APEC 2025

Atlanta, GA

March 16-20

Georgia World Congress Center

Securing Electric Vehicle Charging Stations

Patrick Rempel
Professor at Hochschule Harz

Patrick Rempel (Harz University of Applied Sciences)
André Büttner (Actain Engineering)

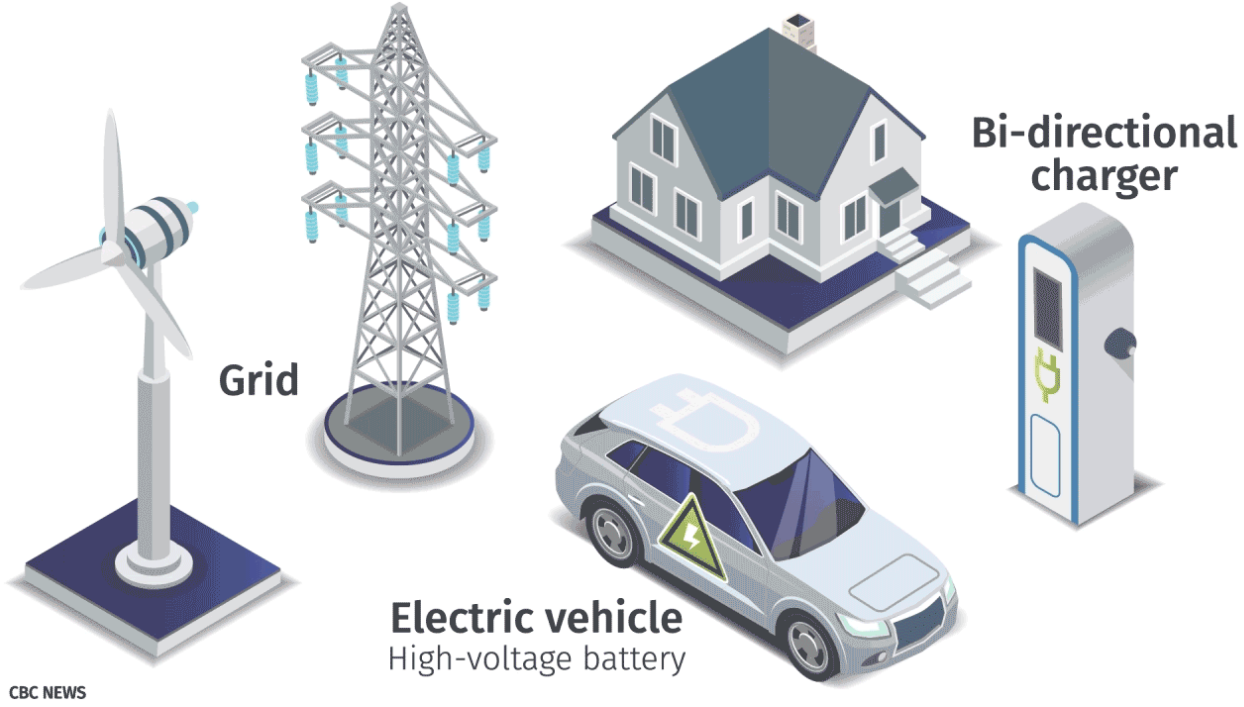
prempel@hs-harz.de | andre.buettner@actain.de

