Cyber Security Study for Automotive Ethernet in Japan Automotive Industry

JASPAR Next Generation High-Speed Network WG
Architecture Team Leader
Mikio KATAOKA
Hitachi Automotive Systems, Ltd.

Architecture Team, Requirement Definition Sub-team Leader
Keisuke Terada
Yazaki Corporation.

7th IEEE-SA Ethernet & IP Automotive Technology Day, San Jose, CA, USA, Nov. 2017
1. About JASPAR
   - What’s JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG

2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN

3. Future Activities
   - Documentation
   - Conclusion
Agenda

1. About JASPAR
   - What’s JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG

2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN

3. Future Activities
   - Documentation
   - Conclusion
1-1. What is JASPAR?

JASPAR: Japan Automotive Software Platform and Architecture

JASPAR was established to pursue increasing development efficiency and ensuring reliability by standardization and common use of electronic control system and in-vehicle network which are advancing and complexing.

■ Mission

☑ Improvements in development productivity and significantly contribute to the advancement of the world’s technology through standardization activity.
☑ Establish of the fair basis for competition of the whole automobile industry.

■ Achievements

☑ Represent a collective voice of the Japanese companies at the international standardization bodies.
☑ Contribute to development of global standards.
### 1-2. JASPAR members List as of September, 2017

<table>
<thead>
<tr>
<th>OEM</th>
<th>Tier1</th>
<th>Soft/Tool</th>
<th>Semicon/Electronics</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>42</td>
<td>73</td>
<td>25</td>
<td>19B</td>
</tr>
</tbody>
</table>

#### Board member
- HONDA R&D
- Nissan
- TOYOTA
- DENSO

#### Regular member
- **ISUZU**
- Mazda
- SUBARU
- SUZUKI
- ADVICS
- AISIN AW
- AISEN SEIKI
- Akebono Brake
- Alpine
- ALS
- Autoliv
- Autoliv Nissan Brake
- Bosch
- Calsonic Kansei
- Clarion
- Continental Automotive
- FUJITSU TEN
- Furukawa Electric
- Hitachi AMS
- JATCO
- JTKT
- Keihin
- Mitsubishi Electric
- Nidec Elesys
- NIPPON SEIKI
- NSK
- Panasonic
- PIONEER
- Ricoh
- SHOWA
- Sumitomo Electric
- TOKAI RIKA
- Toyoda Gosei
- TOYOTA INDUSTRIES
- YAZAKI
- ADC
- APRESIA
- APTJ
- ATS
- AUBASS
- Cadence
- CATS
- Change Vision
- eSOL
- ETAS
- FFRI
- FTL
- FUJI SOFT
- FUJITSU
- FUJITSU BSC
- Hitachi ICS
- IBM Japan
- KPI
- Mentor Graphics
- miceware
- NEC
- Nihon Synopsys
- OMRON
- OTSL
- SCSK
- STABILITY
- Sunny Giken
- Toshiba Information Systems
- TOYO
- Trend Micro
- Vector Japan
- WITZ
- Harman International
- HRS
- Infineon
- MegaChips
- Microchip
- MJKK
- Murata
- NXP Semiconductors
- Renesas
- TDK
- TOSHIBA
- Tyco Electronics
- DNP
- DTRS
- KDDI
- SECOM
- TOPPAN
- TOYOTA CRDL

#### Associate member
- DAIHATSU
- Hino
- HYUNDAI
- Mitsubishi Motor
- UD Trucks
- Delphi Automotive Systems
- Fujikura
- KYB
- Magna International
- MITSUBA
- NGK SPARK PLUG
- Toyodenso
- TRANSTRON
- Valeo Japan
- Yamaha Motor
- A&D
- A&W Technology
- ACCEL JAPAN
- AIC
- AISIN COMCRUISE
- ANRITSU
- Argus Cyber
- Security
- AXE
- AZAPA
- BITS
- Brison
- Canon IT	S
- Digital Contents
- DIT
- dSPACE
- Eager
- Eiwa
- Elektrobit
- GAJO
- HI CORP
- Hitachi High-Tech
- Ixia
- LAC
- Mamezou
- MITO SOFT
- NEC Solution Innovators
- Netagent
- NTT DATA MSE
- NTT DATA SBC
- PCI Solutions
- Systena
- Takasaki Kyodo
- Tata Consultancy
- Trillium
- TTChic
- Ubiquitous
- USE
- Wind River
- Xilinx
- Yokogawa
- ADI
- ARM
- Cypress Innovates
- HI-LEX
- Hitachi ULSI
- Hosiden
- NTN
- ROHM
- Sanden Automotive
- Components
- SanDisk
- Shindengen
- Thine
- YOKOWO
- Allion Japan
- Biz3
- HAGIWARA
- Kyoei Sangyo
- MACNICA
- NTT DOCOMO
- OEC
- RENESAS
- EASTON
- Ryoden
- Ryoisan
- SANSAN
- Shinko Shoji

