Cyber-Physical System (CPS) Security for EV Charging Ecosystem

Presented by
Shaurya Purohit

CprE 539: Cyber-Physical System Security for Smart Grid
Instructor: Dr. Manimaran Govindarasu
Department of Electrical and Computer Engineering

IOWA STATE UNIVERSITY

Contents

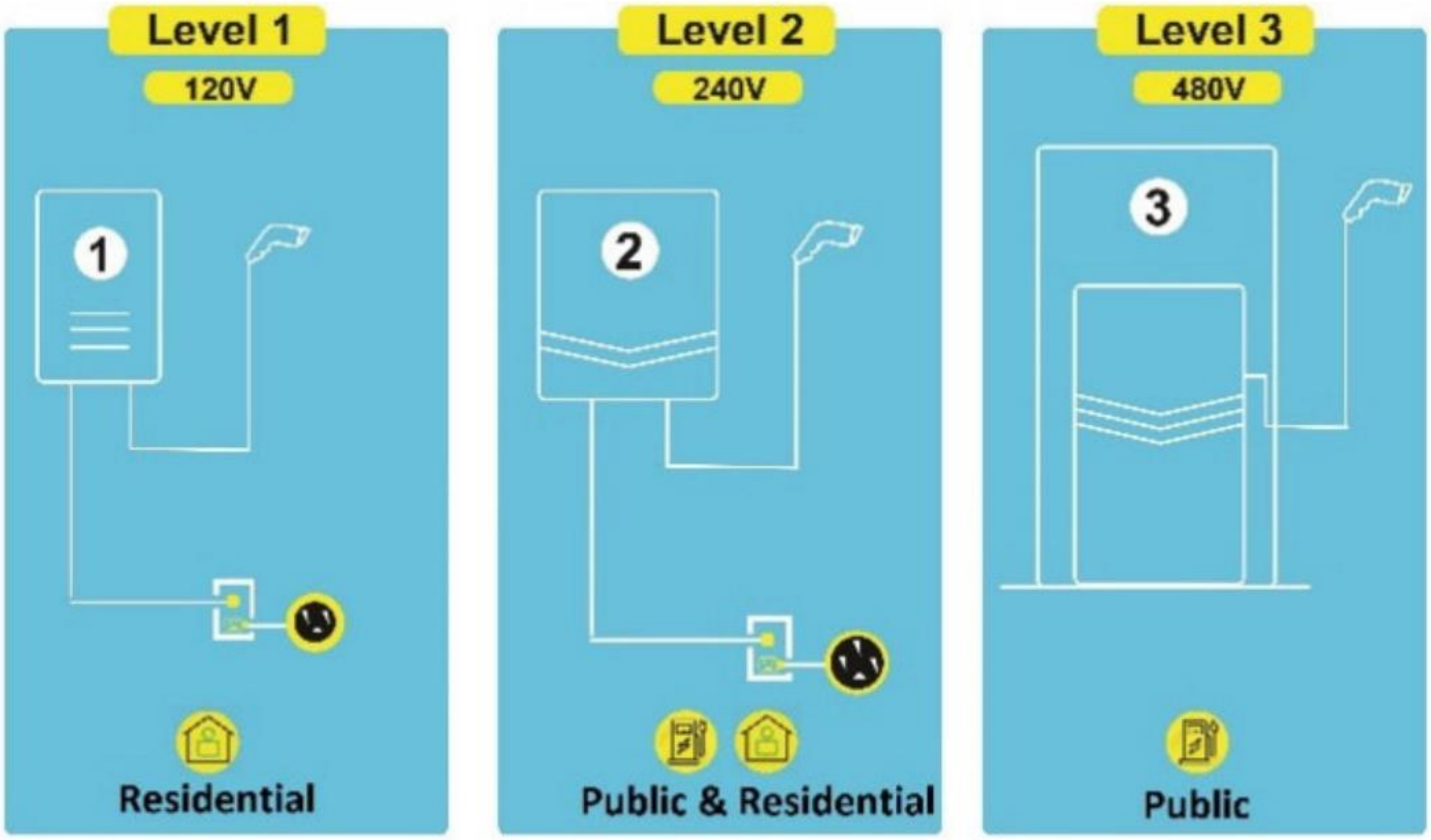
- ***Breif Introduction***
- ***Communication Architecture*** *of the EVCS Ecosystem*
- ***Attack Paths & Vulnerabilities*** *within the EVCS Ecosystem*
- ***Potential Cybersecurity Measures*** *for the EVCS Ecosystem*

Introduction

- A charging station, also called an EV charger or electric vehicle supply equipment is a piece of equipment that supplies electrical power for charging plug-in electric vehicles (including hybrids, neighborhood electric vehicles, trucks, buses, and others).

- EVSE serve for performing important control functions such as authorization, charging electric vehicles, and connecting to the local power grid.

Introduction



- ➢ Level 1 charging provides the slowest charging rate, operating at standard 120 V.
- ➢ Level 2 charging on the other hand uses 240 V and has been utilized for both private and public facilities and requires installation of dedicated charging equipment.
- ➢ Level 3, also referred to as ‘fast charging’, utilizes 480 V and is typically deployed in commercial/public settings with the goal of providing ‘grab and go’ .

Introduction

Supporting Infrastructure – Communication Protocols

CANbus:

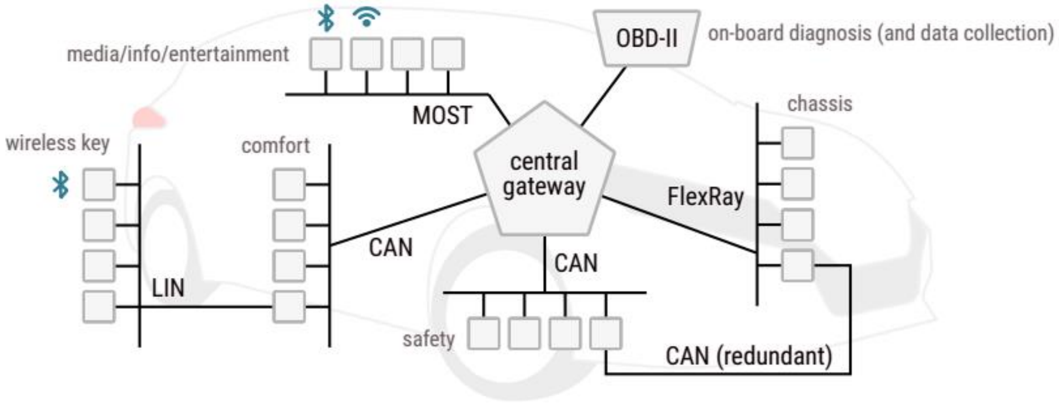
- ➢ Allows electronic components of a car to communicate with each other.
- ➢ Messages are exchanged by ECUs unencrypted.
- ➢ Several safety-critical functions use CAN.

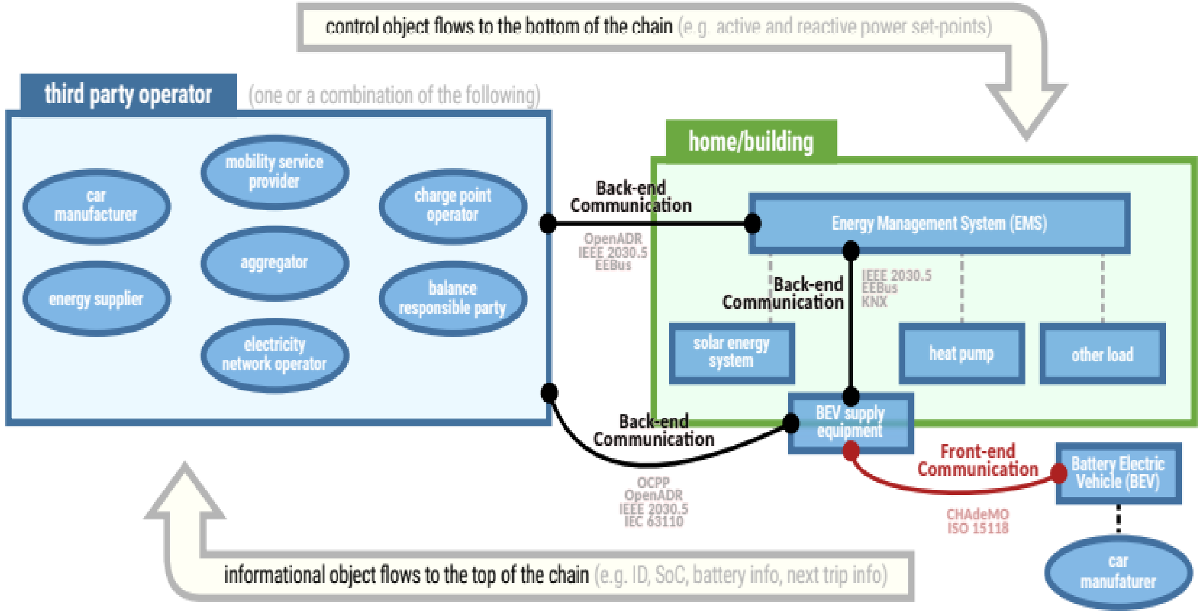
EVCS Front-end protocols:

- ➢ Defines the link between EV and CS.
- ➢ Specify requirements for plugs, charging topologies (on-board/o-board charging equipment; conductive/inductive charging), communication, safety and cyber-security.
- ➢ Protocols such as ***CHAdeMO*** and ***ISO15118-20*** allow bidirectional power flow (i.e., V2G) between the car and a charger.

