Designing Security & Trust into Connected Devices

Eric Wang
Sr. Technical Marketing Manager

Tech Symposia China 2015
November 2015
Agenda

- Introduction
- Security Foundations on ARM® Cortex®-M
- Security Foundations on Cortex-A
- Use cases
- Certification
- Summary
ARM TrustZone Technology – A Security Foundation

Today

Authentication  Mobile Payment  Content Protection  Enterprise Security

System Security
IoT Security Enables New Business Opportunities

- If you can trust devices and the little data you can transform industries
- Electricity meter example – if you can trust a remote meter reading on a consumer meter…
  - No need to send someone to the house
  - Billing costs are reduced

- Home security example – if you can trust a connected security system …
  - You will be more likely to purchase and enable remote monitoring
Security is a Balance

**HW Attacks**
- Physical access to device – JTAG, Bus, IO Pins,
- Well resourced and funded
- Time, money & equipment.

**Software Attacks**
- Buffer overflows
- Interrupts
- Malware

**Communication Attacks**
- Man In The Middle
- Weak RNG
- Code vulnerabilities

---

**Cost/Effort To Attack**

**Level 1**

**Level 2**

**Level 3**

---

**Cost/Effort to Secure**

---
ARM Builds Layers of Hardware Security - Hierarchy of Trust

Secure Domain
- Security Subsystem or SE
  - Isolated & small security boundary

Trusted Domain
- Trusted code and data
  - with TrustZone® & Trusted Software

Protected Domain
- Hypervisor, Virtual Machines

Rich Domain
- Rich OS and user applications
How Do We Build the Internet of Trustworthy Things?

- Make end to end security easier by providing right sized secure foundations that scale for different use cases and market needs

- Make it easier
  - Build security in or enable easy integration of subsystems
  - Trusted software that is free and easy to use

- Make it right sized
  - Security for any ARM platform
  - Provide multiple solutions

- Keep it agile
Security Foundations for Cortex-M

- Software – ARM mbed™ OS, mbed uVisor, mbed TLS & 3rd party ecosystem

- TrustZone for ARMv8-M
  - New microcontroller architecture gains TrustZone

- TrustZone CryptoCell-310
  - Adds a configurable security system close to the root of trust suitable for microcontrollers
ARM mbed Device Platform for Microcontrollers

Productivity  Security  Connectivity  Management  Efficiency
TrustZone for ARMv8-M

TrustZone for ARMv8-A

Applications Processors

TrustZone for ARMv8-M

ARMv8-M Microcontroller
# ARM TrustZone Architecture Extensions

<table>
<thead>
<tr>
<th>Feature/Architecture</th>
<th>TrustZone for ARMv7-A &amp; ARMv8-A</th>
<th>TrustZone for ARMv8-M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Security States</td>
<td>SEL0* – Trusted Apps&lt;br&gt;SEL1 – Trusted OS&lt;br&gt;EL3 – Trusted Boot &amp; Firmware (ARMv8-A)</td>
<td>Secure Thread – Trusted code/data&lt;br&gt;Secure Handler – Trusted device drivers, RTOS, Library managers…</td>
</tr>
<tr>
<td>Secure Interrupts</td>
<td>Yes</td>
<td>Yes (Fast)</td>
</tr>
<tr>
<td>State Transition (Boundary crossing)</td>
<td>Software transition</td>
<td>Hardware transition (Fast)</td>
</tr>
<tr>
<td>Memory Management</td>
<td>Virtual Memory MMU with secure attributes</td>
<td>Secure Attribution Unit (SAU) &amp; MPU memory partitions</td>
</tr>
<tr>
<td>System Interconnect Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Code, Data and Memory?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trusted Boot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Software</td>
<td>ARM Trusted Firmware (+ 3rd party TEEs)</td>
<td>Keil CMSIS, ARM mbed OS, mbed uVisor + 3rd party software</td>
</tr>
</tbody>
</table>

*Secure Exception Level
TrustZone for ARMv8-M Use Cases

Protection from attack
- Protect assets from scalable software attacks
- Compartmentalization
- Least Privilege
- Protect assets from “shack” hardware attacks

Preventing code theft
- Protect valuable firmware assets
- IP protection

Safety critical system / system liability / multi party
- Sandbox certified software
- Secure peripherals and drivers
ARM TrustZone CryptoCell

