Your EV Charger is an OT Asset – Start treating it like one

Alina Tan
Co-Founder, HE&T Security Labs

#whoami

Alina Tan

- Co-founder at HE&T Security Labs
- Security Architect
- Team Lead & Founder, Car Security Quarter (CSQ)
  Part of a wider cybersecurity community group – Division Zero (Div0)
- Expertise – Automotive Security, Operational Technology (OT), Industrial Control System (ICS) & Supervisory Control & Data Acquisition (SCADA) Systems
- Interest – Car Racing, Pentesting OT & Automotive Systems

H E & T
SECURITY LABS

What we will cover today: Agenda

Who This Presentation Is For

Fleet Operators

Logistics, transportation & delivery companies managing vehicle charging at scale

Utilities & Grid Operators

Organisations responsible for grid stability, distribution, and energy management

Facility Managers

Corporate campuses, hospitals, logistics depots deploying EVSE on-premises

Charge Point Operators

CPOs managing public or semi-public charging networks and back-end platforms

OT / ICS Security Teams

Security practitioners responsible for operational technology and industrial control systems

This list is not exhaustive, if your organisation deploys, manages, secures, or depends on EV charging infrastructure, this session is relevant to you.

EVSE: The Security Blind Spot You're Ignoring

~9.3M

Public charging points globally (IEA, 2025)

12.6%

Organizations with full OT/ICS visibility (SANS, 2025)

2,207

ICS advisories issued in 2025 with EVSE rarely in scope

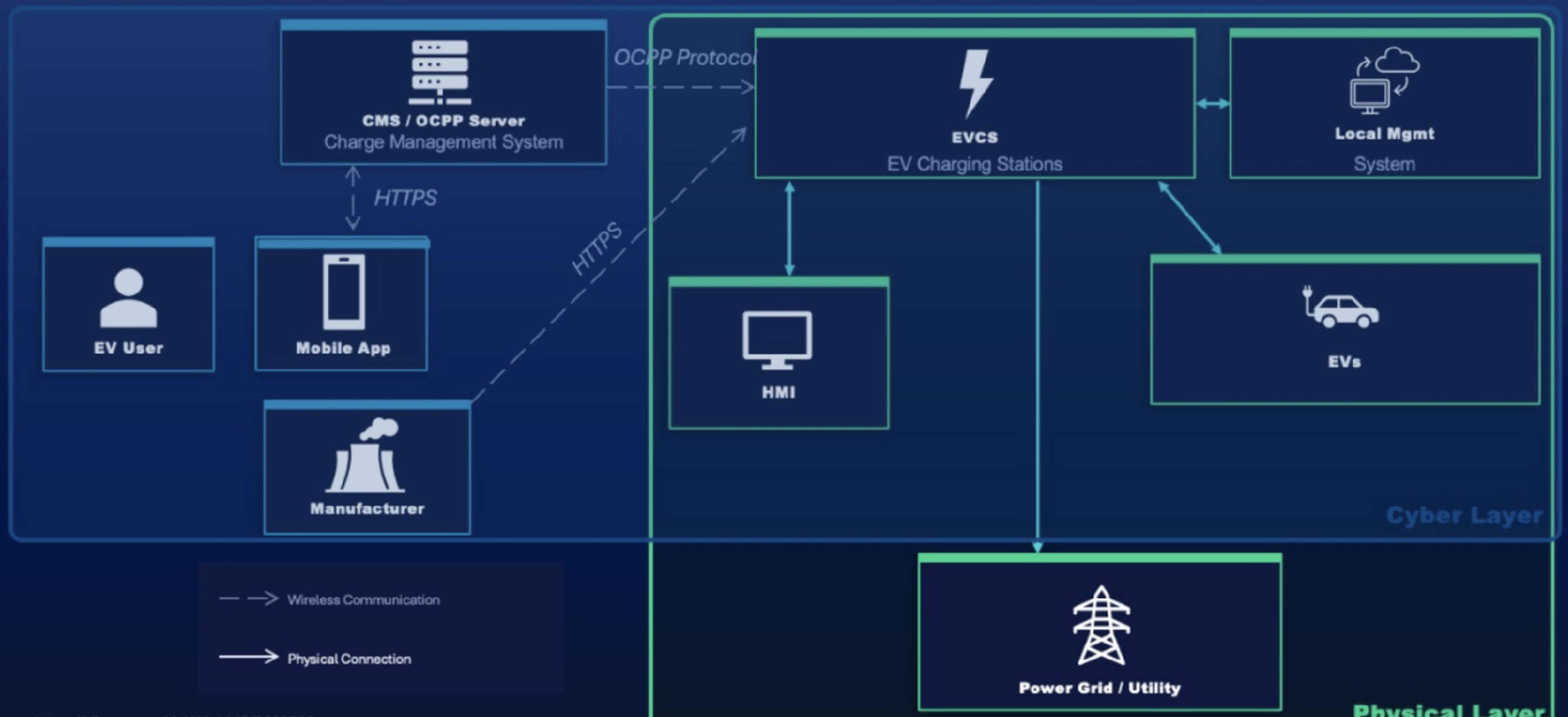
- Chargers are network-connected OT assets and not IT peripherals
- Managed by facilities or fleet teams, not security teams
- Run real-time firmware with direct grid interaction
- Often on flat or under-segmented networks
- OCPP and ISO 15118 protocols largely unmonitored
- Many EVSE vendors lack a formal PSIRT or coordinated disclosure process
- Residential and enterprise units treated identically
- Growing attack surface as EV adoption accelerates