André Büttner
Acting on sustainable electronics

Hochschule Harz

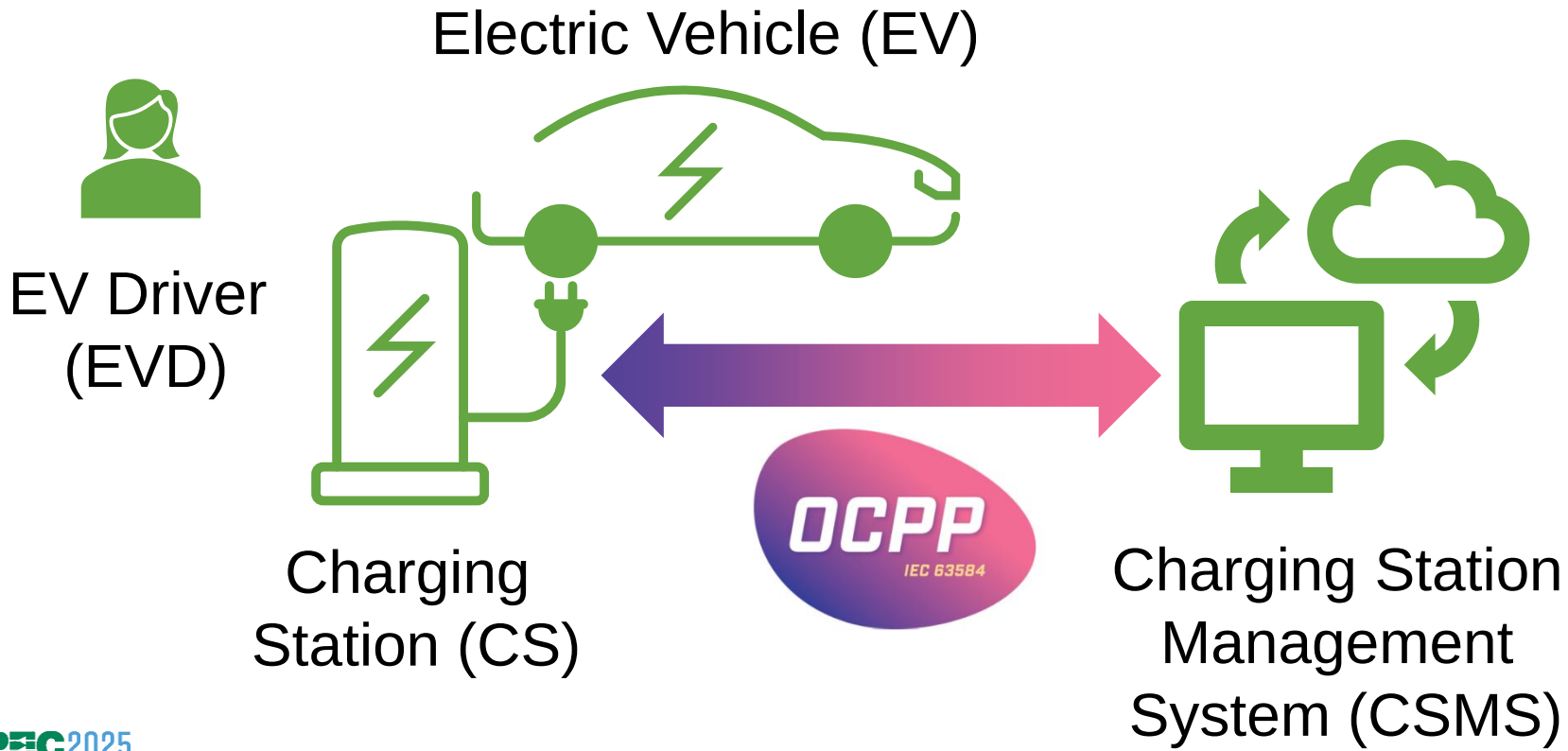
actain engineering

Electric Vehicle Charging



[https://www.cbc.ca/news/science/ev-to-grid-1.6100454, Accessed 03/19/2025]

Open Charge Point Protocol (OCPP)



