Vulnerability Research Update

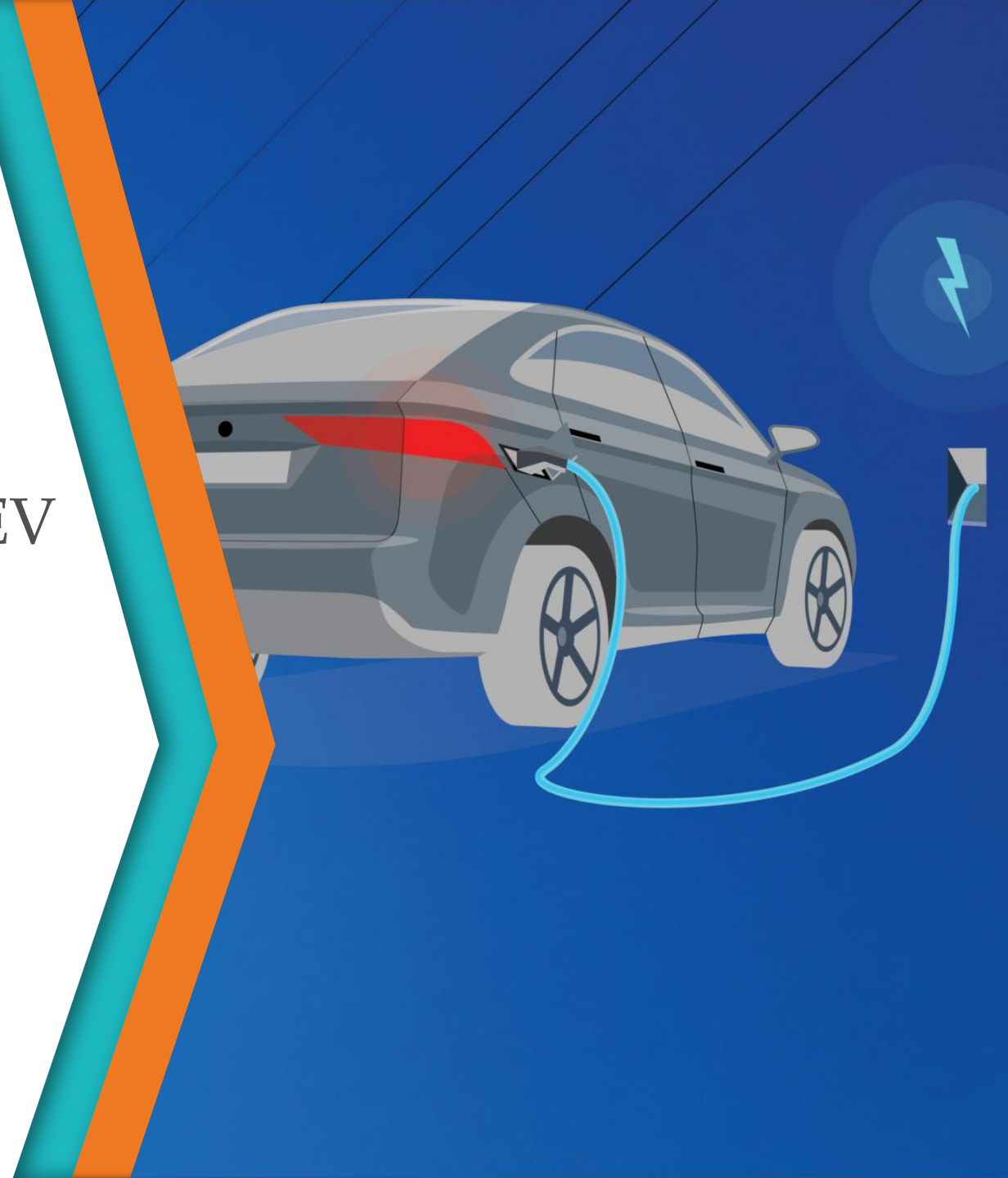
Mohammad Sayed
Independent researcher
Concordia University

