Security for Connected/Autonomous Car

September 2017

Jaeson YOO
(jyoo@pentasecurity.com)
Chief Security Evangelist

http://www.nanalyze.com/2017/04/10-connected-car-technology-startups/
‘All That Connections’ of Connected Car

V2H (Home)

V2V (Vehicle-to-Vehicle)

V2I (Vehicle-to-Infra)

I2V (Infra-to-Vehicle)

V2N (Vehicle-to-Network)

V2S (Vehicle-to-Service)

V2D (Vehicle-to-Nomadic Device)

V2P (Vehicle-to-Pedestrian)

Manufacturer

Telematics

TelCo

TelCo (Mobile Manufacturer)

Government
Extended Vehicle (ISO 20077 & 20078)

3rd Party Connected Services

Mobile Brought-in Connectivity

OEM Connected Services

Industry Standards Development

Built-in Connectivity

GNSS Antenna Beamed-in Connectivity

Security for Connected Car
“Cars are mobile devices.”

- Feature Phone
  - Connectivity (constrained)
  - Pre-installed SW

- Smart Phone
  - Connectivity (no-constrained)
  - User-selected SW
  - Personalized
  - Online Services
  - Autonomous Driving

- Connected Car
  - Connectivity (constrained)
  - Pre-installed SW

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

**Smart mobility services**
- Travel: hotels, flights, trains, more
- Robo-taxi services
- Ride sharing
- Car sharing
- Rental

**Other services (used in-car)**
- Advertising
- Services: health, education, Fintech, more
- Communication, social media, collaboration
- Commerce, payment
- Content (video, music, more)

**Connected car packages**
- Vehicle management features
- Connected car features and services
- Consumer features
- Commercial features

**Supply-side technologies**
- Advanced driver assistance systems
- Human-machine interface
- Infotainment
- Connectivity, computing, and cloud-based enabling services

Current world roles (and strengths)
- Internet and tech companies; specialist service firms
- Increasing competition

Auto OEMs
- Increasing competition

Auto suppliers
Value Shifts in the Auto Industry, 2015-2030

Revenue

- 2015: ~ $5 trillion
  - 14% Shared mobility
  - 12% Digital services
  - 8% Supplier (new technology/software)
  - 14% Supplier (traditional/hardware)
  - 49% Insurance
  - 10% Financing
  - 7% Aftermarket
  - 7% Vehicle sales

- 2030 (scenario): ~ $7.8 trillion
  - 10% Shared mobility
  - 7% Digital services
  - 10% Supplier (new technology/software)
  - 13% Supplier (traditional/hardware)
  - 44% Insurance
  - 7% Financing
  - 10% Aftermarket
  - 10% Vehicle sales

Profits

- 2015: ~ $400 billion
  - 14% Shared mobility
  - 14% Digital services
  - 11% Supplier (new technology/software)
  - 16% Supplier (traditional/hardware)
  - 41% Insurance
  - 11% Financing
  - 10% Aftermarket
  - 10% Vehicle sales

- 2030 (scenario): ~ $600 billion
  - 20% Shared mobility
  - 14% Digital services
  - 5% Supplier (new technology/software)
  - 11% Supplier (traditional/hardware)
  - 29% Insurance
  - 11% Financing
  - 10% Aftermarket
  - 10% Vehicle sales

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)

Security for Connected Car
“Safety begins with Security”

The existing cyber threats that risked monetary or physical loss are now being applied to Vehicles which can place severe liability to a person’s life.

Remote Shutdown
- Hack into car dealership security system remotely disables a car’s ignition system and causes horn to honk.

Stolen Cars
- Thieves use kits to create new keys to drive off with BMWs using OBD-II tool meant to diagnosis vehicle issues.

Hack via Smart Phone App
- An Android smart phone app allowed remote hackers to hack into a car’s ECU via the smart phone as a communication bridge

Electric Car Hack
- Chinese white hat hackers are able to remotely hack into Tesla Model S to control its doors, windows, etc.