---

**Japan Automotive Software Platform and Architecture**

---
1-3. JASPAR Organization (as of September 2017)

Organizations:
- Executive Board
- Auditor
- Administrator
- Board Members
- Steering Committee

Working Groups:
- Functional Safety
- Intellectual Property
- AUTOSAR Standardization
- In-vehicle LAN
- Bluetooth Conformance
- Mobile Device Interface
- Next Generation High-Speed NETwork
- Dynamic Vehicle Information Sharing
- Cyber Security Promotion
- Cyber Security Technical
- OTA Technical

Legend:
- : In action
- : Out of Action
Define in-vehicle requirements for the next-generation high-speed network technology.

Study certification/authentication mechanisms to ensure conformance and interoperability, as required.

Keep close cooperation with associated domestic/international organizations and companies to accomplish stated goals.
Agenda

1. About JASPAR
   - What’s JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG

2. Status of Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Result
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN

3. Future Activities
   - Documentation
   - Conclusion
Hacker trends

Hacking level for cars has increased year by year

FCA recall 1.4 million units

(Target)
Uconnect implemented car.
<Attack>
Control the display, steering and transmission.
(Accidents caused by a remote attack has not occurred.)

(Target)
FCA Jeep
<Attack>
Send the maintenance command from the diagnosis connector. Impersonated a regular ECU and control the steering.

’16
Control the car using maintenance mode (When driving)

’15
Hacking from remote (At low speed)

’13
Hacking in the car

Hacking in the car

Hacking from remote

(Hacking from remote)

Hacking in the car

(FCA recall 1.4 million units)

(Target)
Uconnect implemented car.
<Attack>
Control the display, steering and transmission.
(Accidents caused by a remote attack has not occurred.)

(Target)
FCA Jeep
<Attack>
Send the maintenance command from the diagnosis connector. Impersonated a regular ECU and control the steering.

’16
Control the car using maintenance mode (When driving)

’15
Hacking from remote (At low speed)

’13
Hacking in the car

(Hacking in the car)
2-1-2. In-vehicle Ethernet Security

- There are the important issues that we discuss the security measures against cyber attacks.

Also in the Next Generation High-Speed Network WG, the in-vehicle Ethernet security has been studied from 2015.
2-2-1. JASPAR’s Presumed Security Configuration

- The gateway separates outside and inside of vehicle as a attack surface and filters illegal data for intrusion prevention.
- Data communicated with outside of vehicle should be encrypted.
- Message authentication code is adapted for communication data of in-vehicle.

**Diagram:**
- Data encryption (TLS)
- Access Control List
- Communication monitoring
- Mutual authentication
- VLAN filtering
- Spoofing countermeasure
- Server authentication
- Mutual authentication
- Access Control List
- Communication monitoring
- Mutual authentication
- VLAN filtering

**Nodes:**
- Server
- Tool
- IVI/NAVI
- TCU
- OBD (DoIP)
- Gateway
- FW 1
- FW 2
- FW 3
- ECU (Switch)
- End-node
- DMZ
- FW: Firewall
- TCU: Telematics Control Unit

**Description:**
- The gateway separates outside and inside of vehicle as an attack surface and filters illegal data for intrusion prevention.
- Data communicated with outside of vehicle should be encrypted.
- Message authentication code is adapted for communication data of in-vehicle.
Enumerate the security technologies related the Ethernet.

