Implementation challenge in vehicle cyber security

SG17 mini-workshop

Kaname Tokita

ISO-ITU-JVDS ISO Convener

26 August 2019

Motivation

- “Connected Vehicle” became so popular, still expected.
- Vehicle external communication started from OBD, added telematics and V2X.
- Charging communication of ISO 15118(V2G) is latest candidate, added in 2013.
- V2X and V2G required secure connection, just preparing.
- Latest topic of implementation will be introduced.

Presenter's profile

- Education
  The University of Tokyo, Master of Engineering of Mechanical engineering

- Organization
  - Honda R&D Co., Ltd., Chief Engineer
  - 06M/Y EU5D, 09M/Y US4D/2D CIVIC Project leader of electrical system test/design
  - Field of specialty; Vehicle control/communication system design&test

- ISO / IEC Expert
  - ISO TC22 SC31 data communication expert, HOD of Japan
  - ISO 15118-2 ED2 V2G CI PT2 Project leader (2015-2017)
  - ISO TC22 SC31 WG8 "*Vehicle domain service*" Convener

Contents

- Introduction of ISO 15118 ~ V2G CI
- Scope of ISO 15118
- Procedure of ISO 15118
- Identification in ISO 15118
- Certificates in ISO 15118
- Challenges in ISO 15118
- Challenges in vehicle cyber security

Introduction of ISO/IEC 15118 ~ V2G CI

- Charging control communication between EV and EVSE
- V2G CI = vehicle to grid communication interface
- Developed by ISO TC22/SC31~Data communication and IEC TC69 ~ Electric vehicle
- NWIP was approved in 2009, ISO 15118-1 general information and use case definitions issued in 2013.
- ISO 15118-2 network and application protocol requirements issued in 2014.

Scope of ISO 15118

- All OSI layers and sequences between EVCC and SECC *1
- Part of messages sent to SA *2
- High speed PLC(HPGP) on control pilot line
- IPv6 based TCP/IP, TLS, EXI
- Message defined by XML schema

Procedure of ISO 15118

- Session set up
- (Identification)
- Service / Charge parameter discovery
- Authorization
- Power delivery
- Session stop

Challenge in identification

Identification in ISO 15118

- 2 types identification, PnC and EIM
- PnC (plug and charge) is completed in V2G CI communication
- EIM uses credit card reader, RF-ID or other general devices

Change from ID to certificate

- Early project phase, IDs are addressed to identification
- Various IDs, vehicle-ID, EVSE-ID or contract-ID were listed.
- Later phase, e-mobility account is applied.
- Contract-ID was replaced by V2G CI certificate, changed to e-mobility (user) account and embedded in certificate.
- Dedicated message exchange for identification was integrated in TLS connection establishment.
- Most of vehicle implementers are not familiar to certificates.

Challenge in certificate handling

Implementation of PnC

- Vehicle OEM had big problem to find charge service operator who issues certificates.
- VDA issued DIN SPEC 70121 without PnC, helpful to separate it.
- Most of charge service operators installed only EIM chargers.
- US charge operator issued assessment report of PnC.
- ISO 15118-2 was issued in 2014, but we have no PnC vehicles past 6 years.

Other implementation challenges

- There still exists long distance from cert standard to specification.
- Certificate management also to be defined in detail.
- Specific hardware will be required to handle security information.
- Vehicle OEMs knew how cyber security is necessary, but never knew when it is necessary.

6 years later, PnC service got to be available.

- Intermediate service company which could provide complemental certificate service appeared in the market.
- It will require additional development and costs, but accepted.
- They can be addressed as future updates.

Challenges in Vehicle Cyber Security

Challenges in Cyber Security introduction

- OEMs must have better understanding about service account.
- Certificate based service for vehicles must be more popular.

Thank you for attention!