EVCS Back-end protocols:

- ➢ Defines the link between CS and a third-party operator.
- ➢ Some of these open protocols are ***OCPP, IEC63110, OpenADR, EEBus and IEEE2030.5.***





control object flows to the bottom of the chain (e.g. active and reactive power set-points)
third party operator
(one or a combination of the following)
car manufacturer
mobility service provider
charge point operator
aggregator
energy supplier
balance responsible party
electricity network operator
home/building
Back-end Communication
OpenADR
IEEE 2030.5
EEBus
Energy Management System (EMS)
Back-end Communication
IEEE 2030.5
EEBus
KNX
solar energy system
heat pump
other load
BEV supply equipment
Back-end Communication
OCPP
OpenADR
IEEE 2030.5
IEC 63110
Front-end Communication
CHAdeMO
ISO 15118
Battery Electric Vehicle (BEV)
car manufaturer
informational object flows to the top of the chain (e.g. ID, SoC, battery info, next trip info)

Ref: Metere et al., Securing the Electric Vehicle Charging Infrastructure, 2021

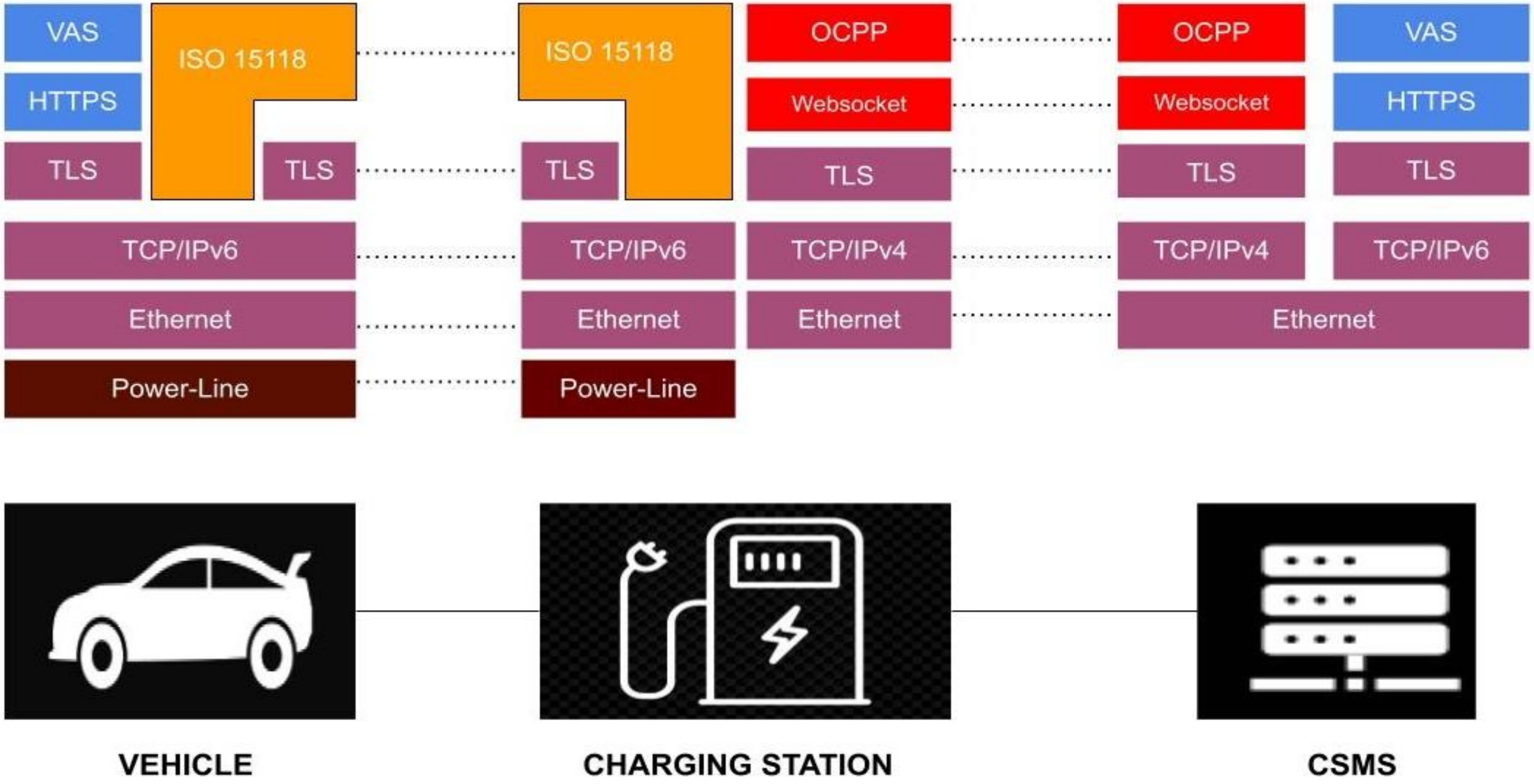
Communication Architecture of EVCS Ecosystem

Protocols

- ❖ ***ISO 15118*** is an international standard that outlines the digital communication that an electric vehicle (EV) and charging station should use to recharge the EV’s high voltage battery.
    - ✓ Facilitates not just the charging, but also advanced features like
        - ▪ Plug-and-charge (PnC)
        - ▪ Bidirectional charging, supporting the integration of EVs into the smart grid.

- ❖ ***Open Charge Point Protocol (OCPP)*** is an open communication protocol that allows electric vehicles charging stations and central management software to communicate with each other.
    - ✓ OCCP communicates information in clear text
    - ✓ Widely adopted due to its open and interoperable nature, allowing different brands of charging stations and management software to work together.

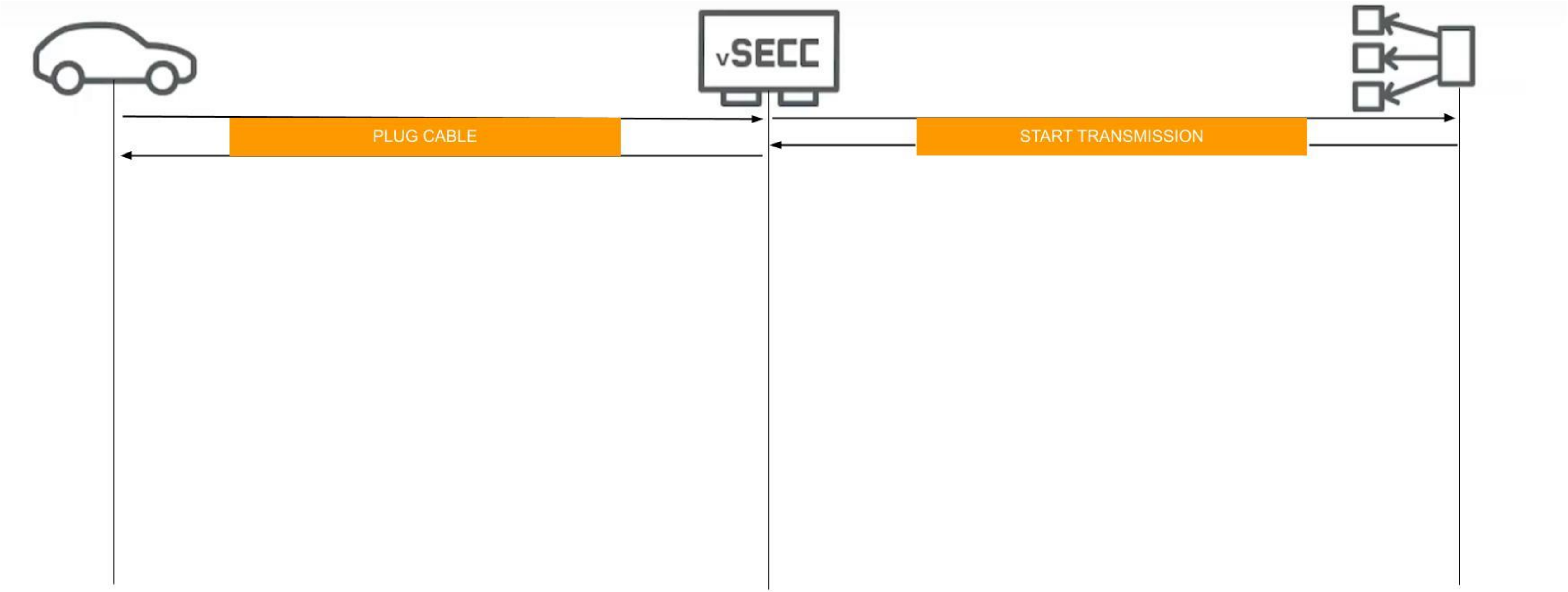
Communication Architecture of EVCS Ecosystem



S. Purohit and M. Govindarasu, "Cybersecurity Investment Analysis for Electric Vehicle Charging Infrastructures," 2023 Resilience Week (RWS), National Harbor, MD, USA, 2023, pp. 1-6

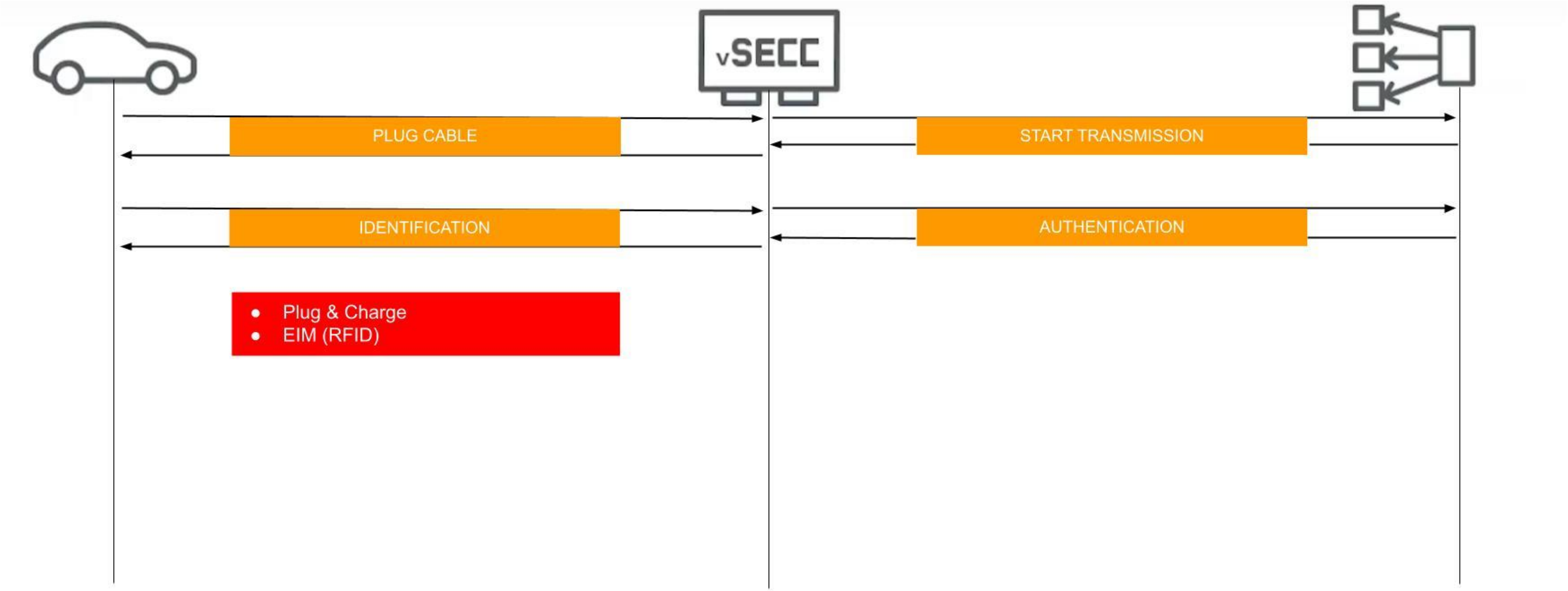
Communication Architecture of EVCS Ecosystem