Uncovering Covert Attacks on EV Charging Infrastructure

Presented by Khaled Sarieddine

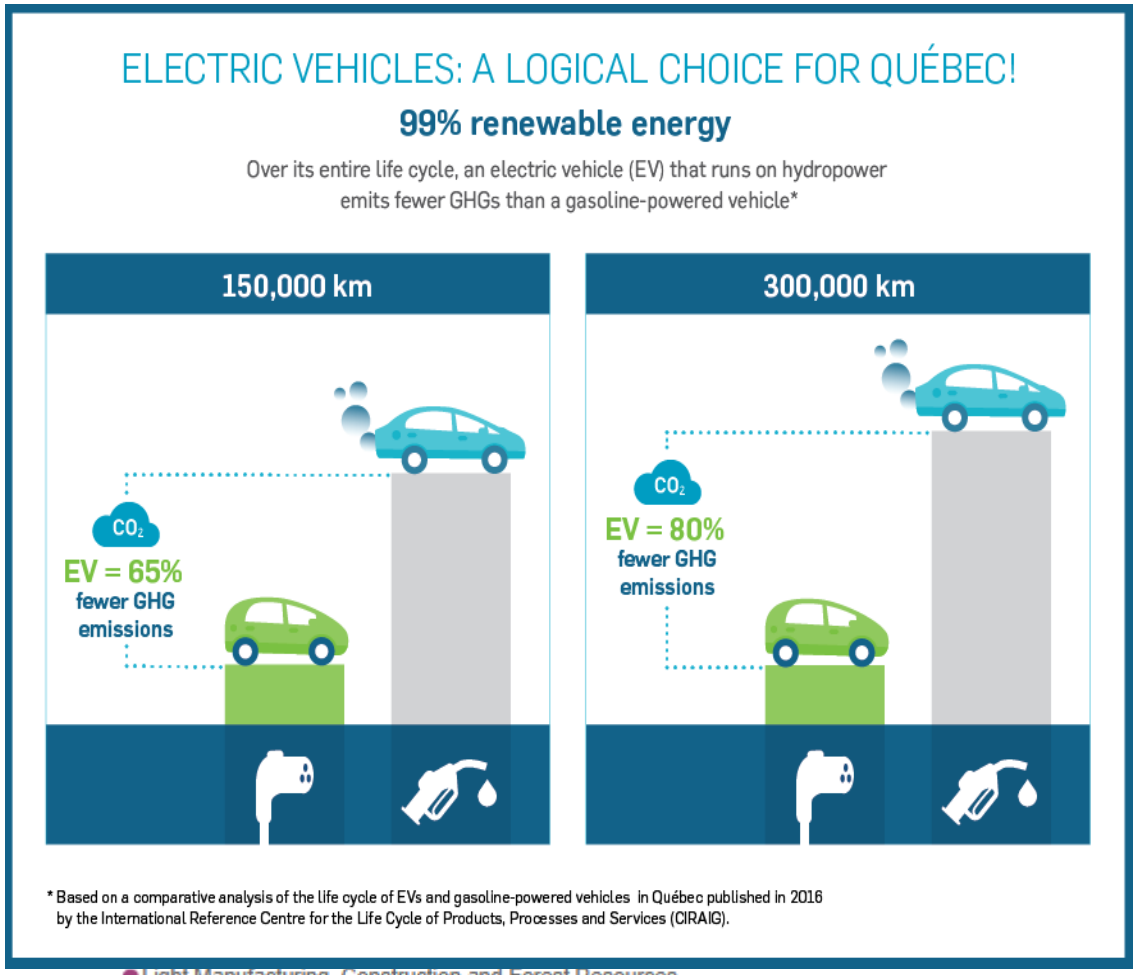
Mohammad Ali Sayed

Presentation Date May 12, 2026



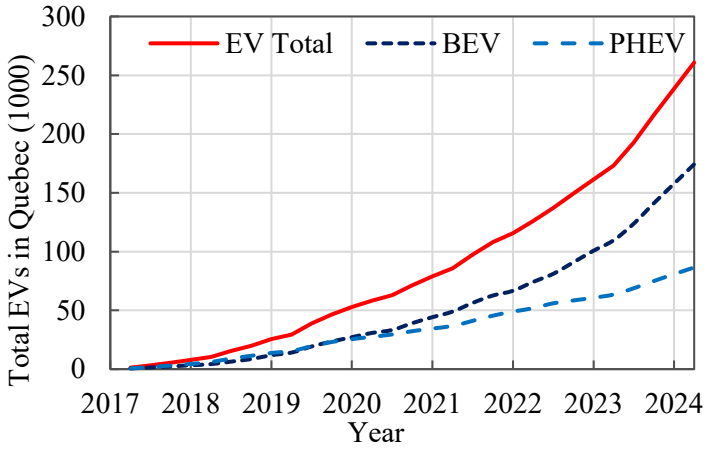
GHG Emissions and Electrification

- The Earth's temperature is about 1.3°C warmer than in the late 1800s due to rising GHG emissions.
- One main contributor (22% in Canada) is transportation.
- As a result, Transportation electrification has emerged as a goal set by governments worldwide to reduce emissions.

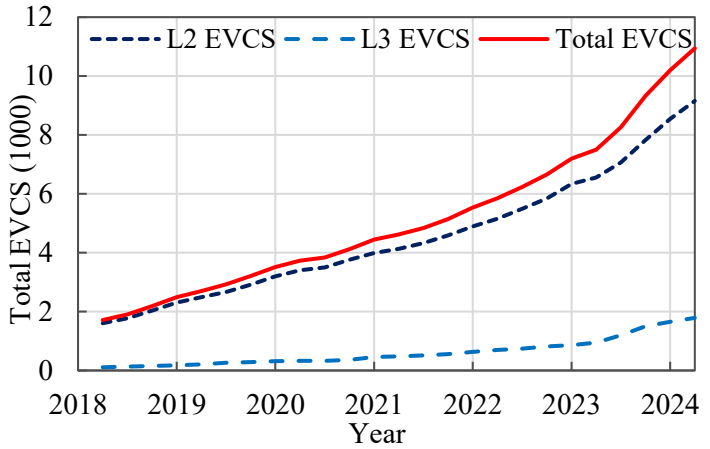


Background and Challenges

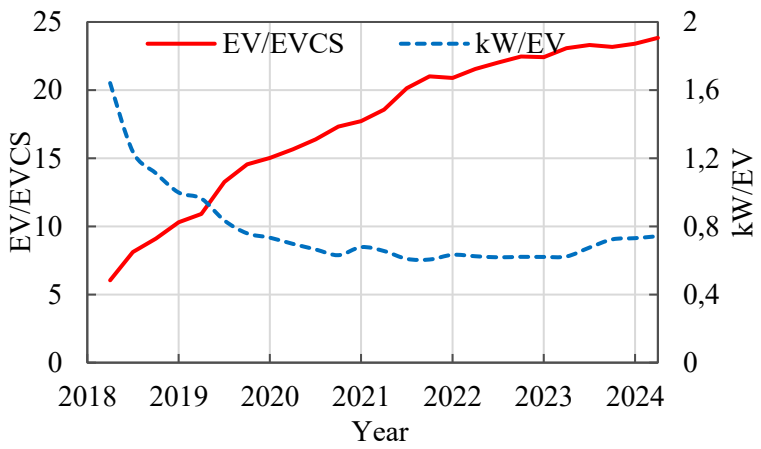
Status of EV Ecosystem Demand



EV proliferation



EVCS expansion



EV:EVCS ratios

- The average demand per EVCS is increasing which is deteriorating the quality of service
- Manufacturers and operators are hastily deploying charging stations without giving due attention to security considerations.
- This has contributed to the EV ecosystem's lack of proper security measures.

Recent Attacks

- In March 2022, Russian EVCSs were hacked through a backdoor and were rendered unavailable by EVs while displaying messages supporting Ukraine and messages against Russia.
- In February 2023, a security researcher was able to compromise an Electrify America EVCS and gain remote control and access by using TeamViewer exposing it to a wide range of attacks.
- In 2024, thousands of Wallbox chargers were recalled in the UK due to fears their vulnerabilities would be weaponized against the national grid.