<table>
<thead>
<tr>
<th>Category</th>
<th>L2</th>
<th>L3</th>
<th>L4 or above</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Port based VLAN</td>
<td>Tagged VLAN</td>
<td>Private VLAN</td>
<td>Input Port</td>
</tr>
<tr>
<td></td>
<td>Sub network based VLAN</td>
<td></td>
<td></td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td>MAC filtering</td>
<td>Port security</td>
<td>IEEE802.1X</td>
<td>Mac Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC Authentication bypass</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static MAC Table</td>
<td>Dynamic ARP Inspection</td>
<td>IP Source Guard</td>
<td>MAC Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IP filtering</td>
<td>ARP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VLAN ACL</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAT(Network Address Translation)</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAPT(Network Address Port Translation)</td>
<td>IP Address + PortNo.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DDoS Open Threat Signaling (dots)</td>
<td>Traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OCSP (Online Certificate Status Protocol)</td>
<td>Certification</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td></td>
<td>DPI(IPS/IDS)</td>
<td>DPI : Deep Packet Inspection</td>
<td>payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPS: Intrusion Prevention System</td>
<td>IDS: Intrusion Detection System</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WAF(Web Application Firewall)</td>
<td>http/https</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAC(Message Authentication Code)</td>
<td></td>
<td>Payload</td>
<td></td>
</tr>
<tr>
<td>Cipher</td>
<td>MACsec</td>
<td>IPSec</td>
<td>IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DTLS</td>
<td>UDP/IP</td>
<td>TCP/IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSL/TLS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Kerberos Authentication</td>
<td>RADIUS</td>
<td>ID/PASSWORD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Remote Authentication Dial In User Service)</td>
<td>RADIUS (Remote Authentication Dial In User Service)</td>
<td>Identification Information (ID/PASSWORD, Certification)</td>
<td></td>
</tr>
</tbody>
</table>
### 2-2-3. Priority Consideration Items

- Priority consideration items are selected for in-vehicle Ethernet network.
  - Decided by the interests of participating companies.
- The following 3 items are selected.
  - VLAN, Filtering, SSL/TLS.

<table>
<thead>
<tr>
<th>Category</th>
<th>Discussion items</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>• Usage of the VLAN as the network configuration.</td>
</tr>
<tr>
<td></td>
<td>• Routing using the VLAN. (consider domains)</td>
</tr>
<tr>
<td>Filtering</td>
<td>• Scope of filter application as the in-vehicle systems.</td>
</tr>
<tr>
<td></td>
<td>• Performance of the automotive microcomputer / switch.</td>
</tr>
<tr>
<td>Message authentication</td>
<td>• This category is discussed by other WG in JASPAR. So, exclude from discuss point in this WG.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>• Investigate the specification and the compatibility with the in-vehicle systems.</td>
</tr>
<tr>
<td></td>
<td>• Performance applied to automotive microcomputer.</td>
</tr>
<tr>
<td>DPI</td>
<td>• Investigate the technologies. (what kind of attack can be detected)</td>
</tr>
<tr>
<td>MACSec, IPSec</td>
<td>• Feasibility based on required processing capacity</td>
</tr>
<tr>
<td></td>
<td>Performance in software / hardware.</td>
</tr>
</tbody>
</table>

VLAN: Virtual LAN  SSL: Secure Socket Layer  TLS: Transport Layer Security  
DPI: Deep Packet Inspection
We discussed the implementation points of filtering. As a result, we presume the following points as implementation points.

By matching between the filtering function set for each point and the received packet, it is selected whether the packet is passed or discarded.
Select the security technologies as a prerequisite to discuss the filtering function.

Scope: Standardized or discussing technologies created by IEEE, IETF, etc.

