Trusted Platform Module (TPM) on Zynq

Javier González:
- javierg@xilinx.com
- jgon@itu.dk

October 28, 2014
Run-Time Security Mechanisms for Zynq-based Designs

1. New Component
2. Existing Components

You are here

TPM??

Processors

Programmable Logic

Peripherals & Memory

Memory

Hypervisor
ARM TrustZone
Microkernel RTOS
MMU
Certified RTOS
Secure Boot

Xilinx PS7 AXI Interconnect
ARM TrustZone
MMU
SecMon 3.0
Secure Boot

Xilinx PS7 AXI Interconnect
ARM TrustZone
MMU

ZIMED
On Chip Memory & BRAM

Isolation
Monitoring
Certification
Cryptography
Secure Boot
What this talk is NOT about

- Getting into TPM details and specification
- Reporting on the difference between TPM 1.2 and 2.0
- Analyzing the security properties of TPM
- Discussing TPM use cases
What this talk is IS about

Agenda

➤ What is TPM in a nutshell.
➤ What are the HW and SW requirements to build a TPM?
➤ What does it mean to be TPM conforming?
  – All according to TCG specification (v 1.2 & v 2.0)
➤ TPM on Zynq:
  – What is it needed to attach an external TPM to Zynq?
    • Supported interfaces and secure world access (TrustZone).
    • Commercial alternatives.
    • Risks
  – What does it take to build a TPM using Zynq components?
What this talk is IS about

Agenda

- What is TPM in a nutshell.
- What are the HW and SW requirements to build a TPM?
- What does it mean to be TPM conforming?
  - All according to TCG specification (v 1.2 & v 2.0)
- TPM on Zynq:
  - What is it needed to attach an external TPM to Zynq?
    - Supported interfaces and secure world access (TrustZone).
    - Commercial alternatives.
    - Risks
  - What does it take to build a TPM using Zynq components?
What is TPM?

TPM is a specification...
What is TPM?

“… TPM is only a generator storage device and protector of symmetric keys...” – TPM 1.2 specification (Design Principles)

A secure cryptoprocessor that stores state, keys, passwords, and digital certificates
  – TPM can evaluate the state of a system through its Platform Configuration Registers (PCRs)

Sealing: Map keys to an specific PCR state (configuration measurements)

Tamper-resistant functionality, state, and operations
  – Protect data at rest: keys in secure storage + encryption
    – Tamper-resistance != Tamper-proof

Typically affixed to the target device (e.g., PC, SoC) – tamper evidence
What is TPM?

Untrusted Area

Communication Bus

Trusted Area

Gate Keeper

I/O

Crypto Engine

Random Number Generator

PCR Registers (≥ 16 registers)

Non-Volatile Memory (≥ 1280 bytes)

Volatile Memory

Execution Engine

...
What is TPM?
Run-Time security paradigms

- Separate Computation
- Enforced Usage Policies
Sensitive data never leaves the trusted area, which is accessed through narrow library-like interfaces.
What this talk is IS about

Agenda

- What is TPM in a nutshell.
- What are the HW and SW requirements to build a TPM?
- What does it mean to be TPM conforming?
  - All according to TCG specification (v 1.2 & v 2.0)
- TPM on Zynq:
  - What is it needed to attach an external TPM to Zynq?
    - Supported interfaces and secure world access (TrustZone).
    - Commercial alternatives.
    - Risks
  - What does it take to build a TPM using Zynq components?
TPM Requirements (TPM 1.2)

Hardware

- I/O component attached to the main system bus
  - Manage the information flow to the TPM – access control

- Separate execution environment for “secure” computation

- Secure volatile storage for shielded locations
  - Shielded location: An area where data is protected against interference from the outside exposure

- “Secure” non-volatile storage – r/w NVRAM!! *
  - “…20 bytes mandatory of NVRAM in v1.2… platform specific specification can require a larger amount of NVRAM…” (Version 1.2 FINAL – Revision 116, March 1, 2011)
  - “A conformant TPM for the PC Client SHALL provide a minimum of 1280 bytes of NV Storage.” (Version 1.2. FINAL – Revision 1.00, July 11, 2005)
    - [http://www.trustedcomputinggroup.org/files/resource_files/87BCE22B-1D09-3519-ADEBA772FBF02CBD/TCG_PCClientTPMSpecification_1-20_1-00_FINAL.pdf](http://www.trustedcomputinggroup.org/files/resource_files/87BCE22B-1D09-3519-ADEBA772FBF02CBD/TCG_PCClientTPMSpecification_1-20_1-00_FINAL.pdf)
SOFT TPM
“Secure” is a loose term
- Secure NVRAM can be interpreted differently
  - Tamper-resistant storage unit + clear text
  - Protected key + encryption + “normal” NVRAM
  - Isolated NVRAM with exclusive access (e.g., TrustZone) + clear text
  - ...

