CheckOCPP: Automatic OCPP Packet Dissection and Compliance Check

Soumaya Boussaha, ACSW'25, 30th June 2025

Authors

Soumaya Boussaha
SAP, EURECOM
Biot, France
soumaya.boussaha@sap.com

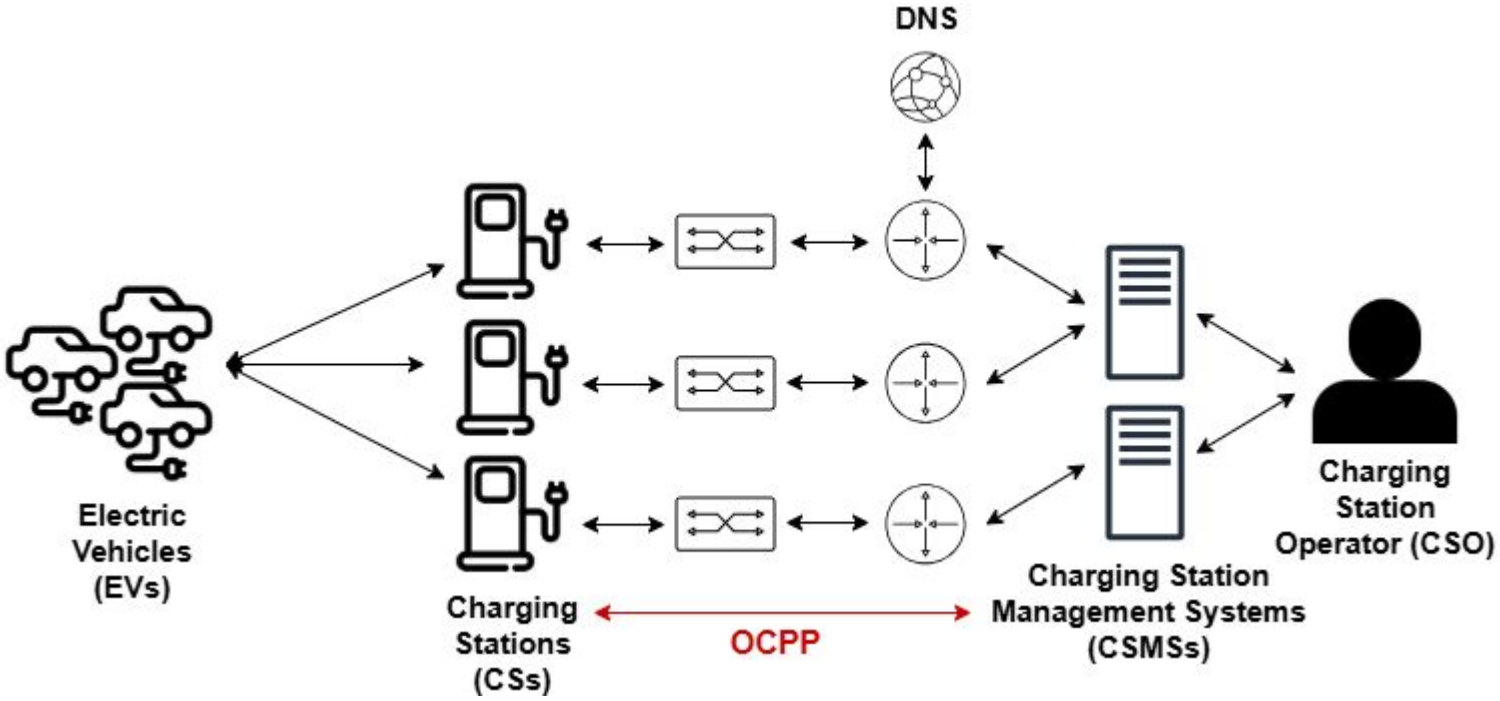
Victor Fresno Gómez
EURECOM, UPM
Madrid, Spain
victorfresno@live.com

Thomas Barber
SAP
Baden-Wurtemberg, Germany
thomas.barber@sap.com

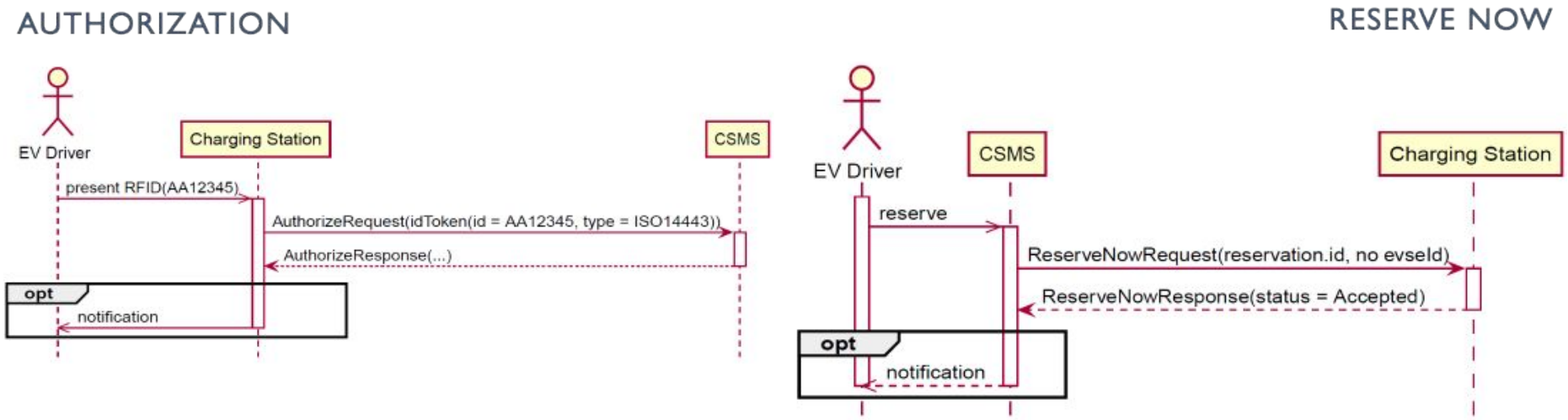
Daniele Antonioli
EURECOM
Biot, France
daniele.antonioli@eurecom.fr