Electric Vehicle Driver Authentication

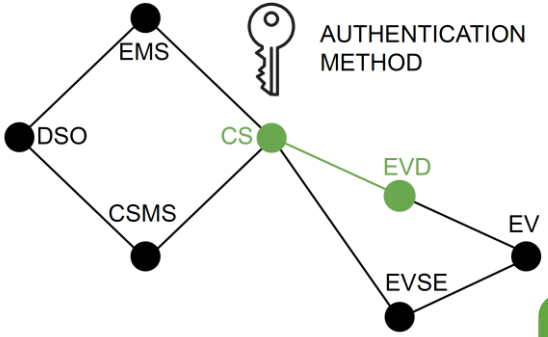
Access Control

Fraud Prevention

Billing & Payment

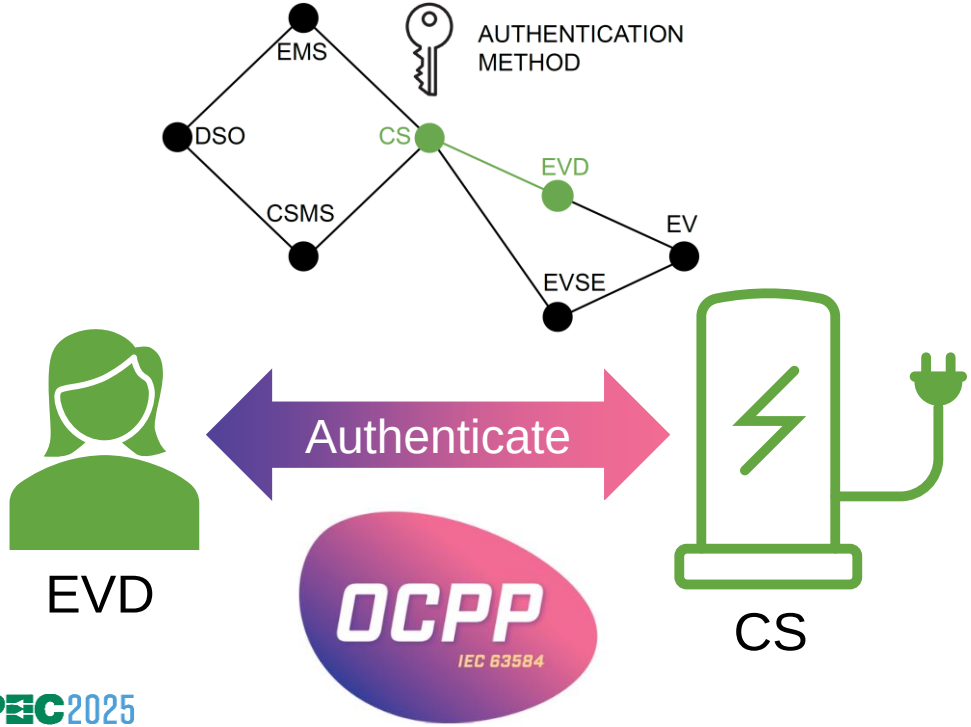
Load Managemt.