Not all soft implementations are the same
- Zynq does provide authenticated soft components (secure boot)

Conclusion: Be clear about your (client’s) requirements
- Tamper resistance level and attack model are the key requirements
TPM Requirements (TPM 1.2)

Software

- **Cryptographic engine**
  - RSA, SHA-1, HMAC
  - Key sizes of 512, 1024, 2048 bits
  - P1363 format for signature output
  - OAEP encoding
  - Signatures performed using the scheme RSASSA-PKCS1-v1.5

- **Key generator**
  - Asymmetric key pair

- **Random Number Generator (RNG)**
  - TPM does not require a HW RNG but…
  - … RNG output for internal TPM use **must** be held in a **shielded** location
TPM Requirements (TPM 1.2)

Software

- **Platform Configuration Registers (PCR)**
  - Allow to *bind* crypto operations to a specific *state*
  - At least 160-bit storage location for integrity measurements
  - No need for NVRAM

- **Data Integrity Register (DIR)**
  - At least 160-bit values that must be held in *shielded locations*
  - Space for DIR **must** be reserved in the *NV storage area*

- **State Register**
  - TPM state store in the *NV storage area*

- **... a long list of other musts**
  - Which **must** be implemented to be TPM conforming!
TPM 2.0 – Why you might want to upgrade?

➤ Algorithm flexibility
  – Support for more algorithms
  – Staying away from specific algorithms:
    • (e.g., SHA1)
      ▪ NIST SP800-131A (Government Requirements):
        » Generation: deprecated 2011–2013, disallowed after 2013)
        » Verification: Legacy-use after 2010
        **TPM 1.2 not acceptable in current products…**
      ▪ Microsoft not accepting SHA1 certificates after 2016
      ▪ Google penalizing sites using SHA1 certificates that expire during 2016

➤ Other differences (not backwards compatible):
http://www.trustedcomputinggroup.org/resources/tpm_main_specification
What this talk is IS about

Agenda

- What is TPM in a nutshell.
- What are the HW and SW requirements to build a TPM?
- What does it mean to be TPM conforming?
  - All according to TCG specification (v 1.2 & v 2.0)

TPM on Zynq:

- What is it needed to attach an external TPM to Zynq?
  - Supported interfaces and secure world access (TrustZone).
  - Commercial alternatives.
  - Risks
- What does it take to build a TPM using Zynq components?
Attach a TPM to Zynq

Commercial examples

Can I buy a TPM and just plug it in?
Yes! Just showing some examples...

- STMicroelectronics ST19NP18-TPM-I2C (I2C)
- ATMET FIPFS 140-2 TPM (SPI, LPC, and I2C)
- Infineon SLB 9645 X-Family (I2C and LPC)
- Nuvoton NPCT-Family (I2C and LPC)
- ...

http://tinyurl.com/xswg2014-video
Attach a TPM to Zynq
Hardware Interfaces

LPC: Low Pin Count

- Used to connect “legacy” I/O devices
- Available during the early system bootstrap (before any other device is initialized)
- Normally ad-hoc connections – fabricant independent
  - E.g., ASUS TPM-Infineon: LPC 20-pin (19 pins + 1 blanked). Attachable to motherboards implementing this header.
  - Adapter can be built using LPC’s FMC in Zynq.
Attach a TPM to Zynq

Hardware Interfaces

SPI: Serial Peripheral Interface

- 4-wire serial communication interface
- Very low power
- No throughput limitation (no max. clock speed)
- Arbitrary choice of message size, content, and purpose
- Established protocol, but no standard - variants

I2C: Inter-Integrated Circuit

- 2-wire serial communication protocol
- It is a standard protocol
- Speed (max. throughput) up to 3.4 Mbps
- Support for multiple devices on the same bus by design
- Ensures that data is received by the slave device
Attach a TPM to Zynq

Supported Interfaces in Zynq

* Image courtesy of *The Zynq Book*
Attach a TPM to Zynq
Supported Interfaces in Zynq

http://www.wiki.xilinx.com/SPI+Zynq+driver
Attach a TPM to Zynq

Supported Interfaces in Zynq

http://www.wiki.xilinx.com/Linux+I2C+Driver
Attach a TPM to Zynq

Supported Interfaces in Zynq

Interfaces also supported from within TrustZone!

