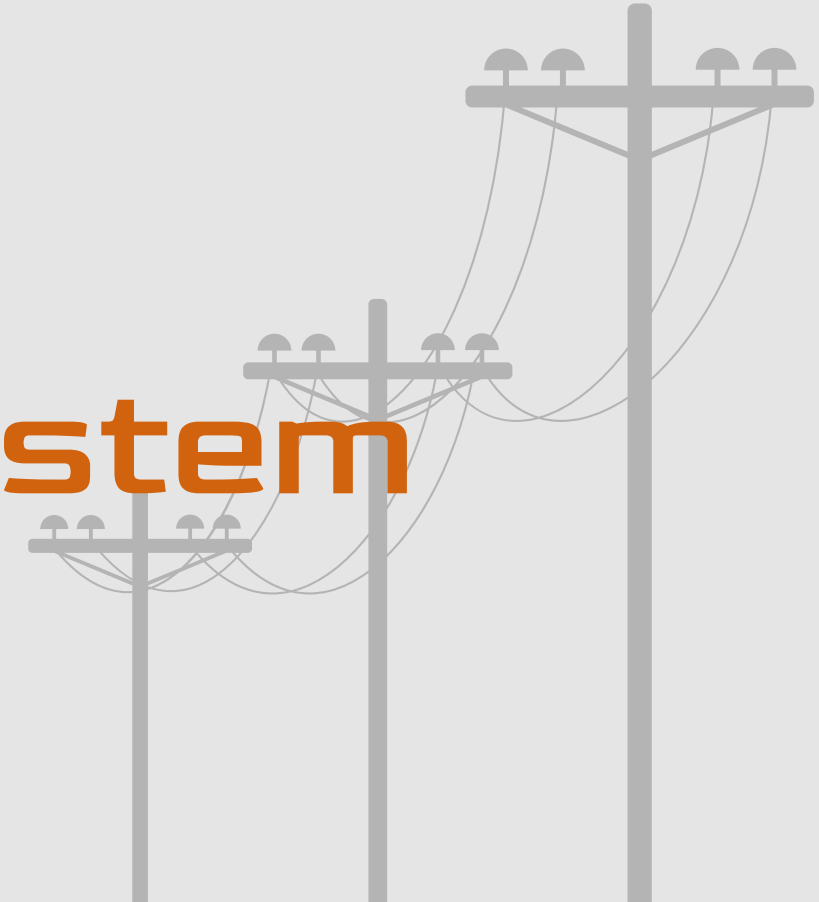
Securing the EVSEcosystem

Prepared by Danielle McGuire
for Pittsburgh OTSec, October 2024



Introduction

Who Am I

Danielle McGuire, she/her

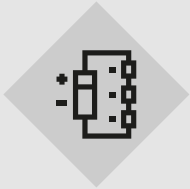
Sr OT Cybersecurity Analyst
Duquesne Light Company
2016-present

Industry Advisor
Pitt Cyber Energy Center
2024-present

Interests

At work: electric power cybersecurity, process automation and tooling creation, integration of novel systems

At home: electronics, computers, cooking, history



Objectives

Convince yinz that EVSE is Damn Vulnerable at the hardware and protocol level, and dip our toes into hardware hacking