<table>
<thead>
<tr>
<th>Security technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based VLAN</td>
</tr>
<tr>
<td>Tagged VLAN</td>
</tr>
<tr>
<td>Private VLAN</td>
</tr>
<tr>
<td>Sub network based VLAN</td>
</tr>
<tr>
<td>MAC filtering, Port security, IEEE802.1X, MAC authentication bypass</td>
</tr>
<tr>
<td>Static MAC Table</td>
</tr>
<tr>
<td>Dynamic ARP Inspection</td>
</tr>
<tr>
<td>IP Source Guard</td>
</tr>
<tr>
<td>IP filtering</td>
</tr>
<tr>
<td>VLAN ACL</td>
</tr>
<tr>
<td>NAT (Network Address Translation)</td>
</tr>
<tr>
<td>NAPT (Network Address Port Translation)</td>
</tr>
<tr>
<td>DDoS Open Threat Signaling (dots)</td>
</tr>
<tr>
<td>OCSP (Online Certificate Status Protocol)</td>
</tr>
</tbody>
</table>
2-3-3. Filtering Fields and Applied to In-vehicle Network

- Enumerate filtering items for each OSI layers.
- Implementation function.
- Applied to in-vehicle network.
- With or without hardware support.

Enumerated filtering items

<table>
<thead>
<tr>
<th>OSI layers</th>
<th>Filtering items</th>
<th>Overview</th>
<th>Security technologies</th>
<th>Applied to in-vehicle network</th>
<th>Hardware supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2</td>
<td>VLAN number</td>
<td>VLAN number</td>
<td>Port-based VLAN</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td>VID[ VLAN Identifier]</td>
<td>VID[ VLAN identifier]</td>
<td>Private VLAN</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>Source MAC address</td>
<td>Source MAC address</td>
<td>MAC filtering, Port security, MAC authentication bypass</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Static MAC Table</td>
<td></td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dynamic ARP Inspection</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>ID, password, Digital certificate</td>
<td>ID, password, Digital certificate</td>
<td>IEEE802.1X</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>L3</td>
<td>Protocol number</td>
<td>Type of network protocol</td>
<td>IP filtering</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in the transport layer</td>
<td>VLAN ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source IP address</td>
<td>Source IP address</td>
<td>Sub network based VLAN</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dynamic ARP Inspection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IP filtering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VLAN ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAT(Network Address Translation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAPT(Network Address Port Translation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L4</td>
<td>Destination IP address</td>
<td>Destination IP address</td>
<td>IP filtering</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VLAN ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAT(Network Address Translation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAPT(Network Address Port Translation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L4</td>
<td>Source port number</td>
<td>Source port number</td>
<td>IP filtering</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VLAN ACL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NAT(Network Address Port Translation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/F</td>
<td>Destination port number</td>
<td>Destination port number</td>
<td>Same as above</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>Source port number</td>
<td>Physical port</td>
<td>Private VLAN</td>
<td>O</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Same as above</td>
<td>O</td>
<td>×</td>
</tr>
</tbody>
</table>
We discussed the implementation point of TLS. As a result, we presume the following points as implementation points.

Since there is a possibility that the internal ECU may become the end point of TLS, the implementation point of TLS is the entire network including gateway, ECU, and end node.
2-4-2. TLS Function and Technologies Related TLS

Discuss the TLS function and technology elements.

Technology overview and recommendation.