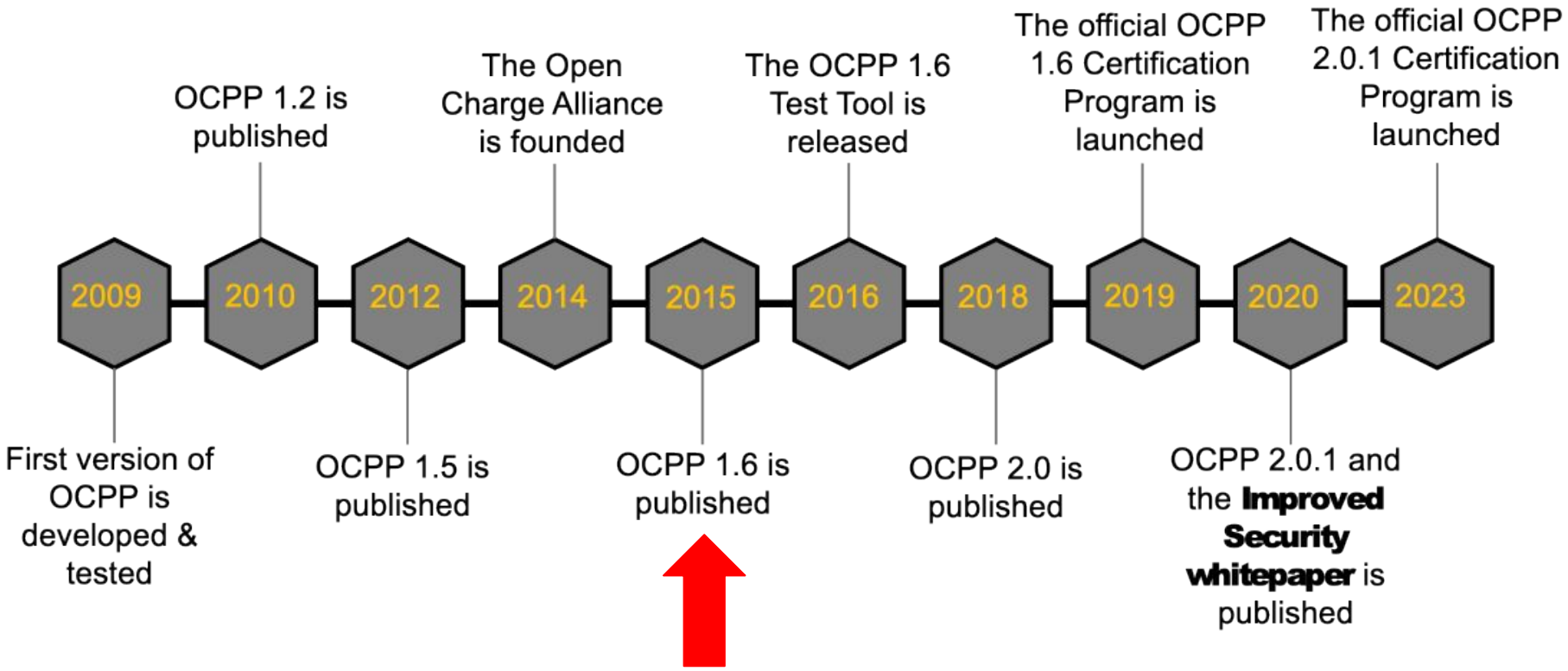

Open Charge Point Protocol (OCPP)