Authentication Use Cases in OCPP



C01: RFID

Authentication Use Cases in OCPP



C01: RFID

C02: Start Button

C03: Debit/Credit card

C04: PIN-code

C05: App

C06: Parking Ticket

…

Electric Vehicle Driver Authentication

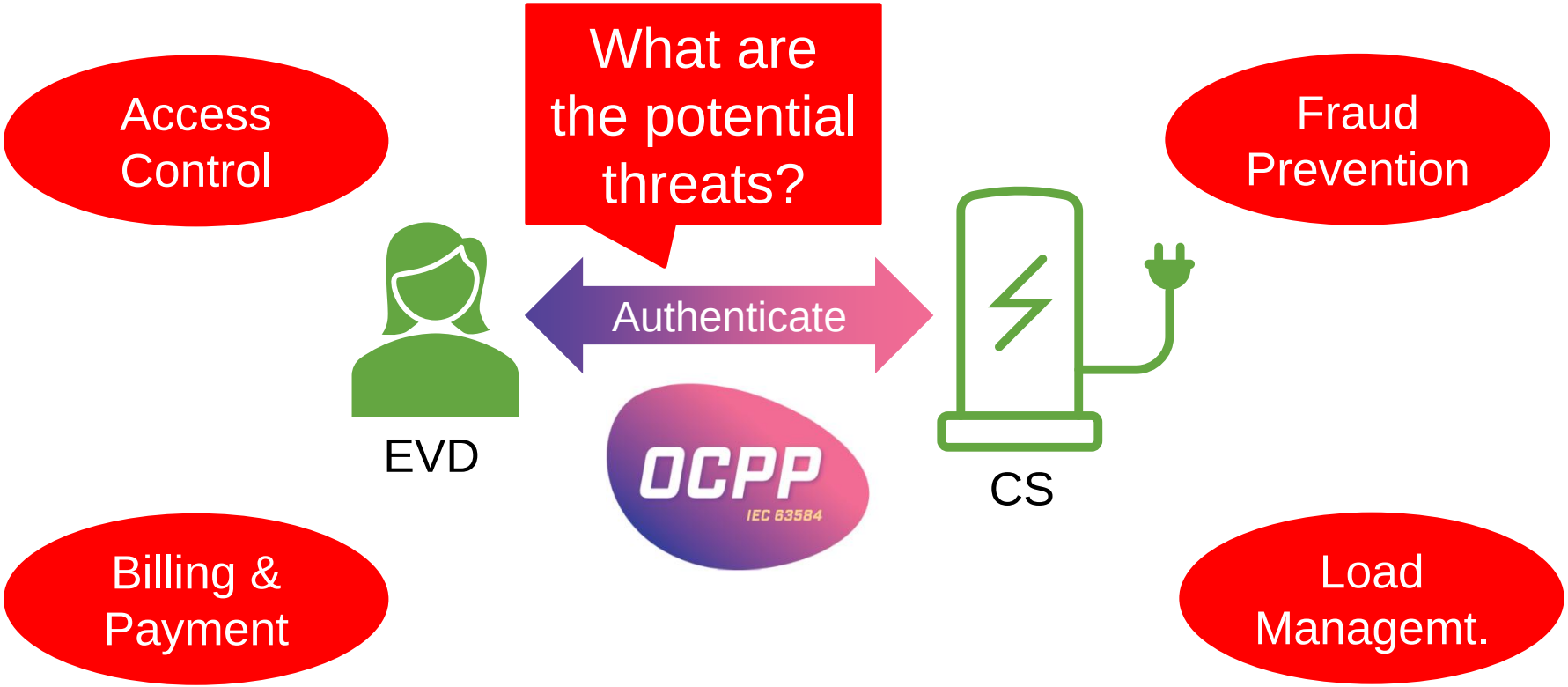
Access Control

Fraud Prevention

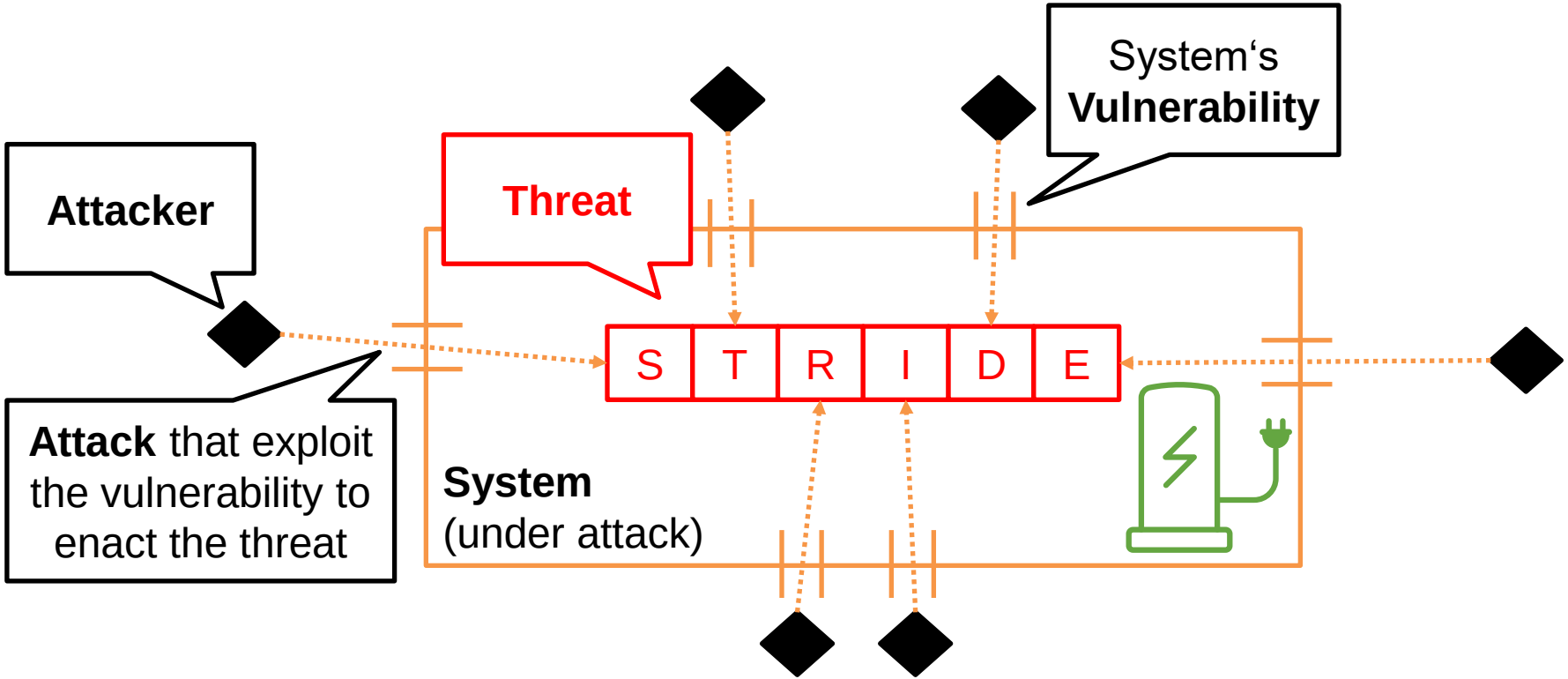
Billing & Payment

Load Managemt.