Electric car charger pulled amid warnings hackers could attack National Grid

Regulator says Copper SB charger, which sells for around £500, does not comply with cyber security laws

Gareth Corfield
Transport Correspondent

Related Topics
Electric cars, National Grid, Cyber attacks, GCHQ

21 February 2024 5:00pm GMT

745

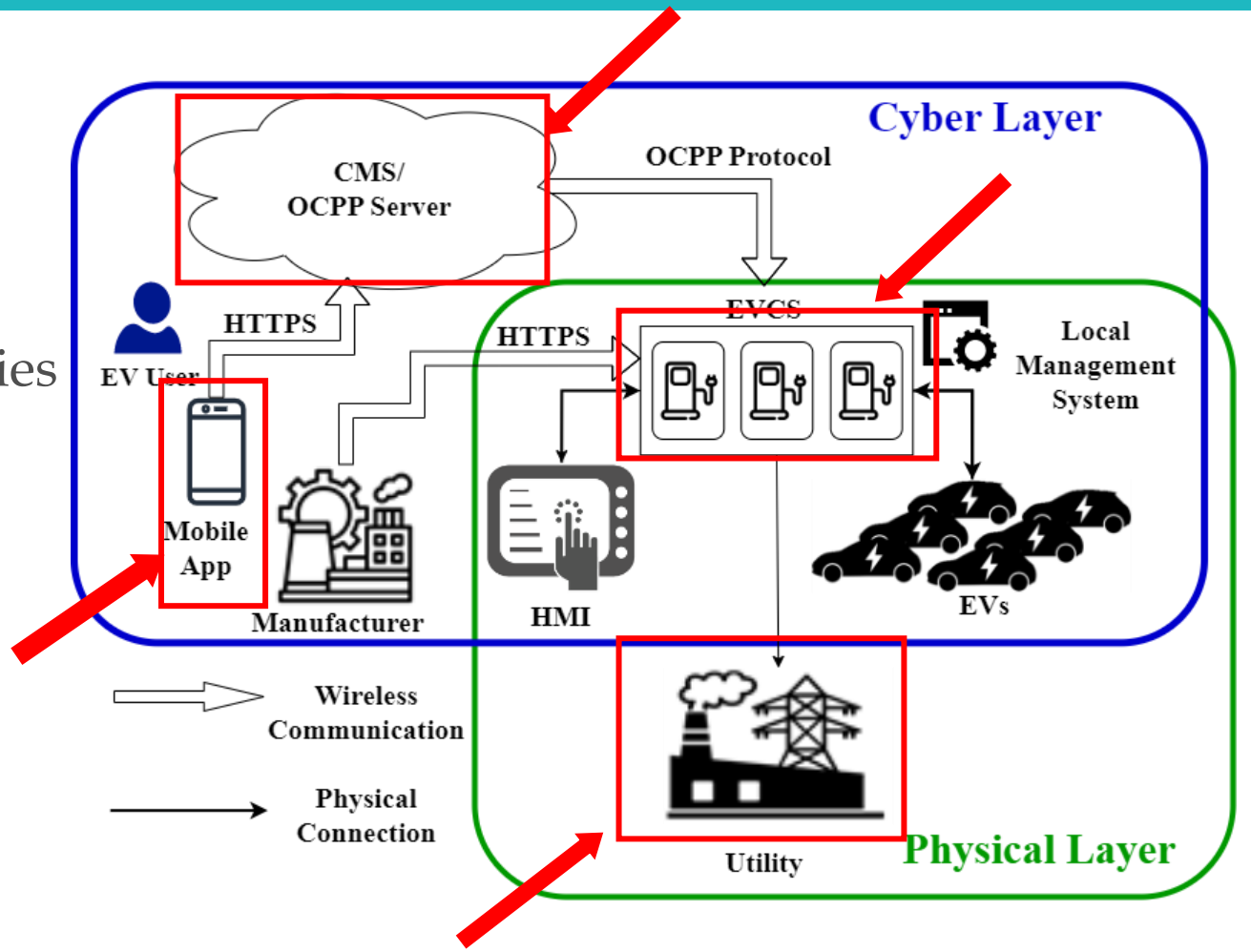
Gift this article free

Wallbox has sold close to 40,000 electric car chargers in Britain, although it is not known how many of these are the affected model

EV Ecosystem Security

EV Ecosystem Security Project

- EV-based attacks against the power grid
  - Unique EV-load characteristics amplify impact
  - New Load Altering (LA) attack families formulated
- EV charging mobile application vulnerabilities
- EV Charging Station (EVCS) vulnerabilities
  - Malware infection
  - Hijacking EVCSs by exploiting design flaws
  - Hijacking EVCSs by exploiting vulnerabilities
- OCPP backend vulnerabilities



EVCSs Vulnerabilities

"Electric vehicle attack impact on power grid operation," International Journal of Electrical Power & Energy Systems 2022

EVCS Vulnerabilities

- EVCSs are IoT devices hosting firmware
  - Inherit a multitude of vulnerabilities from all the participating systems

- Firmware vulnerabilities
  - SQL Injection
  - XML/External Entity Injection
  - Cross-Site Scripting (XSS)
  - …

- These vulnerabilities allow attackers to remotely gain control over EVCS operation