Remote Hack
- White hat hackers remotely hack into a Jeep Cherokee via a UConnect vulnerability bring to serious potential dangers (cut engine while in motion on highway, disable brakes, etc.)

Telematics Hacking
- University security researchers hack a Corvette via an OBD-II dongle by using SMS from an Android to execute commands to the car’s CAN bus – manipulating the brakes and windshield wipers
Security Threats

The number of vehicular related hacking incidents become more present to the public as time goes by. Vehicular vulnerabilities will continue to grow as the variety of car models increase. Security will play an ever more important role in this evolving society of connected vehicles.

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

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

Stolen Cars
Type C: Packet Injection via OBD dongle

DC: Drive Components
TMS: Telematics
ADAS: Advanced Driver Assistance System
AVN: Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC: Network Interface Controller
"SPY CAR" (Security and Privacy in Your Car) Act (2015.07)

I. Cybersecurity Standards

- **Hacking protection**: all access points in the car should be equipped with reasonable measures to protect against hacking attacks, including isolation of critical software systems and evaluated using best security practices, such as penetration testing;

- **Data security**: all collected information should be secured to prevent unwanted access—while stored on-board, in transit, and stored off-board; and

- **Hacking mitigation**: the vehicle should be equipped with technology that can detect, report and stop hacking attempts in real-time.

II. Privacy standards

- **Transparency**: owners are made explicitly aware of collection, transmission, retention, and use of driving data;

- **Consumer choice**: owners are able to opt out of data collection and retention without losing access to key navigation or other features (when technically feasible), except for in the case of electronic data recorders or other safety or regulatory systems; and

- **Marketing prohibition**: personal driving information may not be used for advertising or marketing purposes without the owner clearly opting in.

III. Cyber dashboard

NHTSA, in consultation with FTC, should establish a “cyber dashboard” that displays an evaluation of how well each automobile protects both the security and privacy of vehicle owners beyond those minimum standards. This information should be presented in a transparent, consumer-friendly form on the window sticker of all new vehicles.

“SPY CAR” (Security and Privacy in Your Car) Act (2017.03)

I. Cybersecurity Standards

- Protection against Hacking: equipped with reasonable measures to protect against hacking attacks.
  - Isolation Measures: to separate critical software systems from noncritical software systems.
  - Evaluation: evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.
  - Adjustment: adjusted and updated based on the results of the evaluation.

- Security of Collected Information
  - All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access – (a) stored onboard, (b) transit to another location, and (c) offboard storage or use.

- Detection, Reporting, and Responding to Hacking
  - Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.

II. Cyber Dashboard

- inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements.

III. Privacy Standards for Motor Vehicles

- Cont’d
III. Privacy Standards for Motor Vehicles

- **Transparency**: Each motor vehicle shall provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle.

- **Consumer Control**: The option of terminating the collection and retention of driving data.

- **Access to Navigation Tools**: If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data, the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.

- **Exception**: Not apply to driving data stored as part of the electronic data recorder system or other safety systems on board the motor vehicle that are required for post incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.

**Limitation on Use of Personal Driving Information**

- A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.
  - Consent requests shall be clear and conspicuous.
  - Consent requests shall be made in clear and plain language.
  - Consent requests may not be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.
“Federal Automated Vehicles Policy” (2016.09)

"Federal Automated Vehicles Policy (2016.09)"

Scope & Process Guidance
- Test/Production Vehicle
- FMVSS Certification/Exemption
- HAV Registration

Guidance Applicable to All HAV Systems on the Vehicle
- Data Recording and Sharing
- Privacy
- System Safety
- Vehicle Cybersecurity
- Human-Machine Interface
- Crashworthiness
- Consumer Education and Training
- Post-Crash Vehicle Behavior
- Federal, State and Local Laws
- Ethical Considerations