Electric Vehicle Driver Authentication

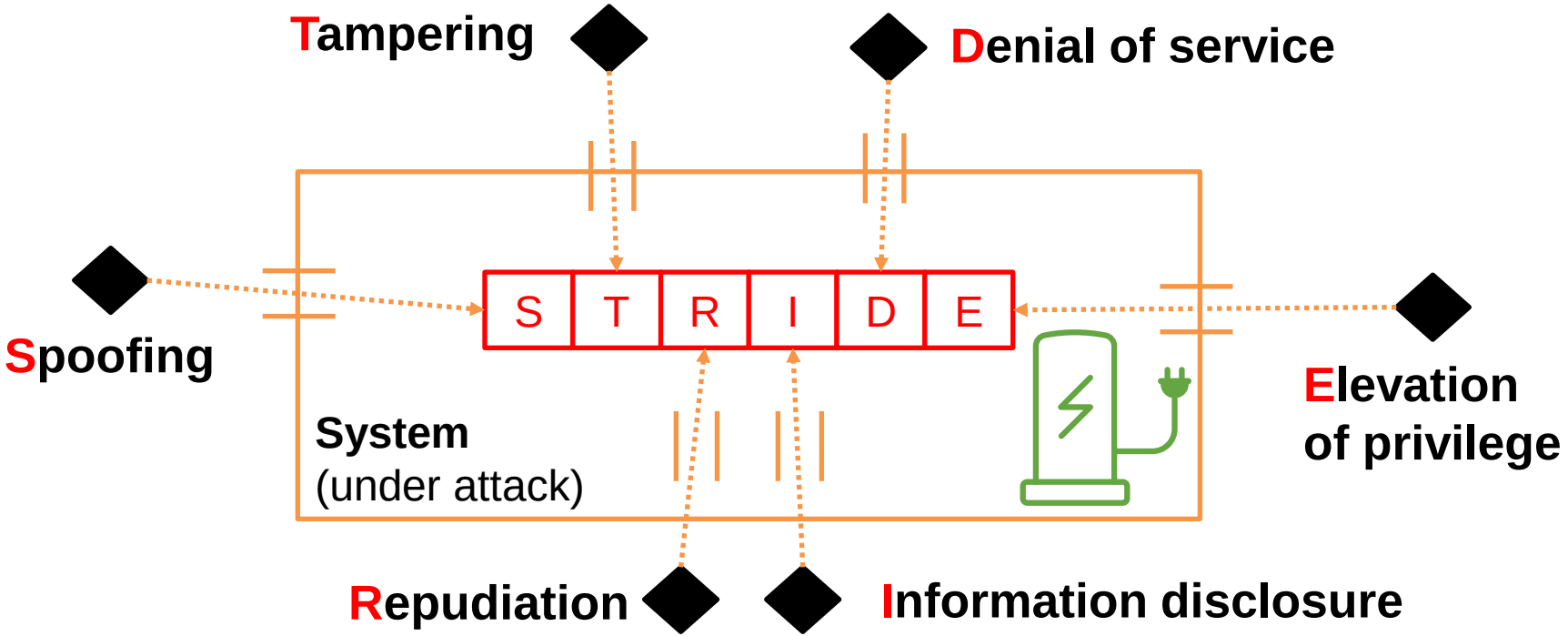


Threat Modeling with STRIDE



[Kohnfelder and Garg 1999, "The threats to our products"]

Threat Modeling with STRIDE

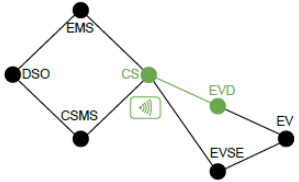
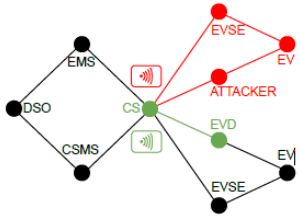


Survey

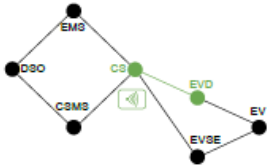
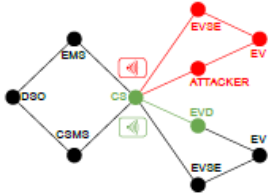
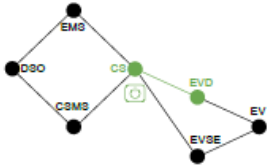
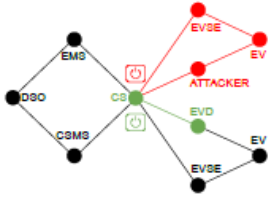
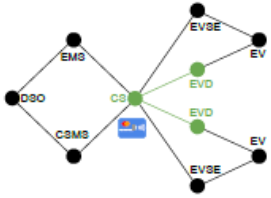
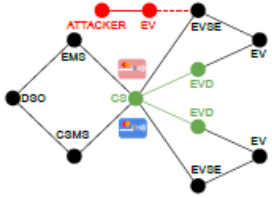
- Systematic literature survey
- Snowball sampling (three seeds)
- Candidates: 247 papers
- Included: 23 papers
- Inclusion criteria
  - Paper must examine authentication vulnerabilities (C01..C06)
  - Published in 2018 or later (OCPP 2.0.1)

