this is to facilitate the firmware update process and prevent the charger from relying on remote network resources—like the unsafe Internet—to fetch a potentially malicious firmware update. The security service will download and scan the firmware update, and if concluded as safe, it will be presented to the charger for installation. Other future work includes TLS integration, preventing OCPP “over-messaging” scenarios, preventing chargers from connecting to the CSMS directly and skipping the security service, and smart charging features, such as reenforcing charging profiles if a charger disconnects and reconnects.

Customer-oriented future work includes allowing charging station operators to configure the security service to their liking on a proper management system that would contain multiple OCPP security services throughout a region.

6.0 References

1. Saposnik, L. R., and D. Porat. 2023. “Hijacking EV Charge Points to Cause DoS.” Saiflow. Last Modified February 1, 2023. Accessed February 13, 2024. https://www.saiflow.com/blog/hijacking-chargers-identifier-to-cause-dos/.

2. “OCPP 2.0.1, Protocols, Home - Open Charge Alliance.” n.d. Www.openchargealliance.org. https://openchargealliance.org/my-oca/ocpp/.
3. Carlson, B., Rohde, K., Crepeau, M., Salinas, S. et al. 2023. "Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure," SAE Technical Paper 2023-01-0047. https://doi.org/10.4271/2023-01-0047.

4. Alcaraz, C., J. Cumplido, and A. Triviño-Cabrera. 2023. “OCPP in the Spotlight: Threats and Countermeasures for Electric Vehicle Charging Infrastructures 4.0.” *International Journal of Information Security* 22 (5): 1395–1421. https://doi.org/10.1007/s10207-023-00698-8.

Pacific Northwest National Laboratory

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

1-888-375-PNNL (7665)

www.pnnl.gov