Charging Sequence



Communication Architecture of EVCS Ecosystem

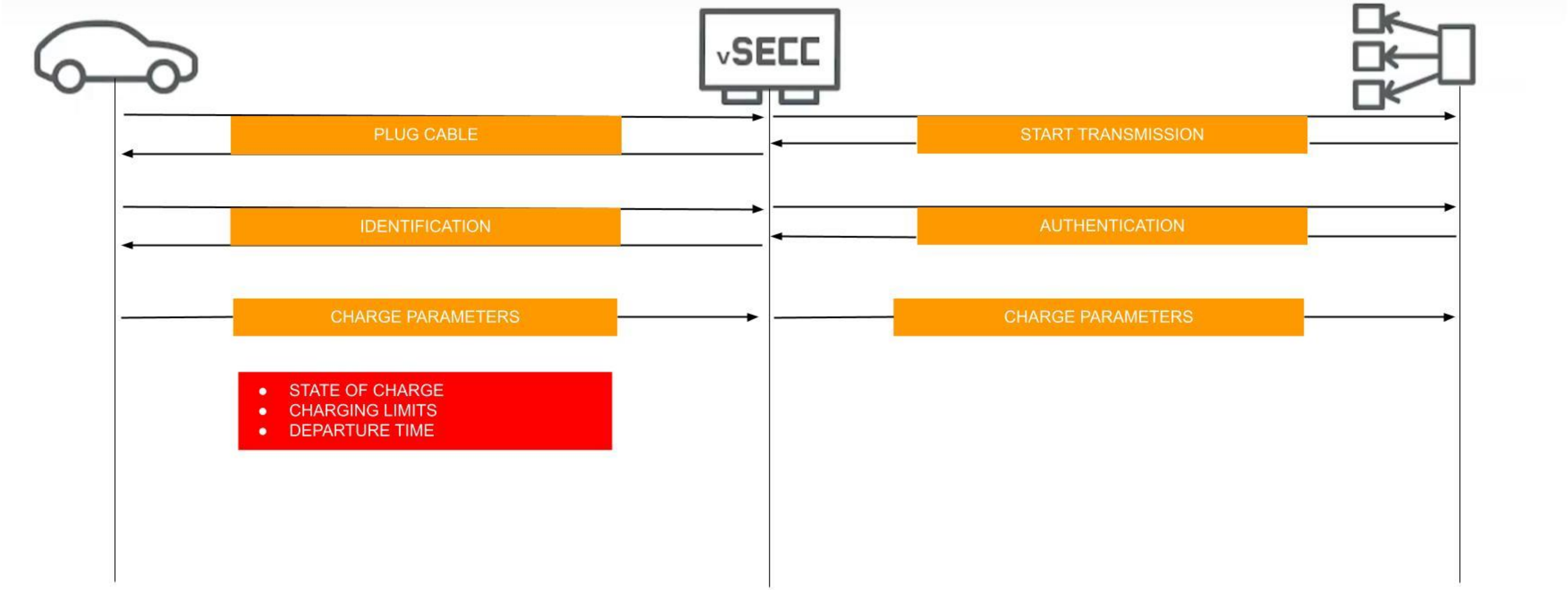
Charging Sequence



- Plug & Charge
- EIM (RFID)

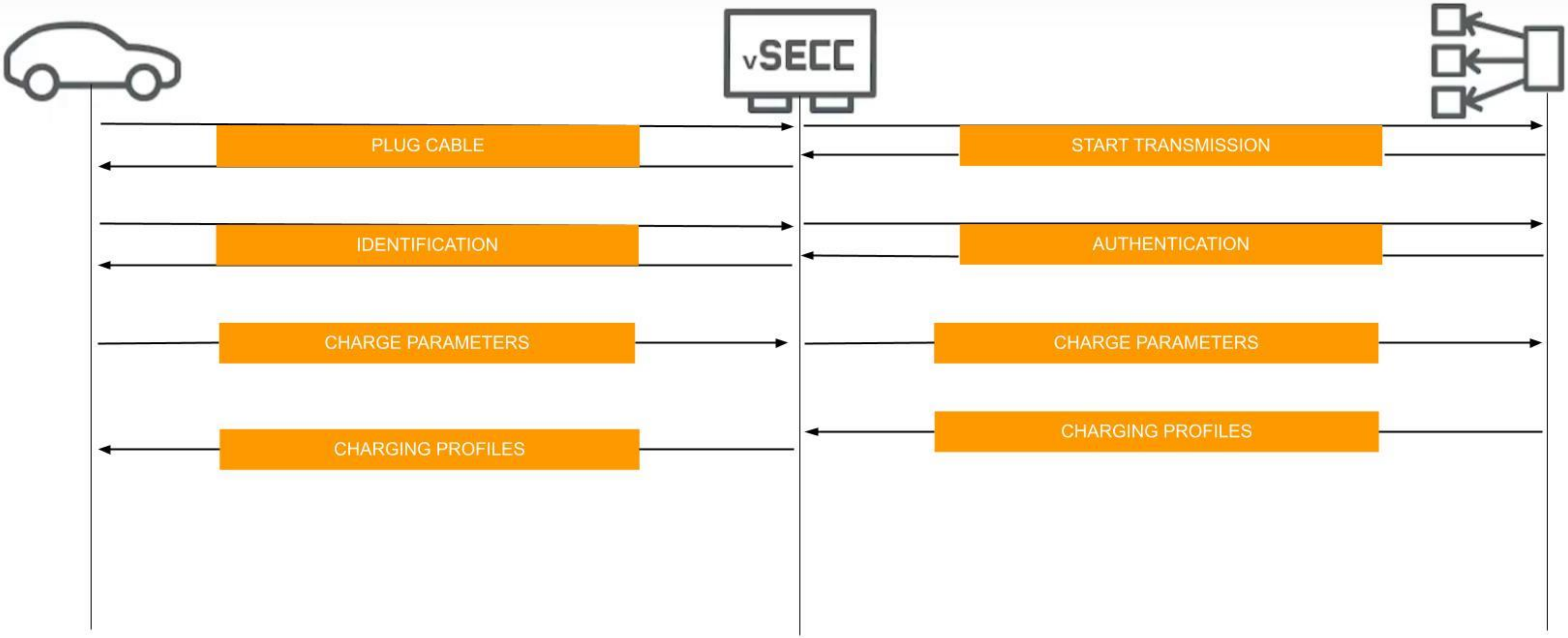
Communication Architecture of EVCS Ecosystem

Charging Sequence



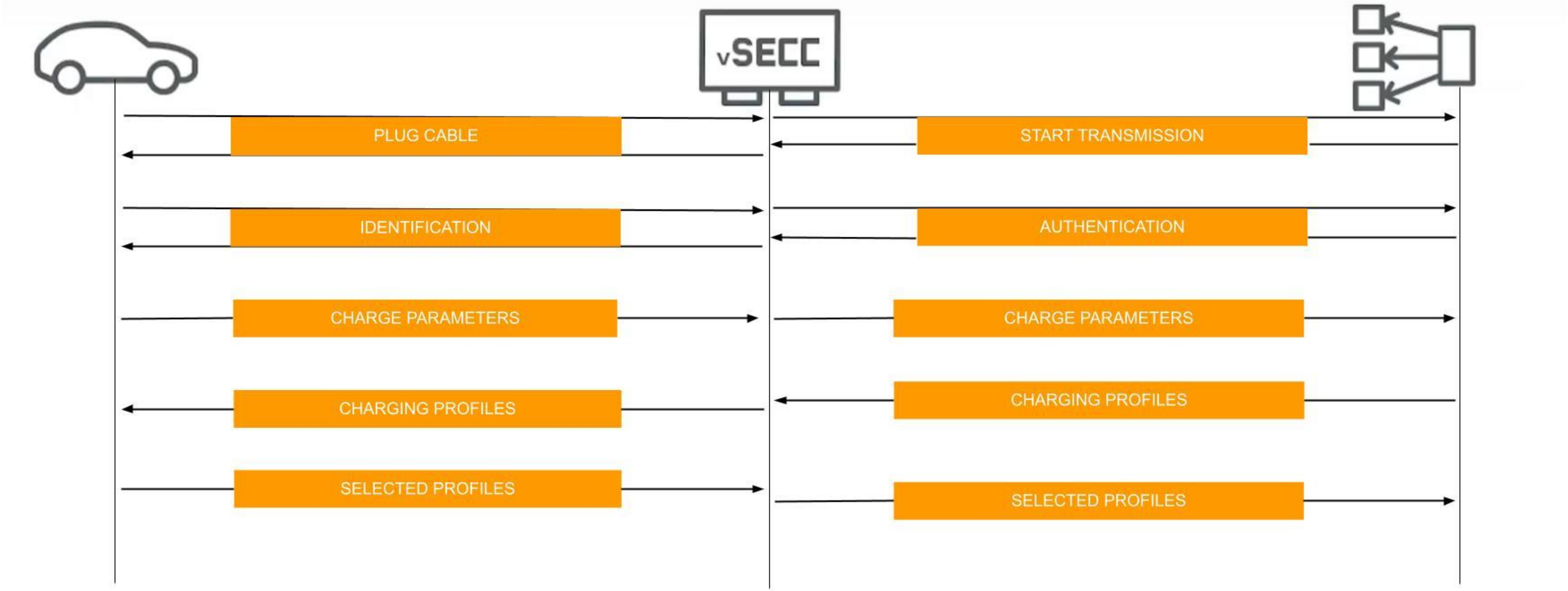
3. Communication Architecture of EVCS Ecosystem

Charging Sequence



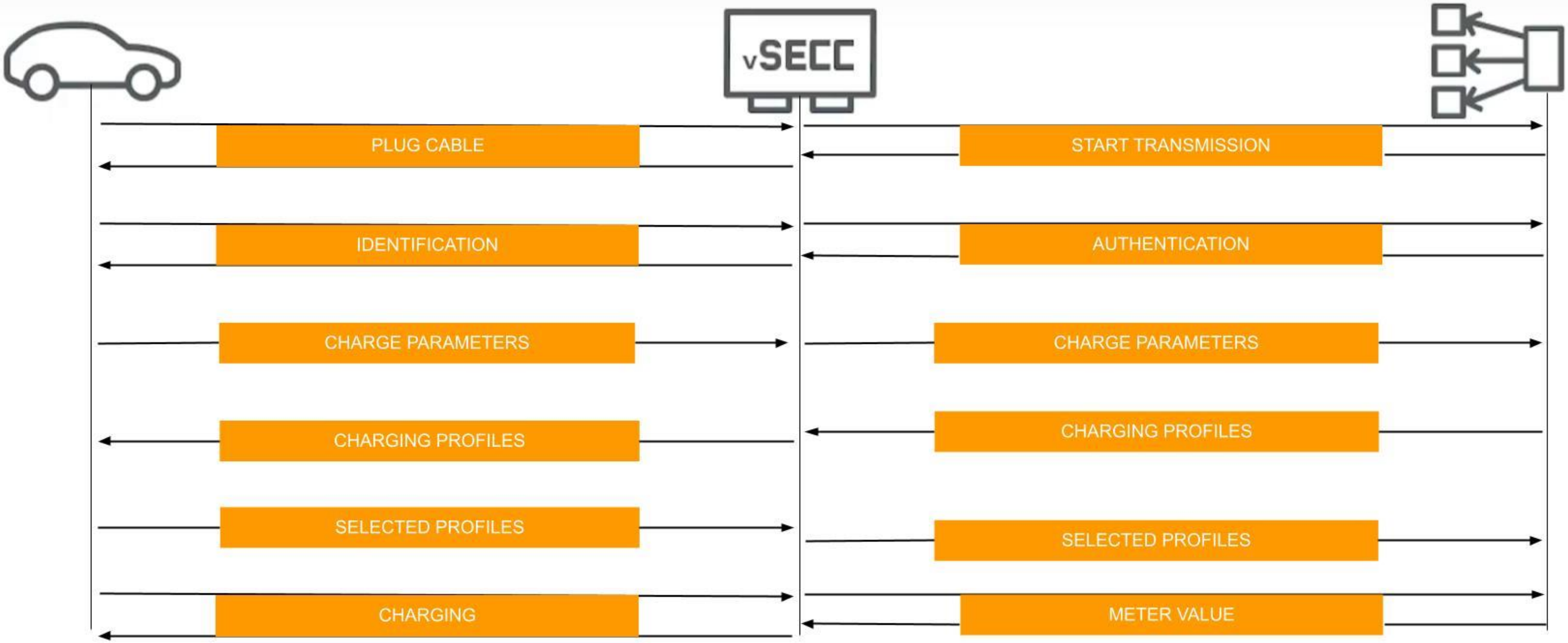
Communication Architecture of EVCS Ecosystem