Survey Results

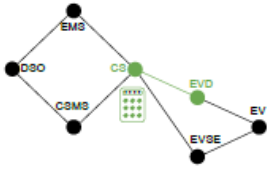
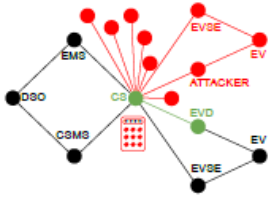
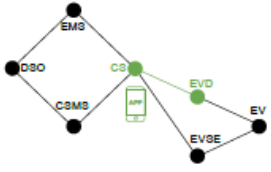
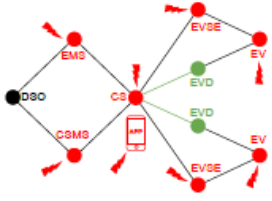
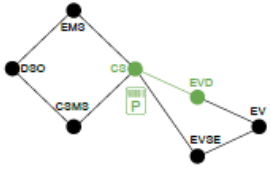
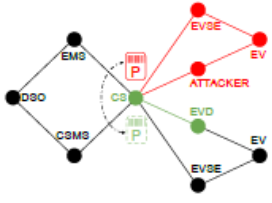
LITERATURE SURVEY RESULTS - GROUPED BY OCPP AUTHENTICATION USE CASE AND STRIDE ATTACK TYPE

Use Case	Initial Situation	Weakness	STRIDE Attack Type	Relevant Study	Relative Frequency
C01: Driver Authentication using RFID			Spoofing Tampering Repudiation Information Disclosure Denial of Service Elevation of Privilege	[4], [34], [8], [9], [26], [17] - - - - [4], [8], [17]	85.71% - - - - 42.86%

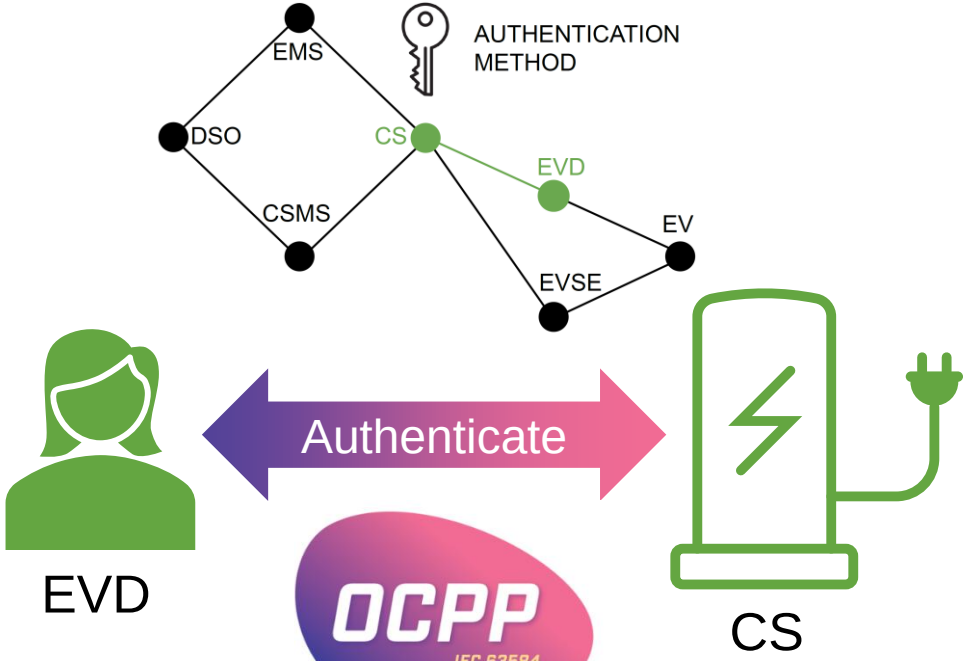
Survey Results: C01 – C03

Use Case	Initial Situation	Weakness	STRIDE Attack Type	Relevant Study	Relative Frequency
C01: Driver Authentication using RFID			Spoofing	[4], [34], [8], [9], [26], [17]	85.71%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	-	-
			Denial of Service	-	-
			Elevation of Privilege	[4], [8], [17]	42.86%
C02: Using a Start Button			Spoofing	[4], [32]	28.57%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	-	-
			Denial of Service	-	-
			Elevation of Privilege	[4]	14.28%
C03: Using a Credit/Debit Card			Spoofing	[4], [17]	28.57%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	-	-
			Denial of Service	-	-
			Elevation of Privilege	[4]	14.28%