Guidance Specific to Each HAV System
- Describe the ODD (Where does it operate?)
  - Geographic Location
  - Roadway Type
  - Speed
  - Day/Night
  - Weather Conditions
  - Other Domain Constraints
- Object and Event Detection and Response
  - Normal Driving
  - Crash Avoidance - Hazards
- Fall Back Minimal Risk Condition
  - Driver
  - System

Testing and Validation
- Simulation
- Track
- On-Road
Cybersecurity Best Practices (2016.10)

Cybersecurity Best Practices (2016.10)

- Self-Auditing
  - Risk Assessment
  - Penetration Testing and Documentation
  - Self-Review

- Fundamental Vehicle Cybersecurity Protections
  - Limit Developer/Debugging Access in Production Devices
  - Control Keys
  - Control Vehicle Maintenance Diagnostic Access
  - Control Access to Firmware
  - Limit Ability to Modify Firmware
  - Control Proliferation of Network Ports, Protocols and Services
  - Use Segmentation and Isolation Techniques in Vehicle Architecture Design
  - Control Internal Vehicle Communications
  - Log Events
  - Control Communication to Back-End Servers
  - Control Wireless Interfaces
Joint Agenda

a. Coherent international, European and national rules
   - The aim is to work towards the removal of barriers and to promote legal consistency. The legal framework should offer sufficient flexibility to accommodate innovation, facilitate the introduction of connected and automated vehicles on the market and enable their cross-border use.

b. Use of data
   - Data generated through the use of connected and automated vehicles can serve public and private value-added services. Clarification is needed on the availability for public and private use and responsibilities of the parties involved.

c. Ensure privacy and data protection
   - Respecting existing legislation on privacy and data protection, the conditions for the (re-)use and sharing of data generated by connected and automated vehicles need to be clarified.

d. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication
   - In order to maximize benefits in road safety and environmental performance, it is essential to ensure that new services and systems are compatible and interoperable at European level and to coordinate investments towards reliable communication coverage, exploit the full potential of hybrid communications, where relevant, and improve the performance of location accuracy, benefiting in particular from the use of GALILEO and EGNOS.
Joint Agenda

- **e. Security**
  - In the light of the increase in cyber-threats and serious vulnerabilities, it is essential to ensure security and reliability of connected and automated vehicle communications and systems. Common trust models and certification policies should be developed to prevent risks and support cybersecurity, whilst ensuring safe and interoperable deployment.

- **f. Public awareness and acceptance**
  - It is important to manage societal expectations, to raise awareness and increase acceptance and appreciation of connected and automated vehicle technologies.

- **g. Common definitions of connected and automated driving**
  - Common definitions of connected and automated driving should be developed and updated, based on the Society of Automotive Engineering levels (SAE levels) as a starting point.

- **h. International cooperation**
  - It is important to develop and maintain close cooperation with other regions, particularly the US and Japan, to work towards a global framework and international standards for connected and automated vehicles.
ENISA – Cyber Security and Resilience of Smart Cars

ENISA – Cyber Security and Resilience of Smart Cars

**BODY CONTROL**
- ECU and sensors: instrument cluster, climate control, door locking...
- Dashboard display, air conditioning, lights, direction/warning lights, doors, windows, seat belts, motorized/heating seats...

**INFOtainment Control**
- ECU and sensors (Head unit Audio/video, navigation, telephone...)
- External media/drives/phone content...
- Infotainment subnetwork (e.g. MOST)
- Ad-hoc internal networks (e.g. Bluetooth, Wifi...)

**DIAGNOSTIC AND MAINTENANCE SYSTEMS**
- OBD II ports
- Aftermarket dongles
- Garage or maintenance equipment

**COMMUNICATIONS CONTROL**
- Gateways ECU with Telematics and communications
- External communication networks

**POWERTRAIN CONTROL**
- Engine, transmission...
- ECU and sensors: engine control, transmission control, speed control / gear control, driving support (ABS), power train sensors...