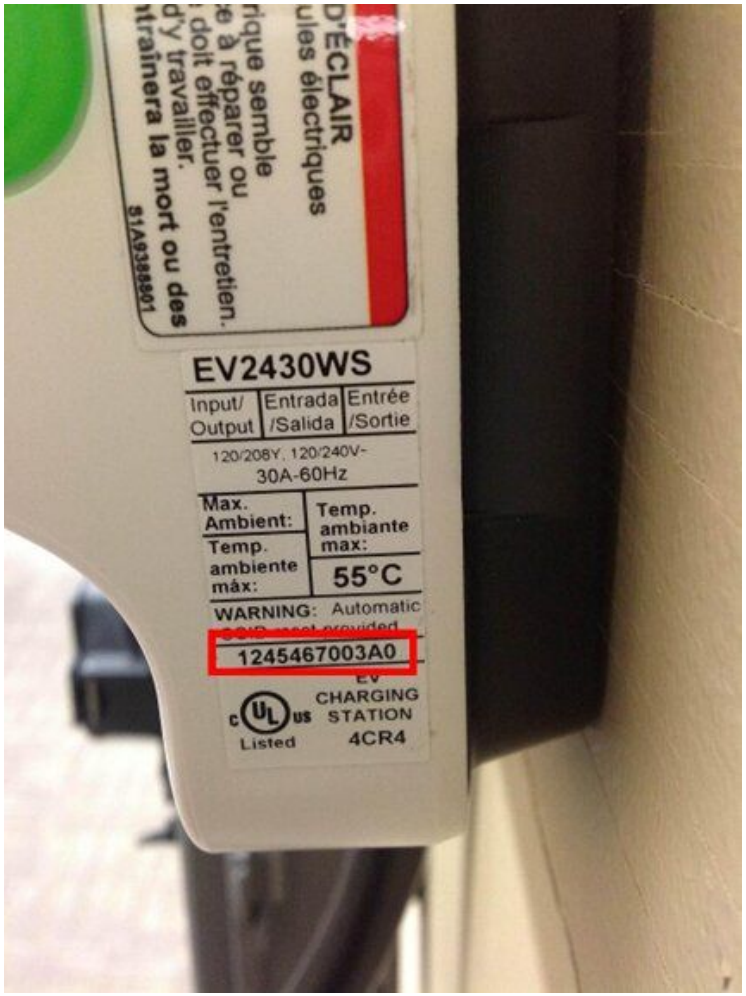
Open Charge Point Protocol (OCPP)



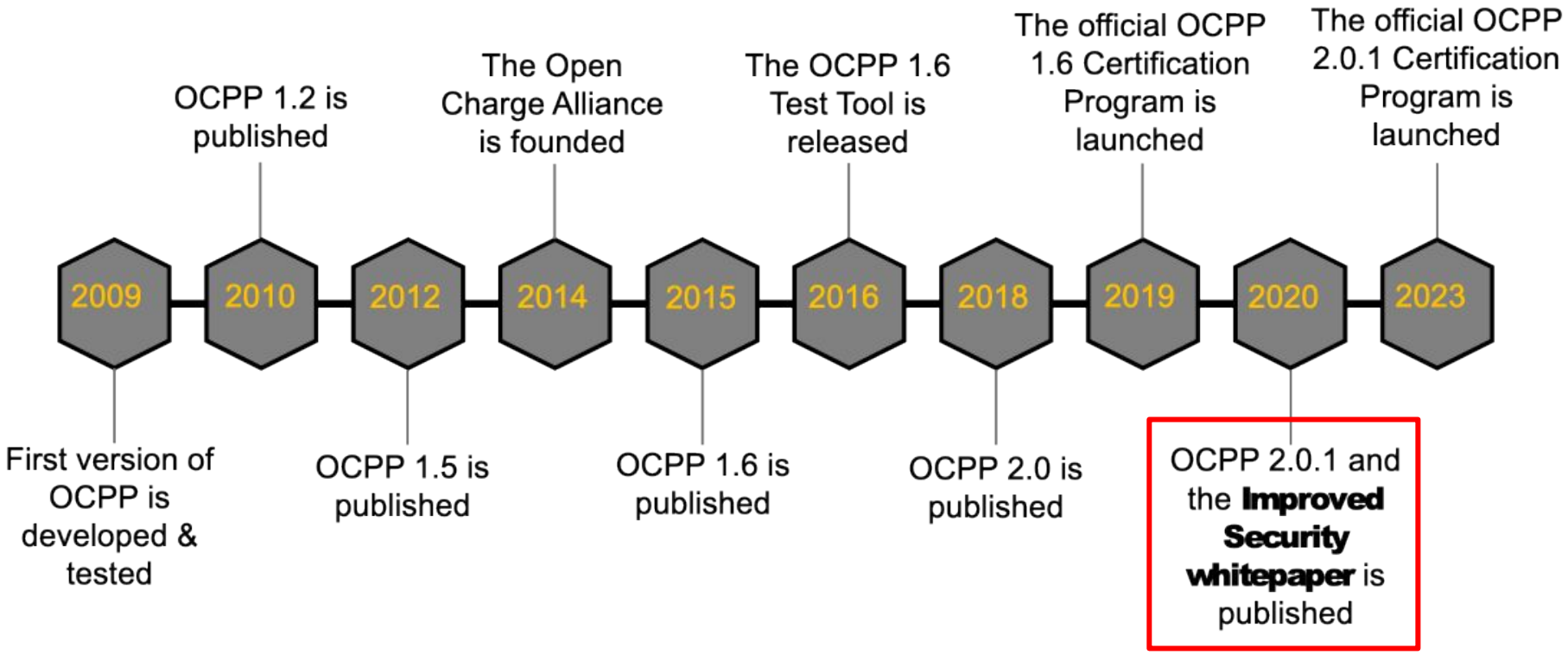
Open Charge Point Protocol (OCPP)