Overview of EVSEcosystem

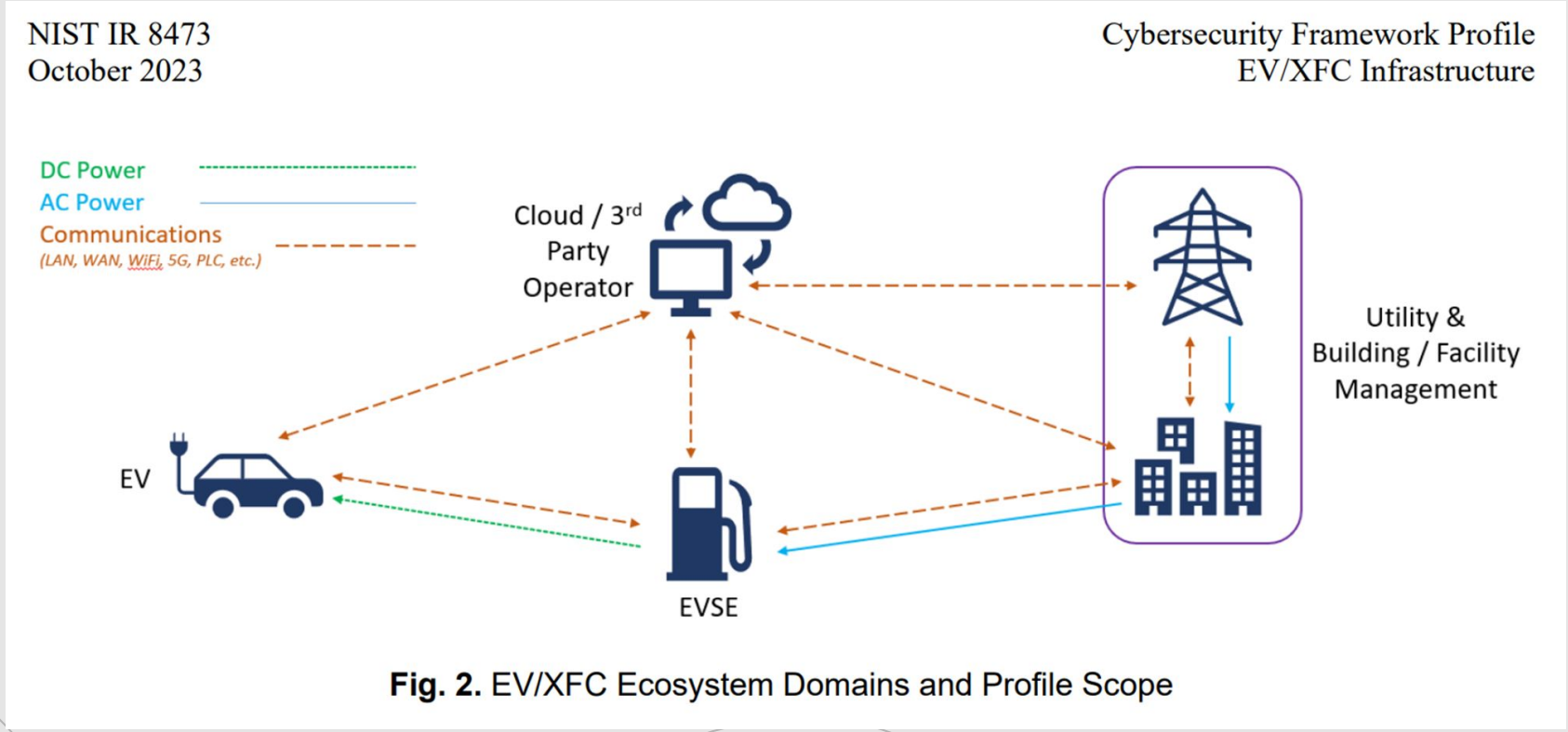


Fig. 2. EV/XFC Ecosystem Domains and Profile Scope

Type of Charging	Level 1 – 110V (~1.4kW)	Level 2 – 220V (~7.2kW)	DC Fast Charger (50kW)	Tesla SuperCharger (140kW)	Extreme Fast Charging (350kW)*
Charging Station 101	Provides same electricity as a regular electrical outlet	More powerful than Level 1 charging	DC current directly supplied to vehicle	Only available for Tesla vehicles	Provides significantly faster charge rates than anything else on market
		Comprises the majority of stations in the U.S	Commonly adds 40 to 60 miles of range in ~20 minutes	Offers fastest charging rate currently available	
Range Gained per Hour of Charge	3-5 miles	25 miles	100 miles	330 miles	787.5 miles
Time to Charge for 200 miles	40 hours	8 hours	2 hours	36.55 mins	15.25 mins