**CHASSIS CONTROL**
- ECU and sensors: steering control, airbag control, braking systems, ADAS systems...
- Steering, brakes, airbag, embedded cameras, rearview mirrors, windshield wiper...

**ASSETS**

**Protocols:**
- CAN, LIN/SAE J2602, RF...
- OBD II, Ethernet...
- CAN, FlexRay, RF...
- MOST, Bluetooth, Wifi...

**Services:**
- Entertainment (audio/video)
- Driving services: traffic information, maps...
- Additional services (fleet management, chronotachygraph, geofencing...)
- 3G, Wifi...
- eCall services
- V2V, V2I communication...

**Keyless/passive entry...**

Security for Connected Car
ENISA – Cyber Security and Resilience of Smart Cars

**DAMAGE / LOSS (IT ASSETS)**
- Loss of information in the cloud
- Loss of (integrity of) sensitive information
- Damage caused by a third party
  - Loss from DRM conflicts
  - Information leakage

**FAILURES / MALFUNCTIONS**
- Failures / malfunctions of devices or systems
- Failures or disruptions of the power supply
  - Software bugs
- Failures / malfunctions of parts of devices
- Failures or disruptions of communication links
- Failures or disruptions of main supply

**UNINTENTIONAL DAMAGES (ACCIDENTAL)**
- Information leakage or sharing
- Erroneous use or administration of devices and systems
  - Using Information from an unreliable source
- Unintentional change of data in an information system
- Inadequate design and planning or lack of adaption

**PHYSICAL THREATS**
- Fault injection / glitching
- Side channel
- Access to HW debug ports

**NEFARIOUS ACTIVITY / ABUSE**
- Denial of service
- Malicious code / software activity
- Manipulation of hardware & software
- Manipulation of information
- Unauthorised access to information system / network
- Compromising confidential information
- Identity fraud
- Abuse of information leakage
- Unauthorized use of administration of devices & systems
- Unauthorized use of software
- Unauthorized installation of software
- Abuse of authorizations
- Malicious software
- Remote activity (execution)

**NETWORK OUTAGE**

**ADVANCED PERSISTENT THREATS**

**EAVESDROPPING / INTERCEPTION / HIJACKING**
- Interception of information
- Replay of messages
- Interfering radiations
- Man in the middle / session hijacking
- Network reconnaissance and information gathering
- Repudiation of actions

**LEGEND:**
- Threats perceived as significant by ≥80% answers
- Threats perceived as significant by ≥60% answers
UN Task Force on Cyber security and OTA issues (CS/OTA)

Browse the child pages below for more information on "UN Task Force on Cyber security and OTA issues" meetings documents.

10 하위 페이지

- CS/OTA 1st session
- CS/OTA 2nd session - review ToR
- CS/OTA 3rd session
- CS/OTA ad hoc "Threats"
- CS/OTA 4th session
- CS/OTA ad hoc "Threats 2"
- CS/OTA 5th session
- CS/OTA 6th session
- CS/OTA 7th session
- CS/OTA 8th session

https://wiki.unece.org/pages/viewpage.action?pageId=40829521
Threats for Autonomous Driving

Traffic Management System

Road Side Equipment

Environment

SW Delivery/Update

Non-Critical System

Critical System

Service Cloud

User Device

Security for Connected Car
Adaptive Security Architecture (Gartner)

Source: Gartner (February 2014)
Inputs into the Adaptive Protection Architecture

- Reputation Feeds (IP, URL, ...)
- FS-ISAC, US-CERT
- Signature, Rule, Pattern
- Internal Guideline, External Influences
- Proactively Testing
- Context-awareness

Next-generation security protection platforms

Continuous monitoring

Embedded analytics

IoT Security
Adaptive Security Architecture - Lifecycle

**Predict**
- Proactive Exposure Analysis
- Predict Attacks
- Baseline Systems
- RemEDIATE/Make Change
- Design/Model Change