Raw OCPP


D'ÉCLAIR
ules électriques
rique semble
e à réparer ou
doit effectuer l'entretien.
d'y travailler.
trainera la mort ou des
EV2430WS
Input/ Output
Entrada /Salida
Entrée /Sortie
120/208Y, 120/240V-
30A-60Hz
Max. Ambient:
Temp. ambiante max:
Temp. ambiente máx:
55°C
WARNING: Automatic
1245467003A0
EV CHARGING STATION
Listed
4CR4

Open Charge Point Protocol (OCPP)



Motivation

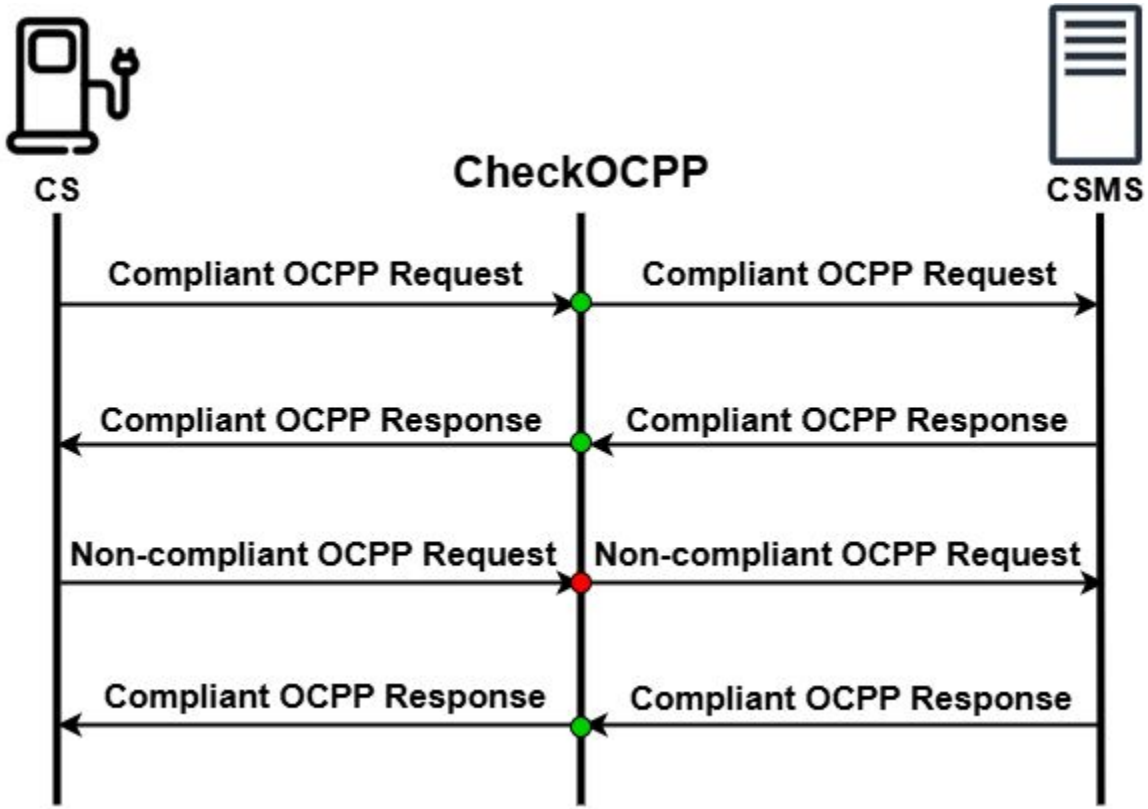
- **Non-compliance –>** Can introduce exploitable implementations.

  Existing tool (OCTT) maintained by OCA is closed-source and behind a paywall (€3,000–€18,000).

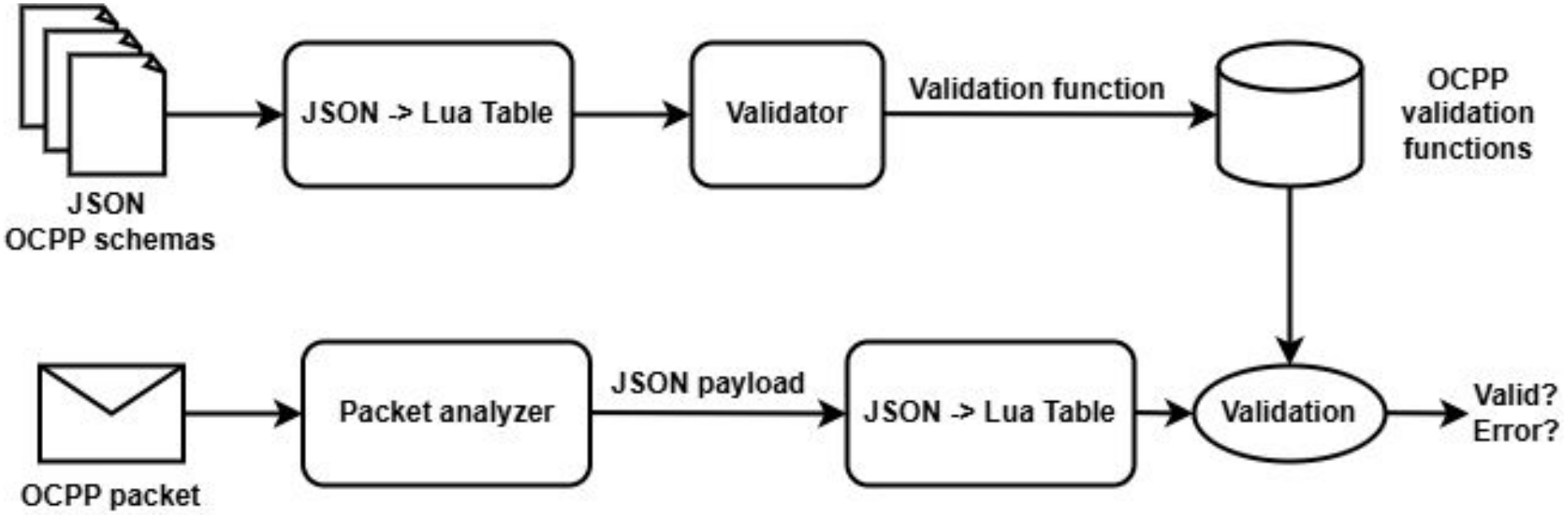
- **Multiple versions and features makes it hard to conduct traffic analysis without proper dissection of OCPP packets.**