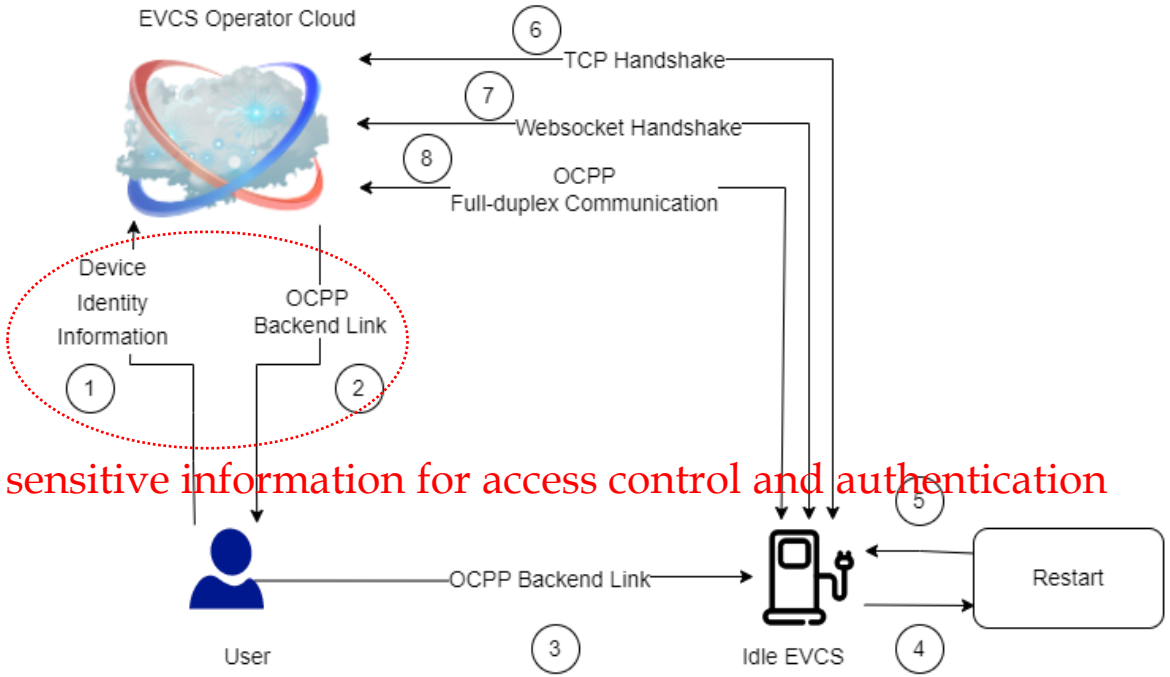
OCPP Backend Vulnerabilities

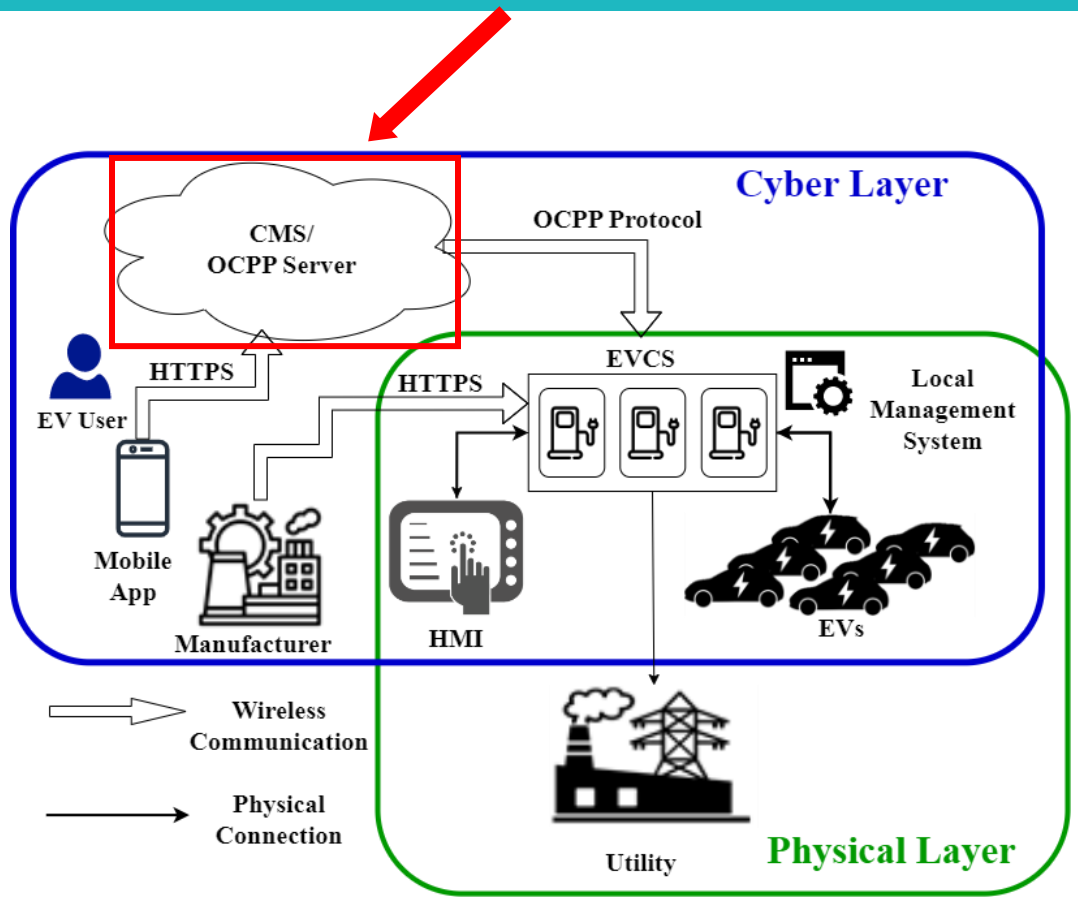
"Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System," Asia CCS 2024

OCPP Backend Vulnerability Testing

- We studied **16 live** OCPP backends and tested them for vulnerabilities.

- We dissected the communication between an EVCS and the CMS upon initiation of the communication and mapped out the communication process.