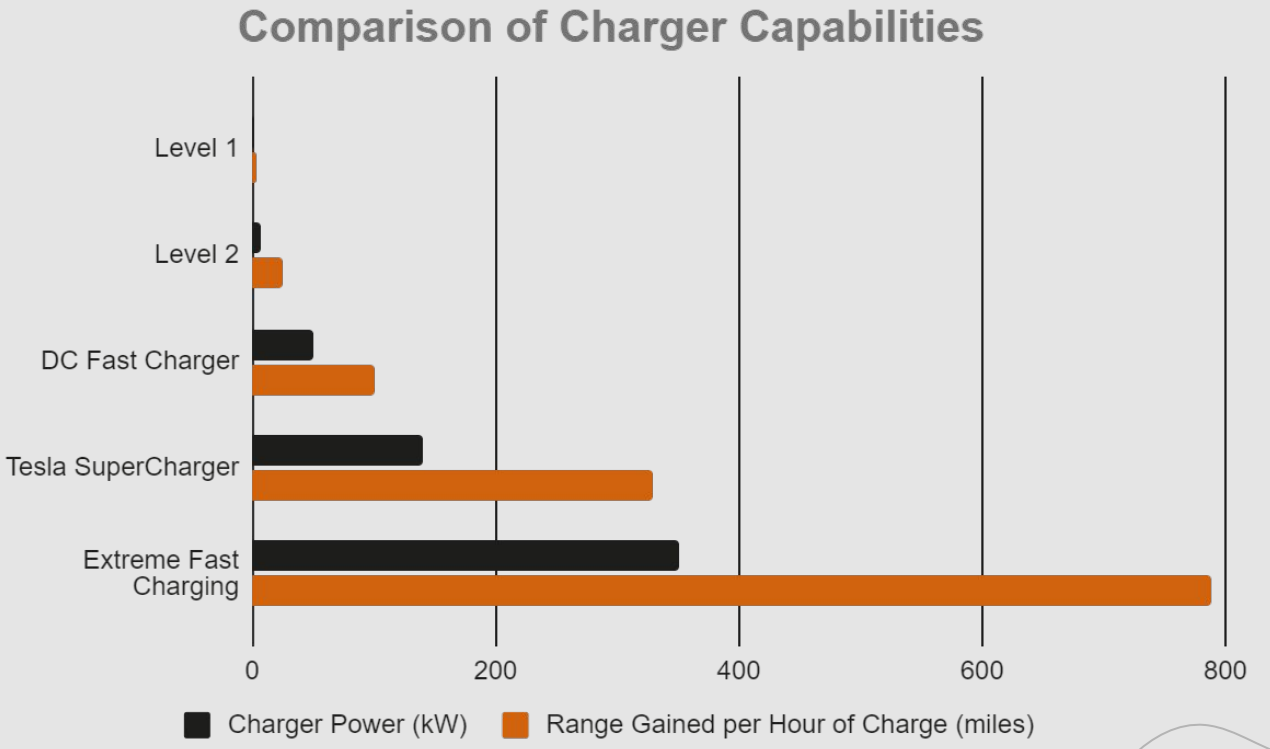
*Estimates based on DOE calculations

EVSE is a Growth Industry

- EEI projects 24.6M EVs by 2030
- 48,000 public chargers in 2023, projected to grow to 500,000 by 2030
- EVSE market valued at $3.15B in 2022, projected to grow to $24B by 2030

- XFC is a game changer
- Most customers have Lv2 or DC Fast

EVSE is Becoming More Powerful



Power Consumption of Household Appliances

appliance	watts	appliance	watts	appliance	watts
Coffee Pot	200	Garage door opener	350	Compact fluorescent	
Coffee Maker	800	Ceiling fan	10-50	Incandescent equivalents	
Toaster	800-1500	Table fan	10-25	40 watt equivalent	11
Popcorn Popper	250	Electric blanket	200	60 watt equivalent	16
Blender	300	Blow dryer	1000	75 watt equivalent	20
Microwave	600-1500	Shaver	15	100 watt equivalent	30
Waffle Iron	1200	Waterpik	100		
Hot Plate	1200	Well Pump (1/3-1 HP)	480-1200	Electric mower	1500
Frying Pan	1200			Hedge trimmer	450
		Computer		Weed eater	500
Dishwasher	1200-1500	Laptop	20-50	1/4" drill	250
Sink waste disposal	450	PC	80-150	1/2" drill	750
		Printer	100	1" drill	1000
Washing machine		Typewriter	80-200	9" disc sander	1200
Automatic	500	Television		3" belt sander	1000
Manual	300	25" color	150	12" chain saw	1100
Vacuum cleaner		19" color	70	14" band saw	1100
Upright	200-700	12" black and white	20	7-1/4" circular saw	900
Hand	100	VCR	40	8-1/4" circular saw	1400
Sewing machine	100	CD player	35		
Iron	1000	Stereo	10-30	Refrigerator/Freezer	
		Clock radio	1	20 cu. ft. (AC)	1411 watt-hours/day*
Clothes dryer		AM/FM auto cassette player	8	16 cu. ft. (AC)	1200 watt-hours/day*
Electric NA	4000	Satellite dish	30		
Gas heated	300-400	CB radio	5	Freezer	
		Electric clock	3	15 cu. ft. (Upright)	1240 watt-hours/day*
Heater				15 cu. ft. (Chest)	1080 watt-hours/day*
Engine block NA	150-1000	Radiotelephone			
Portable NA	1500	Receive	5		
Waterbed NA	400	Transmit	40-150		
Stock tank NA	100				
Furnace blower	300-1000	Lights:		Note: TV's, VCR's and other devices left plugged in, but not turned on, still draw power.	
Air conditioner NA		100 watt incandescent	100		
Room	1000	25 watt compact fluor.	28		
Central	2000-5000	50 watt DC incandescent	50		
		40 watt DC halogen	40		
		20 watt DC compact fluor.	22		

* The daily energy values listed here are for the most efficient units in their class and the infromation was obtained from *Consumer Guide to Home Energy Savings* by Alex Wilson and John Morrill.