**Prevent**
- Harden and Isolate Systems
- Divert Attackers
- Prevent Incidents
- Detect Incidents
- Confirm and Prioritize Risk

**Detect**
- Investigate/Forensics
- Contain Incidents

**Respond**
- Post-incident (minutes ~ months)

**In-line, real time** (sub-second)
- Adjusting security strategies/policies/controls
- Anticipating future attacks and targets
- New systems/applications
- Changes are implemented/pushed/orchestrated
- Changes to policies or controls

**Near real time** (seconds ~ minutes)
- Whitelisting, Data Encryption, Patch Mgmt., Sandboxing
- Wasting hacker’s time (Honeypot, …)
- Signature/Behavioral Signature + “Threat Intelligence”
- Detecting Indicators of Compromise (IOC)
- Pervasive Monitoring, Behavior Analytics, Change Monitoring
- Isolating the compromised system/network, account, process, …

**Continuous Monitoring and Analytics**
- Deterring and detecting Indicators of Compromise (IOC)
- Pervasive Monitoring, Behavior Analytics, Change Monitoring
- Isolating the compromised system/network, account, process, …
Adaptive Security & Autonomous Car

Context-Aware Intelligence
- Model, Simulate, Act, Protect
- Knowledge
- Analyze
- Information
- Collect, Correlate
- Big Data
- Logs, Events, Costs, Usage, Attacks, Breaches

Source: Gartner (February 2014)

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

Security for Connected Car
Cybersecurity Concept for Connected Car

- **S1. Secure External Communication**
  - Crypto library
  - Secure boot & Remote Attestation
  - Secure Update
  - HW trust anchor (HTA)

- **S2. Secure Gateway**
  - Controls traffic flow
  - Detects malicious traffic
  - Data Security & Privacy

- **S3. Secure Internal Communication**
  - Authentication, Confidentiality & Integrity of Messages
  - Key Management

- **S4. Secure Platform**
  - Secure communication to anything

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person (Owner, Driver, Pedestrian), etc.
S1. Secure External Communication

Telematics on Cloud

Certificate Authority (of Manufacturer)

Certificate Authority (of Government)

Cross Certification

Network: 3GPP (4G/5G)
Transport: IEEE 1609.3
Security: IEEE 1609.2

Network: IEEE 802.11p
Transport: IEEE 1609.3
Security: IEEE 1609.2

Certificate

Certificate
S1. Secure External Communication – TelCo & Manufacturer

Authentication based on Certificate

Service Connection

Internet (closed)

Authentication via USIM

3GPP (4G/5G)

Manufacturer

Authentication Management

User

Device Info.

Enrollment

Certificate

Service Ctrl.

TelCo

Authentication Management

Device Info.

Subscription Info.

Connection Ctrl.
S1. Secure External Communication - Ecosystem and Security Infrastructure

Security Infrastructure

- Key Management
- Authentication Management
- Privilege Management

Service Provider
S/W Provider

Virtual Connection

Cloud + Big Data

Internet of Things
S2. Secure Gateway

Security Mechanisms for Embedded Automotive Systems

Security Mechanisms allocated in Example Architecture
S2. Secure Gateway – Detects malicious traffic
S2. Secure Gateway – Controls traffic flow
S2. Secure Gateway – Data Security & Privacy

![Diagram of secure gateway and data security measures in a connected car system](image-url)
S3. Secure Internal Communication

Security Infrastructure

External Network

Key Management Policy

KMS : Key Management System

Secure Communication

External NIC

External Firewall

Secure Storage

KMS

Internal Firewall

External Gateway

Head Unit

TMS

ADAS

AVN

V2X

Internal Gateway

Powertrain DC

Body DC

Chassis DC

ECU

Key Management
S3. Secure Internal Communication - Key Management

Key Hierarchy Structure

1. Root KMS
2. Sub-KMS
3. In-Vehicle KMS

Security Policy

Key Distribution (registration)