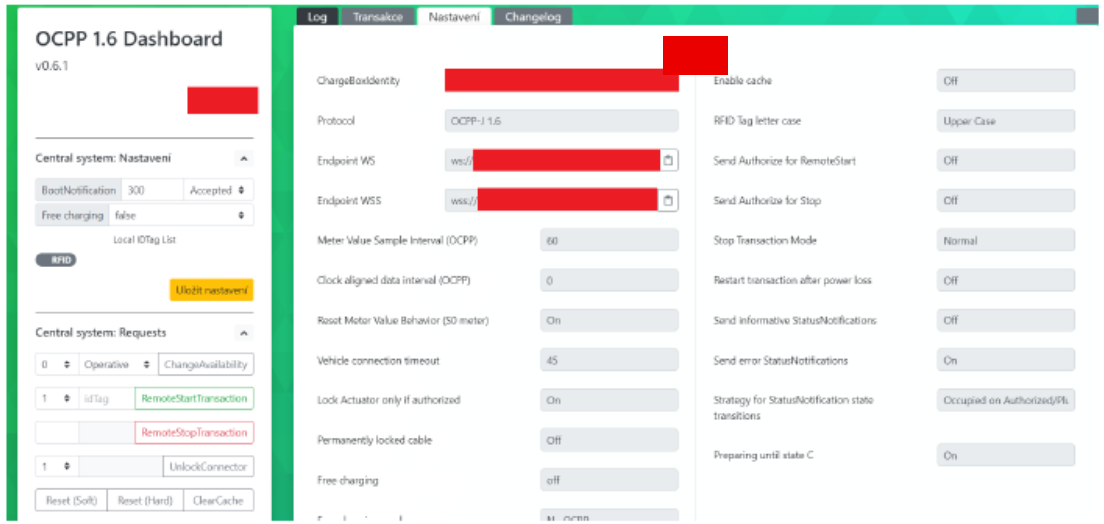




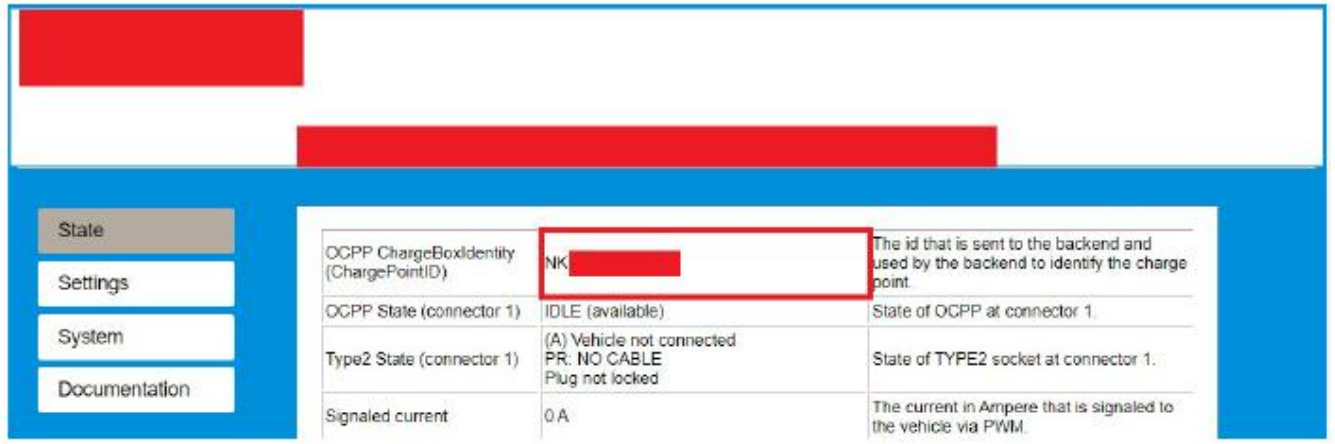
Reconnaissance: OCPP Backends URLs & EVCS IDs

- To gather the OCPP backend and EVCS ID information, we use
  - Device search engines
  - LLMs
  - Discover EVCSs with default configuration online (~ 5K EVCSs were found with default configurations).
  - Publicly accessible maps displaying EVCS IDs

OCPP backend discovered on Zoomeye

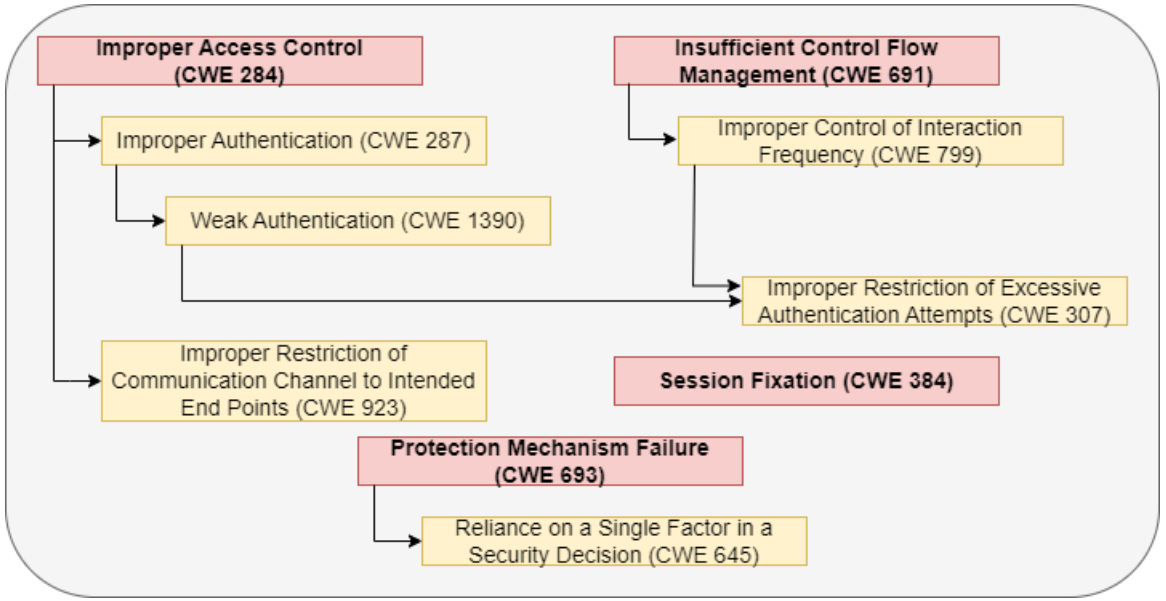


EVCS web portal that publicly exposes the critical information, namely the EVCS ID.



Discovered OCPP Backend Vulnerabilities

- Discovered 6 unique zero-day vulnerabilities in each of the 16 backends.



M. A. Sayed and K. Sarieddine

Vulnerability	CWE	Specific EV Vulnerability
Improper and Weak Authentication	284/287	When a phantom EVCS claims to have a given identity the backend does not sufficiently verify and validate that.
Improper Restriction of Communication Channel to Intended Endpoints	923	Attackers can spoof the real EVCS using a phantom EVCS, thus gaining the same level of access as the real EVCS and continuing to communicate without validating the identity ever again.
Improper Control of Interaction Frequency	799	The backend does not limit the interaction with the EVCS which allows a phantom EVCS/real EVCS to send excessive messages leading to DDoS.
Improper Restriction of Excessive Authentication Attempts	307	The backend does not implement a mechanism by which it can block repeated connections to it allowing the attacker to easily brute force the correct EVCS IDs or even launch a DoS attack on the authentication endpoint.
Session Fixation	384	The backend maintains all previous sessions open with all EVCSs having the same ID but only communicates to the last EVCS with that given ID
Reliance on Single Factor in a Security Decision	654	The authentication process of an EVCS relies solely on the EVCS ID that can easily be obtained by the attacker

Responsible Disclosure

- Post-publication: 47 CVEs assigned across 12 companies via 12 CISA ICS advisories

Company	CVEs Assigned	CISA Advisory	Published	CWEs
EVMAPA	CVE-2025-53968, CVE-2025-54816, CVE-2025-55705	ICSA-26-022-08	01/22/2026	306, 307, 613
CloudCharge	CVE-2026-20781, CVE-2026-25114, CVE-2026-27652, CVE-2026-20733	ICSA-26-057-03	02/26/2026	306, 307, 613, 522
EV2GO	CVE-2026-24731, CVE-2026-25945, CVE-2026-20895, CVE-2026-22890	ICSA-26-057-04	02/26/2026	306, 307, 613, 522
Chargemap	CVE-2026-25851, CVE-2026-20792, CVE-2026-25711, CVE-2026-20791	ICSA-26-057-05	02/26/2026	306, 307, 613, 522
SWITCH EV	CVE-2026-27767, CVE-2026-25113, CVE-2026-25778, CVE-2026-27773	ICSA-26-057-06	02/26/2026	306, 307, 613, 522
EV Energy	CVE-2026-27772, CVE-2026-24445, CVE-2026-26290, CVE-2026-25774	ICSA-26-057-07	02/26/2026	306, 307, 613, 522
Mobility46	CVE-2026-27028, CVE-2026-26305, CVE-2026-27647, CVE-2026-22878	ICSA-26-057-08	02/26/2026	306, 307, 613, 522
Mobiliti	CVE-2026-26051, CVE-2026-20882, CVE-2026-27764, CVE-2026-27777	ICSA-26-062-06	03/03/2026	306, 307, 613, 522
ePower	CVE-2026-22552, CVE-2026-27778, CVE-2026-24912, CVE-2026-27770	ICSA-26-062-07	03/03/2026	306, 307, 613, 522
Everon	CVE-2026-26288, CVE-2026-24696, CVE-2026-20748, CVE-2026-27027	ICSA-26-062-08	03/03/2026	306, 307, 613, 522
CTEK Chargeportal	CVE-2026-25192, CVE-2026-31904, CVE-2026-27649, CVE-2026-28204	ICSA-26-078-06	03/19/2026	306, 307, 613, 522
IGL-TechnologieseParking.fi	CVE-2026-29796, CVE-2026-31903, CVE-2026-32663, CVE-2026-31926	ICSA-26-078-07	03/19/2026	306, 307, 613, 522