Charging Sequence



Communication Architecture of EVCS Ecosystem

Charging Sequence



3. Communication Architecture of EVCS Ecosystem

Public Key Infrastructure

One PKI for each Plug & Charge market role

Charge Point Operator (CPO)

Operates and maintains the charging stations via its backend IT system

Certificate Provisioning Service (CPS)

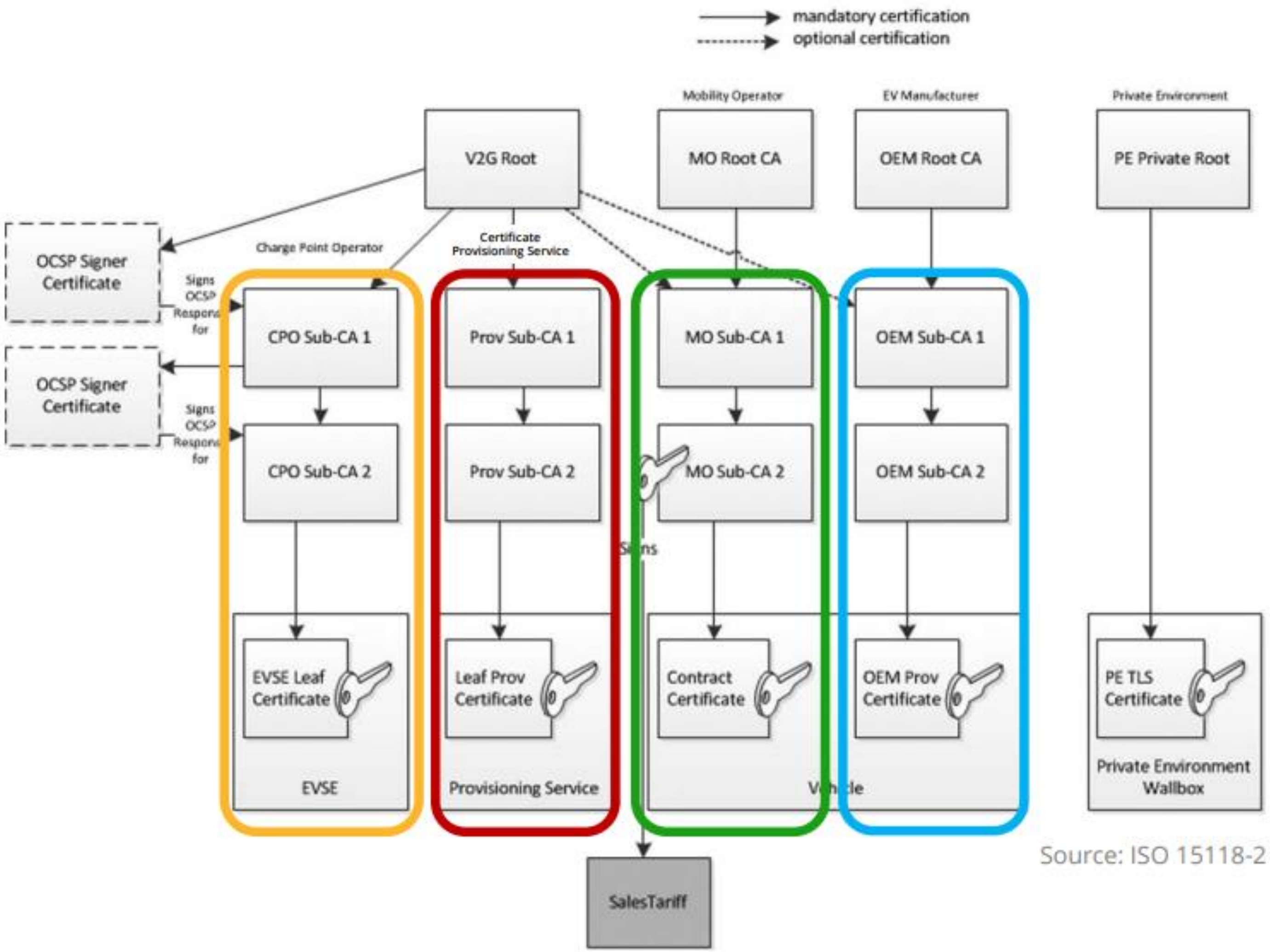
Facilitates the installation of a new contract certificate for the EV through a digital signature

Mobility Operator (MO)

Provides a legal e-mobility contract and issues contract certificates associated with that legal contract

Car manufacturer (OEM)

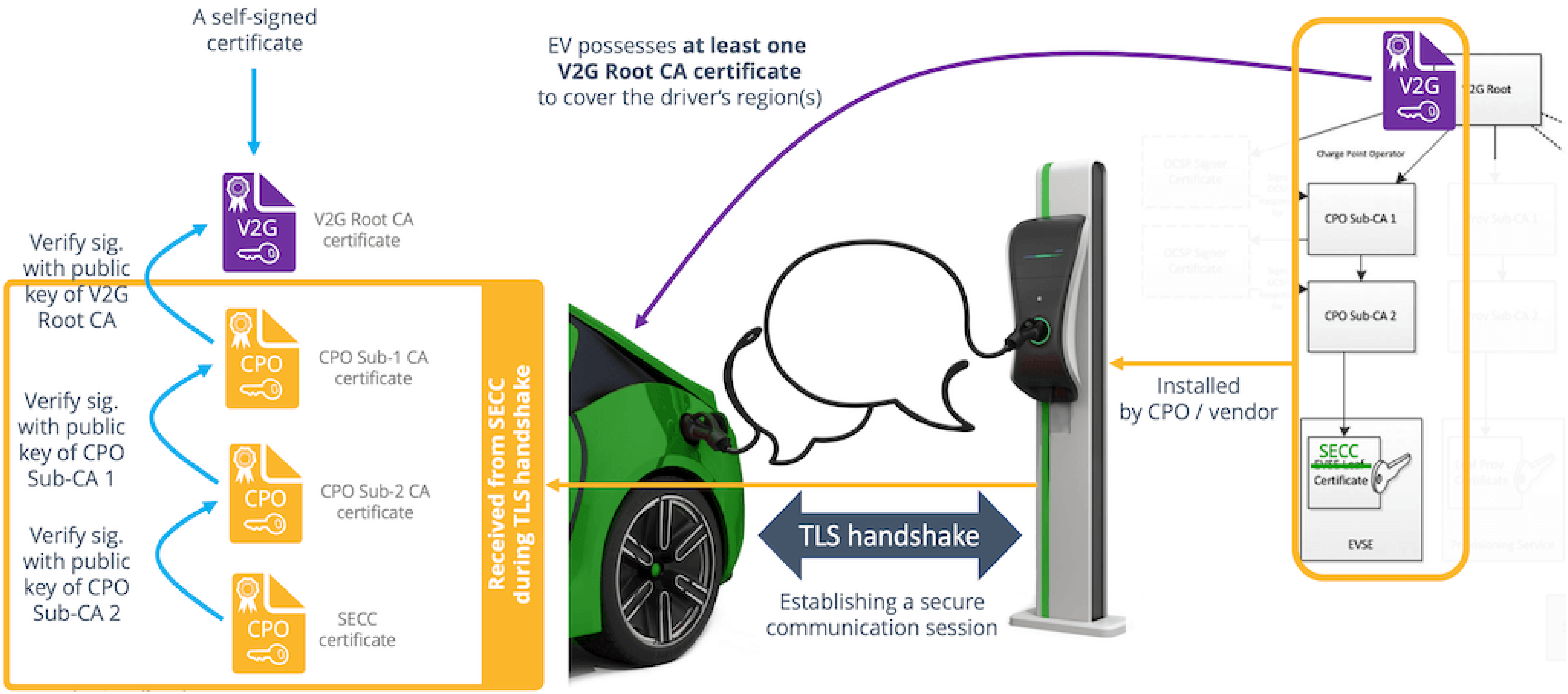
Issues the unique OEM provisioning certificate needed to install a new contract certificate for Plug & Charge