Sources: IEA Global EV Outlook 2025 (iea.org) · SANS State of ICS/OT Security 2025 (sans.org) · EmberOT ICS/OT Vulnerability Intelligence Report 2024–2025 (emberot.com)

What Is EVSE? The Full Stack

1 Cloud / CSMS	Charge Management Software, APIs, billing, remote control
2 Network Layer	Cellular / Wi-Fi / Ethernet · OCPP 1.6 / 2.0.1 · TLS
3 Firmware / OS	Embedded Linux, RTOS, Bootloaders · OTA update mechanisms
4 Hardware / Physical	Power electronics, RFID reader, display, cable · SAE J1772 / CCS / CHAdeMO

EV Ecosystem



Source: https://dl.acm.org/doi/10.1145/3609508

The EVSE Threat Landscape at a Glance

Physical Tampering

Skimmers, cable abuse, hardware implants

Firmware Attacks

Unsigned OTA, bootloader bypass, persistence

OCPP Protocol

MiTM, replay, spoofed commands, DoS

Energy Theft

Auth bypass, session hijacking, free charging

Residential L2

Home network pivot, UPnP exposure, WAN access

Cloud / CSMS

API abuse, credential stuffing, mass control

Physical Tampering Attacks

Skimming Devices

Overlay hardware captures RFID credentials; low cost, difficult to detect without regular inspection.

Cable & Connector Abuse

Modified charging cables inject malicious signals via PLC HomePlug Green PHY (ISO 15118), enabling CAN bus-level attacks on connected vehicles.

Hardware Implants

Physical access to unlocked enclosures allows USB drops, cellular implants, or hardware keyloggers for persistent access.

Tamper-Evident Failures

Many units lack tamper seals or functional tamper alarms; post-intrusion detection is rare in practice.

Documented Incidents

- Nov 2024: 116,000 records breached from global CPOs: PII, VINs, RFID tokens
- Oct 2023: Dutch CPO API leaked all RFID UIDs resulting in mass cloning enabled
- Shell Recharge 2023: millions of charging logs & customer PII sold on dark web
- 2022: EV chargers in the UK taken offline after unauthorised access; separate incidents reported internationally — specific threat-actor attribution was not officially confirmed (BBC News, Apr 2022)
- INL Research: simultaneous shutdown of hundreds of DC fast chargers can destabilize local grid segments

Sources: Upstream Security · Harm van den Brink/Medium · Hoplon Infosec · CyberScoop/INL

Firmware Manipulation

1

Reconnaissance

OSINT on charger vendor, model, firmware version via OCPP heartbeat or HTTP headers

2

Firmware Extraction

UART/JTAG debug ports often exposed in production units; binwalk extraction via SPI flash

3

Analysis & Backdoor

Identify hardcoded creds, unsigned update checks, missing secure boot enforcement

4

Malicious Firmware

Inject modified image: disable safety interlocks, exfiltrate RFID tokens, join botnet. CVE-2024-37310: heap overflow in open-source EV firmware allows payment bypass and private key theft.