OCPP Backend Vulnerability Testing

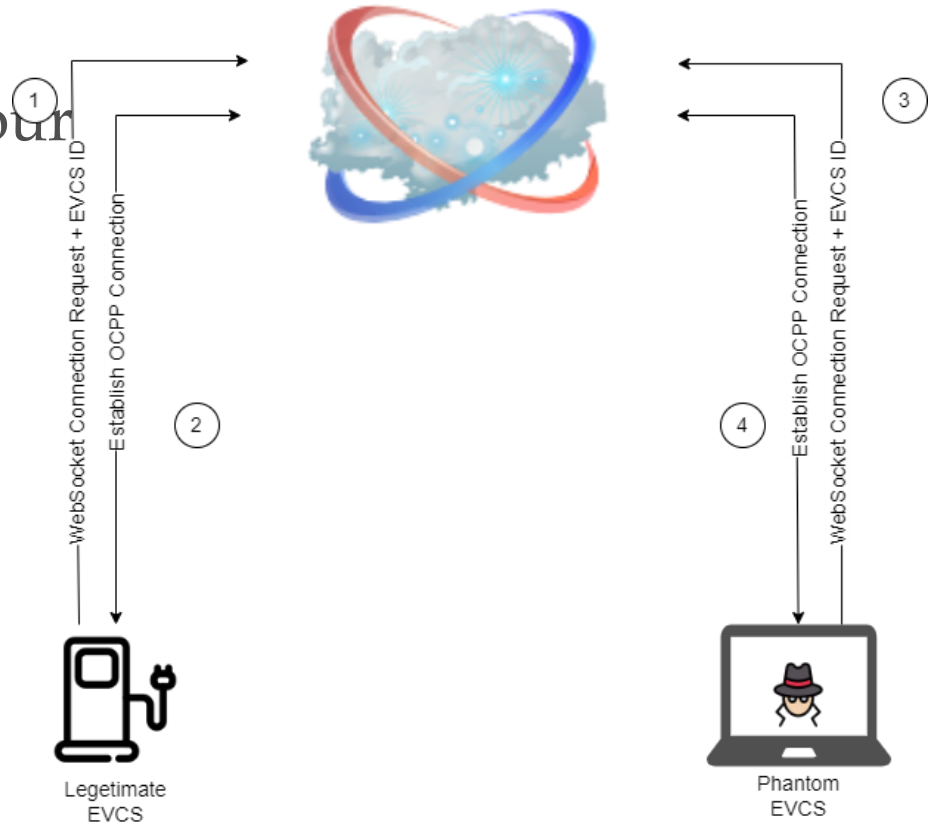
- We run the phantom EVCS with an EVCS ID.
- The CMS mistakenly establishes a connection with our phantom EVCS, impacting the existing connection with the real EVCS.

```
GET /ocpp/AL0012********** HTTP/1.1
Host: ********************************
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: Y0uV9twZ1VSMufPeKuuFIA==
Sec-WebSocket-Version: 13
Sec-WebSocket-Extensions: permessage-deflate; client_max_window_ bits
Sec-WebSocket-Protocol: ocpp1.6
User-Agent: Python/3.10 websockets/10.3

HTTP/1.1 101 Switching Protocols
Date: Fri, 11 Nov 2022 23:23:34 GMT
Connection:  upgrade
Upgrade: websocket
Sec-Websocket-Accept: pMY2xx7ja0ibXDSIMuWMCoFJTQA=
Sec-WebSocket-Protocol: ocop1.6

.....x...Z.....A.....A....U...A.....O.....6.....Z.....Z.....
.....%.x[3,"ce6f83e9-****-****-
****-**********",{"currentTime":"2022-11-11T23:23:34.828Z","interval":
180,"status":"Accepted"}].H(2,dce7ebf0-****-****-****-
**********","GetConfiguration",{"key":[]}].....Y.*.f.c.g.`./.4.5.6.g.+.;.7.d.?.4.3.c.?.
.}.a.h.l.s.c.o.l.c. .]. .c. .$. .$.g.b.l...8.g.q.*.t.j.g.<. .[._
```

TCP flow showing the acceptance of the connection from the phantom EVCS by the OCPP backend showing the date of the discovered vulnerability

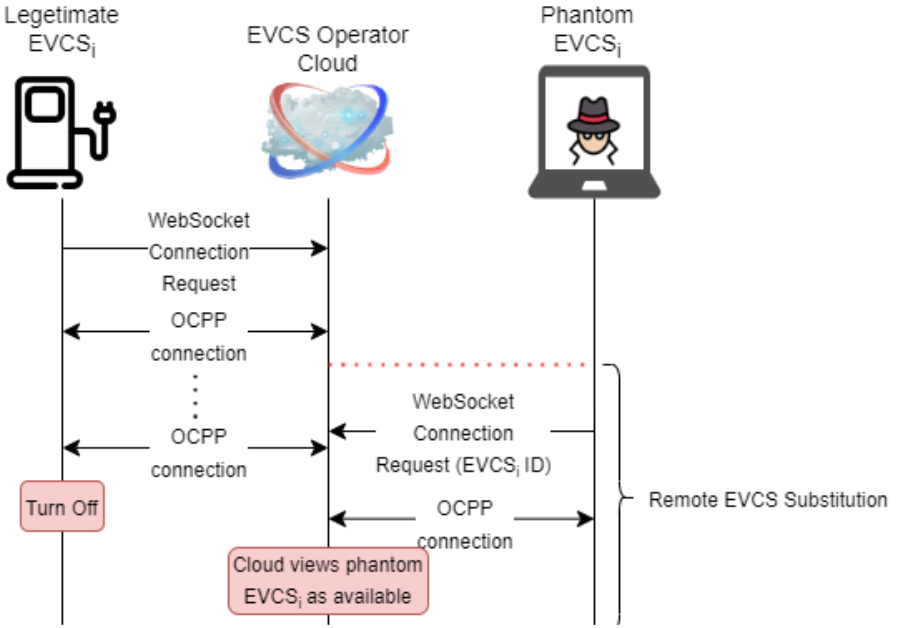


Phantom EVCS imitates a real station and runs OCPP client.