→ Need for an open-source solution to dissect and compliance check OCPP traffic for all versions.

CheckOCPP : Design



CheckOCPP :Architecture



CheckOCPP : Implementation

CheckOCPP supports the **76** distinct OCPP **messages** across ver **1.6, 2.0, and 2.0.1.**

TABLE 1. CHECKOCPP OCPP MESSAGE COMPATIBILITY

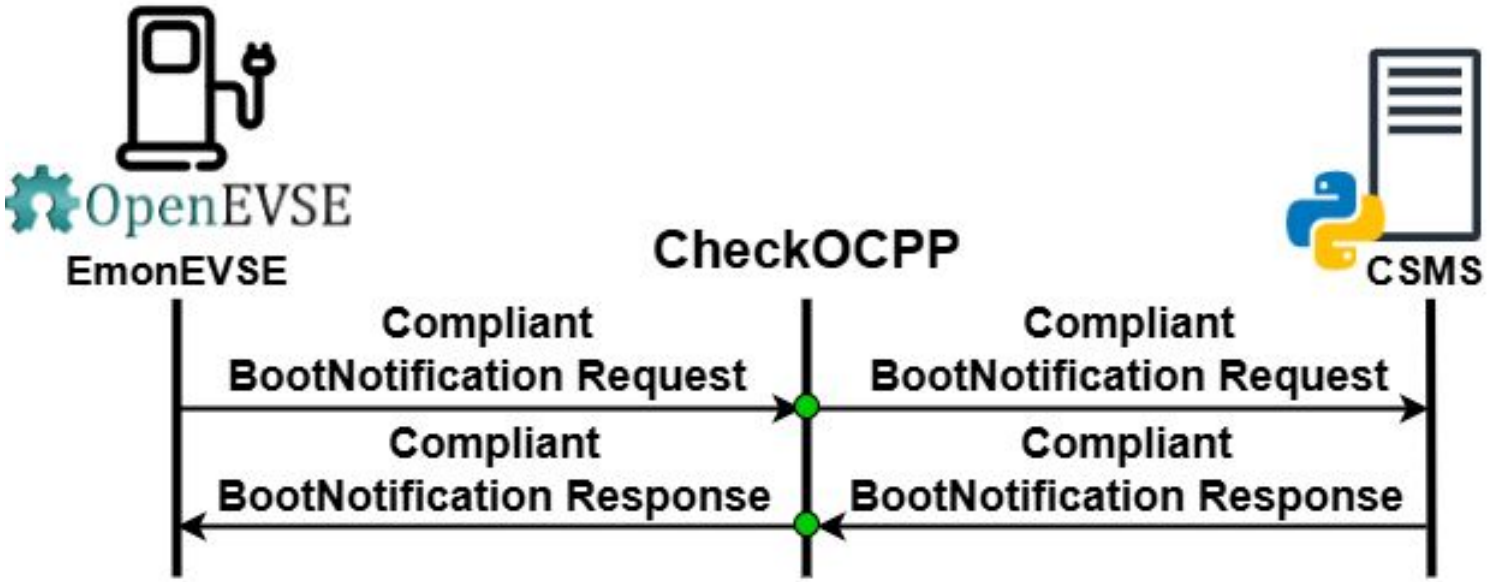
Message	Version
Heartbeat	1.6, 2.0, 2.0.1
BootNotification	1.6, 2.0, 2.0.1
Authorize	1.6, 2.0, 2.0.1
StatusNotification	1.6, 2.0, 2.0.1
TransactionEvent	2.0, 2.0.1
Reset	1.6, 2.0, 2.0.1
MeterValues	1.6, 2.0, 2.0.1
CancelReservation	1.6, 2.0, 2.0.1
ReserveNow	1.6, 2.0, 2.0.1
ClearCache	1.6, 2.0, 2.0.1
ChangeAvailability	1.6, 2.0, 2.0.1
ClearChargingProfile	1.6, 2.0, 2.0.1
DataTransfer	1.6, 2.0, 2.0.1
SendLocalList	1.6, 2.0, 2.0.1
SetChargingProfile	1.6, 2.0, 2.0.1