5

OTA Delivery

Poison update server or MiTM HTTP update channel; charger accepts unsigned images silently. Pwn2Own Automotive 2024: 29 zero-days found across EVSE products in a single competition which resulted in 50%+ enabled remote code execution.

Sources: CVE-2024-37310 (PlaxidityX / NVD) · Pwn2Own Automotive 2024 — VicOne/Trend Micro (vicone.com)

OCPP-Layer Attacks

Open Charge Point Protocol (OCPP)

OCPP is the de-facto standard for charger-to-CSMS communication but it was designed for interoperability, not security. In November 2024, a single breach exposed 116,000 records from global EV charging networks.

MiTM & Interception

- OCPP 1.6 WebSocket often runs over plain WS (no TLS)
- Attacker on same segment intercepts auth tokens
- Session replay attacks such as reusing valid StartTransaction messages
- Credential harvest across multiple stations

Spoofed Commands

- RemoteStartTransaction with stolen RFID idTag
- ChangeConfiguration to disable max-current limits
- Reset commands cause mass simultaneous outages
- Firmware update trigger pointing to malicious server

Denial of Service

- OCPP heartbeat flooding exhausts CSMS threads
- Trigger repeated BootNotification loops
- TLS renegotiation attacks on OCPP 2.0 endpoints
- Grid-impact: coordinated charge-stop during peak load

Sources: C2A Security — 30 EV Ecosystem Statistics 2025 (c2a-sec.com) · Dark Reading ICS/OT · Driivz OCPP Security Analysis (driivz.com)

Energy Theft & Financial Fraud

RFID Cloning
MIFARE Classic tokens used by legacy chargers are cryptographically broken and clonable with <$20 hardware. In 2025, Dutch operator Check reported a spike in RFID card cloning fraud using off-the-shelf scanners.

Session Hijacking
Active OCPP session tokens intercepted from unencrypted WebSocket streams allow real-time session takeover and free charging across a network.

Authorization Bypass
Some chargers default to 'free vend' mode if CSMS is unreachable resulting in a misconfiguration attackers can deliberately trigger via OCPP flood.

API Credential Abuse
Mobile app APIs with weak JWT validation allow mass free-charging across operator networks; account takeover via credential stuffing and API key exposure is documented across multiple CPO platforms.

Documented Impact

2×
EV charger theft & fraud doubled in 2024 vs. 2023

£410K
Cost to InstaVolt from ~100 theft/vandalism incidents

215
Charging cords cut at Electrify America in 2024

$4,000
Replacement cost per DC fast-charging cord

Sources: Transport & Energy (Jan 2025) · EV Infrastructure News (InstaVolt) · Claims Journal (Sep 2024, Electrify America) · Tap Electric case study (tapelectric.app)

Home Chargers: Same Architecture, Same Risk

A residential L2 charger and a commercial EVSE unit are architecturally near-identical:

Similar OCPP Stack

OCPP 1.6/2.0.1: Identical protocol implementation and attack surface regardless of deployment location

Firmware Patterns

Embedded Linux / RTOS with similar update mechanisms, CVE exposure, and vendor support lifecycles

Utilises ISO 15118

V2G interface present in smart home chargers (Wallbox Quasar, Ford Intelligent Backup Power) with the same protocol vulnerabilities

Grid Connection

Connected to the same distribution network. Draws 7–22 kW per unit. Grid-connected metering and demand-response APIs present

What the Research Shows: Grid-Level Risk

INL research models that coordinated manipulation of large numbers of grid-connected EV chargers can cause frequency deviations beyond grid tolerance thresholds [modelled, not yet observed in the wild]

Unmanaged residential charging creates synchronised demand peaks on distribution circuits with load variability that grid operators must account for as EV penetration grows

V2G-capable home units enrolled in demand-response programmes become a target: a compromised aggregator or charger firmware could issue false discharge commands affecting grid balancing

Sources: Idaho National Laboratory (INL) Load Altering Attack Research 2022–2023 · ISO 15118 V2G Specification · IEA Global EV Outlook 2025

Same Risk, Your Network

Credential & Web UI Exposure

Default or weak management credentials and exposed web UIs are just as common on depot and workplace chargers and here they sit inside your corporate network perimeter.

