Automotive Security

Due to the increased networking of automotive Electronic Control Units (ECU) - each involving increasingly complex software - and the fact that ECUs carry out more and more sensitive tasks, the attack surface and the resulting financial loss caused by a successful attack on an ECU will grow significantly in the near future. In order to harden ECUs against attacks, security mechanisms preventing unauthorized access to sensitive data or successful manipulation of the ECU software must be used.

Automotive Hardware Security Modules

For security at ECU level, pure security solutions in software cannot sufficiently protect the integrity of an embedded automotive system. Therefore, a Hardware Security Module (HSM) is a necessary prerequisite to harden embedded systems. HSMs are optional on-chip extensions to any given microcontroller intended to support the protection of secret keys, to increase data throughput of cryptographic functionality and to reduce security-related CPU load on the main cores.

Bosch HSM Specification Workshop

However, classical secure elements (Smartcards, TPM, security IC) do not satisfy specific automotive requirements, e.g. availability of debug/test interfaces, automotive qualification requirements and resilience against attacks on communication interfaces. This motivated Bosch to specify a dedicated automotive-qualified HSM.

ESCRYPT has extensive experience in implementing HSMs and supporting HSM specification through a long history of industrial and research projects. Thus, our highly-experienced technical HSM experts will enable any chip manufacturer during an effective two-day workshop to

- Understand the main implementation requirements and challenges
- Estimate the cost-benefit relationship of the implementation
General information & Benefits

- Effective two-day workshop at ESCRYPT location in Germany (Bochum, Stuttgart, Munich, Wolfsburg, Berlin)
- Comprehensive training material as hand out
- 6 hours Q&A time available for a 4-week period after the training
- Catering included

Training Schedule & Content

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Day 1</th>
<th>Day 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session A</td>
<td>Introduction to Automotive HSMs and the</td>
<td>SHE / SHE+ integration and compatibility</td>
</tr>
<tr>
<td>(2 h)</td>
<td>Bosch HSM</td>
<td></td>
</tr>
<tr>
<td>Session B</td>
<td>The Bosch HSM in detail (part I)</td>
<td>System integration aspects</td>
</tr>
<tr>
<td>(2 h)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session C</td>
<td>The Bosch HSM in detail (part II)</td>
<td>Safety aspects</td>
</tr>
<tr>
<td>(2 h)</td>
<td></td>
<td>Application SW integration</td>
</tr>
<tr>
<td>Recap</td>
<td>Summary and Q&amp;A</td>
<td>Summary and Q&amp;A</td>
</tr>
<tr>
<td>(1 h)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Introduction to Automotive HSMs / Bosch HSM-OS

- Use cases for automotive HSMs, scenarios for secure elements in automotive
- Journey through the „HSM world“: SHE, EVITA light/medium/full, SHE+, Bosch HSM
- Example of future HSM-supported EEA
- Trends and users of HSMs
- Introduction to Bosch HSM
  - Idea and history
  - High-level architecture and main security functions
  - Exemplary use cases (e.g. Secure Boot, Secure Flash, Runtime Tuning Detection)

Bosch HSM in detail – Part I & II

- Integration into the microcontroller
  - HSM enabling/disabling
  - System bus connection
  - Secure flash (code vs. data)
  - Internal Structure
    - Main components
      - Secure core
      - Memory protection unit (MPU)
      - System timer
      - Secure local RAM
    - Interfaces
      - Interrupt interface module
      - Debug interface module
    - Cryptographic modules
      - AES hardware module
      - HSM device keys for AES
      - True random number generator (TRNG)
      - Pseudo random number generator (PRNG)

- System Environment and main functions
  - Unique chip identifier
  - (Secure) system boot mechanism
    - Main core boot
    - HSM boot
- Debug Interface Protection
  - Test Interface Protection
- Deep-dive: Cryptographic modules & protocols
  - Implementation pitfalls: What can go wrong with “bad” cryptography?
  - Advanced Encryption Standard (AES)
    - General design principle
    - Modes of operation (e.g. ECB, CBC, CTR, OFB, CFB, GCM, XTS)
    - Standardization
  - Random Number Generators
    - TRNG vs. PRNG
    - Design principles
    - Standardization and output validation (e.g. statistical test suites)
  - Challenge-response protocol for authorized debug/test access

SHE/SHE+ integration

- Introduction SHE/SHE+
- Differences between SHE/SHE+ and the Bosch HSM
- SHE/SHE+ emulation on the Bosch HSM

System integration aspects

- Implementation requirements and challenges
- Example use cases: Specific aspects and challenges regarding
  - Secure Boot
  - Secure Storage
  - Host and HSM reprogramming

Safety aspects

- Overview: General HW safety mechanisms (lockstep, ECC memory)
- Deployment of HSM in safety-critical environments
  - Pitfalls and challenges
  - Side-effects
  - Freedom from Interference

Application SW integration

- AUTOSAR integration (e.g. CSM, CRY)
- Outlook: The CycurHSM software stack

For further information please contact
christian.schleiffer@escrypt.com
+49 (0) 89 208039 - 132
alexander.meurer@escrypt.com
+49 (0) 234 43870 - 249