Secure Systems Group, Aalto University

Radu Pogonariu, Philip Ginzboorg (Aalto University), Panagiotis Papadimitratos (KTH), Jose Luis Martin Navarro, Mika Lehmusto (Aalto University)

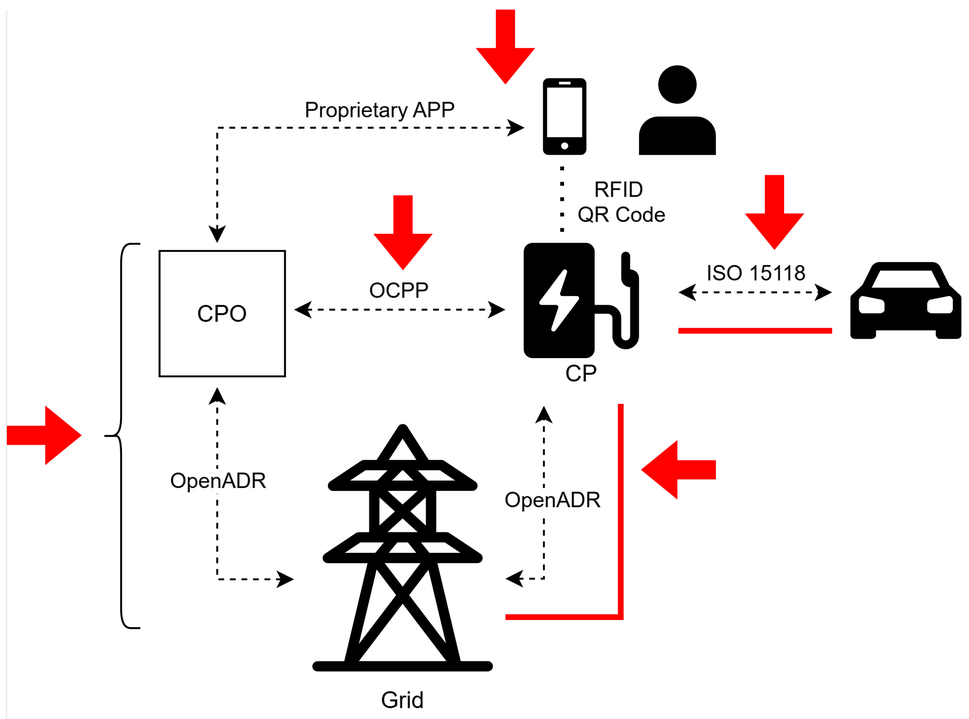
Cyber Threats on Electric Vehicle Charging Systems

Objectives

- Define a system model of EVCS based on a literature survey.
- Analyze the cybersecurity threats to EVCS within that model.
- Analyze the cybersecurity threats to parts of a commercial EVCS.

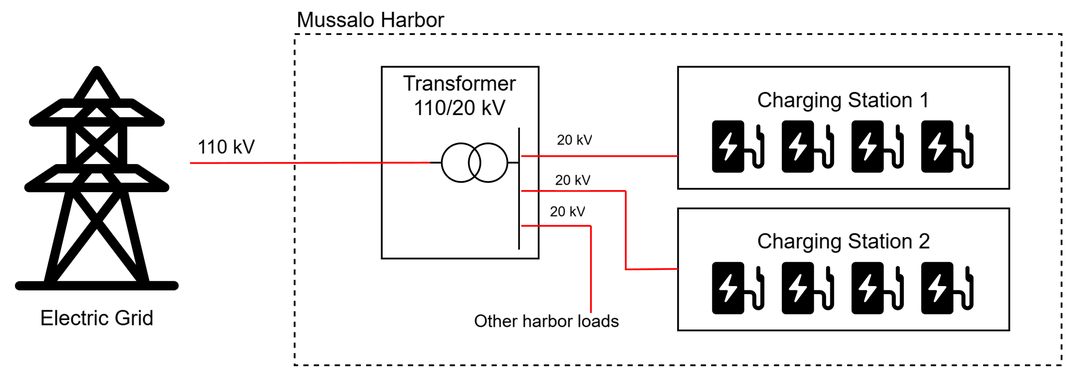
Figure 1: Examples of EV Charging Points

Threats on the system

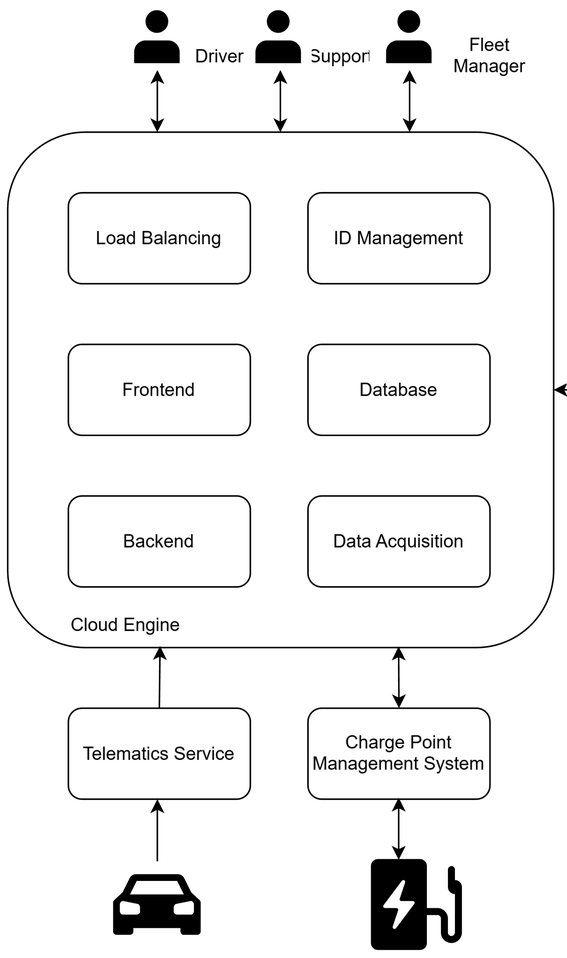


System interface	Attack	Countermeasure
OOB Channel	QR code spoofing	Dynamic QR Code
	NFC token cloning	Tamper-proof hardware
	Charging session hijacking	Association EV – charging session
CP-EV Interface	Electrical Vehicle Impersonation Attack	PKI in ISO 15118 interface
	Wireless Denial of Service	Software fix, cable isolation
Grid	Abnormal load on the grid	Automatic grid segment isolation
Network	Network based attacks	Updated firmware
	OCPP	TLS with Client-Side Certificates

Case study: Charging stations deployment in Mussalo harbor



Security Assessment of PragmaCharge Cloud Engine



Based on:

- Developer interviews
- Access to Cloud Engine
- SBOM Analysis

SBOM Analysis

	Severity of vuln.	
Component	**Moderate**	**High**
Backend	2 (b, c)	1 (a)
Frontend	2 (b, d)	1 (a)
Service A	2 (b, d)	
Service B	2 (b, d)	

Threats on Cloud Engine

Attack	Countermeasure
False charging session via unauthorized truck	Dynamic QR Code
Synchronized charging attack	Scheduling algorithm
False data injection from CPMS	Anomaly detection
False telematics data injection	Anomaly detection
GPS spoofing or jamming	Multi-factor location verification
Identity Manager Compromise or Outage (Single Point of Failure)	Define a business continuity plan

Aalto University

KTH VETENSKAP OCH KONST