No Network Segmentation

Enterprise EVSE is rarely placed on a dedicated isolated segment it typically shares network infrastructure with facilities or building management systems, creating adjacency to higher-value targets regardless of whether formal segmentation exists

Automatic OTA Updates

Vendor-pushed OTA updates on enterprise chargers bypass your change management and patch approval workflow, a compromised update pipeline hits your entire fleet silently.

Mobile App Attack Surface

CSMS mobile apps with weak token storage or session management could expose remote charger control to a credential compromise.

Vehicle-Side Risk

CISA issued an advisory on a critical ISO 15118 V2G vulnerability (SwRI, Nov 2025): a compromised enterprise charger can attempt attacks against the EV charging ECU over PLC.

Corporate Spillover

Your depot charger is the last-mile touchpoint for every fleet vehicle. A compromise here propagates across your entire fleet estate and into the enterprise systems those vehicles report back to.

Sources: SwRI / CISA ISO 15118 Advisory (Nov 2025) — swri.org · DOE Joint Office Cybersecurity for EV Charging Infrastructure — driveelectric.gov

Common Level 2 EV Charging Infra and Mobile App lateral movement

01

Recon: Charging App

Decompile the EV mobile app. Enumerate API endpoints, hardcoded tokens, OAuth flows, and OCPP WebSocket URLs.

02

Target: OCPP Station

Interact with the OCPP 1.6/2.0 backend directly. Probe for unauthenticated RemoteStart, StopTransaction, or GetDiagnostics commands.

03

Pivot: Account Takeover

Exploit weak password-reset flows or API IDOR vulnerabilities to assume another vehicle owner's identity in the cloud backend.

04

Impact: Vehicle Control

Issue remote charge commands, pull GPS location history, or leverage backend trust to probe vehicle telematics APIs further inward.

KEY INSIGHT The charging app is a trusted bridge between the public internet and vehicle cloud services. Misconfigured APIs and weak auth in this layer can expose vehicle location, owner identity, and remote-action capabilities without ever touching the car directly.

Attack Path #1 – EV Charger “Z”

S1 Attacker enters BLE radio range

The charger is discoverable over BLE from nearby.

S2 Establish BLE connection and observe FFE4 traffic

After connecting and enabling notifications, charger status/version messages are visible on FFE4.

S3 Identify password-gated BLE command path

Captured traffic shows a password-bearing command sequence is required before higher-privilege operations.

S4 Weak/default credential risk

A 6-digit password is used, and default/common credentials may materially reduce attack cost.

S5 Valid credential obtained in testing

A known/default credential was accepted in the test environment, enabling an authenticated BLE session.

S6 Authenticated BLE session established

After successful authentication, the app can issue a broader set of BLE commands to the charger.

S7 Read/write management functions become accessible

Observed traffic suggests authenticated access enables device-management operations such as status queries and configuration-related commands.

S8 Send OTA START via WiFi or BLE

Charger accepts OTA on both channels

S9 Push firmware via BLE or WiFi

Legitimate packages accepted; modified binaries blocked by signing

S10 Post-authentication impact could be significant if update or management paths are abused

Privileged firmware access enables attackers to disrupt service, misconfigure devices, or cause unsafe behaviour.

EV Charger “Z” – Technique 1

CVE-2026-9394 · Weak Password Requirements (BLE)

CVE-2026-9395 · Cleartext Credential Exposure (BLE/UDP)

F-01 **Default or Embedded Credentials**

① Extract from firmware binary

A 6-digit credential appears in plaintext in APK

```
0x0041F2C0:  6 digit code   ← default credential
```

② Credential exposure via BLE and UDP

BLE: btsnoop capture (record 8330), password visible in plaintext at byte offset

```
06 01 00 1A                 ; opcode AUTH
00 33 80 73 58 73           ; device_id
71 21 81                    ; fixed header
31 32 33 34 35 36           ; ← '123456' plaintext
80  [seq]  04  [chk]  0F 02 ; trailer
```

③ Default credentials never rotated

Use of shared or default-style credentials can materially reduce attack cost. Per-device credential uniqueness was not conclusively established across all units.

