AUTOSAR as a driver for automotive security?

DENSO Automotive Deutschland
Corporate Research & Development

Robert SCHMIDT
r.schmidt@denso-auto.de

Martin PRISCHING
m.prishing@denso-auto.de

October 29th, 2015
Tokyo, Japan
Increasing complexity of ECUs
Diagnostics require guided fault search
Possibility to send signals to the vehicle
Increasing motivation to "test" your own car

Intended or unintended manipulation of the car
Steep increase of the risk in the automotive domain

- Likelihood of attack per car
- Risk
- Impact of attack
- Time

1990s 2005 2010 2015+

- Diagnostics in garage
- OBD2 adapters & apps
- OEM Connected Services
- Open in-vehicle platform
Part 1 – DENSO Global Concept for Defense in Depth Security

+ 

Part 2 – Regional Applications and Variants

Part 3 – Global efforts for globally appropriate security standards
Part 1 – Global Approach to Automotive Security

![Diagram showing a network of components and their connections]

- **Vehicle**: Components like DCM, BT, Wi-Fi, C2X, PLC WiFi, Multimedia (HU), ADAS (ACC, PCS), Powertrain (ENG, AT), Chassis (EPS, Brake), A/C, Door.

- **Gateway**: Connected Vehicles, Cloud, 3G/LTE/5G, Data Center, Smart Phone, EVSE, Diagnosis.

- **Infrastructure**: Ext. Comm., Gateway, Onboard Comm., ECU.

- **Example security services**: Layer I (IPsec/TLS, Other security service), Layer II (Filtering, Anomaly detect), Layer III (Message authentication, Other security service), Layer IV (Reprograming, Secure Storage).

*This information is the exclusive property of DENSO CORPORATION. Without their consent, it may not be reproduced or given to third parties.*
Part 2 – Regional Approach – Example: Reprogramming

Scenario

OEM server

End ECU

Application running

Change to re-programming

Erase flash

Re-programm (DL/decr/write)

Check integrity (CRC/MAC)

ECU reset

International: ISO/TC22/SC31

Diagnostics protocol

Regional: German consortium

Flash loader specification

Performance of reprogramming does not suffer from security

Minimum ECU downtime (total)

Time [sec]

Size of application [KiB]

30,86

512

60,47

1024

180,07

3072

36,35 sec

54,35 sec

56,59 sec

59,7 sec

w/o crypto

w/ crypto

0

20

40

60

Programm Session

Erase

DL/(Decr)/Write

CRC/MAC

DENSO INTERNATIONAL EUROPE

This information is the exclusive property of DENSO CORPORATION. Without their consent, it may not be reproduced or given to third parties.
Part 3 – DENSO's Coverage of Security Standards

DENSO contributes to Standardization Organization world

- Common Criteria
- ISO
- IEC
- IEEE
- Public Key, C2X security
- JasPar Security
- SAE Cyber Security Guidebook
- NIST Digital Signature Standard
- Protection Profiles, TRNG

- Generic software guidelines
- Generic methods
- Specific methods
- Automotive software guidelines
- Industry application-specific standards

DENSO engages in

- Basic software & interfaces
- Interoperable methodology
- Software architecture for ECUs

For DENSO, AUTOSAR specs for security are an essential building block

DENSO's Company standards

- Software implementation
- Company tools and know-how
- Production standards
History of Security in AUTOSAR

Urgent need for secure on-board communication
AUTOSAR & security experts gathered to define concept SecOC

Permanent need for various security topics
Further experts form new AUTOSAR workpackage WP-X-SEC

Tasks
- Continuation of security concepts
- New security concepts
- Reviews for other WPs

Members

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP-X SEC</td>
<td>25</td>
<td>54</td>
</tr>
<tr>
<td>WP-A</td>
<td>43</td>
<td>93</td>
</tr>
<tr>
<td>WP-A1</td>
<td>20</td>
<td>38</td>
</tr>
<tr>
<td>WP-M</td>
<td>44</td>
<td>78</td>
</tr>
</tbody>
</table>
Secure Onboard Communication – SecOC (AR4.2)

- Authenticity of PDUs by Message Authentication Code (MAC)
- Requires shared secret key between sender and receiver

Effective to detect
- ✔ Replay
- ✔ Spoofing
- ✔ Tampering
- ✗ Eavesdropping
- ✗ Denial of Service

Caveat - Key management & freshness aspects currently not covered by AUTOSAR.

Application to CAN
- ✔ NIST recommendation: Truncate MAC to minimum 64 bit
  → Larger payload available in CAN-FD

AUTOSAR standard software module is already available

WP-X-SEC
Security Glossary, SOTA case study,
Reference Security E/E Architecture

Subgroup: FoA Security
Security for Adaptive AUTOSAR

Subgroup: Key Management
Generation, identification, sharing, storage, invalidation of crypto keys

Concepts for AUTOSAR 4.3

- Security Policy Manager
  Set of rules about what is allowed or not allowed

- Crypto Interface
  Standard interface between CSM and security SW/HW, e.g. to handle multi-application access to crypto services
Open Issue: Key Management Systems (KMS)

WP-X-SEC
- FoA Security
- Key Management

**Standardization areas**
- Common key handling, key provisioning, key transport, key revocation
- IT interfaces to a common key and certificate management infrastructure
- Identification and meta information for key material
- Functionality of in-vehicle key management

**Continuous discussion on-going on weekly basis**

**Unification of key management needed to handle complexity**
Does AUTOSAR drive automotive security?

What is not covered by AUTOSAR

 Guantanamo
 Applications are not standardized, different security policies of applications
 Guantanamo
 ‘Zero-day' incidents have to be addressed immediately
 Guantanamo
 Security must be addressed by the whole organization

How automotive security is driven by AUTOSAR

 Guantanamo
 High reuse of widely discussed security concepts
 Guantanamo
 Filling gaps of standards in a diverse standardization world
 Guantanamo
 Complying to standards is a boost in confidence in the public

What else is needed beyond AUTOSAR?

 Guantanamo
 Common automotive key and certificate management
 Guantanamo
 EE architecture design, and implications to & from security
 Guantanamo
 Systematic risk analyses to identify assets to be protected and appropriate countermeasures

DENSO is committed to support global security standardization efforts!