Attack Workflow

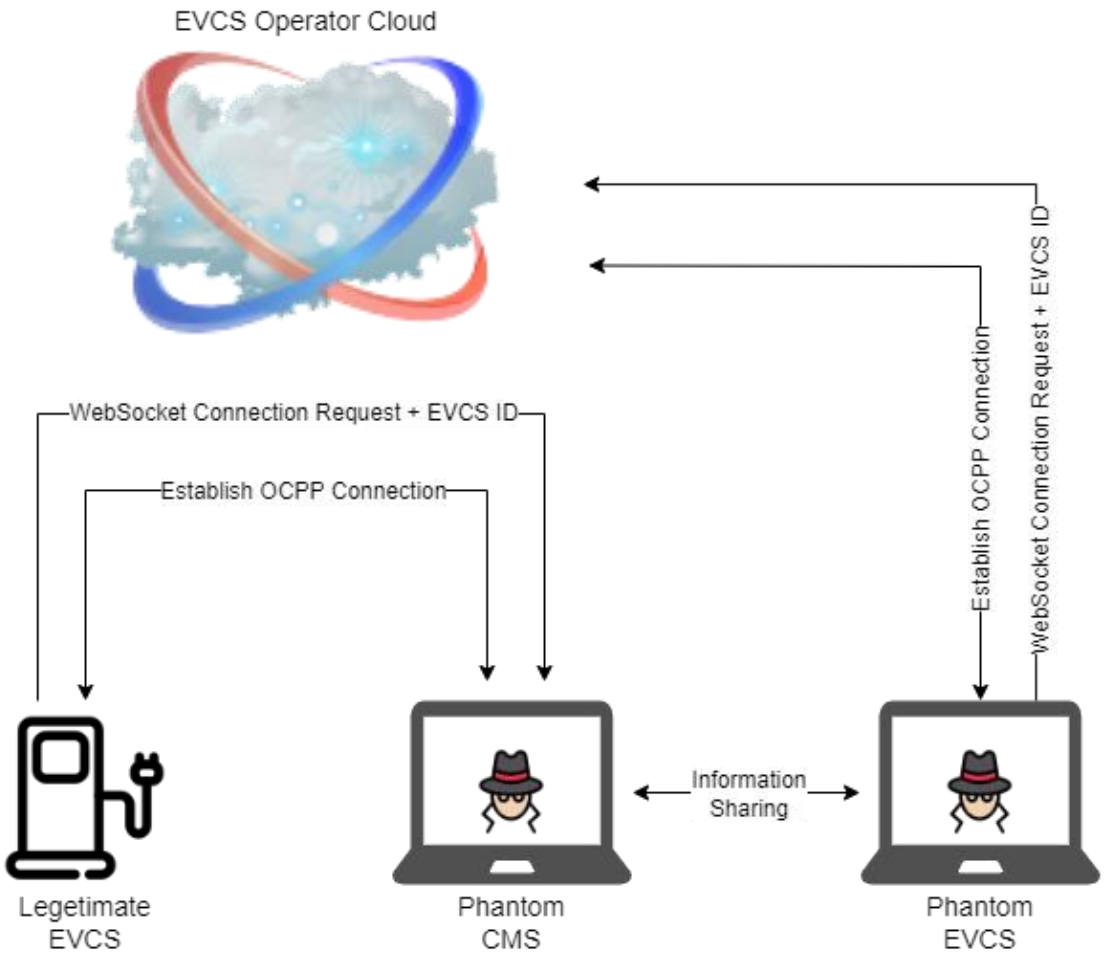
- Remote EVCS Substitution:
  - When turning off the EVCS, the cloud shows it is offline
  - After spinning on a phantom EVCS, the cloud shows the EVCS is now online.
  - When sending commands from the cloud, the phantom EVCSs receives them.

- Remote EVCS OCPP Connection Hijacking:
  - After turning on the real EVCS we spin off a phantom EVCS concurrently.
  - The cloud maintains a connection with the real EVCS.
  - However, future traffic is routed to the latest session initiated in our case by the phantom EVCS.



Attack Scenarios

- OCPP Backend Denial of Service (multiple Phantom EVCSs can connect)
- EVCS Denial of Service
- Firmware Theft
- Data Collection and Data Poisoning
- Covert Attacks
  - Stealthy Ransom Attack
  - Stealthy Power Grid Attack



Mitigation and Prevention

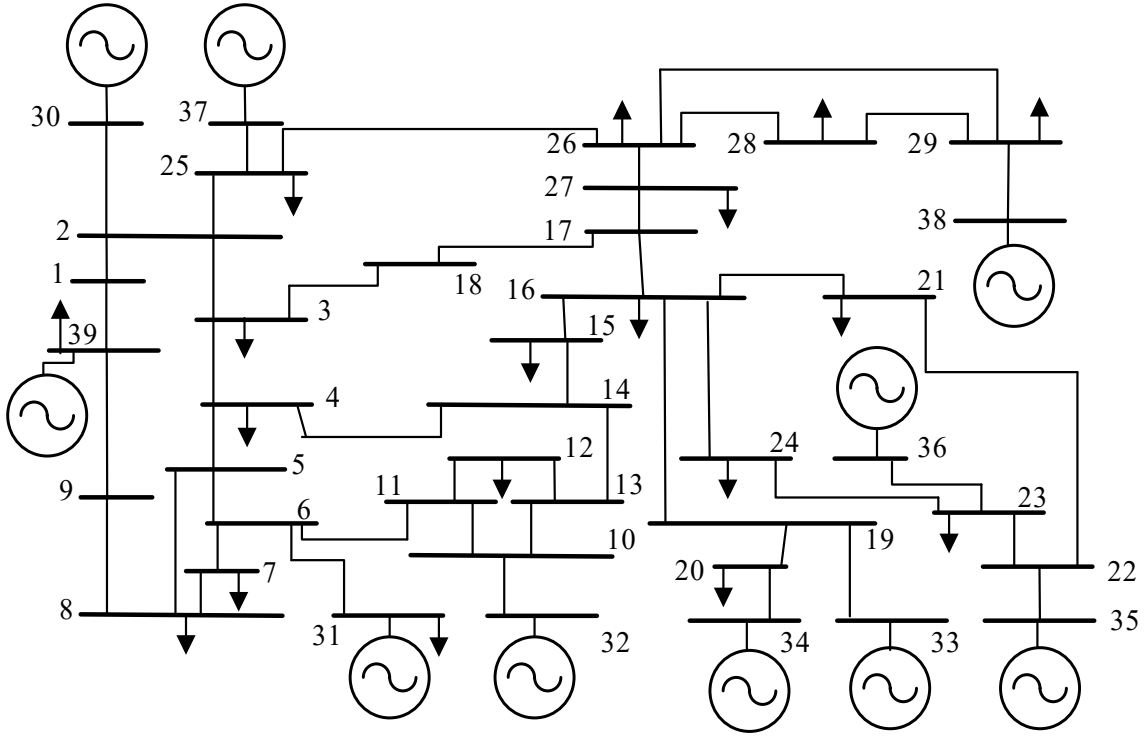
- Certificates must be used for mutual authentication between an EVCS and the backend
- The backend must invalidate sessions from multiple EVCSs having the same ID
- Rate limiting must also be adopted to restrict an attacker's ability to perform repeated connection attempts and brute-force IDs that are not known.
- The backend must limit the frequency at which EVCSs can interact with it to prohibit excessive messages leading to DDoS.