EV Charger “Z” – Technique 2

CVE-2026-9395 · Cleartext Credential Exposure (BLE/UDP)

CVE-2026-9398 · Unauthorised Command Tampering (BLE/WiFi/UDP — No Encryption/Integrity Protection)

F-02 **BLE Weak Authentication -> Charge Tampering**

① BLE command identification

Authentication outcomes appeared distinguishable in BLE traffic during testing, allowing success/failure

```
cmd=0x02 → AUTH SUCCESS ✓
cmd=0x55 → AUTH FAIL    ✗  (no lockout)
```

② Charge Tampering: Authenticated or Direct

These tampering outcomes are reachable via two independent paths: authenticated via FFF2 with no additional authorisation required, or unauthenticated via unprotected UDP packet replay.

Stop Charge	Send opcode 0x0030: active charging session halted immediately
Modify Current	Rewrite max_current register: reduce or deny charging speed
Trigger OTA	Push firmware via BLE or WiFi: escalates directly to F-03

③ Charge tampering demonstration

```
# Step 1: authenticate with discovered PIN  (F-01 + F-02)
send_ble(FFF2, build_auth(pin='123456'))  # opcode 0x0029
# Step 2: halt active charging session
send_ble(FFF2, build_cmd(0x0030, b'\x00'))  # halt charge
```

EV Charger “Z” – Technique 3

CVE-2026-9396 · UI Manipulation & Clickjacking

CVE-2026-9397 · Improper Authorization (OTA Handler)

Real update server

Examplefirmwarewebsite.com

Intercepted

APP

EV Charger APP

redirected

Fake update server

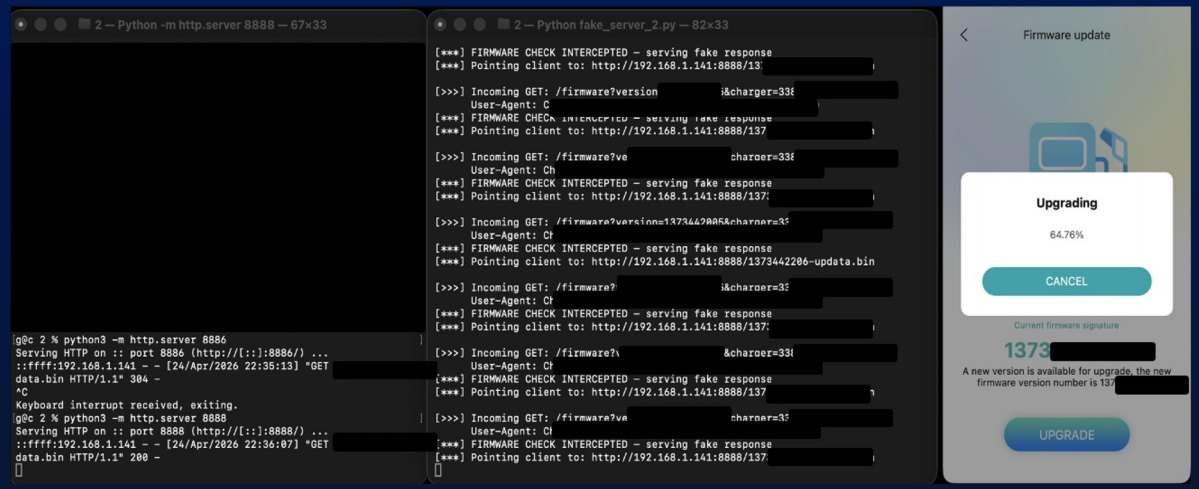
Attacker-controlled

test firmware

WiFi or BLE

EV Charger

EV Charger



Legitimate (blocked) path

Attack path

Summary of attack path

F-01 **Hardcoded passwords**

A 6-digit credential appears in plaintext in at least one firmware image, and plaintext password fields were observed in BLE authentication traffic.

F-02 **BLE Weak Authentication -> Charge Tampering**

Once authenticated via FFF2, an attacker can halt charging sessions, modify current limits, and trigger OTA firmware updates with no additional authorisation required.

F-03 **OTA Delivery**

Update-related functionality exists over BLE and/or Wi-Fi, and verified across, but charger-side acceptance requires further testing.