Source: ISO 15118-2

Communication Architecture of EVCS Ecosystem

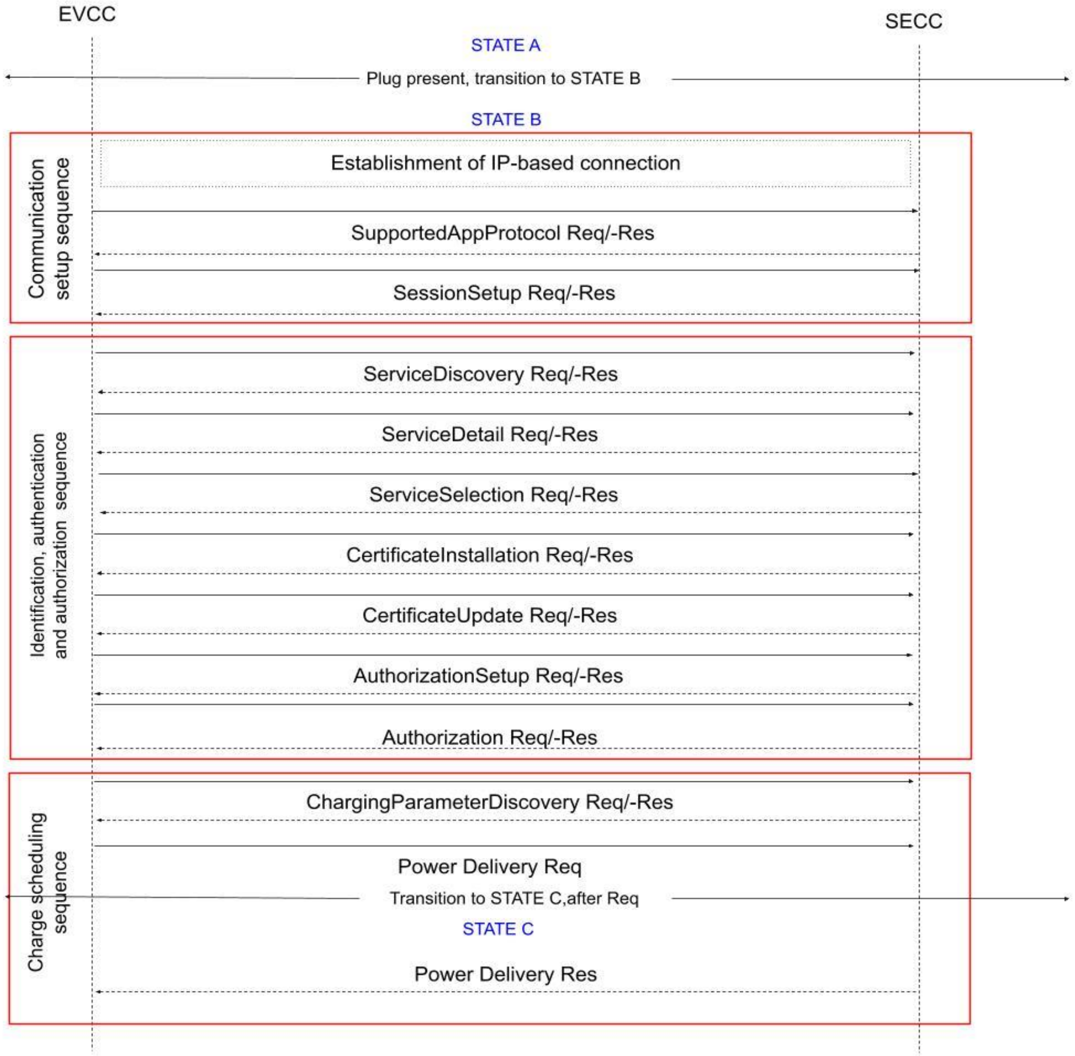
Establishing trust between the EV and charging station using a TLS handshake


A self-signed certificate
V2G
V2G Root CA certificate
Verify sig. with public key of V2G Root CA
CPO
CPO Sub-1 CA certificate
Verify sig. with public key of CPO Sub-CA 1
CPO
CPO Sub-2 CA certificate
Verify sig. with public key of CPO Sub-CA 2
CPO
SECC certificate
Received from SECC during TLS handshake
EV possesses **at least one V2G Root CA certificate** to cover the driver's region(s)
TLS handshake
Establishing a secure communication session
Installed by CPO / vendor
V2G
2G Root
Charge Point Operator
OCSP Signer Certificate
OCSP Signer Certificate
CPO Sub-CA 1
CPO Sub-CA 2
SECC
~~EVSE Leaf~~
Certificate
EVSE
Prov Sub-CA 1
Prov Sub-CA 2
Leaf Prov Certificate
Provisioning Service

CPO certificates that the charging station presents to the EV during a TLS handshake

Communication Architecture of EVCS Ecosystem

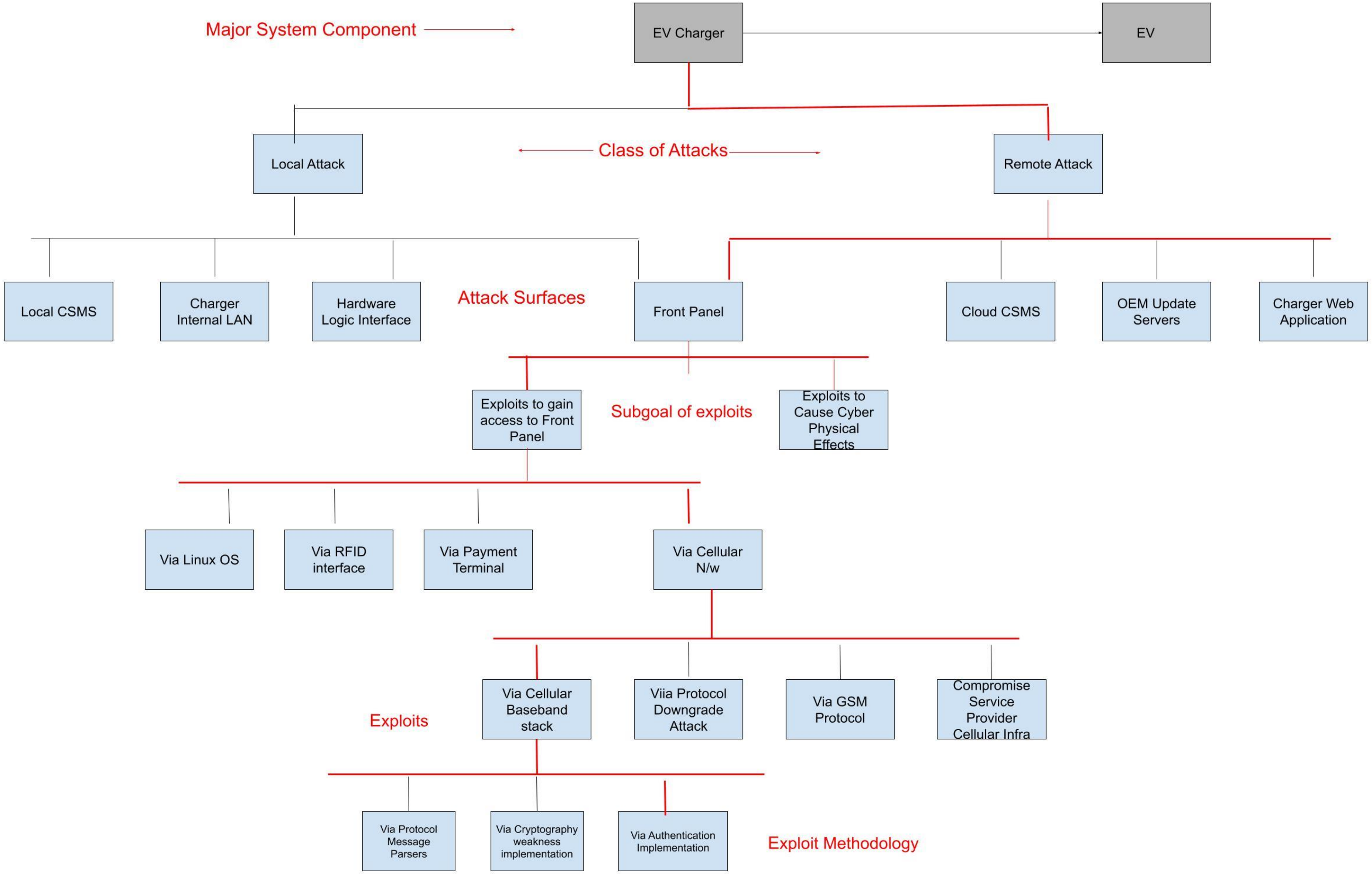
Message Sequence



EVCC
SECC
STATE A
Plug present, transition to STATE B
STATE B
Communication setup sequence
Establishment of IP-based connection
SupportedAppProtocol Req/-Res
SessionSetup Req/-Res
Identification, authentication and authorization sequence
ServiceDiscovery Req/-Res
ServiceDetail Req/-Res
ServiceSelection Req/-Res
CertificateInstallation Req/-Res
CertificateUpdate Req/-Res
AuthorizationSetup Req/-Res
Authorization Req/-Res
Charge scheduling sequence
ChargingParameterDiscovery Req/-Res
Power Delivery Req
Transition to STATE C,after Req
STATE C
Power Delivery Res

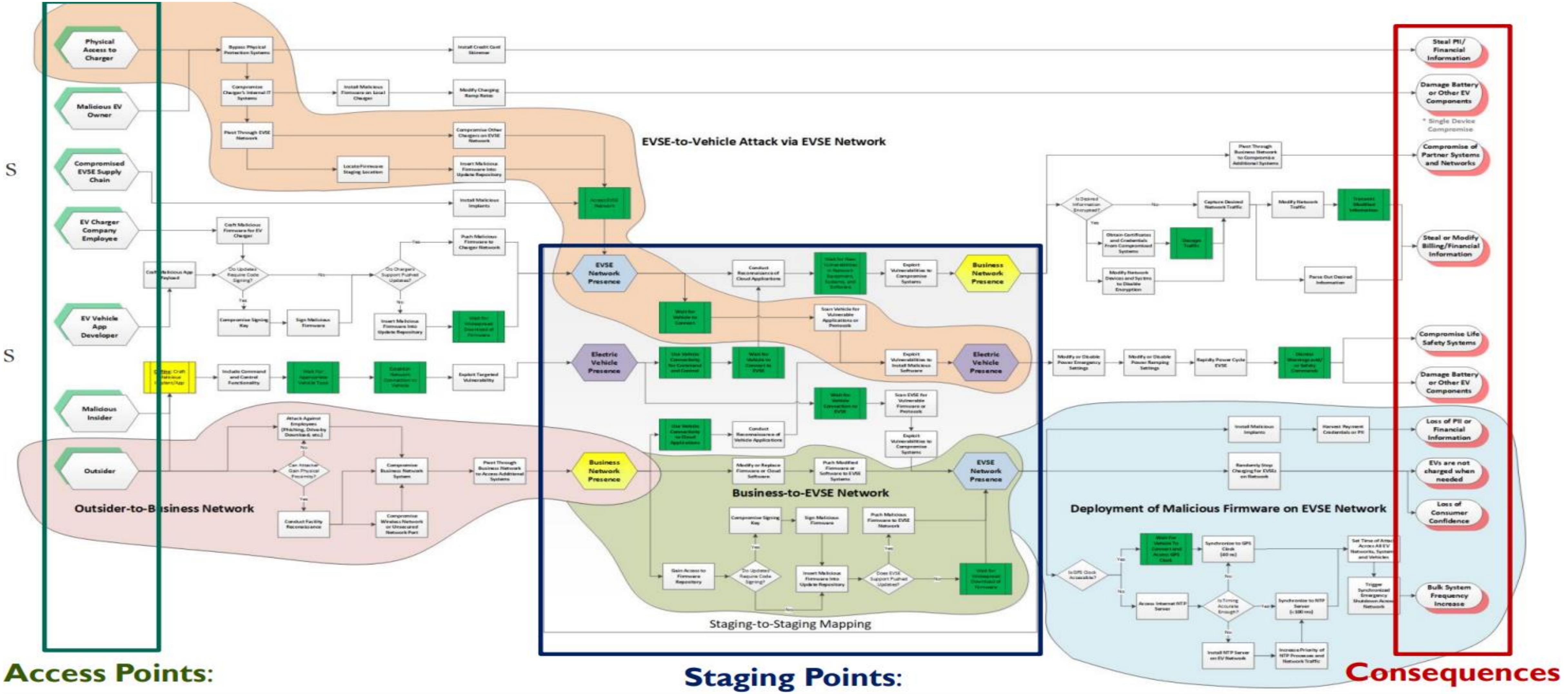
STATE A: No EV Connected
STATE B: EV Detected, Not ready to charge yet
STATE C: EV Detected, Ready to charge