10th Edition • Solar Electric Products Catalog • March 2003

Wholesale Solar, Inc.
www.wholesalesolar.com

EEVSE (Example EVSE) – ChargePoint Home Flex (CPH50)

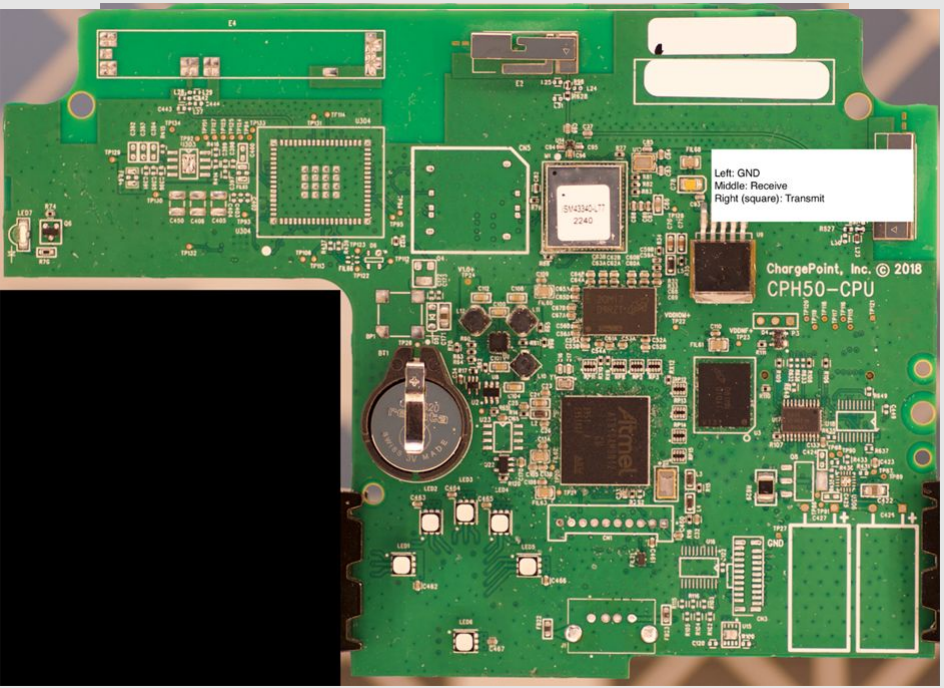
Overview

L2 charger with max 12kW output
Consumer grade, $550 as of Sep 2024
SAE J1772 connector (most common)
2.4/5 GHz 802.11 abgn WiFi
Retains past 90 days of charge data locally
Over-the-air firmware updates

