5G 환경에서 자동차 보안
미래 자동차 사업의 신뢰 환경

2019. 11. 06.

SangGyoo SIM, Ph.D. (sgsim@pentasecurity.com)

CTO @ Penta Security Systems Inc.
### Experiences in Cybersecurity for Connected Cars

<table>
<thead>
<tr>
<th>Year</th>
<th>Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>C-ITS Infrastructure for Express Railroads</td>
</tr>
<tr>
<td></td>
<td>Threat Assessment for Connected Cars</td>
</tr>
<tr>
<td></td>
<td>Machine Learning based Data Analytics of CAN BUS Data</td>
</tr>
<tr>
<td></td>
<td>Seoul C-ITS Project</td>
</tr>
<tr>
<td></td>
<td>Jeju Province C-ITS Project</td>
</tr>
<tr>
<td></td>
<td>Design &amp; Plan for C-ITS Infrastructure</td>
</tr>
<tr>
<td>2018</td>
<td>Auto-Link Premium Service</td>
</tr>
<tr>
<td></td>
<td>V2P (Vehicle-to-Pedestrian)</td>
</tr>
<tr>
<td></td>
<td>‘Plug&amp;Charge’ for Electric Vehicle</td>
</tr>
<tr>
<td></td>
<td>Security for Next Generation In-Vehicle Infotainment</td>
</tr>
<tr>
<td></td>
<td>Security for Electricity Vehicle Charging System</td>
</tr>
<tr>
<td></td>
<td>Security for Rail Transport System</td>
</tr>
<tr>
<td></td>
<td>K-City (Testbed for Autonomous Vehicles)</td>
</tr>
<tr>
<td></td>
<td>Security for C-ARS (Cooperative Automated Driving Roadway System)</td>
</tr>
<tr>
<td></td>
<td>Security for C-ITS Testbed (Cooperative Intelligent Transport System)</td>
</tr>
<tr>
<td>2017</td>
<td>Security for TMS on Cloud</td>
</tr>
<tr>
<td></td>
<td>Firewall for Smart Cars</td>
</tr>
<tr>
<td></td>
<td>AutoCrypt® Launched</td>
</tr>
<tr>
<td>2016</td>
<td>V2X Security over WAVE telecommunication</td>
</tr>
<tr>
<td></td>
<td>Security for Patrol Cars</td>
</tr>
<tr>
<td></td>
<td>Security between Vehicle and Nomadic (Mobile) Device</td>
</tr>
<tr>
<td></td>
<td>Security between Vehicle and Diagnostic Device</td>
</tr>
<tr>
<td>2015</td>
<td>Vehicle Data Management System</td>
</tr>
<tr>
<td></td>
<td>Telematics Security (Consulting)</td>
</tr>
<tr>
<td>2014</td>
<td>TMS on Cloud</td>
</tr>
<tr>
<td>2013</td>
<td>Security for TMS on Cloud</td>
</tr>
<tr>
<td>2012</td>
<td>Security for Patrol Cars</td>
</tr>
<tr>
<td>2011</td>
<td>Security between Vehicle and Nomadic (Mobile) Device</td>
</tr>
<tr>
<td>2007</td>
<td>Security between Vehicle and Diagnostic Device</td>
</tr>
</tbody>
</table>

**AutoCrypt**

Smarter security for smart cars

- **G** Government or Public Organization
- **M** Manufacturer or Supplier
### TU-Automotive (June 2019)