### Register Summary

<table>
<thead>
<tr>
<th>Register Name</th>
<th>Address</th>
<th>Width</th>
<th>Type</th>
<th>Reset Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>security2_sdio0</td>
<td>0xE0200008</td>
<td>1</td>
<td>WO</td>
<td>0x00000000</td>
<td>SDIO0 slave security setting.</td>
</tr>
<tr>
<td>security3_sdio1</td>
<td>0xE020000C</td>
<td>1</td>
<td>WO</td>
<td>0x00000000</td>
<td>SDIO1 slave security setting.</td>
</tr>
<tr>
<td>security4_qspi</td>
<td>0xE0200010</td>
<td>1</td>
<td>WO</td>
<td>0x00000000</td>
<td>QSPI slave security setting.</td>
</tr>
<tr>
<td>security6_apb_slaves</td>
<td>0xE0200018</td>
<td>15</td>
<td>WO</td>
<td>0x00000000</td>
<td>APB slave security setting.</td>
</tr>
<tr>
<td>security7_smc</td>
<td>0xE020001C</td>
<td>1</td>
<td>WO</td>
<td>0x00000000</td>
<td>SMC slave security setting.</td>
</tr>
<tr>
<td>DMAC_RST_CTRL</td>
<td>0xF800020C</td>
<td>32</td>
<td>RW</td>
<td>0x00000000</td>
<td>DMA Controller SW Reset Control</td>
</tr>
<tr>
<td>TZ_OCM_RAM0</td>
<td>0xF8000400</td>
<td>32</td>
<td>RW</td>
<td>0x00000000</td>
<td>OCM RAM TrustZone Config 0</td>
</tr>
<tr>
<td>TZ_OCM_RAM1</td>
<td>0xF8000404</td>
<td>32</td>
<td>RW</td>
<td>0x00000000</td>
<td>OCM RAM TrustZone Config 1</td>
</tr>
<tr>
<td>TZ_OCM</td>
<td>0xF8000408</td>
<td>32</td>
<td>RW</td>
<td>0x00000000</td>
<td>OCM RAM TrustZone Config</td>
</tr>
<tr>
<td>TZ_DDR_RAM</td>
<td>0xF8000430</td>
<td>32</td>
<td>RW</td>
<td>0x00000000</td>
<td>DDR RAM TrustZone Config</td>
</tr>
</tbody>
</table>

Attach a TPM to Zynq

Comments

- Attaching an external TPM to Zynq is an easy way to adding TPM functionality to an existing design
  - TPM + software update
- Available external TPMS are *normally* compliant with the TPM specification, and there do count on a NVRAM module.
  - They are as secure as they are as a component

- However...

...It is important to understand the risks of an external TPM
- Pins are exposed: force, monitor, snoop traffic, etc.
- HW removal/substitution is simpler – lower level of tamper evidence
Attach a TPM to Zynq

Risks

*Images taken from Johannes Winter’s presentation at Europki’11
https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=59565

http://link.springer.com/chapter/10.1007%2F978-3-642-29804-2_12
What this talk is IS about

Agenda

- What is TPM in a nutshell.
- What are the HW and SW requirements to build a TPM?
- What does it mean to be TPM conforming?
  - All according to TCG specification (v 1.2 & v 2.0)

TPM on Zynq:

- What is it needed to attach an external TPM to Zynq?
  - Supported interfaces and secure world access (TrustZone).
  - Commercial alternatives.
  - Risks

- What does it take to build a TPM using Zynq components?
Build a TPM using Zynq components

Recap

- Read/Write NVRAM
- Volatile storage
- Separate processor (TPM’s execution environment)
- RNG
- Gate keeper (for system bus): I/O component
Build a TPM using Zynq components

“Secure” Read / Write NVRAM: Session Key + Encrypted NVRAM

- Primary Key (master key):
  - Deliver session key in bitstream
    - This solution is not DPA resistant
  - Generate the key at run-time (e.g., using RNG)
    - Store it in registers (preferred)
    - Store it in On Chip Memory (OCM) – multiple keys
      - Up to 256KB

- Encrypted NVRAM
  - Flash memory used for “normal” secondary storage
  - Encryption algorithm of choice (DPA resistant or not)

Conclusion: Encrypted container in “normal” NVRAM acting as “secure” NVRAM for TPM exclusive use
Build a TPM using Zynq components

Design

- "Secure" volatile storage
  - MMU isolation
  - TrustZone secure memory
- TPM separate processor
  - Soft processor in Programmable Logic (PL)
    - Microblaze
- Random Generator Number
  - Microblaze in PL too
  - Pure software implementation
- I/O Component
  - Implemented in TrustZone's secure world
    - Adding a level of indirection
  - Part of the TPM separate processor
TPM on Zynq
Conclusions

» External TPM

– Pros:
  • Easy to add TPM functionality to existing Zynq design
  • Possibility to choose different fabricants
    ▪ Based on requirements, support, implemented components, etc.
  • Zynq fully supports I2C and SPI *out-of-the-box*.
    ▪ Also available from TrustZone’s secure world
  • LPC also supported, but ad-hoc pin layout is needed.

– Cons:
  • Generic solution: might be difficult to map requirements to functionality
  • Tamper-resistance is weakened
    ▪ Physical attacks to external pins
  • Tamper-evidence also weakened
    ▪ Easier to remove/replace TPM unit
  • TPM 1.2 and 2.0 conforming
    ▪ 2 TPMs?; Either, or?
TPM on Zynq

Conclusions

Soft TPM built with Zynq

Pros:
- Ad-hoc solution: perfectly map requirements
- No need for adding an external component
- Possible only because of Zynq’s runtime security mechanisms
  - Secure boot + certification + crypto + monitoring + isolation
- TrustZone’s secure world allows to add an extra level of indirection
  - Secure specific components
  - Secure all components
- Possible to support TPM 1.2 and 2.0 simultaneously

Cons:
- Engineering effort
  - Extra overhead when moving to TPM 2.0
- Lower portability
- It is a Soft TPM: Might not be viable depending on the requirements
  - Soft features, but authenticated ones!
Trusted Platform Module (TPM) on Zynq

Javier González:
- javierg@xilinx.com
- jgon@itu.dk

October 28, 2014