Cybersecurity of Smart Car and Trustworthy Car Data

October 2018

SangGyoo SIM, Ph.D.

Head of Penta IoT Convergence Lab. / Penta Security Systems, Inc.
CEO / AMO Labs Pte. Ltd.
Evolution toward Smart Car

- Connected Vehicle
- Automated Vehicle
- Electric Vehicle

Value-Added Service

Infrastructure (Smart Roadway, Smart Grid, ...)

Smart Car / Smart Mobility
Trend Keywords for Smart Cars

Security  Platform  Autonomous  Connectivity  Electrification

https://www.csis.org/analysis/implications-ultra-low-cost-access-space
Security for Plug&Charge Service of Electric Vehicles

Vehicle

OEM PKI System

Enrollment Certificate

ISO 15118

Station

Contract Certificate

OCPP (Open Charge Point Protocol)

Charger Certificate

OSCP (Open Smart Charging Protocol)

Server Certificate

ISO 61850

Payment Operator

V2G PKI System

Verification of Enrollment Certificate

Electricity Provider

Server Certificate

Cybersecurity of Smart Car and Trustworthy Car Data
Secure Communication for Connectivity

- **V2V** (Vehicle-to-Vehicle)
- **V2H** (Home)
- **V2G** (Vehicle-to-Grid)
- **V2S** (Vehicle-to-Service)
- **V2C** (Vehicle-to-Cloud)
- **V2D** (Vehicle-to-Nomadic Device)
- **V2P** (Vehicle-to-Pedestrian)
- **I2V** (Infra-to-Vehicle)
- **V2I** (Vehicle-to-Infra)

Manufacturers:
- Telematics
- Government
- TelCo (Mobile Manufacturer)
- TelCo (Telematics Manufacturer)
- Manufacturer

Secure Communication

Cybersecurity of Smart Car and Trustworthy Car Data
Security for Autonomous Vehicles
Security for Service Platform

Service Platform

Security
Security for Smart Car & Smart Mobility

Platform
- Cooperative Driving
- Fleet Management
- Infotainment
- Internal Gateway
- ADAS
- On-Board Sensor
- Body Control
- Chassis Control
- Powertrain Control

Autonomous
- Resilience System

Connectivity
- Secured Comm.
- V2H
- V2G
- V2N
- V2I
- V2D
- V2P

Electrification
- OEM PKI System
- Station
- Payment Operator
- Vehicle
- Electricity Provider
- V2G PKI System
- Trusted Ecosystem

Security
- Service Platform
Experiences about Connected Car

Secure First, then Connect™ … Cars

- 2007. Security between Vehicle and Diagnostic Device
- 2011. Security between Vehicle and Nomadic(mobile) Device
- 2012. Security for Patrol Cars
- 2013. V2X Security over WAVE telecommunication
- 2014. Telematics Security (consulting)
- 2015. AutoCrypt® Launched
- 2016. Security for C-ITS Testbed (Cooperative Intelligent Transportation System)
- 2018. Electric Vehicle ‘Plug&Charge’

Security for Electricity Vehicle Charging System
Security for Rail Transportation System
K-City (Testbed for Autonomous Vehicles))

Firewall for Smart Cars

G for Government
M for Manufacturer
Cybersecurity Concept for Smart Cars

- Crypto library
- Secure boot & Remote Attestation
- Secure Update
- HW trust anchor (HTA)

- Authentication, Confidentiality & Integrity of Messages
- Key Management

- Controls traffic flow
- Detects malicious traffic
- Privacy & Data Security

- Secure communication to anything

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person (Owner, Driver, Pedestrian), etc.
Cybersecurity Concept for Smart Cars: AutoCrypt®

1. Secure External Communication
   - Crypto library
   - Secure boot & Remote Attestation
   - Secure Update
   - HW trust anchor (HTA)

2. Secure Gateway
   - Authentication, Confidentiality & Integrity of Messages
   - Key Management

3. Secure Internal Communication
   - Controls traffic flow
   - Detects malicious traffic
   - Privacy & Data Security

4. Secure Platform
   - Secure communication to anything

On-Demand Solutions
- AutoCrypt KMS
- AutoCrypt IDS
- AutoCrypt WAF
- AutoCrypt VDM
- AutoCrypt V2X
- AutoCrypt LCM
- AutoCrypt V2G
- AutoCrypt PKI

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person (Owner, Driver, Pedestrian), etc.