- Family of security subsystems applicable to any ARM platform
- CryptoCell-700 series for Cortex-A & CryptoCell-300 series for Cortex-M –“right size”
- Enhances usability e.g. time for DTLS handshake & door lock to open
- Acts as Root of Trust / Trust Anchor for the system
- Compatible with TrustZone architecture extensions on CPU
- Robust security solution suitable for most use cases
- Simplifies security implementations
AMBA 5 AHB5: Extending Security to the System

Extends security foundation to the SoC

Efficient security control across all of the SoC

Optimized for embedded SoCs

Security state extends across Cortex-A and Cortex-M systems
AMBA 5 AHB5: Extending Security to the System

Extends security foundation to the SoC

Efficient security control across all of the SoC

Optimized for embedded SoCs

Security state extends across Cortex-A and Cortex-M systems

- CPU
- Flash
- SRAM
- Non-Trusted Peripheral A
- TrustZone CryptoCell-310
- DMA

Trusted region
Non-trusted region
Secure Foundations for Services

**Communication**
- mbed TLS

**Software / OS**
- mbed OS, mbed uVisor

**Hardware/System**
- TrustZone, CryptoCell (Root of Trust), System IP, AMBA 5
Security Foundations for Cortex-A

- Software – ARM Trusted Firmware & 3rd party TEE ecosystem
  - Security certification for TEE via GlobalPlatform

- TrustZone for ARMv8-A & ARMv7-A
  - Established architecture protecting billions of devices and services
  - TrustZone Media Protection architecture

- TrustZone CryptoCell-710
  - Configurable security subsystem adds a deep layer of hardware based security easily integrated into SoC
TrustZone Based Trusted Execution Environment

- Hardware root of trust
  - A basis for system integrity
- Integrity through Trusted Boot
- Secure peripheral access
  - Screen, keypad, fingerprint sensor etc.
- Secure application execution
- Technology called TrustZone
- Trust established outwards
  - With normal world apps
  - With internet/cloud apps
ARM Trusted Firmware for ARMv8-A
Authenticated Trusted Boot & Runtime

- Reference implementation:
  - Authenticated Trusted Boot
  - Runtime Firmware

- Provides basis for integrity

- Provides foundation for Trusted Board Boot
  - Open Source at GitHub
    - BSD License

+ Reference implementation:
  - Authenticated Trusted Boot
  - Runtime Firmware

- Provides basis for integrity

- Provides foundation for Trusted Board Boot
  - Open Source at GitHub
    - BSD License

Key:

- BL3 Non-Trusted Firmware (e.g. U-Boot, EDK2)
- BL3 Secure-EL1 Payload
- BL2 Trusted Boot Firmware
- BL1 AP Boot ROM
- BL31 EL3 Runtime Firmware
- SMCCC
- PSCI
- World Switch Library
- S-EL1 Payload Dispatch
- Trusted Board Boot
- Trusted OS Kernel

Loading

1st level Boot Loader (BL1) loads 2nd level image

2nd level Boot Loader (BL2) loads all 3rd level images

Application Processor (AP)

Normal World

Trusted World
Cortex-A: Putting it All Together

- **Normal World OS EL1/EL2**
- **Trusted OS Secure-EL1**
- **Trusted App Secure-EL0**
- **App EL0**

**Interface between Trusted Firmware and SoC/platform**

**Interface between Trusted Firmware and Trusted OS Dispatcher**

**OSS or TEE Vendor**

**Security Platform Design Documents**

- **HDMI HDCP**
- **TrustZone CryptoCell**
- **Trusted Peripherals**
TrustZone CryptoCell for Every Platform

- CryptoCell acts as a trust anchor and security subsystem for the platform
Technology Model

- **Apps**
- **Guest OS**
- **Hypervisor**
- **TEE on TrustZone**
- **TrustZone CryptoCell**
- **ROT (Root of Trust)**

**TrustZone CryptoCell**

- Secure Boot, key handling, crypto
- Trusted Boot, TEE & Trusted Apps, Trusted Hardware
- Launch of authenticated Hypervisor
- OS / App Integrity

**Root of Trust** e.g. Keys, ROM
GlobalPlatform has developed a TEE certification program

- 3 Month Evaluation
- Enables independent evaluation of partner solutions
- Builds confidence for users
- Enables Silicon Partners to differentiate on security
Summary

- ARM is making end to end security easier by providing right sized secure foundations that scale for different use cases and market needs.

- All platforms, including the tiniest IOT devices, will be able to benefit from new TrustZone technology.

- ARM TrustZone CryptoCell brings easy to implement security systems to all platforms.

- Together we can make the Internet of Trusted Things.
Thank you