#### Awards Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Award Name</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>OEM of the Year</td>
<td></td>
<td>Mitsubishi Motors</td>
</tr>
<tr>
<td>Best Connected Product/Service</td>
<td></td>
<td>Honda - Smart Intersection</td>
</tr>
<tr>
<td>Best Connected Product/Service for the Commercial Market</td>
<td>Tactile Mobility - Tactile Sensing and Data Platform</td>
<td></td>
</tr>
<tr>
<td>Best Auto Digital Insurance Product/Service</td>
<td>Cambridge Mobile Telematics - DriveWell Tag</td>
<td></td>
</tr>
<tr>
<td>Best ADAS or Autonomous Product/Service</td>
<td></td>
<td>PreAct Technologies</td>
</tr>
<tr>
<td>Best Auto Mobility Product/Service</td>
<td></td>
<td>Amazon for Alexa</td>
</tr>
<tr>
<td>Best Auto Cybersecurity Product/Service</td>
<td></td>
<td>Penta Security Systems - AutoCrypt®</td>
</tr>
<tr>
<td>Best Data/A.I. Product/Service</td>
<td></td>
<td>SafeRide Technologies - eXRay</td>
</tr>
<tr>
<td>Best eMobility Product/Service</td>
<td></td>
<td>Konetik Deutschland GmbH - Konetik Electric Vehicle Feasibility Assessment</td>
</tr>
<tr>
<td>Newcomer of the Year</td>
<td></td>
<td>Wavesense</td>
</tr>
<tr>
<td>Influencer of the Year</td>
<td></td>
<td>Navistar, Inc. - Andrew Donadliger, VP GM, Navistar</td>
</tr>
<tr>
<td>Rising Star of the Year</td>
<td></td>
<td>GuardFinn - Jillian Goldberg</td>
</tr>
</tbody>
</table>
Shift in Business Paradigm: Mobile Phone

Feature Phone

- User Interface
- 2G
- Pre-loaded Service

Device  Call/SMS

Smart Phone

- User Interface
- LTE
- User-selected Service

Device + Software + 3rd Party Service
Shift in Business Paradigm: Automobile

Legacy Car

Automobile Driving

Smart Car

Device + Software + 3rd Party Service
Future Car

Autonomous Driving
Connectivity
Electrification

Service Platform
Online Services
User-selected SW
Personalized

Car is Smart Device

Car uses Smart Phone

Car carries Smart Phone
Connected Car Technologies and Services

**Consumer Services (Digital Cloud Based)**

- TRAVEL
- HOTEL
- FLIGHT
- ROBO-TAXI SERVICES
- INSURANCE
- LEASE
- RIDE SHARING
- CAR SHARING
- CAR HAILING
- RENTAL

**Connected Car Packages**

- Vehicle Management
- Connected Car Feature & Service
- Consumer Features
- Commercial Features

**Supply-side Technologies**

- Safety
- Autonomous driving

**Future Business**

- Fluid Boundaries
- Enabling the use of consumer services

- Current world roles (and strengths)
  - Internet & tech companies; Specialist services firms

- Increasing Competition
  - Auto OEMs
  - Increasing Competition
  - Auto suppliers

**Smart Mobility**

- TRAVEL
- HOTEL
- FLIGHT
- ROBO-TAXI SERVICES
- INSURANCE
- LEASE
- RIDE SHARING
- CAR SHARING
- CAR HAILING
- RENTAL

**Other Services**

- COMMUNICATION
- SOCIAL MEDIA
- COLLABORATION
- MEDIA CONTENTS
- EDUCATION
- HEALTH
- FINTECH
- ADVERTISING
- COMMERCE
- PAYMENT

**Future Business**

- Current world roles (and strengths)
  - Internet & tech companies; Specialist services firms

- Increasing Competition
  - Auto OEMs
  - Increasing Competition
  - Auto suppliers

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)
Momentum Technologies: 1. Electrification

Vehicle

OEM PKI System

Enrollment Certificate

ISO 15118

Contract Certificate

Station

Verification of Enrollment Certificate

Charger Certificate

V2G PKI System

Electricity Provider

Mobility Operator / Charge Point Operator

OCP (Open Charge Point Protocol)

Server Certificate

OSCP (Open Smart Charging Protocol)