Cybersecurity of Smart Car and Trustworthy Car Data
S1. Secure External Communication

Manufacturer

Telematics on Cloud

Certificate Authority
(of Manufacturer)

Certificate

Network: 3GPP (4G/5G)
Transport: IEEE1609.3
Security: IEEE1609.2

Government

V2I/I2V

Certificate Authority
(of Government)

Certificate

Network: IEEE802.11p
Transport: IEEE1609.3
Security: IEEE1609.2

Cross Certification
S1. Secure External Communication - TelCo & Manufacturer

Authentication based on Certificate

Service Connection

Internet (closed)

Authentication via USIM

3GPP (4G/5G)

Manufacturer

Authentication Management

Device Info.

Enrollment

Certificate

Service Ctrl.

User

TelCo

Authentication Management

Device Info.

Subscription Info.

Connection Ctrl.
C-ITS: Authenticated Communication

Secure Comm. (V2V)

Sender
- Retrieving the sender's certificate
- Generating the signature
- Traffic Info. + Signature + Certificate

Receiver
- Verifying the signature
- Validating the certificate

Secure Communication (V2I)

Hardware (HW)

Operating System (OS)

IEEE802.11p
SCMS Design (2017)

Source: SCMS CV Pilots Documentation, CAMPLLC, 2017
S2. Secure Gateway - Detects malicious traffic

- **Telematics Hacking (Jeep Cherokee)**
  - Type A: Packet Injection via External Network

- **Stolen Cars**
  - Type C: Packet Injection via OBD dongle

- **Hack via Smart Phone App**
  - Type B: Malware Injection via SD/USB port

- **Network Interface Controller (NIC)**
  - External NIC
  - Internal NIC

- **Firewall**
  - External Firewall
  - Internal Firewall

- **Components**
  - Head Unit (AVN/IVI)
  - ADAS
  - Chassis Control
  - Powertrain Control
  - Body Control

**Abbreviations**
- ADAS: Advanced Driver Assistance System
- AVN: Audio, Visual & Navigation
- IVI: In-Vehicle Infotainment
- NIC: Network Interface Controller
S2. Secure Gateway - Controls traffic flow

- **Designated Traffic**
- **Undesignated Traffic**

**ADAS**: Advanced Driver Assistance System
**AVN**: Audio, Visual & Navigation
**IVI**: In-Vehicle Infotainment
**NIC**: Network Interface Controller
S2. Secure Gateway - Data Security & Privacy Preserving

Cloud (OEM, Government, 3rd Party)

External Network

External NIC

External Gateway

Head Unit (AVN/IVI)

Internal Gateway

Data Recording

ADAS

Chassis Control

Body Control

Powertrain Control

Data Security & Privacy Preserving

ADAS: Advanced Driver Assistance System
AVN: Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC: Network Interface Controller
S3. Secure Internal Communication

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller
KMS : Key Management System
S4. Secure Platform - Secure Boot & Remote Attestation

ADAS: Advanced Driver Assistance System
AVN: Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC: Network Interface Controller
KMS: Key Management System
TPM: Trusted Platform Module

Attestation Server

Integrity Verification for Secure Boot
Remote Attestation

External NIC
External Gateway
Internal Gateway
Head Unit (AVN/IVI)
Powertrain Control
Body Control
Chassis Control

External Network

Data Recording
On-Board KMS
ADAS

Application
OS
Bootloader
Hardware

Attestation Server

Bootloader
OS
Application

On-Board KMS

Data Recording

Integrity Verification for Secure Boot
Remote Attestation

Chassis Control
S4. Secure Platform - Secure Update (OTA)

**Update Server**

**Authentication Server**

- Key Registration (Certificate)
- Update Data (Signed Data)

**External NIC**

**External Gateway**

**Internal Gateway**

**Update Manager**

**Head Unit (AVN/IVI)**

**Chassis Control**

**Body Control**

**Powertrain Control**

**ADAS**

**Signature Verification**

ADAS: Advanced Driver Assistance System
AVN: Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC: Network Interface Controller
KMS: Key Management System
TPM: Trusted Platform Module
Incident Response & Hacking Mitigation

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person(Owner, Driver, Pedestrian), etc.
Adaptive Security Architecture (Gartner)
Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person(Owner, Driver, Pedestrian), etc.
1 Autonomous Car  2,666 Mobile Devices
“Cars are mobile devices.”