Survey Results: C04 – C06

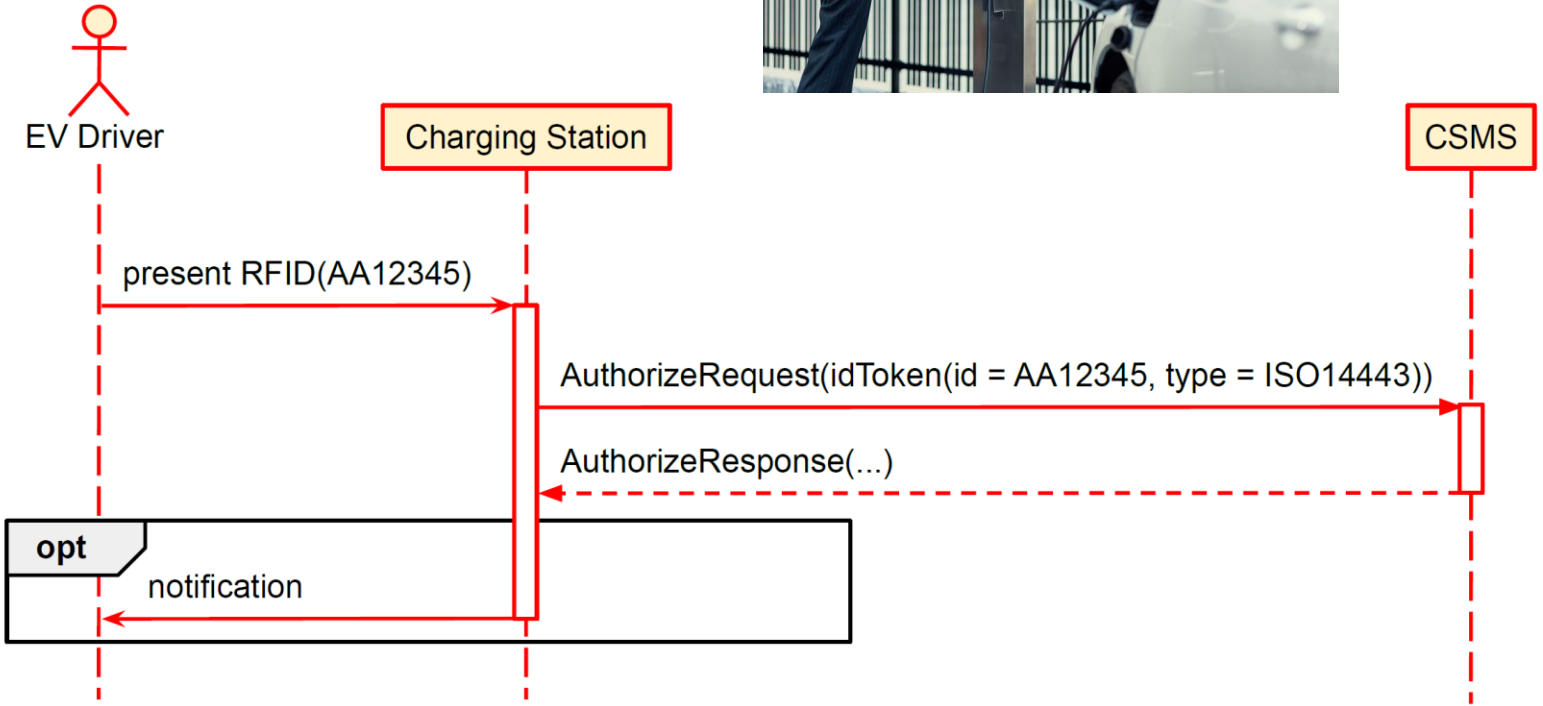
Use Case	Initial Situation	Weakness	STRIDE Attack Type	Relevant Study	Relative Frequency
C04: Using a PIN Code			Spoofing	[4], [26], [17]	42.86%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	-	-
			Denial of Service	-	-
			Elevation of Privilege	[4], [17]	28.57%
C05: CSMS Initiated Transaction			Spoofing	[4], [17]	28.57%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	[4]	14.28%
			Denial of Service	[4], [8], [26]	42.86%
			Elevation of Privilege	[4], [8], [17]	42.86%
C06: Local ID Type			Spoofing	[4], [17], [8]	42.86%
			Tampering	-	-
			Repudiation	-	-
			Information Disclosure	-	-
			Denial of Service	-	-
			Elevation of Privilege	[4], [17]	28.57%