ISO 61850

Server Certificate

OEM Service

Enrollment Certificate

Vehicle

OEM PKI System
Momentum Technologies : 2. Connectivity

V2H (Home) → V2V (Vehicle-to-Vehicle) → V2G (Vehicle-to-Grid)

Manufacturer

V2S (Vehicle-to-Service) → V2C (Vehicle-to-Cloud)

V2D (Vehicle-to-Nomadic Device) → V2I (Vehicle-to-Infra)

Government

V2P (Vehicle-to-Pedestrian)

Secure Communication

Mobility-as-a-Service
Momentum Technologies: 3. Autonomous Driving

- Fleet Management
- Cooperative Driving
- External Network
- External NIC
- External Gateway
- Internal Gateway
- External Firewall/IDS
- Internal Firewall/IDS
- ADAS
- Infotainment
- Chassis Control
- Body Control
- Powertrain Control
- Unsecure ECU
- On-Board Sensor
Momentum Technologies: 4. Platform

Service Platform

Security

Service Provider/SW Provider
Manufacturer/Supplier
Government/Authority

Open Mobility Cloud
Open Location Platform

android auto
Apple CarPlay
Amazon Alexa
BMW
HERE
Momentum Technologies : 5. Security

UN-ECE WP.29 “World Forum for Harmonization of Vehicle Regulations”
SB-327 of CA, US “Information privacy : connected devices”
In-Vehicle Security

Online Service
(Cloud)

Infrastructure

User (Mobile)

Security Threat

Security Area
In-Vehicle Security

1. Secure External Communication
   - 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

2. Secure Gateway

3. Secure Internal Communication

4. Secure Platform

On-Demand Solutions
* Collaboration with third-party vendors

- External Network
- Gateway
- ECU
- Internal Network
- User (Mobile)
- Infrastructure
- Online Service (Cloud)
Security between Vehicles and Infrastructures

Online Service (Cloud)
Infrastructures
User (Mobile)

Security Threat
Security Area
Security Threats and Security Area @ C-ITS
S1. Secure External Communication : V2I & V2V

SCMS : Security Credential Management System
Security Threats and Security Area @ C-ITS

- IT Security
- Firewall, IDS, System Hardening
- Firewall, IDS, System Hardening

Authenticated Communication via Digital Signature (Service)

Encrypted Communication over SSL (Certificate Management)

Infrastructure (Backend)

Authenticated Communication via Digital Signature (Service)

Infrastructure (RSU: Road Side Unit)
S1. Secure External Communication - Ecosystem and Security Infrastructure

- Key Management
- Authentication Management
- Privilege Management
S1. Secure External Communication – V2C & V2S

- Authentication based on Certificate
- Service Connection
- Internet (closed)
- Authentication via USIM
- 3GPP (4G/5G)
- TelCo
- Manufacturer
- User

- Device Info.
- Enrollment
- Certificate
- Service Ctrl.

- Device Info.
- Subscription Info.
- Connection Ctrl.
Adaptive Security Architecture

Source: Gartner (February 2014)
Incident Response & Hacking Mitigation

Context-Aware Intelligence
- Model, Simulate, Act, Protect

Knowledge
- Community
- Threat Intelligence
- Dependencies, relationships

Information
- Collect, Correlate
- Big Data
- Logs, Events, Costs, Usage, Attacks, Breaches

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

Internal Network
- Gateway
- ECU

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person(Owner, Driver, Pedestrian), etc.
Online Service as a Platform & Security
Online Service as a Platform
Online Service Platform

- App Store
- Big Data
- OEM Service

Service Platform

Security

- IoT Devices
- Users (Mobile)
- Partners

Service Provider

S/W Provider
Online Service Platform + Security
Online Service Platform + Security
Online Service Platform + Internal ICT Infra System

Service Provider
S/W Provider

Employees
Suppliers

App Store Big Data OEM Service
Online Service (Cloud)

ICT Infra Systems

IoT Devices
Users (Mobile)
Partners
Online Service Platform + Internal ICT Infra System