Observed BLE auth packet structure

06 01 [opcode 2B LE] [device_id 6B]

71 21 81 FF FF FF FF FF FF [dir 1B]

[password 6B ASCII] 09 [chk] 0F 02

Impact

- Authenticated attackers may be able to invoke privileged charger-management functions
- Sensitive configuration data such as Wi-Fi-related settings may be exposed
- Update-related paths (OTA) may increase impact if further exploited
- Potential brick of device permanently if modified updates are pushed successfully

The Workplace Charger: Shadow OT Asset Inside Your Perimeter

Why This Matters for OT Security Teams

- Workplace chargers are typically procured by facilities teams and deployed on facilities networks, which is outside of IT security scope and absent from the CMDB
- Whether on a separated guest network, facilities VLAN, or OT segment, the charger is often absent from the asset inventory - meaning no zone was deliberately assigned and no one owns it from a security perspective
- Even on a guest network or correctly zoned EVSE segment, lateral movement paths remain - the outbound OCPP channel to a cloud CSMS, a CSMS hosted inside the OT network rather than a DMZ, and shared management infrastructure across zone boundaries are all attack paths that zone assignment alone cannot prevent.
- Without an asset inventory entry, CVEs assigned to your deployed charger models never reach your patch team and with most EVSE vendors lacking a formal PSIRT, there is no disclosure notification to trigger the process in the first place

Bringing EVSE Into Scope: Operational Challenges

01 Who Owns EVSE?

Facilities, IT, Fleet, and OT teams all have partial ownership. No single team has full responsibility, security gaps form at the seams.

02 Asset Discovery

EVSE isn't in the CMDB, SCADA historian, or IT asset inventory. Passive network discovery rarely fingerprints OCPP traffic correctly.

03 Vendor Fragmentation

Dozens of charger vendors, each with proprietary firmware and management portals. No unified patch or CVE feed. Coordinated disclosure is rare.

04 Maintenance Windows

Chargers run 24/7 in public or semi-public spaces. Planned downtime for patching conflicts with availability expectations of fleet operators.

Visibility Gaps & Asset Classification

Current State

- EVSE is rarely classified as OT, usually treated as facility infrastructure
- No passive network traffic baseline for OCPP communications
- Firmware versions unknown across entire charger fleet
- Authentication logs not forwarded to SIEM
- No alert for unexpected CSMS endpoint changes
- Lateral movement from EVSE VLAN goes undetected

Target State

- EVSE classified as ICS/OT: Level 1/2 Purdue model placement
- Network tap or span captures OCPP WebSocket traffic
- Asset inventory includes make, model, firmware, IP, VLAN
- Auth events and OCPP messages forwarded to SIEM/SOC
- Alerts on CSMS IP/domain change, config modification
- Micro-segmented EVSE VLAN with firewall policy enforcement

Achieving Cyber Resiliency at Scale

1

Asset Inventory

- Discover all EVSE via active + passive scanning
- Tag in CMDB: vendor, firmware, protocol version
- Align to IEC 62443 zone/conduit model

2

Network Segmentation

- EVSE VLAN isolated from IT and OT network
- Firewall rules: OCPP only to known CSMS IPs
- Deny all inter-EVSE lateral communication

3

Continuous Monitoring

- Ingest OCPP traffic to IDS/ICS-aware SIEM
- Alert on auth anomalies and config changes
- Integrate with OT network monitoring platform

4

Patch & Firmware Mgmt

- Vendor firmware advisory subscription
- Staged OTA rollout with rollback capability
- Validate firmware integrity before deployment

5

Policy & Governance

- Include EVSE in OT risk assessment annually
- Procurement checklist: security requirements
- Incident response runbook for EVSE scenarios

Key Takeaways & Call to Action

01

Reclassify EVSE as OT Assets today

If your asset inventory doesn't yet include EV chargers, it's worth reviewing where EVSE sits within your IEC 62443 zone model and whether it should be treated as a Level 1 or 2 asset.

02

The Full Stack Needs Defending

Physical, firmware, protocol, and cloud layers all present real attack surfaces. A charger is not just a plug, it is a network-connected industrial control device.

03

Turn Classification into Action

Classification on paper means nothing without following-through: get chargers into your CMDB, assign them to a dedicated network zone, and pull them into your vulnerability management process the same way you would any other OT device.

04

Visibility Before Enforcement

You cannot protect what you cannot see. Start with passive monitoring of OCPP traffic and a complete firmware asset inventory before deploying controls.

05

Build It In Before the Fleet Grows

Security retrofitted on 10,000 chargers costs 10× more than security built into a 500-charger rollout. Make EVSE security a procurement requirement now.

THANK YOU