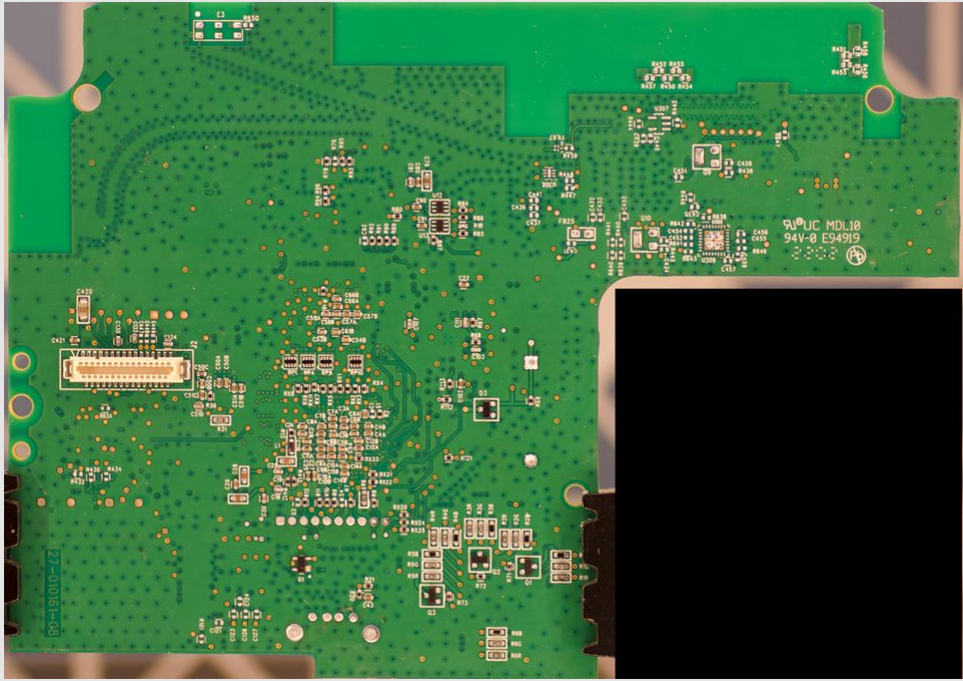
Internals

Atmel AT91SAM9N12
32-bit ARM9 processor
Up to 400 MHz, 128 KB ROM, 32 KB SRAM.
Located on Control board
Micron MT47H64M16NF-25E IT:M
1GB DRAM.
Located on Control board.
Micron MT29F4G08ABBDAH4-IT:D
4GB NAND flash.
Located on Control board
Inventek ISM43340
Wi-Fi Bluetooth SIP Module. Located on Control board.
TI MSP430F67651A
Polyphase metering SoC
25 MHz, 128KB Flash, 16KB RAM.
Located on Metrology board.