Attacks Against the Power Grid

"Grid Chaos: An uncertainty-conscious robust dynamic EV load-altering attack strategy on power grid stability," Applied Energy 2024

Attacks Against the Power Grid

- EV-based attacks were simulated against the NE 39 bus grid.

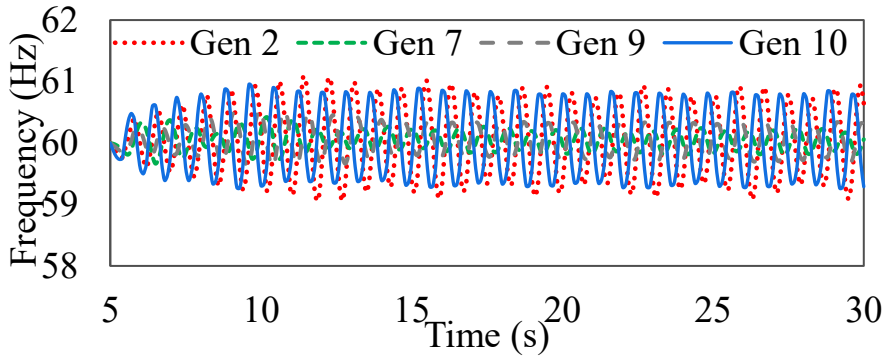


Static Attacks

- Attacks especially during peak times cause
  - Shift the system away from the optimal dispatch point
  - Extra costs
  - Increased transmission losses
  - Cause line outages
  - Voltage imbalance

Switching Attacks

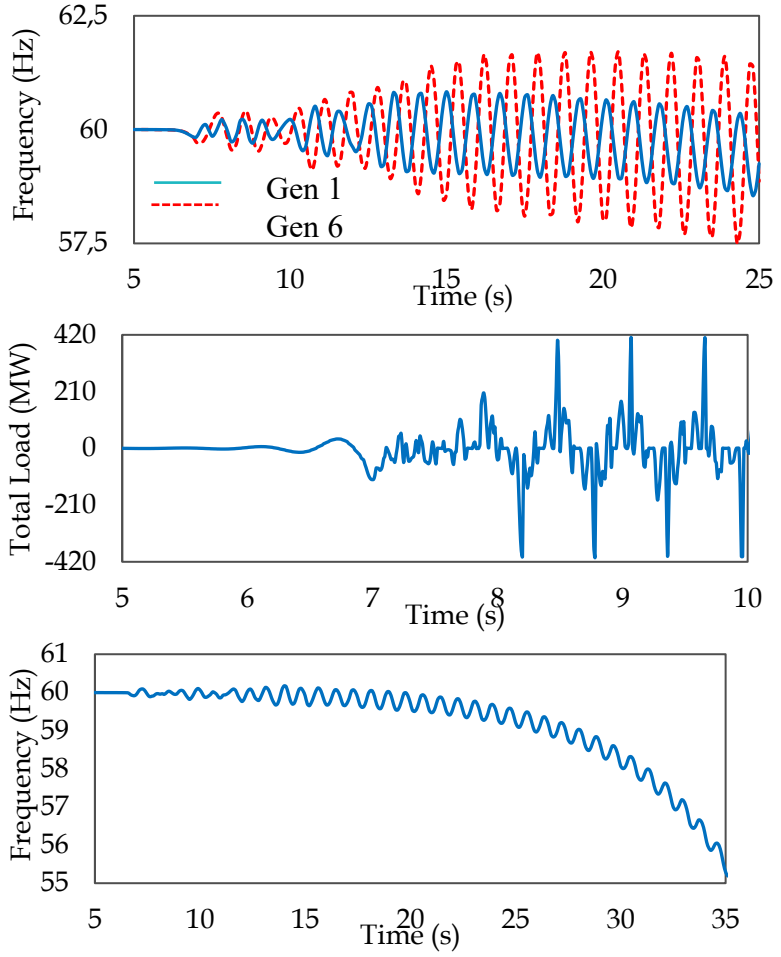
- Switching attacks can excite certain unstable modes in the power grid.
  - During the reconnaissance phase, the attacker needs to determine the frequency of an unstable mode that exists in the power grid.
  - The loads are then switched on and off at that specific frequency to excite the unstable mode.
  - Even in the absence of violations, sustained oscillation causes damage to generators



Dynamic Attacks

- Dynamic Attacks force new unstable modes onto the power grid by crafting the trajectory of the attack load to maximize its impact on the grid.
  - The EV load is modeled as a feedback gain controller and oscillated following the mathematical model developed to shift the system towards new unstable modes

- EVs are ideal for this type of attack due to their controllable load, power factor, reactive power, and V2G abilities



Conclusion

Conclusion

- OCPP backends and EVCS IDs are discoverable using public sources

- Using a backend URL and an EVCS IDs, a malicious actor can:
  - Connect and authenticate a charging station script they control to the backend
  - Launch DoS attacks against this backend
  - Perform long-term stealth reconnaissance

- Combined, EVCS and backend vulnerabilities can be used to launch undetectable attacks against the power grid