HARDWARE SECURITY MODULE
For automotive applications

Presented by Pieter Willems
Pieter.willems@silexinsight.com
December 2019
What we do: **IP provider for security and video in embedded systems**

- Headquarters in Brussels, Belgium
- Global presence
- Worldwide customer base
- Founded in 1991 – 28 years experience
- Silex Insight = Silicon experts with know-how
- 45 employees
Choose single or a complete module
We build for your specific needs

Security enclave
eSecure ROT provides full system security

Networking solutions
Accelerate your complete TLS, MACsec and IPsec traffic

Memory protection
Secure your flash and DDR

Crypto accelerators & processors
Accelerate your crypto operations

CONFIGURABLE
Include features as needed

SCALABLE
Define performance and footprint depending on your requirement

CUSTOMIZABLE
Adapt to your specific needs
Introduction

The connected car

- Ever-increasing number of connected cars
- Many applications
  - Infotainment
  - ADAS
  - V2X gateway
  - Power systems
  - Comfort/safety systems
- Gartner identifies “trusted cars/hardware” as part of the Top 3 autonomous driving technologies
GONE IN 3 MINUTES: KEYLESS BMWS A BOON TO HACKER THIEVES

New vulnerability lets attackers hijack Chrysler vehicles remotely

Hackers were able to remotely control a moving Tesla Model S

Car hacking remains a very real threat as autos become ever more loaded with tech
Securing a connected car and its sub-modules is all about trust

- Trust Firmware running on your module?
- Identity of modules and other connected cars?
- Secure communication channel?
  - Privacy
  - Authenticity
  - Integrity
Securing your device

Product lifetime

- What is the lifetime of your car/module?
  - Consumer electronics – few years
  - Industrial, automotive, infrastructure – up to 10s of years

- How to handle ownership changes

- Software is susceptible to bugs and must be updated over the product lifecycle
  - Firmware updates in the field required
  - How will these updates be performed securely?
A **hardware security module (HSM)** safeguards and manages digital keys for strong authentication and provides crypto processing.
- Security Enclave/Root-of-trust
- Firewall between application and secure module
- Flexible and scalable solution using any processor
- eSecure contains a flexible crypto off-loading block

- Wide range of cryptographic algorithms available
  - Asymmetric: RSA/ECC/ECDSA/Curve25519/EdDSA/SRP/J-PAKE ..
  - Symmetric: AES/SHA/ChaCha20-Poly1305/ARIA…
  - TRNG + DRBG (NIST 800-90A/B/C)

- Algorithms specific to the Chinese market also available
  - Asymmetric: SM2/SM9
  - Symmetric: SM3/SM4

- Post-quantum cryptography (PQC) algorithms also available
A hardware security module (HSM) safeguards and manages digital keys for strong authentication and provides crypto processing.
HSM FOR AUTOMOTIVE
For Xilinx Zynq UltraScale+ MPSoC

- Software stack available
- Scalable (Tradeoff features, area, performance)
- Configurable (All common algorithms supported)
Boot process

Firmware initialization
(clear RAM, move data to RAM, initialize stack)

Hardware modules
configuration & initialization
(e.g. setup watchdog)

Hardware crypto modules
self-tests
(e.g. AES self-test)

Main loop
(handling of host commands)

< 0.1ms
HSM Driver
- For non-AUTOSAR applications
- Bare-metal support only

AUTOSAR CryptoDriver
- AUTOSAR R4.3.1 compliant
- Wrapper around HSM driver

Software stack

- AUTOSAR CryptoDriver
  - Running on Cortex-(R5)
  - Stored in flash
  - Run from system memory

- HSM Driver
  - For non-AUTOSAR applications
  - Bare-metal support only

- HSM firmware
  - Running on μBlaze
  - Stored in & run from HSM ROM
  - Data & stack in HSM RAM

3 October 2019
Secure storage
Encrypted and signed in external memory

**Option 1 – Based on key from PUF**
- Storage Root Key (SRK) generated by the PUF
  - Unique per device
  - Requires PUF (ordering code)
  - Requires Hardware Root of Trust boot (no RMA)
  - Can use only AES-GCM in CSU

**Option 2 – Based on key from eFUSEs**
- Storage Root Key (SRK) generated from eFUSE seed
  - Could be unique per device
  - Requires seed initialization
  - Requires 128 user eFUSEs (limited resource)
  - Can use AES-GCM in the CSU or PL
HSM

- Configuration of CSU tamper responses
- CSU tamper status reading and clearing
- CSU tamper trigger

CSU tamper sources
- CSU register
- MIO pin
- JTAG toggle
- PL SEU
- Temperature alarm
- Voltage alarm

CSU tamper responses
- Interrupt (custom response by host)
- System reset
- Secure lockdown
- BBRAM erase
Since the HSM is security critical, all detected errors are considered tampers.

**HSM tamper sources**
- Watchdog timeout
- RAM CRC error
- RAM unauthorized access
- Hardfault
- Software assertion
- Command authorization error
- Periodic integrity check error
- Self-test error
- TRNG health test error

**HSM tamper responses**
- Level 1: interrupt
- Level 4: above and wait for reset (halt CPU)
- Level 5: above and trigger CSU tamper response

**Anti-tampering**
HSM contains its own anti-tampering module
Ensuring the secure boundary of the HSM

- Xilinx Peripheral Protection Unit to provide HSM exclusive access to
  - CSU
  - CSU DMA
  - eFUSEs

**Boot mode**
- CSU functions directly available
- eFUSEs directly available
- XPPU not configured

**HSM mode**
- CSU functions partly available through HSM only
- eFUSEs available through HSM only
- XPPU configured and locked

- Xilinx Isolation Design Flow ([XAPP1335](#)) in PL can provide extra robustness
Frequently Asked Questions

- **What is the resource usage?**

- **Can I remove or add functionality to the HSM IP?**
  - Yes. Generic statements allow removing or adding functionality, depending on the required features and footprint. A robust library of cryptographic IPs is available for integration.

- **What are the deliverables?**
  - Netlist or RTL
  - Reference design
  - Firmware binary
  - Driver source code
  - Self-checking testbench
  - Documentation

- **What is the business model?**
  - Silex has a conventional IP licensing model, with license fee, royalties and annual support. NRE and design services are also available through Silex.

---

<table>
<thead>
<tr>
<th>Device</th>
<th>LUT</th>
<th>FF</th>
<th>DSP</th>
<th>BRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZU11EG</td>
<td>6%</td>
<td>3%</td>
<td>0.2%</td>
<td>6%</td>
</tr>
<tr>
<td>ZU7EV</td>
<td>8%</td>
<td>4%</td>
<td>0.4%</td>
<td>11%</td>
</tr>
<tr>
<td>ZU5EV</td>
<td>16%</td>
<td>8%</td>
<td>0.6%</td>
<td>25%</td>
</tr>
<tr>
<td>ZU4EV</td>
<td>22%</td>
<td>11%</td>
<td>1.0%</td>
<td>28%</td>
</tr>
<tr>
<td>ZU3EG</td>
<td>27%</td>
<td>14%</td>
<td>1.9%</td>
<td>17%</td>
</tr>
<tr>
<td>ZU2EG</td>
<td>41%</td>
<td>20%</td>
<td>2.9%</td>
<td>24%</td>
</tr>
</tbody>
</table>

*All ZU+ devices are supported*
Silex Insight HSM IP addresses security needs across multiple markets
- Cryptographic offloading
- Secure key management
- Secure key storage
- Flexible and scalable

Smart integration to Zynq UltraScale+ MPSoC enables adding security to a complex design

Further investments on features and functional safety planned