Experimental Spoofing Attack

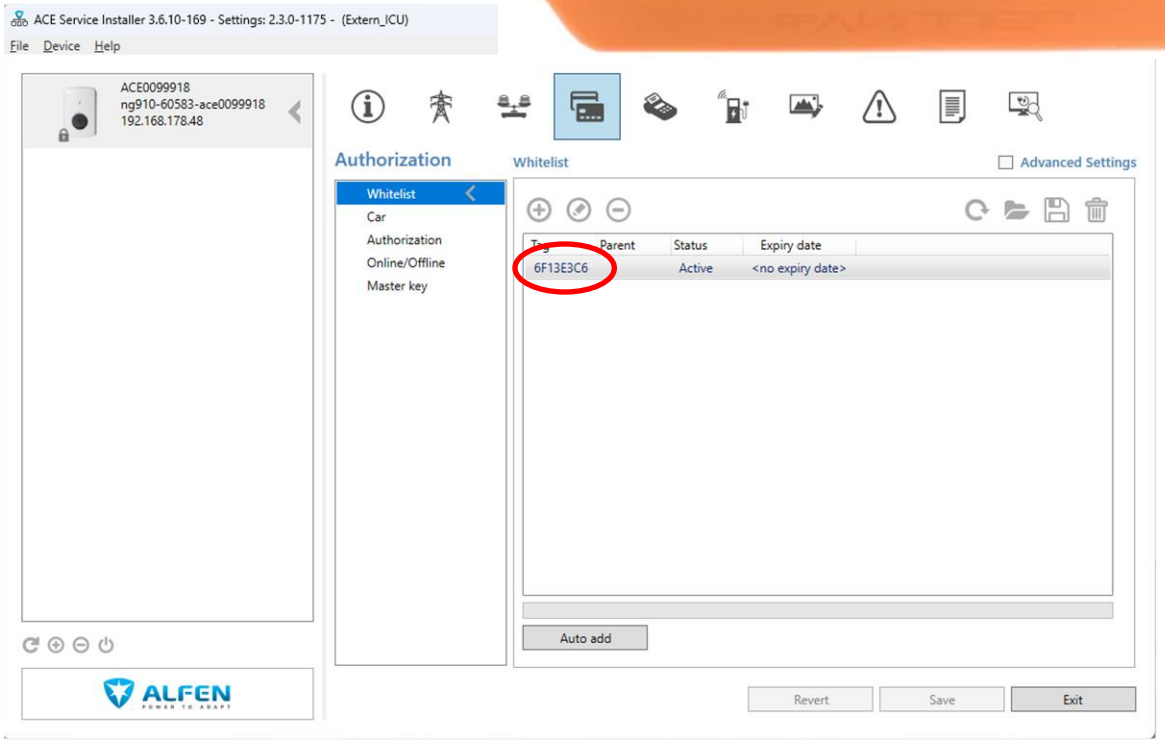


C01: RFID

OCPP – C01: RFID



Experimental Setup



Study Findings

- Significant **security vulnerabilities** in OCPP 2.0.1
- Most prevalent attack types
  - **Spoofing**
  - **Elevation of privilege**
- RFID based authentication
  - Exhibits **significant security vulnerabilities**
  - Low requirements (knowledge, budget, and time)
  - Likelihood of such an attack is **high**

Next Steps

SACHSEN-ANHALT

Kofinanziert von der Europäischen Union

- Research Project “Secure Systems for Industry 4.0”
- Funded by Saxony-Anhalt & European Union
- Milestones (03/2025 – 12/2027)
  - Digital Twin of the E-Charging Infrastructure
  - Demonstrator for Mobile Ad-Hoc Security Analysis
- Partners

Hochschule Harz
Hochschule für angewandte Wissenschaften

actain engineering

Magnetec

dns

Mittelstand-Digital Zentrum Magdeburg

APEC 2025

ATLANTA, GA | MARCH 16–20, 2025

Patrick Rempel

✉ prempel@hs-harz.de

▲ Hochschule Harz

Patrick Rempel
Professor at Hochschule Harz

André Büttner

✉ andre.buettner@actain.de

actain engineering

André Büttner
Acting on sustainable electronics