Secure Communication (encryption)

ECU

In-Vehicle BUS

KMS : Key Management System

Security Server (Key Management)
S4. Secure Platform - Secure Boot & Remote Attestation

TPM: Trusted Platform Module
S4. Secure Platform - Secure Flash/Update

1. Certificate for code signing

2. Code Signing

3. {Data} + {Code Sign}

4. Certificate Verification

5. Sign Verification & SW Updating

Service Server (update server)

Security Server (Certificate Authority)
## Security Primitives for Usecases

<table>
<thead>
<tr>
<th>Usecase</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A1. Secure Diagnostics</strong></td>
<td>Authentication (GW)</td>
<td>Access Control (GW)</td>
<td>Intrusion Detection (GW)</td>
<td></td>
</tr>
<tr>
<td><strong>A2. Integrity of Head Unit</strong></td>
<td>Authentication (GW) Secure Comm. (GW)</td>
<td></td>
<td></td>
<td>Secure Update (HU) Secure Boot (HU)</td>
</tr>
<tr>
<td><strong>B2. Secure Tethering</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B3. Secure Playback</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C1. Secure ITS</strong></td>
<td>Authentication (GW)</td>
<td>Access Control (GW) Flow Control (GW)</td>
<td>Intrusion Detection (GW)</td>
<td></td>
</tr>
<tr>
<td><strong>C2. Secure Service Delivery</strong></td>
<td>Authentication (GW)</td>
<td>Download Manager (GW) Access Control (GW)</td>
<td>Flow Control (GW) Intrusion Detection (GW)</td>
<td>Contents Integrity (ECU)</td>
</tr>
<tr>
<td><strong>C5. Secure On-Board Comm.</strong></td>
<td>Authentication (GW)</td>
<td></td>
<td></td>
<td>Key Management (GW) Security Policy (GW)</td>
</tr>
</tbody>
</table>
Top 4 Security Primitives

- Telematics
- Bluetooth
- Wi-Fi
- ITS
- SD/USB
- OBD
- PLC
- Head Unit (AVN/IVI)
- Internal Gateway
- External Gateway
- ADAS
- Chassis Control
- Body Control
- Powertrain Control

External Network → DMZ → In-Vehicle Network

- Unauthenticated traffic
- Malicious traffic
- Unprivileged traffic
- Undesignated traffic

Authentication, Intrusion Detection, Access Control, Flow Control

Authenticated, Reliable, Authorized & Designated traffic
Adoption of the Top 4 Primitives

- Transportation Infra
- Car (Crash Avoidance)
- Cloud (OEM)
- Car (Cooperative Driving)

Managed by government:
- Standardized Security
- Standardized Network
- Standardized Channel

Managed by OEM:
- Proprietary Security
- Proprietary Network
- Standardized Channel

Adoption Consideration:
- Architecture: AUTOSAR (JasPar)
- Implementation: MISRA-C/C++
- Process: ISO26262, SAE J3061 (JSAE)

In-Vehicle Appliance (Gateway)
Management of Cybersecurity

Security Infrastructure

- SW Delivery (Update) Server
- Authentication Server (Key Management)

Cloud (OEM)

Security Control

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

Security Agent
Experiences about Connected Car

- 2012. Security for Patrol Car
- 2013. V2X over WAVE
- 2014. Telematics Security
- 2015. AutoCrypt® Launch
- 2016. C-ITS Testbed
- 2017. vPKI for C-ITS, Autonomous Driving
AutoCrypt® Overview

Enforcing a new age of **security** within the connected car to ensure **safety** of the occupant. **AutoCrypt** offers the following products to cover different vulnerabilities existing for the connected car.

