Automotive Cybersecurity
Cybersecurity is defining the next level of quality for the automotive industry

The Automotive Market is currently shaped by four Megatrends. They are all linked to Automotive Cybersecurity

Automated driving
Electro-mobility
Connectivity

Automotive Cybersecurity
Infineon is your trusted advisor for a holistic automotive cybersecurity approach

The combined ATV and CSS divisions result in leading-edge products!

ATV

We have been making cars clean, safe and smart for more than 40 years

CSS

We have been delivering security and wireless communication for the connected world for more than 30 years
Every connection in the car is a potential point for an attacker…
Attack scenarios

...and, unfortunately, they seem to have unlimited creativity!

<table>
<thead>
<tr>
<th>Software</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic attacks</td>
<td>Invasive attacks</td>
</tr>
<tr>
<td>Protocol fuzzing, jamming, replay</td>
<td>FIB manipulation, microprobing</td>
</tr>
<tr>
<td>Side channel attacks</td>
<td>Fault injection</td>
</tr>
<tr>
<td>SPA, DPA, spectre, meltdown</td>
<td>Spiking, radiation, light attacks, clock manipulation, DFA</td>
</tr>
</tbody>
</table>

What countermeasures can be implemented?
Attack scenarios

...What countermeasures can be implemented?

Software

- Logic attacks
  - PKI, digital signatures, encryption, CMAC, blockchain, MISRA C-CERT coding guidelines

- Side channel attacks
  - Run-time invariant SW implementation, randomization in HW and SW, dual-rail HW implementation, encrypted computation

- Fault injection
  - Double computation, all safety HW measures

- Invasive attacks
  - Tamper protection, implanted ROM, full-custom design

Security always consists of a combination of hardware and software
But not everything is bad news. Security is the enabler for new business models.
We offer the most scalable automotive cybersecurity portfolio, meeting the right level of security.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>Pure software protection</td>
</tr>
<tr>
<td><strong>Trusted execution environment</strong></td>
<td>Separation of &quot;secure&quot; and &quot;normal&quot; world in one CPU</td>
</tr>
</tbody>
</table>
| **Integrated HSM** | Separated and protected run-time environment  
E.g. Infineon AURIX™ & TRAVEO II HSM |
| **Discrete security controller** | Hardware trust anchor + software + tamper resistance  
e.g. Infineon OPTIGA™ TPM & SLS37 V2X HSM |

*HSM = Hardware Security Module
Principles of cybersecurity

Different Layers of Security are required in future Car Architectures

- Secure platform
- Secure onboard communication
- Secure network separation
- Secure external communication
Infineon’s automotive security offering
A scalable portfolio for dedicated applications

Telematics / Connectivity (incl. V2X)

Central gateway

Powertrain*
Battery management

Safety / ADAS*
radar

Body / Chassis*
doors

Infotainment*
head-up display

GSM, 3G, 4G, LTE

Telematics / Connectivity (incl. V2X)

Central gateway

high-speed backbone bus

AURIX™ family
TRAVEO™ II family

Integrated HSM

SEMPE™ SECURE Flash

On board security across all domains
› HW Security Module (HSM or SHE) (AURIX™ TC2x & TC3x)
› Cyber Security Realtime Module & Satellites (AURIX™ TC4x)
› Full EVITA compliant (AURIX™ TC3x)
› Ethernet security features (AURIX™)
› Unique chip individual keys
› Security SW lib
› Safety Features against fault attacks (up to ASIL-D)
› Automotive qualified with zero ppm automotive quality

Hardware root-of-trust for Application processors
› ASPICE level 2 firmware
› Secured storage regions
› Hardware crypto engine
› Ephemeral session keys
› Mutual device authentication
› Automotive qualified
› ASIL-B compliant

Authentication, secured key store, on-chip key generation & management
› Tamper resistant hardware
› TPM2.0 SW compliant
› Initial keys and certificates
› Automotive qualified Hardware + Software certified acc. to Common Criteria

Discrete Hardware Security

Enabling cellular connectivity
› Tamper resistant hardware
› eSIM SW functionality
› Initial keys and certificates
› Automotive qualified
› Hardware certified acc. to Common Criteria

Copyright © Infineon Technologies AG 2020. All rights reserved.
A dependable communication in an interconnected system has security as an integral part

No Safety without security
› Security is a mandatory precondition for Safety
› Safety is the most important asset to be protected
› A dependable architecture is secure and safe

Security is a moving target
› Security erodes over time
› Always be ahead of the attacker’s capabilities
› Crypto-agility is a must – the right hardware is an enabler for this

Security is an architecture property
› A secure EE-architecture is always built around a certified root-of-trust
› Hardware/Software co-design is key for a strong protection scheme
› Appropriate security is required on all layers of the EE-architecture

Security needs cooperation
› Security by obscurity is not sustainable
› Security standards allow transparent risk management over the complete lifecycle
› Incident management processes across the whole supply chain have to be established
Infineon – Automotive CyberSecurity Leadership beyond Hardware

- Most scalable security product offering in automotive
- 30+ years experience in security
- Partnership program including software and tool vendors for security
- Hardware and software security expertise
- Security by Design
- Trusted Advisor in security - standardization
Part of your life. Part of tomorrow.
For more information click on the respective image below