
Automotive Security

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

- Automotive security is to protect vehicles from physical threats like theft and digital threats like cyber attacks to ensure safety, privacy, and functionality of connected vehicles.
- Vehicles use protocols for message sharing and passing control.
- Electronic Control Unit (ECU) in the vehicle communicates with each other using the protocols.
- Automotive security (Digital) is to secure the vehicle's complex electronic systems, communication networks, and software against unauthorized access and manipulation by security implementing strategies.

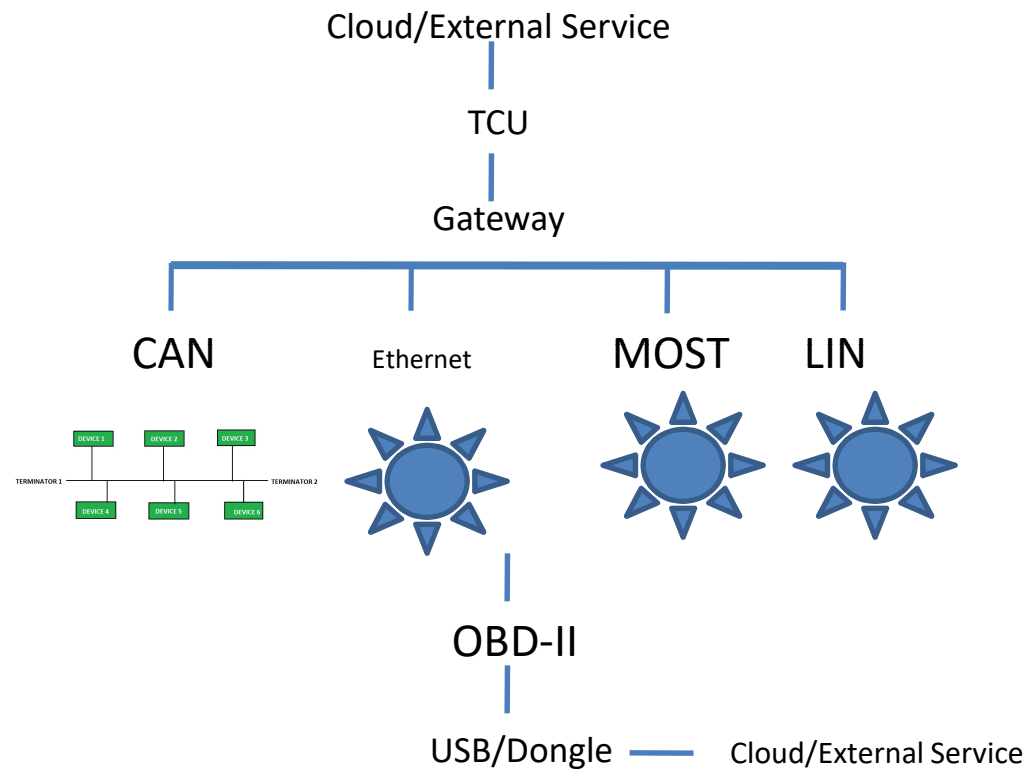
Components

- ECUs to operate the vehicle.
- On-Board Diagnostics
- On-Board Unit
- Telematics Control Unit
- Gateway

Protocols

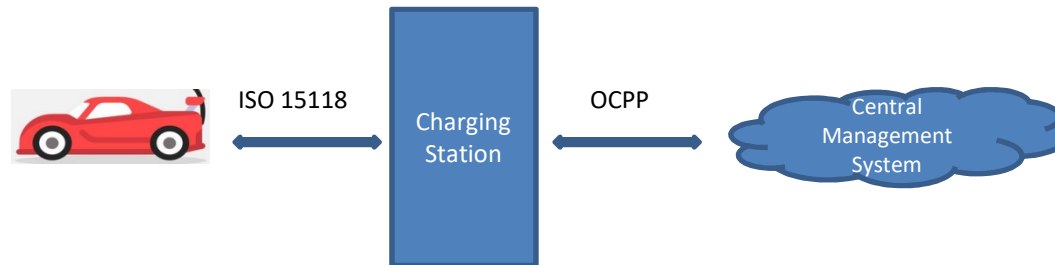
- CAN
- LIN
- FlexRay
- Automotive Ethernet
- ARINC
- MOST

Connection



EV Charging Protocols

- Open Charge Point Protocol (OCPP) for communication between charging stations and central management systems.
- ISO 15118 for vehicle-to-charging station communication (including Plug & Charge and V2G).
- Open Smart Charging Protocol (OSCP), which helps manage power distribution to the grid.