Feature Phone ➔ Smart Phone

Connected Car ➔ Smart Car

Connectivity (constrained) ➔ Connectivity (no-constrained)
Pre-installed SW ➔ User-selected SW
Personalized Online Services ➔ Autonomous Driving
Connected Car Technologies & Services

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)
Value Shifts in the Auto Industry, 2015-2030

Revenue

<table>
<thead>
<tr>
<th>Year</th>
<th>~ $5 trillion</th>
<th>~ $7.8 trillion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>14%</td>
<td>10%</td>
</tr>
<tr>
<td>2030 (scenario)</td>
<td>12%</td>
<td>7%</td>
</tr>
<tr>
<td>2015</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>2030 (scenario)</td>
<td>14%</td>
<td>14%</td>
</tr>
<tr>
<td>2015</td>
<td>49%</td>
<td>44%</td>
</tr>
<tr>
<td>2030 (scenario)</td>
<td>41%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Profits

<table>
<thead>
<tr>
<th>Year</th>
<th>~ $400 billion</th>
<th>~ $600 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>14%</td>
<td>20%</td>
</tr>
<tr>
<td>2030 (scenario)</td>
<td>14%</td>
<td>5%</td>
</tr>
<tr>
<td>2015</td>
<td>41%</td>
<td>29%</td>
</tr>
<tr>
<td>2030 (scenario)</td>
<td>41%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Share addressable by today’s OEM model declining to less than 70%
Share addressable by new entrants (digital services, mobility, new technology supply, Fintech, startup EV players) growing to more than 45% or $3.5 trillion

Share addressable by OEM declining from ~70% to less than 50%
Share that can be captured by new entrants growing to 60% or $360 billion

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)
Cybersecurity of Smart Car and Trustworthy Car Data

28
Value Shifts in the Auto Industry, 2015-2030

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)
Service Business: The Case of Apple

Car-generated data may become a USD 450 - 750 billion market by 2030

USD billions

Today – traditional automotive revenues
Vehicle sales dominant

2030 – new automotive revenues
Recurring revenues significantly increasing

~ 5% p.a. growth

~ 3,500
~ 7,050 - 7,350

+36 - 41%

Car data-enabled services
Shared mobility
Aftermarket

~ 720
~ 450 - 750

1,400

4,000

~ 2,750
One-time vehicle sales

"Significantly larger revenue pool around the car, expanding even faster"

SOURCE: McKinsey
AMO : Blockchain for the CAR DATA Market

Market Participant

Automobile User

Users

Infrastructure

Mobile Devices

AMO Mobile Wallet

AMO Auto Wallet

IoT Devices

Cars

Products & Services

AMO Coin

AMO Market

AMO Blockchain

AMO Platform

Processed CAR DATA

Processed CAR DATA

CAR DATA

CAR DATA

Market Participant

Automobile Manufacturer

Automobile Service Provider

Automobile Manufacturers

Platform Providers

Service Providers

Public Services

Products & Services

AMO Coin

AMO Coin Economy

Exchange or DEX (Decentralized Exchange)

Other Coin Economies

User Security of Smart Car and Trustworthy Car Data
How Can AMO Be Used?

1) Provide car data
2) Receive AMO Mile
3) Exchange car data with AMO Cash

*AMO Mile: Contribution point
**AMO Cash: Internal currency which can be exchanged into AMO Coins
Use Case: In-Car Advertising & In-Car Payment

Today
Car as vehicle to carry the customer to a shop after the decision to purchase has been made.

Tomorrow
Car as touchpoint to recommend to the customer where/what to buy.
Car as service to be provided to support the customer in either buying onboard, reaching the store or enjoying the brand experience.

SOURCE: McKinsey
* The AMO Platform supports the AMO Blockchain for AMO Market operation. It supports communication among participants and manages operational policies and IT systems including software.
Fair Trade between Participants
Retention of Ownership
Open for Everyone
Neutral to Car Models & Services
Trustworthiness
Open Collaboration Platform (Business)

Personal User

OEM

MaaS

AMO

Service Provider

(Technology)

Car Data Market

Cybersecurity of Smart Car and Trustworthy Car Data
thank you

Asian Cyber Security Vendor of the Year

Blockchain for the CAR DATA Market

KOREA  Yeouido, Seoul   www.pentasecurity.co.kr (HQ)
U.S.A.  Houston, Texas   www.pentasecurity.com
JAPAN  Shinjuku-Ku, Tokyo   www.pentasecurity.co.jp