… etc

Evaluation Setup

For OCPP 1.6

Evaluation Setup



EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing

Soumaya Boussaha
SAP, EURECOM, Biot, France
soumaya.boussaha@sap.com

Victor Fresno Gómez
EURECOM, UPM, Madrid, Spain
victorfresno@live.com

Thomas Barber
SAP SE, Walldorf, Germany
thomas.barber@sap.com

Daniele Antonioli
EURECOM, Biot, France
daniele.antonioli@eurecom.fr

Abstract

The Open Charge Point Protocol (OCPP) is the de facto standard for communication between electric vehicle charging stations (CS) and charging station management systems (CSMS). However, its security and privacy have been only partially explored, mainly due to the lack of an adequate testing framework. To this end, we introduce EmuOCPP, a new OCPP security and privacy testing framework. The framework is based on container emulation to reproduce real-world OCPP networks with high fidelity and low cost. We discuss our implementation of EmuOCPP, using open-source software (IPMininet) and low-cost hardware.

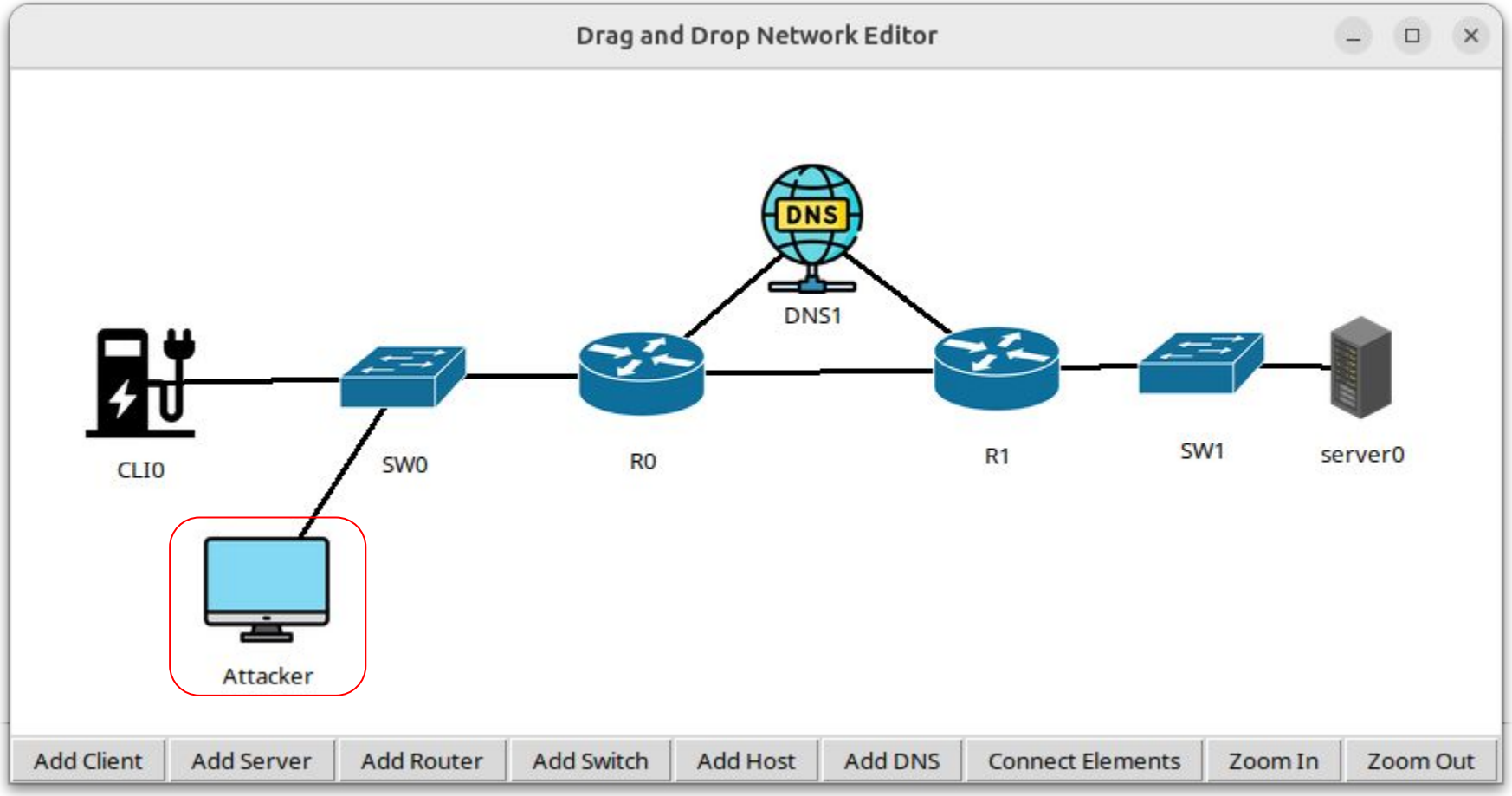
Using EmuOCPP, we uncover five attacks on OCPP 1.6

Numerous studies have examined the security and privacy of OCPP, primarily focusing on 1.6 [2, 14, 29, 30, 32, 36, 47]. These works have highlighted critical security concerns, including man-in-the-middle (MitM) attacks, denial-of-service (DoS) threats, and protocol implementation weaknesses. Additionally, privacy-related risks such as tracking attacks and data leakage have been explored [2, 22, 49]. In contrast, research on OCPP 2.0 and 2.0.1 remains significantly limited, with only a few studies addressing some security aspects [4, 31].