CPH50 Control Board

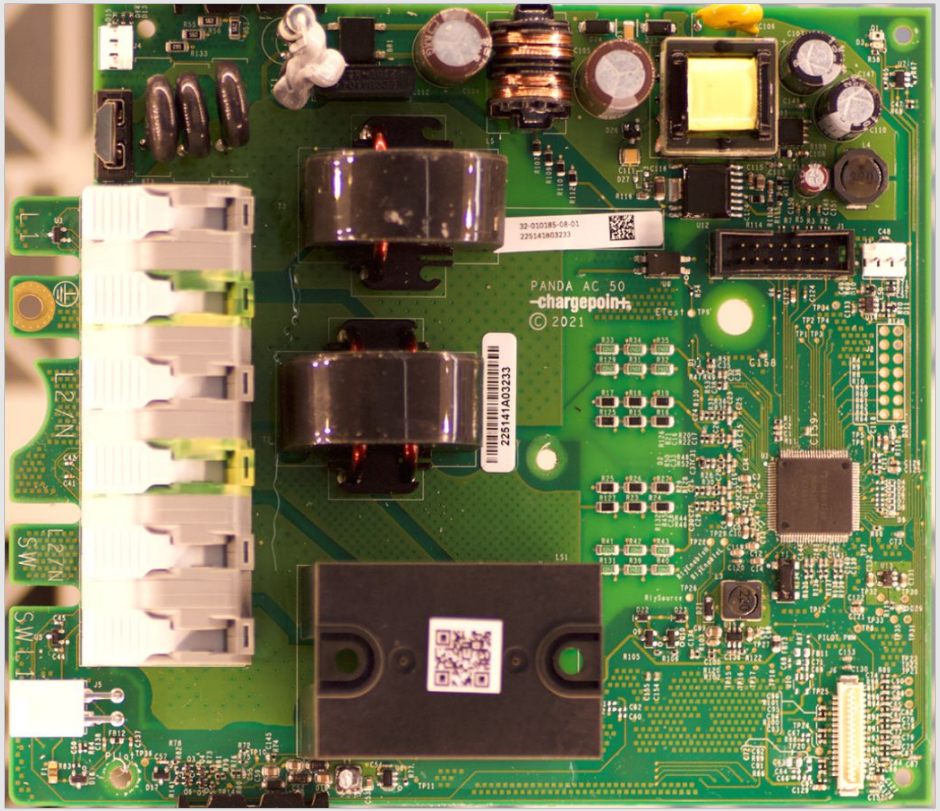


Front

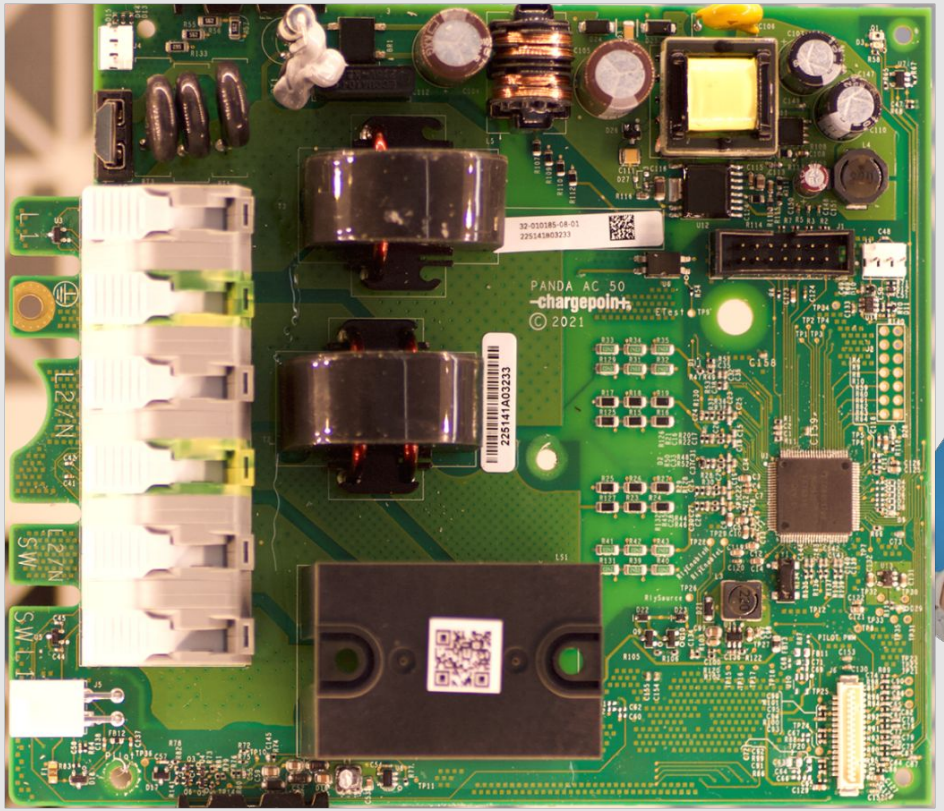


Back

CPH50 Metrology Board



CPH50 Metrology Board



EVSE is Vulnerable

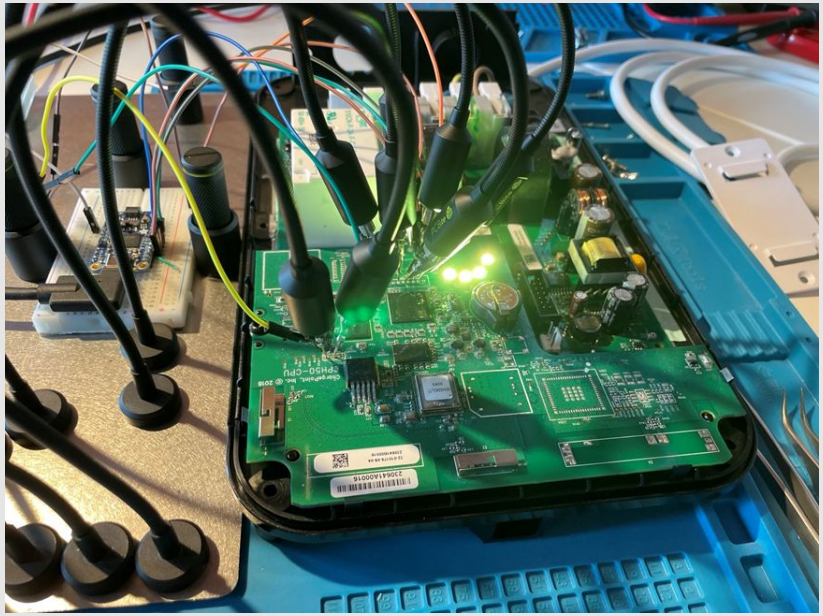
At 2024 Pwn2Own Automotive in Tokyo, EVSE were torn to shreds by experienced vulnerability researchers

> “The reason EVs charging stations David Brumley – have been a special target here [at the event] is it was just the latest thing added”
> Daan Keuper – “It was very clear from the start that security played no role in designing these products. They were not designed to withstand even the most common types of attacks”

ChargePoint released a firmware patch the day before the event which removed a vendor backdoor on all CP products

If an attacker could manipulate EVSE remotely at scale, it would be trivial to cause blackouts by significantly increasing or decreasing bulk electric demand

CPH50 at Pwn2Own: Root in 30



Writeup by CompuTest Sector7

Public Kaspersky research: this is Linux device running U-Boot with JTAG pins on board

Used OpenOCD to use JTAG to disable autoboot
Booted into single-user mode, then added their own user

Telnetd enabled by default and serving setuid shell (discovered right away with login creds, <30 min total)

