Trusted Platform Modules –
Automotive applications and
differentiation from HSM

Cyber Security Symposium 2017, Stuttgart
Martin Brunner, Infineon Technologies
Axiom: Whatever is connected can (and will) be attacked

ATTACKER

Unwanted accesses denied

CAR2CLOUD

ONBOARD
Safety & security

Connected vehicles have as many as 100 million lines of code. If even one in 4,000 lines contains an error/vulnerability this results in 25,000 potential access points.
Challenges in software security – the complexity trap

"Complexity is the enemy of security. As systems get more complex, they get less secure"

Bruce Schneier

A system is only as secure as its weakest link

A Bug is hard to find (attackers have time, developers don't)

Only one entry point needed

Security by design = essential

Software (alone) can not protect software
Automotive security needs more ...

**Overall automotive security goals**

› Provide functional **safety**

› **Finance:** Protect business & IP

› **Operations:** Meet customers quality expectation

› Fulfil **privacy** & regulation requirements

---

**Secret keys** are the basic prerequisite of any secured vehicle function
Secret keys must be protected

Key integrity is essential for system security

› Compromised keys = no security

› Revocation of keys is expensive and takes time

› Key handling must be secured through the whole lifecycle

Hardware Trust Anchors

Provide protected execution environments & tamper resistance for high-security demands

› Key storage & related crypto operation

› Key management and deployment in insecure environment
<table>
<thead>
<tr>
<th>Benefits of hardware security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NO SECURITY</strong></td>
</tr>
<tr>
<td>Open for all to see</td>
</tr>
<tr>
<td><strong>SOFTWARE ONLY</strong></td>
</tr>
<tr>
<td>Secures against casual intrusion and basic software attacks</td>
</tr>
<tr>
<td><strong>HARDWARE SECURITY</strong></td>
</tr>
<tr>
<td>Secures against hardware attacks and hardens against software attacks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software code easily readable by attackers</td>
</tr>
<tr>
<td><strong>Copying</strong></td>
</tr>
<tr>
<td>Software code easily copied and shared by attackers</td>
</tr>
<tr>
<td><strong>Analyzing</strong></td>
</tr>
<tr>
<td>Software code easily analyzed and understood using standard tools</td>
</tr>
<tr>
<td><strong>Root of Trust</strong></td>
</tr>
<tr>
<td>Software has no &quot;Root of Trust&quot;, recovery of broken system practically impossible</td>
</tr>
</tbody>
</table>

| Hardware chip protects itself against code reading |
| Secured hardware cannot be easily copied. |
| Secured hardware use proprietary designs and non-standard code |
| Secured hardware provides "Root of Trust" anchor for system, providing detection, recoverability, secure updates |
How secure is "secure"?
Levels of protection

- **eSE**
  - Software + Hardware Trust Anchor + Certified Tamper Resistant

- **TEE**
  - Software + Hardware Extensions

- **Host**
  - Purely software protection

---

Using Secure Element for tamper-resistant Hardware Trust Anchor

TEE OS runs separate from the general Rich OS – but still using the same HW platform

Storage and processing is done within application running on host
Standard microchips can be attacked by various means:

- **Logical attack**
  e.g. protocol fuzzing

- **Manipulative attack**
  e.g. probing

- **Observative attack**
  e.g. power analysis

- **Semi-invasive attack**
  e.g. laser fault injection
Countermeasures overview
Opportunities and limits

**Logical Attacks** can be thwarted e.g. by using **consistency checks in software**. Often, these can be effectively utilized. Hardware features may support these countermeasures.

**Observative Attacks** can be thwarted e.g. by using **randomization in software**, combined with hardware features in order to build an effective and strong barrier.

**Semi-invasive Attacks** can be thwarted e.g. by **redundant soft- and hardware**, building an effective barrier. Hardware features are needed as an efficient foundation.

**Manipulative Attacks** can be thwarted e.g. by using cryptography in both soft- and hardware, allowing to gain high resistance. The **use of hardware features is absolutely essential**.
The Trusted Platform Module (TPM) is

- a security controller for cryptographic operations
- physically separated from the main processor
- protecting security critical data (e.g. keys, passwords)
- capable to resist logical and physical attacks
- security evaluated by a third-party (common criteria standard)
- a passive device