The limited research on more recent OCPP versions is due to the lack of a comprehensive OCPP security and privacy testing framework. Existing tools are fragmented, restricting researchers from conducting holistic security analysis. For

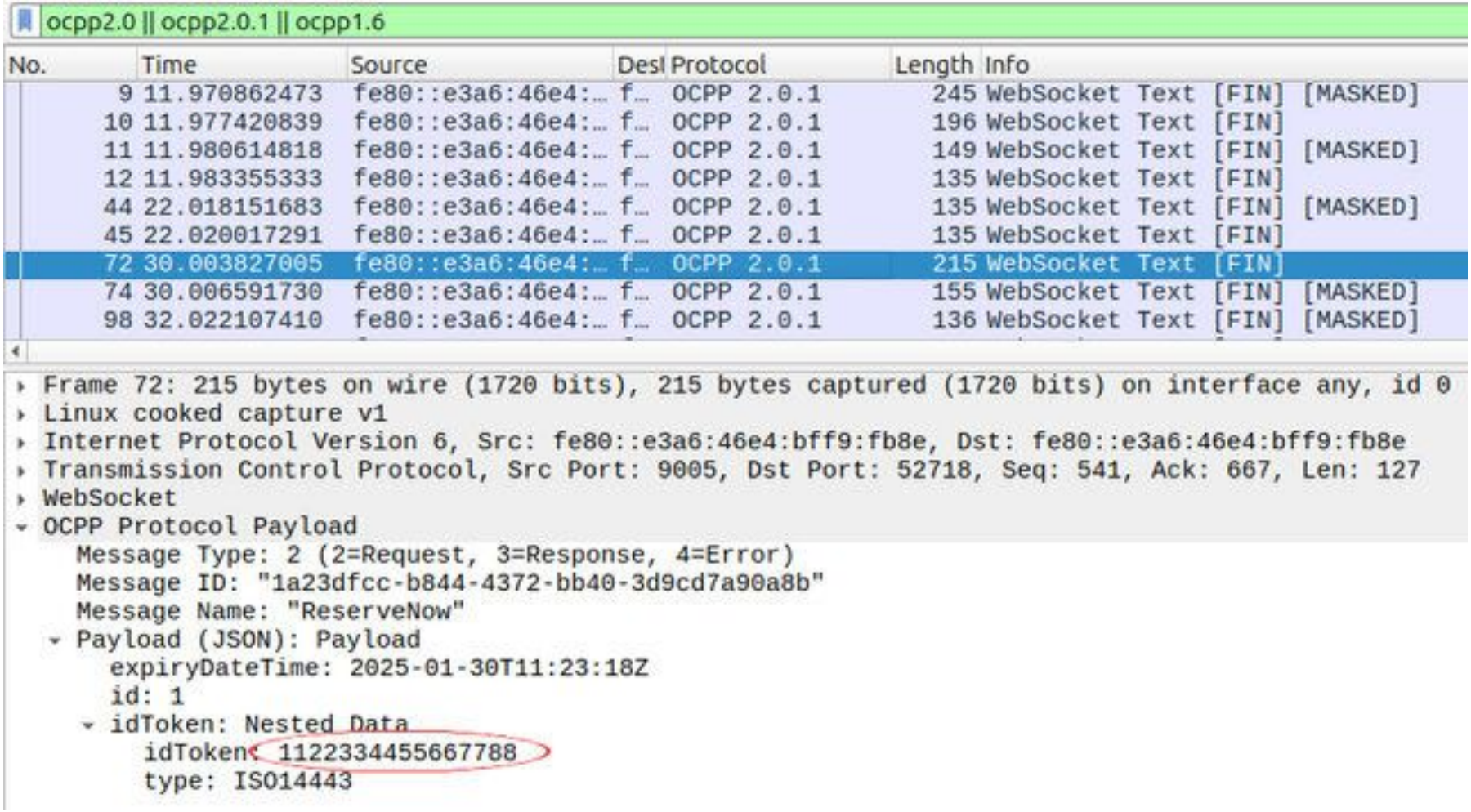
Boussaha, S., Fresno Gómez, V., Barber, T., & Antonioli, D. (2025). *EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing*. In *VEHICLESEC 2025, 3rd USENIX Symposium on Vehicle Security and Privacy* (co-located with USENIX Security), 11–12 August 2025, Seattle, WA.