Enumerated technology elements

<table>
<thead>
<tr>
<th>Technology</th>
<th>Overview</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRF</td>
<td>Pseudo-random number generator to generate session keys</td>
<td>○</td>
</tr>
<tr>
<td>PRNG</td>
<td>Pseudo-random number generator</td>
<td>○</td>
</tr>
<tr>
<td>TRNG</td>
<td>True random number generator</td>
<td>△</td>
</tr>
<tr>
<td>RC4</td>
<td>Stream cipher</td>
<td>×</td>
</tr>
<tr>
<td>AES-CBC</td>
<td>Block cipher</td>
<td>○</td>
</tr>
<tr>
<td>AES-GCM</td>
<td>Authenticated encryption block cipher</td>
<td>○</td>
</tr>
<tr>
<td>ChaCha20-Poly1305</td>
<td>Authenticated encryption stream cipher</td>
<td>△</td>
</tr>
<tr>
<td>Self-signed certificate, server</td>
<td>Certificate whose signature has been generated by server itself</td>
<td>△</td>
</tr>
<tr>
<td>Self-signed certificate, client</td>
<td>Certificate whose signature has been generated by client itself</td>
<td>×</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure for authenticating public keys and their owners</td>
<td>○</td>
</tr>
<tr>
<td>X.509</td>
<td>Standard format for certificates</td>
<td>○</td>
</tr>
<tr>
<td>SHA</td>
<td>Most commonly used hash standard</td>
<td>○</td>
</tr>
<tr>
<td>RSA</td>
<td>One of the public key cryptographic mechanism</td>
<td>○</td>
</tr>
<tr>
<td>DHE-RSA</td>
<td>Key exchange done with ephemeral Diffie-Hellman, authentication with RSA signatures</td>
<td>○</td>
</tr>
<tr>
<td>ECDHE-ECDSA</td>
<td>Key exchange done with ephemeral Elliptic Curve Diffie-Hellman, authentication with Elliptic Curve DSA signatures</td>
<td>○</td>
</tr>
<tr>
<td>ECDHE-RSA</td>
<td>Key exchange done with ephemeral Elliptic Curve Diffie-Hellman, authentication with RSA signatures</td>
<td>△</td>
</tr>
<tr>
<td>Server duplication</td>
<td>Multiple TLS servers are provided in order to handle a large number of clients</td>
<td>△</td>
</tr>
<tr>
<td>PSK</td>
<td>Session keys are exchanged using pre-shared symmetric keys</td>
<td>○</td>
</tr>
<tr>
<td>DHE-PSK</td>
<td>Key exchange done with ephemeral Diffie-Hellman, authentication with PSK symmetric keys</td>
<td>△</td>
</tr>
<tr>
<td>RSA-PSK</td>
<td>Key exchange done with PSK symmetric keys, authentication with RSA signatures</td>
<td>△</td>
</tr>
<tr>
<td>Session resumption</td>
<td>Previous TLS session data is reused across sessions</td>
<td>○</td>
</tr>
</tbody>
</table>
2-4-3. Threat Analysis of TLS Requirements

- Perform the threat analysis by the CIA.
- Consider Confidentiality / Integrity / Availability and related technical elements.

<table>
<thead>
<tr>
<th>CIA</th>
<th>TLS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Confidentiality of session keys</td>
</tr>
<tr>
<td></td>
<td>Confidentiality of messages</td>
</tr>
<tr>
<td></td>
<td>Transport keys</td>
</tr>
<tr>
<td></td>
<td>Session information</td>
</tr>
<tr>
<td>Integrity</td>
<td>Server authentication</td>
</tr>
<tr>
<td></td>
<td>Client authentication</td>
</tr>
<tr>
<td></td>
<td>Message authentication</td>
</tr>
<tr>
<td>Availability</td>
<td>Connection times (Server)</td>
</tr>
<tr>
<td></td>
<td>Throughput</td>
</tr>
<tr>
<td></td>
<td>Connection times (Client)</td>
</tr>
<tr>
<td></td>
<td>Certificate renewal</td>
</tr>
</tbody>
</table>

**Confidentiality**
- Confidentiality of session keys
- Confidentiality of messages
- Transport keys
- Session information

**Integrity**
- Server authentication
- Client authentication
- Message authentication

**Availability**
- Connection times (Server)
- Throughput
- Connection times (Client)
- Certificate renewal

**Confidentiality**
- Server random
- Client random

**Confidentiality of message**
- Bulk encryption
- Ephemeral ECDH (RFC4492)

**Confidentiality of transport key**
- AEAD Cipher
- CHACHA20-POLY1305

**Integrity**
- Server authentication
- Client authentication
- Message authentication

**Confidentiality of session information**
- (abbreviated handshake)

**Integrity**
- Server authentication
- Client authentication
- Message authentication

**Availability**
- Throughput
- Connection times (Server)
- Certificate renewal

**Certificate renewal**
- Same as client
- Server reinitializing

**Throughput**
- Handshake Time (Client)
- Handshake Time (Server)

**Confidentiality**
- Pseudo-Random Number Generator (PRNG)
- True Random Number Generator (TRNG)
- Pseudo-Random Number Generator (PRNG)
- True Random Number Generator (TRNG)

**Integrity**
- Self Signed Certification
- PKI
- x.509 extensions

**Validity**
- Cipher Suite
- Session resumption
- Block Cipher
- Stream Cipher
- AES-CBC
- RC4
- AES GCM

**Availability**
- Handshake Time (Server)
- Certificate Update
Discussion of VLAN configuration based on JASPAR network configuration. => Classified into two types.