**TPM – Security Module**

- Generic functions
- Secured hardware
- Crypto functions

A TPM- The "safe for your platform"
<table>
<thead>
<tr>
<th>OPTIGA™ TPM security functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Authentication</strong></td>
</tr>
<tr>
<td>› One-way authentication</td>
</tr>
<tr>
<td>› Mutual authentication</td>
</tr>
<tr>
<td><strong>Secured Channel</strong></td>
</tr>
<tr>
<td>› Encrypted Communication</td>
</tr>
<tr>
<td>› Key Generation</td>
</tr>
<tr>
<td><strong>User Management</strong></td>
</tr>
<tr>
<td>› Password Protection</td>
</tr>
<tr>
<td>› User management and keys</td>
</tr>
<tr>
<td><strong>Secured Updates</strong></td>
</tr>
<tr>
<td>› Remote maintenance</td>
</tr>
<tr>
<td>› In-field flexibility and reaction</td>
</tr>
<tr>
<td><strong>System integrity</strong></td>
</tr>
<tr>
<td>› Secure Boot</td>
</tr>
<tr>
<td>› Remote platform verification</td>
</tr>
<tr>
<td><strong>Dedicated functions for</strong></td>
</tr>
<tr>
<td>› Platform manufacturer</td>
</tr>
<tr>
<td>› System operators</td>
</tr>
<tr>
<td>› Vendor/User/Enterprises</td>
</tr>
<tr>
<td><strong>Lifecycle Management</strong></td>
</tr>
<tr>
<td>› Key Backup and refurbishment</td>
</tr>
<tr>
<td>› Personalization and identities</td>
</tr>
<tr>
<td>› Supply chain tracking</td>
</tr>
<tr>
<td><strong>Secured Clock and Time</strong></td>
</tr>
<tr>
<td>› Reliable clock when offline</td>
</tr>
<tr>
<td>› Timer and Monotonic Counter</td>
</tr>
</tbody>
</table>
Hardware security module (HSM) and Trusted platform module (TPM) – overview

HSM – Integrated on MCU

› **Integrated security hardware** incl.
  – Protected key & program storage, internal firewall, debug protection, crypto accelerators (AES-128/ECC256/SHA-2), AIS31 compliant True Random Number Generator (TRNG) for key generation, 32 bit CPU...

› **High performance, real-time** capable
  – Full Automotive temperature range and quality (AEC Q-100 Grade 0+, DFR), AUTOSAR compliant

TPM – Discrete security hardware

› **EAL 4+** security certified hardware & software (tamper resistant)
› Ca. **100 standardized crypto functions**
› Supports multiple crypto schemes (incl. AES-256/ECC512/RSA2028)
› AEC-Q100 Grade 2 compatible
› AIS31 compliant (TRNG) for key generation
HSM and TPM
Comparison 1: security software

HSM – Integrated on MCU

- AURIX™ e.g. TC23x
- Eth
- CAN

Flash

TPM – Discrete Chip

- Host Processor e.g. Linux-Based MPU or AURIX™ MCU
- TCG Software Stack (TSS)

Flash

Software / Functionality

Implemented Software

- Crypt.- library SHE+

User programmable

- Crypt.- operations SHE+

Standardized

- Crypt.- Lib.
- Basic SW
- ca.100 funct.
- Host SW
- ECO Syst.

- Keygmt.
- Authorization
- FW Update
- Secured Time

Copyright © Infineon Technologies AG 2017. All rights reserved. Infineon Proprietary
HSM and TPM
Comparison 2: security protection

**HSM – Integrated on MCU**

- AURIX™ e.g. TC23x
- Flash
- HSM

**TPM – Discrete Chip**

- Host Processor e.g. Linux-Based MPU or AURIX™ MCU
- Basic SW
- Firmware
- SPI

### Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>HSM – Integrated on MCU</th>
<th>TPM – Discrete Chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret code &amp; data storage</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protection against read-out</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Encrypted memory, encrypted data bus</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Code execution</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Separated &amp; protected execution, internal firewall, debug protection</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Encrypted data execution, self checking dual-CPU</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Personalization</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unique chip identifier</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personalized and protected processes (in development, supply and ECU lifecycle)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Protection against hardware attacks</td>
<td>N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Maximized protection (e.g. shields, sensors etc.)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Security certification</td>
<td>N/A</td>
<td>✓</td>
</tr>
<tr>
<td>Common Criteria EAL4+ high certified (HW + SW)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
The importance of hardware trust anchors for automotive security

Integrated on MCU (HSM)
- Onboard security
- Protected com. & debug interfaces
- High-speed / real-time critical tasks

Discrete Security Controller
- Protected external communication
- Certified hardware security
- Protecting critical keys & certificates
Hardware trust anchors supporting a granular security architecture

**Protect External Interfaces**
Network and OEM backend authentication; OBD interface protection

**Gateway Protection & Domain Isolation**
Firewall, intrusion detection/prevention system (IDS/IPS), domain isolation, SOTA, on-board key generation & management

**Secure Onboard Communication**
Message authentication, distributed intrusion detection (IDS)

**Secured Data Processing**
Secured boot, run time integrity, SOTA updates, component protection, immobilizer
Example: feature activation
Use case – simplified overview

Setup of new parameters
› Loading of encrypted Enhanced Parameters
› Update TPM key usage authorization to enable new enhanced parameters

Usage of new parameters
› Request access to key
› Key access is granted
› Enhanced Parameters are decrypted and applied
Discrete hardware based security offers unique benefits even beyond strong security

**Discrete hardware-based security** offer strong tamper resistance. Certified hardware-based solutions create trust based on independent evaluations.

**Time to market** and **Scalability** across various platforms for different types of applications.

Hardware based security offers strong performance advantages compared to software-based solutions for securely storing and calculating.

**Enabling the production** in insecure (non-trusted third-party) environments. **Secured tracking** of the value chain.

**Reduced total cost of ownership of security** based on reduced investment in secured manufacturing infrastructure & security knowhow.
Part of your life. Part of tomorrow.