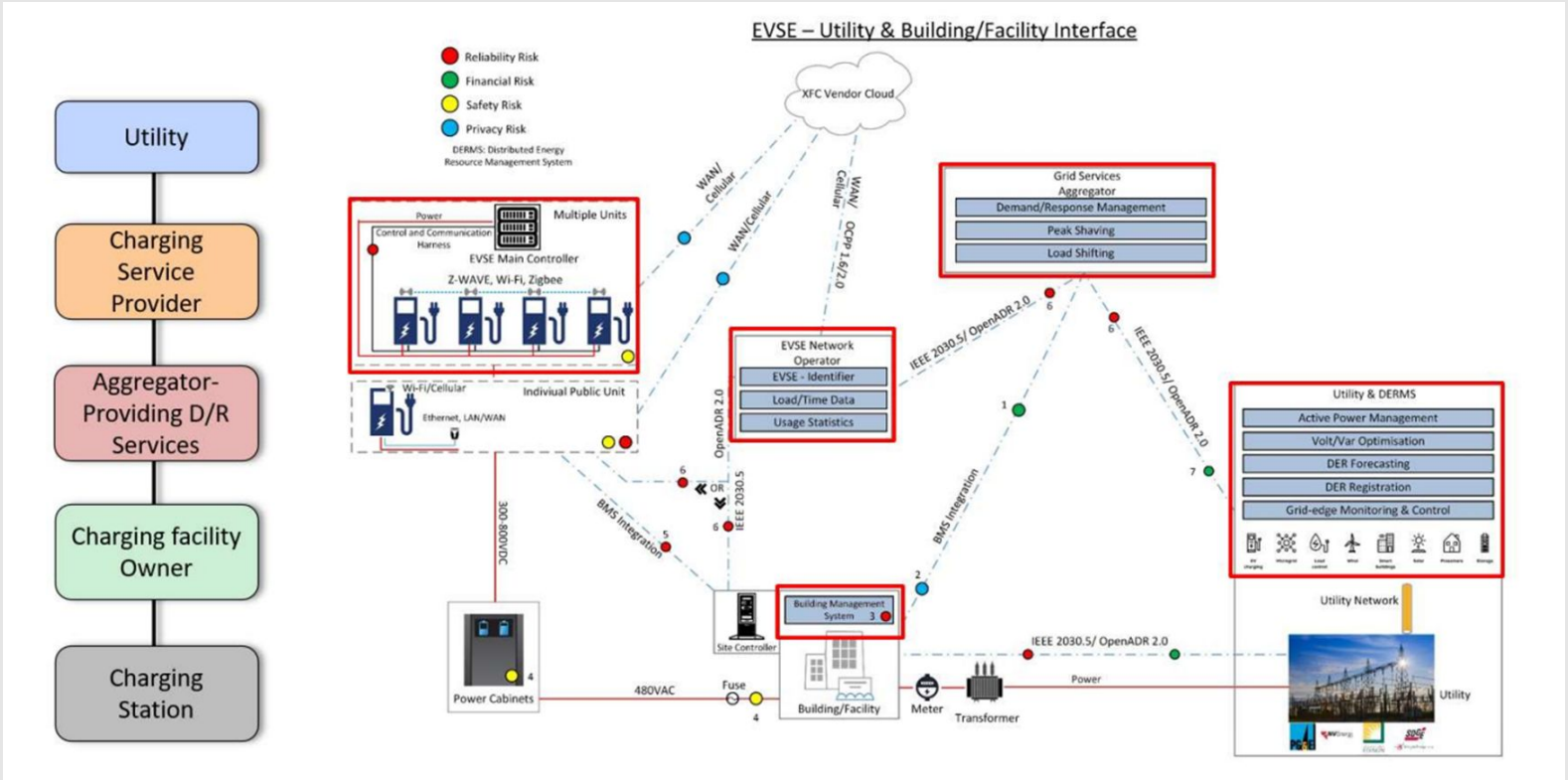
Command injection in the WiFi password field when configuring over Bluetooth
    No auth required for BLE

Read the writeup! Every sentence is scarier than the last
    Publicly observed EVSE attacks currently limited to defacement (Isle of Wight, Russia)

Further EVSE Offensive Research

- https://www.zerodayinitiative.com/blog/2024/8/22/from-pwn2own-automotive-taking-over-the-autel-maxicharger
- https://vicone.com/blog/from-pwn2own-automotive-more-stack-based-buffer-overflow-vulnerabilities-in-autel-maxicharger
- https://www.nccgroup.com/us/research-blog/44con-charging-ahead-exploiting-an-ev-charger-controller-at-pwn2own-automotive-2024/ - Another writeup from Pwn2Own 2024, this one describes how the attackers used tools tools such as firmalyzer, Ghidra, and QEMU
- https://www.youtube.com/watch?v=UmBNgn_9-zY&ab_channel=DEFCONConference - DEFCON32: Building a Secure Resilient Nationwide EV Charging Network, Harry Krejsa and Sarah Hipel

Detailed Overview of EVSEcosystem



OCPP is Potentially Very Vulnerable

OCPP 2.0 has more robust security, but devices in wild support OCPP 1.6 where security is optional

Trouble spots:

- Used for firmware updates, OCPP 1.6 spec recommends doing so over FTP (not FTPS)
- Charge System not well authenticated. Charge System can:
  - Update firmware
  - Change device availability to “not”
  - Cancel charging sessions
  - Refuse to auth charging sessions