- VLAN configurations by domain.
  Assign VLAN ID for each network domain.

- VLAN configurations by application.
  Assign VLAN ID for each application.

VLAN configurations by domain

VLAN configurations by application
In case of applying a firewall to VLAN configurations.

=> Configure the Firewall to forward packets only to the required ports.

1. Communication within VLAN: End-node 3 ⇔ End-node 2
Internal (between ECU1 and ECU2) allows filtering to pass.

2. Communication between VLANs:
   IVI/NAVI (VLAN 3) ⇔ End-node 1 (VLAN 1)
   It is preferable to filter by MAC address, IP address, port number at FW 1 and FW 3 of Gateway.

- White list method
  Check the VLAN ID and the L2, L3, L4 headers permitted for each input (physical) port, only transfer the permitted packets

Example of the firewall in case of VLAN configurations by domain

Example of the firewall in case of VLAN configurations by application

VLAN Application

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Application</th>
<th>Ports</th>
<th>ECU</th>
<th>VLAN Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>FW2 internal comm. (DoIP, before auth.)</td>
<td>0 μC (Gateway) H</td>
<td>x x x</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>FW2 internal comm. (DoIP, after auth.)</td>
<td>1 Tool</td>
<td>x x</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>FW1 internal comm. (SOME/IP)</td>
<td>2 TCU</td>
<td>x x</td>
<td></td>
</tr>
<tr>
<td>2x</td>
<td>FW1 external comm. (application 1)</td>
<td>3 IVI/NAVI</td>
<td>x x x</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>FW3 internal comm. (IP Video)</td>
<td>4 ECU1</td>
<td>x x x x</td>
<td></td>
</tr>
<tr>
<td>3x</td>
<td>FW external comm. (application 2)</td>
<td>5 ECU2</td>
<td>x x x x</td>
<td></td>
</tr>
</tbody>
</table>

VLAN ID 10: Port based VLAN
Others: Tagged VLAN
1. About JASPAR
   - What’s JASPAR
   - Next Generation High-Speed Network WG
   - Activities of WG
2. Status of the Study About In-vehicle Ethernet Security
   - In-vehicle Network Security
   - Study Results
     - JASPAR Supposed Configuration
     - Priority Consideration Items
     - Filtering
     - SSL/TLS
     - VLAN
3. Future Activities
   - Documentation
   - Conclusion
3-1. Documentation

- These results are described for JASPAR guidelines. (within 2017)
- JASPAR members can obtain these documents.
3-2. Future Activities

- We are discussing the security technology verification of in-vehicle. By comparing ICT (Information Communication Technology) security and in-vehicle security, clarifies different factors.

Configuration example in ICT

- Study of TSN requirements
  Started by investigating specifications, under consideration of application examples.
3-3. Conclusion

- Discuss the Ethernet security technologies applied to in-vehicle network.
- Enumerate the Ethernet security technologies.
- Select Filtering, SSL/TLS and VLAN for the priority consideration items.

<table>
<thead>
<tr>
<th>Filtering</th>
<th>Discussed items</th>
<th>Output</th>
</tr>
</thead>
</table>
| - Enumerate the filtering items.  
  L2 : VLAN ID, TPID, VID etc.  
  L3 : Protocol number, Control flag (SYN) etc.  
- Define the implementations of hardware or software. | - Define the requirements of the filtering items. | |
| SSL/TLS | - Discomposed the SSL/TLS technologies into functional elements.  
  Authentication method, Encryption,  
  Connection time and Throughput etc. | - TLS technologies guideline.  
- Clarify the use case, used technologies. | |
| VLAN | Define the network architecture with VLAN.  
- VLAN configurations by domain.  
  Network design (including multi-VLAN)  
- VLAN configurations by application.  
  Network design (DoIP, Image transmission,  
  Map data distribution etc.) | - VLAN design guideline.  
- VLAN design architecture and required technologies. | |
Thank you for your attention.