- **AutoCrypt V2X**: Vehicle-to-Anything
- **AutoCrypt PKI**: Public Key Infrastructure
- **AutoCrypt KMS**: Key Management System
- **AutoCrypt AFW**: Advanced Firewall
AutoCrypt® Major Features

1. Vehicle Public Key Infrastructure
2. Secure Communication
3. Control Traffic Flows
4. Prevent Malicious Access
5. Key Management
6. Privacy Preserving

Route data privacy
Vehicles use a AutoCrypt V2X module and AutoCrypt PKI to securely communicate based on a secure distributed certificate system. The “anything” can include infrastructure, devices, other vehicles.

- Allows for secure encrypted communication between the vehicle and RSUs (Road Side Unit), as well between the road and signal systems.
- AutoCrypt V2X is based off of IEEE1609.2* which makes it in compliance with CAMP VSC** & SCMS***.

* IEEE1609.2: Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
** CAMP VSC: Crash Avoidance Metrics Partnership - Vehicle Safety Communications
*** Security Credential Management System

Road Side Unit

① Distribute Certificate  
② V2V Secure Communication
③ Distribute Certificate

AutoCrypt® PKI

① Distribute Certificate
② V2N Secure Communication

V2I Secure Communication

Road Side Unit
AutoCrypt® PKI

- **CA : Certificate Authority**
  - Generates PKI certificates necessary for V2X authentication

- **MA : Misbehavior Authority**
  - Monitors for certificate abuse or stolen certificates

- **RA(Registration Authority)**
  - Issues PKI certificates necessary

- **LA(Linkage Authority)**
  - Provides a anonymous ID for Pseudonym Certificates
  - Prevents exposure of driver privacy, e.g. location, etc.
AutoCrypt® KMS

Encryption key and certificate cycle management

- Manages the entire in-vehicle encryption key life cycle process including generation and revocation
- Stores and manages keys from the moment issued from the security server
- The external KMS (Security Server) and the in-vehicle KMS continuously sync for constant security.

Road Side Unit

Security Server (Key Management)

In-Vehicle KMS

AutoCrypt® KMS

① Store distributed certificate
② Store key for vehicle internal network's encrypted communications
③ Connect with external KMS
④ Security Policy Synchronization

Security for Connected Car
AutoCrypt® KMS

AUTOSAR Support (Tentative Launch: March 2017)

- Key Management Interface for the Communication Services aspect of AUTOSAR BSW (Basic Software)
  - Key management regarding specifically the SECOC (Secure Onboard Communication) section of Communication Services

AUTOSAR Layered Software Architecture (www.autosar.org)
AutoCrypt® AFW (1/3)

AFW (Advanced Firewall) is an intelligent firewall that also features IDS/IPS capabilities. (1/2)

- Design Concept is based upon a Positive Security Model in which the user defines what is allowed and blocks all other traffic and access.

- The detection engine is based upon patented technology which does not rely on regular signature updates and utilizes a unique logic-based analysis to detect attacks.

- Detection support for protocols running at the Application Layer (L7) such as HTTP.
AFW (Advanced Firewall) is an intelligent firewall that also features IDS/IPS capabilities. (2/2)

- **Network Firewall & IDS/IPS**
  - Controls flow of traffic for both external and internal networks
  - Blacklisting to detect and block unauthorized access
  - Detects unusual behavior in traffic within internal network

* Because the CAN protocol can differ from manufacturer to manufacturer, a certain degree of customization is required.
**AutoCrypt® AFW (3/3)**

**AUTOSAR Support (Tentative Launch: March 2017)**

- AutoCrypt AFW module will conform to the AUTOSAR Basic Software framework
  - Offer individual AFW for CAN use (CAN AFW) as well Ethernet use (ETH AFW)
  - CAN AFWs will be customized to match the manufacturer’s CAN protocols
AutoCrypt

20 year Anniversary

Asian Cyber Security Vendor of the Year

Thank you

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