Attack Paths & Vulnerabilities of EVCS Ecosystem



Attack Path Example

Attack Paths & Vulnerabilities of EVCS Ecosystem


S
S
Physical Access to Charger
Malicious EV Owner
Compromised EVSE Supply Chain
EV Charger Company Employee
EV Vehicle App Developer
Malicious Insider
Outsider
Bypass Physical Protection Systems
Install Credit Card Skimmer
Compromise Charger's Internal IT Systems
Install Malicious Firmware on Local Charger
Modify Charging Ramp Rates
Pivot Through EVSE Network
Compromise Other Chargers on EVSE Network
Locate Firmware Staging Location
Insert Malicious Firmware into Update Repository
Install Malicious Implants
Access EVSE Network
Craft Malicious Firmware for EV Charger
Push Malicious Firmware to Charger Network
Craft Malicious App Payload
Do Updates Require Code Signing?
Yes
No
Do Chargers Support Pushed Updates?
Compromise Signing Key
Sign Malicious Firmware
Insert Malicious Firmware into Update Repository
Wait for Widespread Download of Firmware
Craft Malicious Content/App
Include Command and Control Functionality
Wait for Appropriate Vehicle Type
Establish Network Connection to Vehicle
Exploit Targeted Vulnerability
Attack Against Employees (Phishing, Drive-by Download, etc.)
Can Attacker Gain Physical Proximity?
Conduct Facility Reconnaissance
Compromise Business Network System
Compromise Wireless Network or Unsecured Network Port
Pivot Through Business Network to Access Additional Systems
Outsider-to-Business Network
EVSE-to-Vehicle Attack via EVSE Network
EVSE Network Presence
Conduct Reconnaissance of Cloud Applications
Wait for New Vulnerabilities in Network Equipment, Systems, and Software
Exploit Vulnerabilities to Compromise Systems
Business Network Presence
Wait for Vehicle to Connect
Scan Vehicle for Vulnerable Applications or Protocols
Electric Vehicle Presence
Use Vehicle Connectivity for Command and Control
Wait for Vehicle to Connect to EVSE
Exploit Vulnerabilities to Install Malicious Software
Electric Vehicle Presence
Wait for Vehicle Connection to EVSE
Scan EVSE for Vulnerable Firmware or Protocols
Use Vehicle Connectivity to Cloud Applications
Conduct Reconnaissance of Vehicle Applications
Exploit Vulnerabilities to Compromise Systems
Business Network Presence
Modify or Replace Firmware or Cloud Software
Push Modified Firmware or Software to EVSE Systems
EVSE Network Presence
Business-to-EVSE Network
Compromise Signing Key
Sign Malicious Firmware
Push Malicious Firmware to EVSE Network
Gain Access to Firmware Repository
Do Updates Require Code Signing?
Insert Malicious Firmware into Update Repository
Does EVSE Support Pushed Updates?
Wait for Widespread Download of Firmware
Staging-to-Staging Mapping
Pivot Through Business Network to Compromise Additional Systems
Is Desired Information Encrypted?
Capture Desired Network Traffic
Modify Network Traffic
Transmit Modified Information
Obtain Certificates and Credentials From Compromised Systems
Decrypt Traffic
Modify Network Devices and Systems to Disable Encryption
Parse Out Desired Information
Modify or Disable Power Emergency Settings
Modify or Disable Power Ramping Settings
Rapidly Power Cycle EVSE
Disable Warnings and/or Safety Commands
Install Malicious Implants
Harvest Payment Credentials or PII
Randomly Stop Charging for EVSEs on Network
Deployment of Malicious Firmware on EVSE Network
Is GPS Clock Accessible?
Wait For Vehicle To Connect and Access GPS Clock
Synchronize to GPS Clock (60 ns)
Access Internet NTP Server
Is Timing Accurate Enough?
Synchronize to NTP Server (<100 ms)
Install NTP Server on EV Network
Increase Priority of NTP Processes and Network Traffic
Set Time of Attack Across All EV Networks, Systems and Vehicles
Trigger Synchronized Emergency Shutdown Across Network
Steal PII/ Financial Information
Damage Battery or Other EV Components
* Single Device Compromise
Compromise of Partner Systems and Networks
Steal or Modify Billing/Financial Information
Compromise Life Safety Systems
Damage Battery or Other EV Components
Loss of PII or Financial Information
EVs are not charged when needed
Loss of Consumer Confidence
Bulk System Frequency Increase
Access Points:
Staging Points:
Consequences

Ref: B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020.

Attack Paths & Vulnerabilities within EVCS Ecosystem

Possible cyber attack paths for EVCS (EVSE):

- Man-in-the-middle at charging station
- Denial of service (DoS) attack at EVSEs
- Payment fraud at charging station
- Privacy/tracking issues with using EVSEs linked into Smart Grid
- Intentional overcharging & discharging of batteries
- Malware
- Rapid cycling of heavy loads
- Detected vulnerabilities in RS232 and OCPP protocols
- Physical ports (serial, USB, ethernet) allow access for physical intrusions

Possible cyber attack paths for EVs:

- Man-in-the-middle attacks to monitor vehicle internal communication
- Denial of Service (DoS) attack on the vehicle
- Exploiting vulnerabilities in CANbus architecture
- Exploiting vulnerabilities in FlexRay (air bag ECU), LIN (air-conditioner ECU), and MOST (IVI system) protocols
- False data injection attacks on critical ECUs (such as engine control unit, speed control unit, TPMS)
- Physical ports (USB, SD-card, CD/DVD drive, touchscreen panels) allow access to exploit IVI ECUs
- Injecting malware to hamper ECUs
- Privacy and security issues in communication with EVCS
- Vulnerabilities in wireless/internet service portals in EVs such as Bluetooth, RF transceivers, etc.
- Spoofing and jamming navigation systems such as GPS signals.

Effects on power grid due to cyberattacks on EV:

- Power grid implications of cyberattacks on EV charging are relatively underexplored
- Cyber manipulations of EV ecosystem falls under demand-side management
- Can cause to signal instability in power grid leading to over/under frequency issues causing blackouts and outages
- Over/under voltage situations can lead to damage to the transmission lines
- Manipulation in EVCS control system can cause low power factor and inoperable harmonic distortion

Security challenges of Connected Vehicles (CVs):

- Securing CV data in the cloud
- Scalability of cloud security solutions
- Data privacy in the cloud
- Securing CV to cloud communication networks
- Authentication and validation of CV location information
- Establishing trust relationships with a high number of CVs

Attack Paths & Vulnerabilities of EVCS Ecosystem

Electric Vehicle Charging Stations Open to IoT Attacks

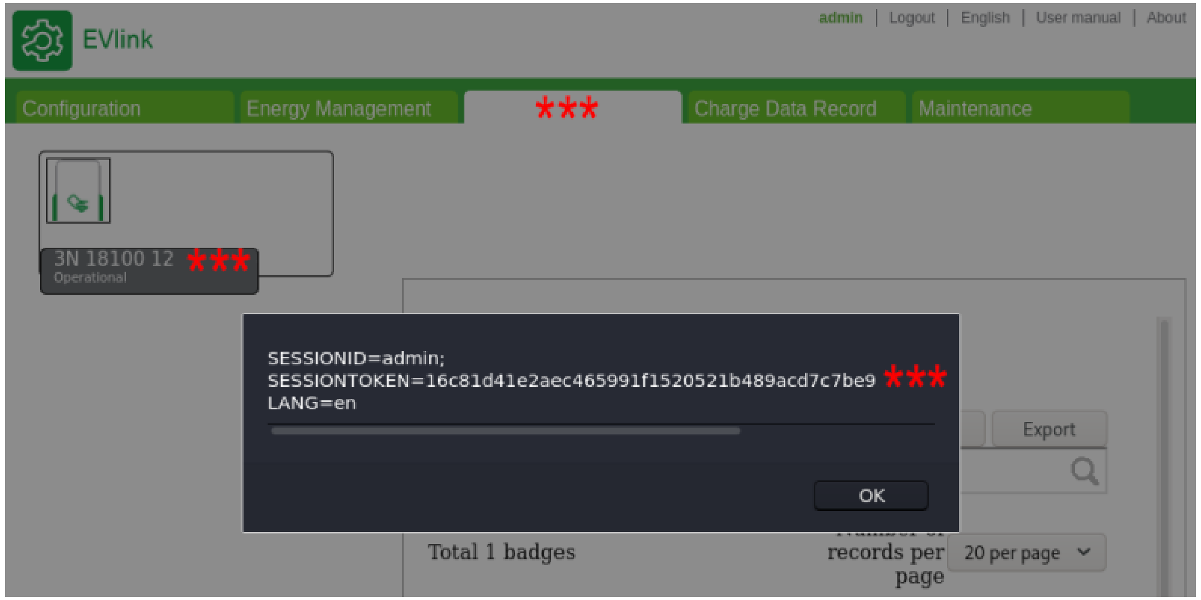
Ref: https://threatpost.com/electric-vehicle-charging-stations/139958/

ChargePoint Home’s mobile application allows the end user to control the charging process remotely.
To register a new account in the application, a user would connect a smartphone to the device via Bluetooth, set the parameters of a Wi-Fi network for an internet connection, and finish the registration process by sending the created user ID and the smartphone’s GPS coordinates to the backend from the device.

All an attacker needs to do to conduct an attack is obtain Wi-Fi access to the network charger.
This means that attackers could gain access easily, for example, by brute-forcing all possible password options.
Once inside the wireless network, the intruders can easily find the charger’s IP address. This, in turn, will allow them to exploit any vulnerabilities.

Attack Paths & Vulnerabilities of EVCS Ecosystem

Example for Charging Station Management Systems Vulnerability (EVlink)



```
SESSIONID=admin;
SESSIONTOKEN=16c81d41e2aec465991f1520521b489acd7c7be9 ***
LANG=en
```

Stored Cross site scripting on EVlink allows hijacking the administrator’s session tokens

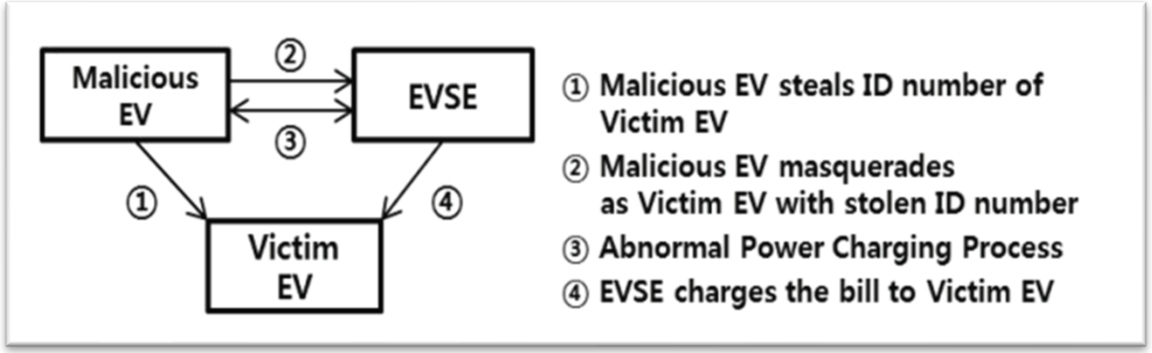
- ❖ Discovered a configuration initialization functionality within EVlink that was vulnerable to Comma-Separated Values injection (CSVi), which can be exploited to embed a cross-site scripting payload that gets triggered and stored on the system database when the crafted CSV file is loaded.