Service Platform

- App Store
- Big Data
- OEM Service

Online Service (Cloud)

- IoT Devices
- Users (Mobile)
- Partners

Service Provider
S/W Provider

Employees
Suppliers

ICT Infra Systems

Security
"Bi-Modal IT" from Gartner
“Bi-Modal IT” from Gartner
Connected Car Technologies and Services

**Mode 2**

**Mode 1**

### Connected Car Packages

- **Vehicle Management**
- **Connected Car Feature & Service**
- **Consumer Features**
  - Commercial Features

### Supply-side Technologies

- Advanced driver assistance systems
- Human-machine Interface
- Infotainment
- Connectivity, computing, and cloud based enabling services

### Connected Car Technologies and Services

- **SMART MOBILITY**
  - TRAVEL
  - HOTEL
  - FLIGHT
  - ROBO-TAXI SERVICES
  - INSURANCE
  - LEASE
  - RIDE SHARING
  - CAR SHARING
  - CAR HAILING
  - RENTAL

- **OTHER SERVICES**
  - COMMUNICATION
  - SOCIAL MEDIA
  - COLLABORATION
  - MEDIA CONTENTS
  - EDUCATION
  - HEALTH
  - FINTECH
  - ADVERTISING
  - COMMERCE
  - PAYMENT

### Fluid Boundaries

**Future Business**

- Current world roles (and strengths)
  - Internet & tech companies; Specialist services firms

- Increasing Competition
  - Auto OEMs
  - Auto suppliers
Online Service Platform + Internal ICT Infra System + "Bi-modal" Security Policy
Data-Driven Business

Service Provider

S/W Provider

Service Platform

App Store  Big Data  OEM Service

Online Service (Cloud)

IoT Devices

Users (Mobile)

Partners
S2. Secure Gateway – Data Security & Privacy Preserving

- Secure Store
- Pseudonymization
- Audit
"Data Economy"

"The World’s Most Valuable Resource is No Longer Oil, but Data"

* Source: The Economist (2017.05.06)
Discovering Value of Data

Data: The World’s Most Valuable Resource

- Protected DATA
- Value-Added DATA
- Connected & Shared
- Data Sharing
- Isolated
- Data Security
- Archived DATA
- Unprotected

Protected

Unprotected
Missed Potential Value of Data

Coffee Production Flow

Seed → Growing → Processing → Brewing → Serving
Maximized Values

Data-enabled Service Flow

Data Generation → Data Collection → Data Archiving → Data Analytics → Data-enabled Service
Missed Opportunities
Data Economy - Ecosystem

Tier x → Tier 2 → Tier 1 → OEM → TMS

- Insurance
- C-ITS
- Parking
- IoT Service

- OEM
- MaaS
- Car Sharing
- Car Hailing
- Public Trans.
- Rent/Lease
- Logistics
- EV Charging

Connected Car Services: Advertisement, Payment, Contents Streaming, Game, Fintech, SNS, …

Data Sharing Platform

SVC Provider

Confidential Subject to NDA
Data Economy - Authentication

Tier x -> Tier 2 -> Tier 1 -> OEM

OEM -> TMS

Tier 1:
- Insurance
- C-ITS
- Parking
- IoT Service

Tier 2:
- OEM

OEM -> MaaS
- Car Sharing
- Car Hailing
- Public Trans.
- Rent/Lease
- Logistics
- EV Charging

SVC Provider

Data Sharing Platform

Security
Data Sharing Platform : Stakeholders & End Entities

- Tier 1
  - HKMC
  - OEM
  - C-ITS
  - IoT Service
  - SVC Provider
- Tier 2
  - Insurance
  - Parking
  - IoT Service
- MaaS
  - Car Sharing
  - Car Hailing
  - Public Trans.
  - Rent/Lease
  - Logistics
  - EV Charging

Data Sharing Platform