ISO 15118

- **Physical layer:** Power Line Communication (PLC) using HomePlug Green PHY for wired communication.
- **Network layer:** IPv6 for addressing.
- **Security layer:** TLS encryption and Public Key Infrastructure (PKI) for secure authentication. Usage of TLS became a requirement in ISO-15118-2 only for V2G sessions which make use of PnC. For ISO-15118-20, TLS is required on any established session.
- **Application layer:** Defines a set of V2G messages to be exchanged by the EV and the EVSE to negotiate charging parameters, charging schedule, PnC and more
- Has many versions, however 2 and 20 includes security largely.

ISO 15118 – Attacks?

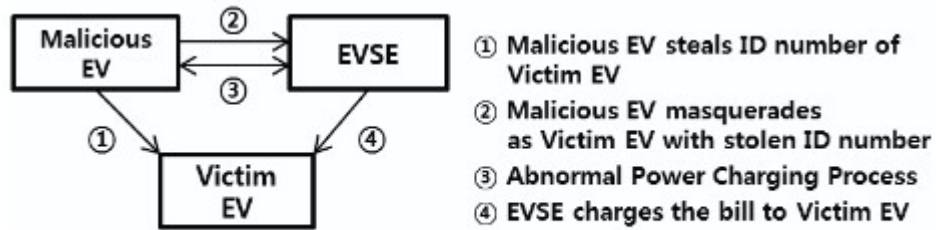


Fig. 3. Vulnerability; MaliciousEV - Changing ID number

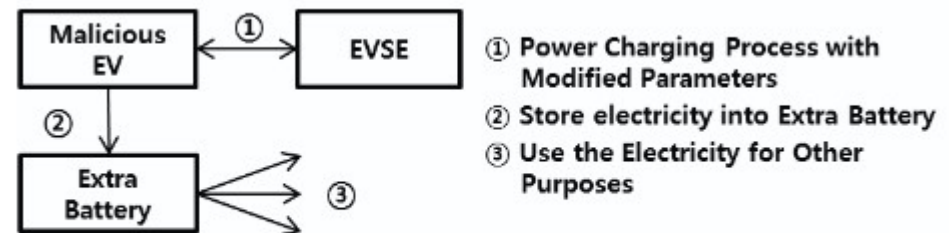


Fig. 4. Vulnerability; MaliciousEV – Power Charging for Abusing

OCPP

- To provide a standard communication interface used by all charging stations to avoid vendor lock-in.
 - Enhances interoperability and flexibility, enabling charging station owners to switch networks or hardware providers without being locked into proprietary systems.
- It also defines end-to-end security architecture and provides implementation guidelines to protect against cyber threats such as server hijacking, eavesdropping, and device impersonation
- Security concepts

– Secrecy of communication	OCPP 1.6	WebSocket over TLS (wss://) or HTTP
– Authentication of server	OCPP 2.0.1	WebSocket over TLS only (mandatory)
– Authentication of Client		

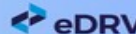
OCPP – Security Profile

Profile	Channel encryption	Server Auth	Charger Auth
Security Profile 1	–	–	Password
Security Profile 2	TLS 1.2 or higher	Server Certificate	Password
Security Profile 3	TLS 1.2 or higher	Server Certificate	Client Side Certificate

- The Electric Vehicle Supply Equipment - EVSE (charging station) acts as a WebSocket client
- The Charging Station Management System - CSMS (backend) acts as a WebSocket server




Open Charge Point Protocol (OCPP)

- It is an **interface** between:
 - **Grid operators or aggregators** (who manage the power constraints)
 - **Charging station operators (CSOs)** or charging management systems

Powered by 

Security Profiles under OCPP

OCPP has three security profiles, each with their own different security measures

PROFILE	Charge Point Authentication	Central System Authentication	Communication Security
 Unsecured Transport with Basic Auth	HTTP Basic Auth	---	---
 TLS with Basic Auth	HTTP Basic Auth	TLS Authentication using Certificate	Transport Layer Security
 TLS with Client Side Certificates	TLS Authentication using Certificate	TLS Authentication using Certificate	Transport Layer Security

EV Roaming Protocols

- OCPI (Open Charge Point Interface) – Between CPOs (Charge Point Operators) and EMSPs (eMobility Service Providers).
- Open Clearing House Protocol (OCHP) - Between CPOs (Charge Point Operators) and Clearing Houses (and eMobility Service Providers).
- OCHP vs OCPI
 - OCHP is more clearing house and financial reconciliation-focused
 - OCPI is a modern, lightweight REST API, designed to enable roaming, real-time status, pricing, and user authentication between EMSPs and CPOs.

References

- https://en.wikipedia.org/wiki/Open_Charge_Point_Protocol
- <https://plaxidityx.com/blog/blog-post/iso-15118-ev-cybersecurity-guide/>
- 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)*, Beijing, China, 2014, pp. 1-4, doi: 10.1109/ICITCS.2014.7021815.