- ❖ This vulnerability leads to a stored XSS, which enables **privilege escalation** by hijacking the administrator’s session tokens.

Ref: Tony Nasr, Sadegh Torabi, Elias Bou-Harb, Claude Fachkha, Chadi Assi, Power jacking your station: In-depth security analysis of electric vehicle charging station management systems, Computers & Security, Volume 112, 2022, 102511, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102511.

Attack Paths & Vulnerabilities of EVCS Ecosystem

Vulnerabilities BASED ON ISO 15118



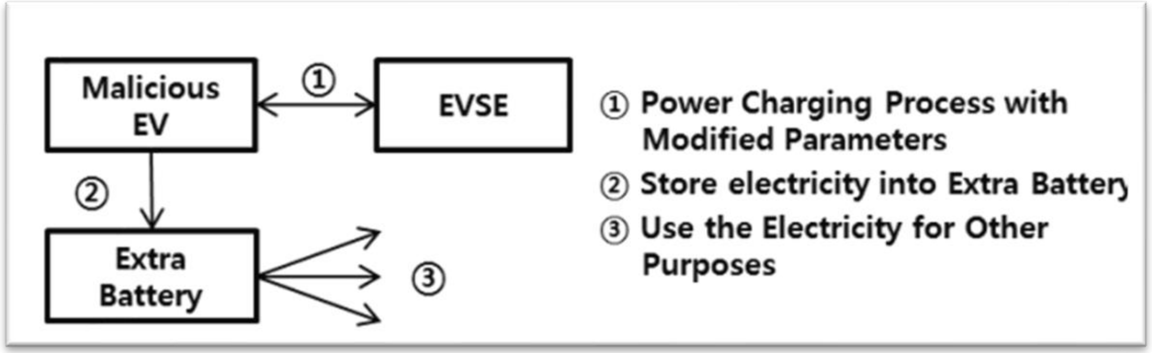
① Malicious EV steals ID number of Victim EV

② Malicious EV masquerades as Victim EV with stolen ID number

③ Abnormal Power Charging Process

④ EVSE charges the bill to Victim EV

Changing ID number

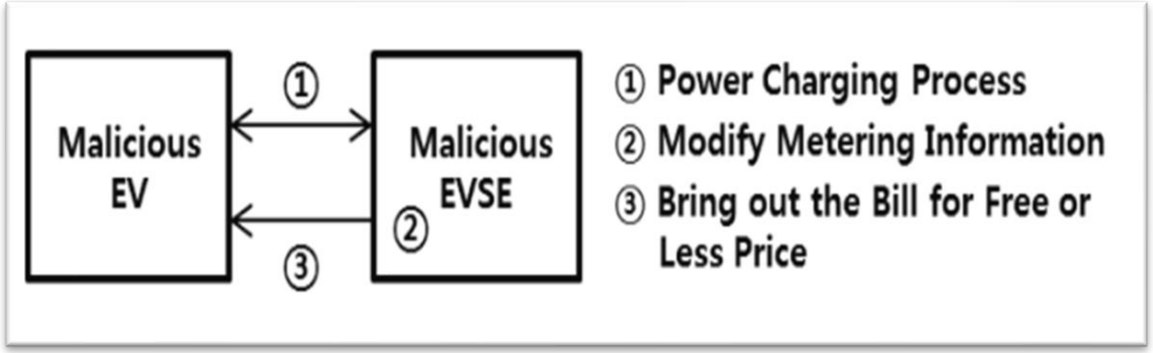


① Power Charging Process with Modified Parameters

② Store electricity into Extra Battery

③ Use the Electricity for Other Purposes

Power charging for abusing

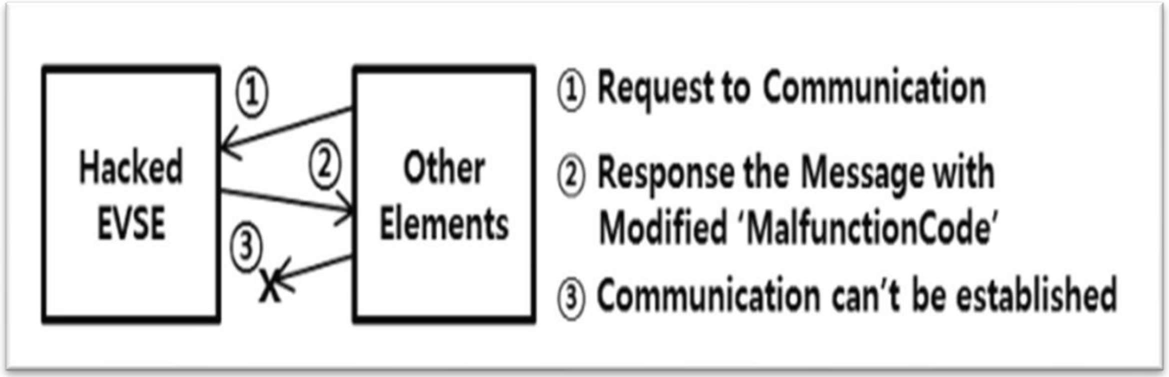


① Power Charging Process

② Modify Metering Information

③ Bring out the Bill for Free or Less Price

Fabrication of metering data



① Request to Communication

② Response the Message with Modified 'MalfunctionCode'

③ Communication can't be established

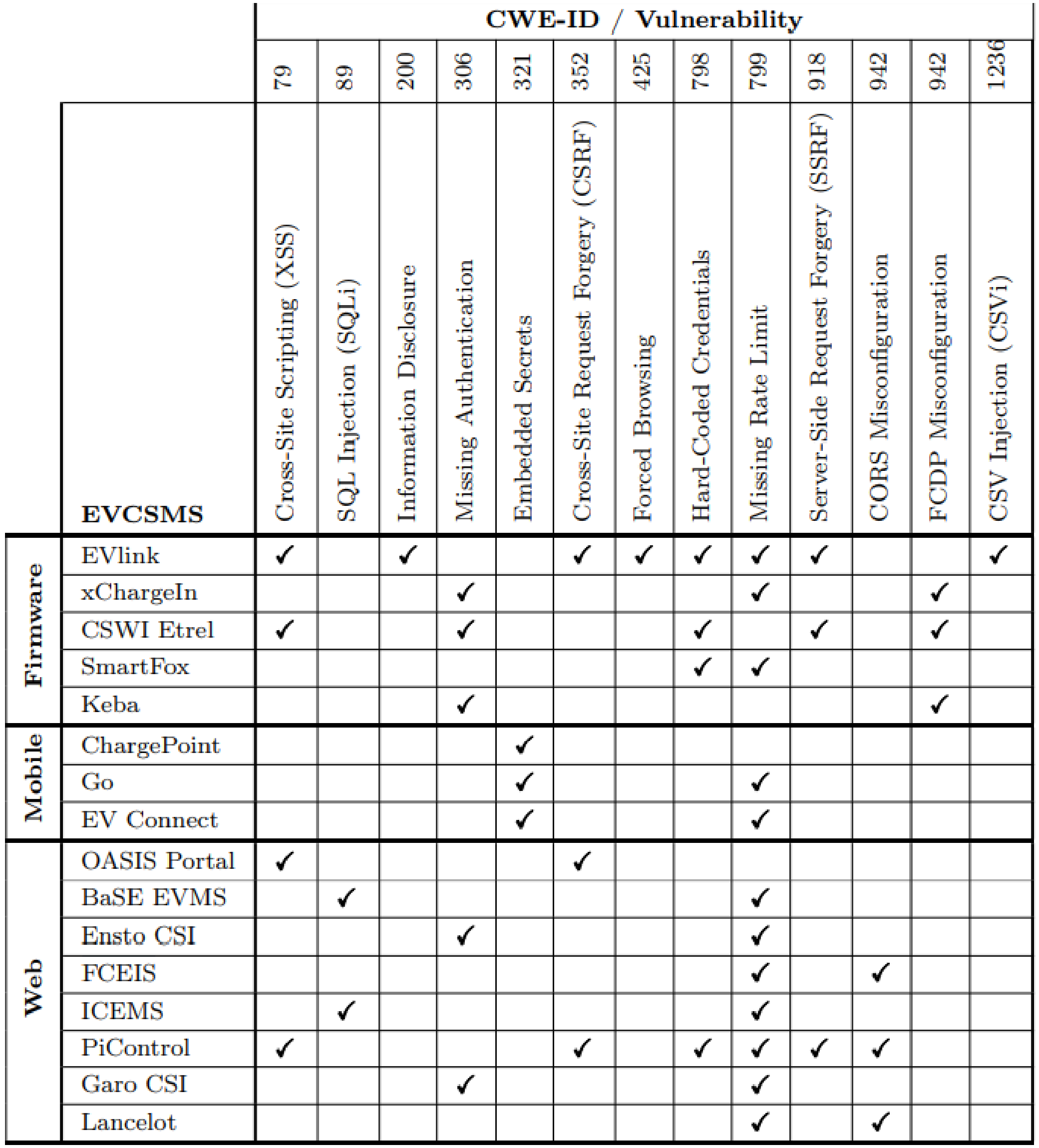
Shutting off service of EVSE

Ref: S. Lee, Y. Park, H. Lim and T. Shon, "Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology," 2014 International Conference on IT Convergence and Security (ICITCS), 2014, pp. 1-4, doi: 10.1109/ICITCS.2014.7021815.