Elmo et al. (2023) have demonstrated that ‘cleartext by default’ OCPP 1.6 implementations are vulnerable to MITM and DoS

Elmo's MITM Attack

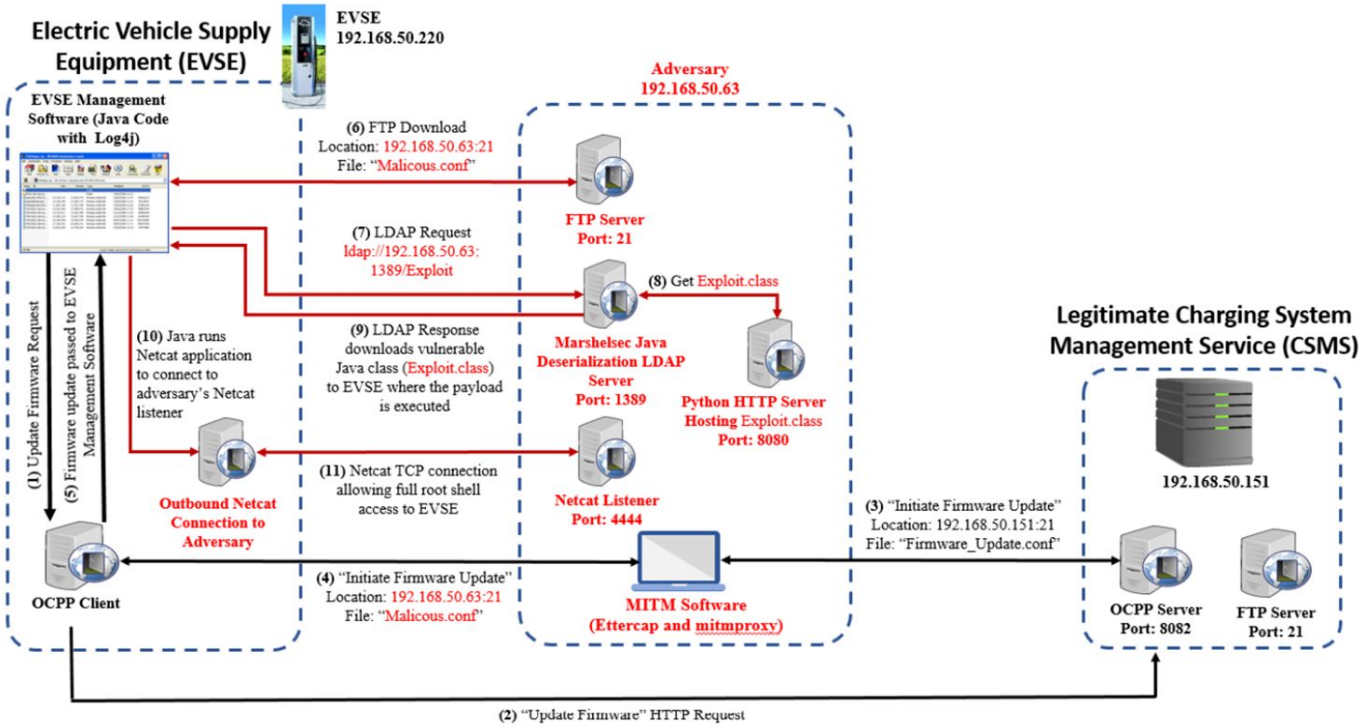


Fig. 2. Sequence diagram of the Log4Shell attack on the OCPP session using the "Update Firmware" request


HACKED=TRUE

Action Items for EVSE Owners/Operators

Create inventory containing, at minimum:
- all EVSE (model number, firmware version),
- all network gear used by EVSE,
- all authorized users of EVSE,
- all user accounts on EVSE

For all user accounts,
- ensure password is securely set and stored in credential management solution.

Ensure procedures to update password(s) are in place and executed regularly.
Ensure device is patched to latest firmware, process exists to regularly check for/install security updates
Ensure device is on secure subnet (i.e. don't put EVSE on guest wifi)

NIST 8473 has guidelines on creating EVSE security program -
https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.pdf

NIST Cybersecurity Framework 1.1

Table 1. Function and Category Unique Identifiers of NIST CSF 1.1

Function	Function Unique Identifier	Category	Category Unique Identifier
IDENTIFY	ID	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PROTECT	PR	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes and Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
DETECT	DE	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
RESPOND	RS	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
RECOVER	RC	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Thank You! Questions?

Please let me know if you have EVSE questions or make EVSE do cool shit:

dmcguire@duqlight.com
https://www.linkedin.com/in/danimcguire/
https://witchofthewires.com