Evaluation Setup

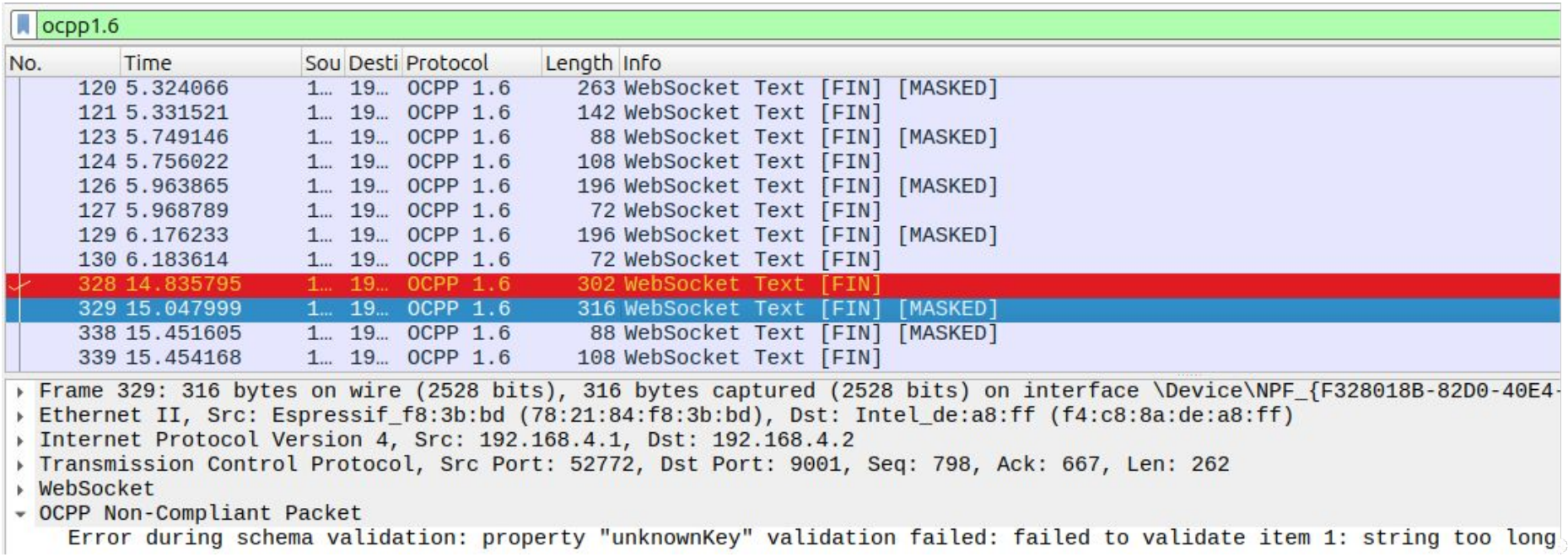


For OCPP all versions

Dissection


ocpp2.0 || ocpp2.0.1 || ocpp1.6
No. Time Source Dest Protocol Length Info
9 11.970862473 fe80::e3a6:46e4:… f… OCPP 2.0.1 245 WebSocket Text [FIN] [MASKED]
10 11.977420839 fe80::e3a6:46e4:… f… OCPP 2.0.1 196 WebSocket Text [FIN]
11 11.980614818 fe80::e3a6:46e4:… f… OCPP 2.0.1 149 WebSocket Text [FIN] [MASKED]
12 11.983355333 fe80::e3a6:46e4:… f… OCPP 2.0.1 135 WebSocket Text [FIN]
44 22.018151683 fe80::e3a6:46e4:… f… OCPP 2.0.1 135 WebSocket Text [FIN] [MASKED]
45 22.020017291 fe80::e3a6:46e4:… f… OCPP 2.0.1 135 WebSocket Text [FIN]
72 30.003827005 fe80::e3a6:46e4:… f… OCPP 2.0.1 215 WebSocket Text [FIN]
74 30.006591730 fe80::e3a6:46e4:… f… OCPP 2.0.1 155 WebSocket Text [FIN] [MASKED]
98 32.022107410 fe80::e3a6:46e4:… f… OCPP 2.0.1 136 WebSocket Text [FIN] [MASKED]
Frame 72: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 6, Src: fe80::e3a6:46e4:bff9:fb8e, Dst: fe80::e3a6:46e4:bff9:fb8e
Transmission Control Protocol, Src Port: 9005, Dst Port: 52718, Seq: 541, Ack: 667, Len: 127
WebSocket
OCPP Protocol Payload
Message Type: 2 (2=Request, 3=Response, 4=Error)
Message ID: "1a23dfcc-b844-4372-bb40-3d9cd7a90a8b"
Message Name: "ReserveNow"
Payload (JSON): Payload
expiryDateTime: 2025-01-30T11:23:18Z
id: 1
idToken: Nested Data
idToken: 1122334455667788
type: ISO14443

Compliance



CheckOCPP successfully identified **three** noncompliant messages, including an improperly formatted GetConfiguration for the EmonEVSE device

Summary

- We present CheckOCPP, a novel OCPP toolkit for packet dissection and compliance checks.
- We validated CheckOCPP in an evaluation against Mobility House (OCPP 2.0 & 2.0.1) and EmonEVSE (OCPP 1.6) & EmuOCPP.
- Open-Sourced here : https://github.com/vfg27/CheckOCPP

Soumaya Boussaha
SAP, EURECOM
Biot, France
soumaya.boussaha@sap.com

Victor Fresno Gómez
EURECOM, UPM
Madrid, Spain
victorfresno@live.com

Thomas Barber
SAP
Baden-Wurtemberg, Germany
thomas.barber@sap.com

Daniele Antonioli
EURECOM
Biot, France
daniele.antonioli@eurecom.fr