Attack Paths & Vulnerabilities of EVCS Ecosystem

Popular Attacks

- ***MitM ATTACKS***
- ***DOS ATTACK***
- ***Spoofing ATTACK***
- ***Masquerade ATTACK***
- ***SQL Injection ATTACK***
- ***Jamming ATTACK***

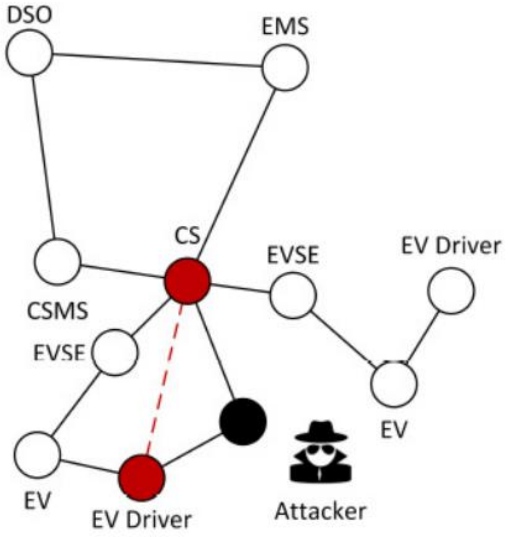


		CWE-ID / Vulnerability												
		79	89	200	306	321	352	425	798	799	918	942	942	1236
	EVCSMS	Cross-Site Scripting (XSS)	SQL Injection (SQLi)	Information Disclosure	Missing Authentication	Embedded Secrets	Cross-Site Request Forgery (CSRF)	Forced Browsing	Hard-Coded Credentials	Missing Rate Limit	Server-Side Request Forgery (SSRF)	CORS Misconfiguration	FCDP Misconfiguration	CSV Injection (CSVi)
Firmware	EVlink	✓		✓			✓	✓	✓	✓	✓			✓
	xChargeIn				✓					✓			✓	
	CSWI Etrel	✓			✓				✓		✓		✓	
	SmartFox								✓	✓				
	Keba				✓								✓	
Mobile	ChargePoint					✓								
	Go					✓				✓				
	EV Connect					✓				✓				
Web	OASIS Portal	✓					✓							
	BaSE EVMS		✓							✓				
	Ensto CSI				✓					✓				
	FCEIS									✓		✓		
	ICEMS		✓							✓				
	PiControl	✓					✓		✓	✓	✓	✓		
	Garo CSI				✓					✓				
	Lancelot									✓		✓		

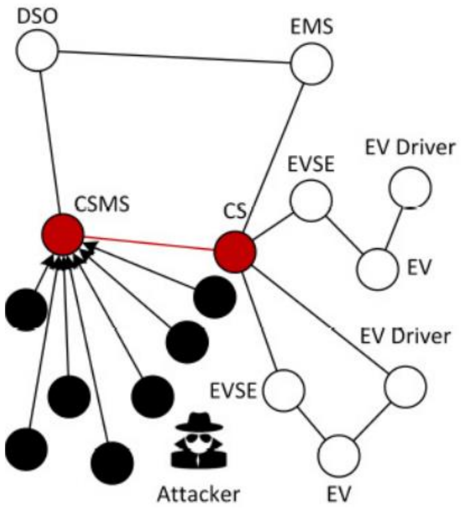
Attack Paths & Vulnerabilities of EVCS Ecosystem

Popular Attacks

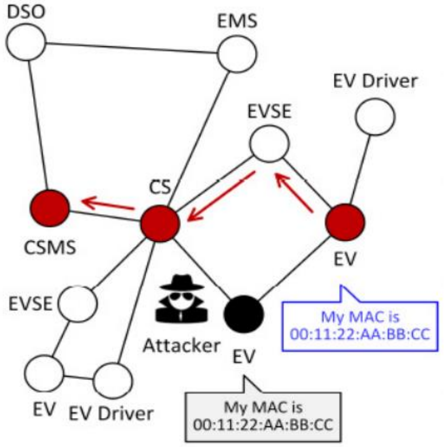
- ***MitM ATTACKS:*** In this attack, an attacker intercepts and possibly alters the communication between two parties without their knowledge.
  - The result could be data corruption or false information, such as misleading the status of a charging station.



- ***DOS ATTACK:*** This type of attack floods a network or system with traffic (eg: bogus charging requests) to overload it, preventing legitimate users from accessing the service.
  - It can shut down a node or network, leading to service disruptions.
  - User credentials can be used to launch DOS attacks against nodes



- ***ARP SPOOFING ATTACK:*** In this attack, an attacker sends false ARP messages in a network to associate their MAC address with the IP of an EVCS.
  - Enables attacker to intercept data intended for the CS, compromising sensitive details like location, availability, and EV credentials.
  - Allows the attacker to intercept, modify, or block data intended for the legitimate address.



Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis and C. Douligeris, "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)"

Attack Paths & Vulnerabilities of EVCS Ecosystem

Impacts of attacks

- ***Disruption of Charging Services***: Attacks can disable charging stations, leaving electric vehicle owners unable to charge their vehicles and potentially stranded without sufficient range to reach their destinations.

- ***Financial Fraud and Theft:*** Cyberattacks could lead to unauthorized access to payment systems, resulting in financial fraud or theft. This includes cloning of RFID cards or exploiting vulnerabilities in payment interfaces to charge services to unauthorized accounts.

- ***Compromise of Personal and Payment Data***: Data breaches can expose sensitive personal and payment information of EV owners, leading to risks of identity theft and unauthorized transactions.

- ***Damage to EV Components:*** Cyberattacks could lead to improper charging processes, causing overcharging or undercharging at rates (rate of charge) not intended for the vehicle. This may damage the battery and other critical EV components, potentially leading to reduced battery life, diminished vehicle performance, or even safety hazards such as overheating

- ***Manipulation of Charging Costs and Services***: Hackers could manipulate charging fees, fraudulently increasing the cost of charging or altering the amount of electricity provided, which could lead to financial losses for users and service providers.

- ***Threats to Power Grid Stability:*** Large-scale attacks could synchronize charging operations or reverse electric flow, destabilizing the power grid and potentially causing widespread power outages.

- ***Erosion of Consumer Confidence***: Repeated cyberattacks could erode trust in EV charging infrastructure, potentially slowing down the adoption of electric vehicles due to concerns over reliability, safety, and privacy.

Potential Cybersecurity Measures

Against Popular Attacks

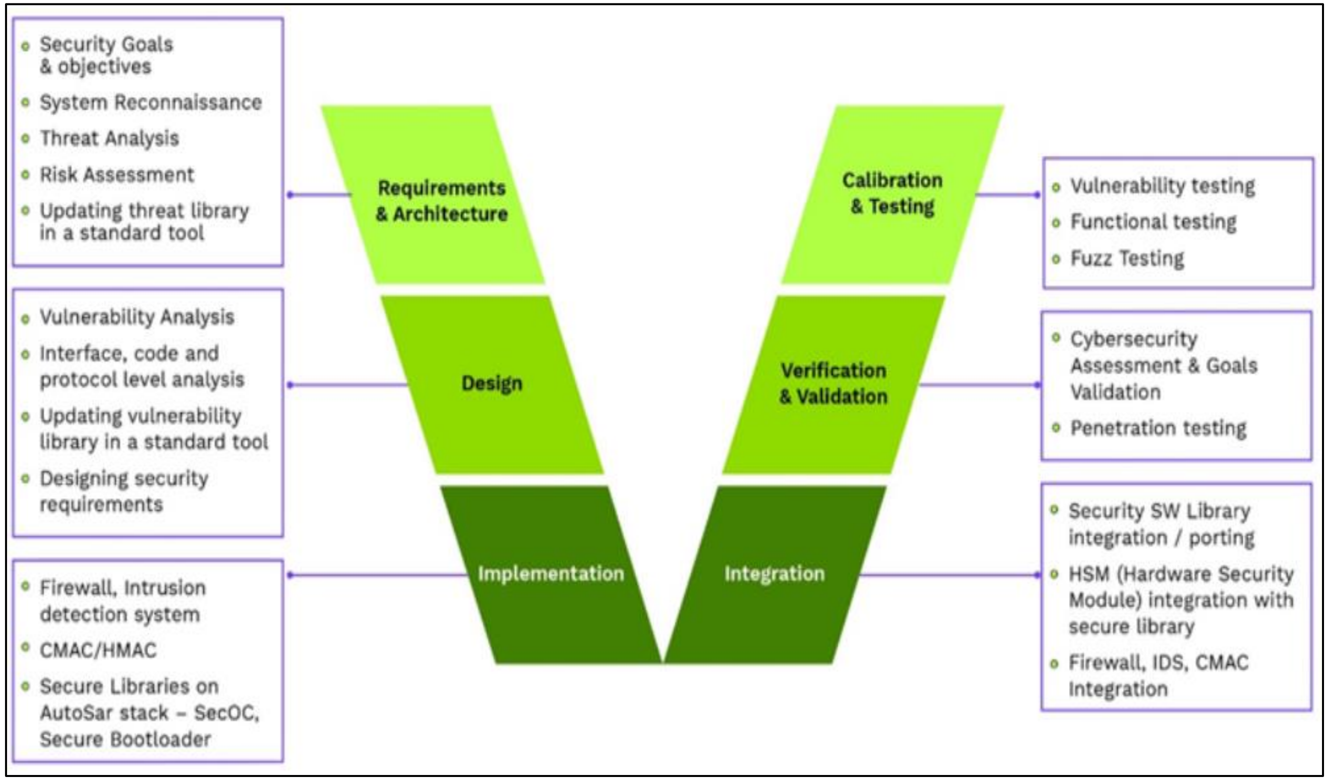
- ***MitM ATTACKS:***
  - *Contract Certificate Authentication*: Validate EVs with contract certificates.
  - *Blockchain Encryption*: Secure data with digital signatures.
  - *DAA and TPM*: Encrypt and authorize communications.
  - *Elliptic-Curve Keys*: Secure the initial EV to EVCS communication with a temporary Elliptic-Curve key pair, until a session-specific ID key is established, to prevent unauthorized access.

- ***DOS ATTACK:***
  - *ML-ADS :* Use AI for identifying irregular traffic patterns.
  - *Multi-Factor Authentication:* Implement for pre-charging negotiation security.
  - *Blockchain CS Selection:* Utilize blockchain for secure and private CS communication.

- ***ARP SPOOFING ATTACK:***
  - *Network Segmentation:* Limit traffic to confined segments.
  - Using Encryption techniques
  - Implementation of Intrusion Detection Systems

Potential Cybersecurity Measures for EVCS Ecosystem

EV Cybersecurity ‘V’ Model



Security Goals & objectives
System Reconnaissance
Threat Analysis
Risk Assessment
Updating threat library in a standard tool
Vulnerability Analysis
Interface, code and protocol level analysis
Updating vulnerability library in a standard tool
Designing security requirements
Firewall, Intrusion detection system
CMAC/HMAC
Secure Libraries on AutoSar stack – SecOC, Secure Bootloader
Requirements & Architecture
Design
Implementation
Integration
Verification & Validation
Calibration & Testing
Vulnerability testing
Functional testing
Fuzz Testing
Cybersecurity Assessment & Goals Validation
Penetration testing
Security SW Library integration / porting
HSM (Hardware Security Module) integration with secure library
Firewall, IDS, CMAC Integration

<u>Vulnerability Assessment, Risk Analysis & Mitigation:</u>

- Implementation of threat modeling techniques to identify potential cyber vulnerabilities.
- Quantitative and qualitative risk assessment and impact characterization.

Security of Communication Architecture:

- Implementation of ML-based Anomaly Detection in EVCS Protocols.
- Implementation of data security features such as encryption, multi-factor authentication.

EV Charging Station security:

- Prevention and mitigation of cyber attacks.
- Data privacy research related to cloud connectivity, billing infrastructure, etc.

Ref: https://www.kpit.com/insights/cyber-security-for-your-smart-charging-system/

Thank you

“This Is How Easy It Is to Hack EV Chargers” | Wall Street Journal YouTube