Agenda

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

Today

Authentication  Mobile Payment  Content Protection  Enterprise Security

ARM TRUSTZONE
System Security
Security is a Balance

Cost/Effort To Attack

- Level 1
  - Communication Attacks
    - Man In The Middle
    - Weak RNG
    - Code vulnerabilities
  - Software Attacks
    - Buffer overflows
    - Interrupts
    - Malware

Value to attacker

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

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
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
Cortex-A: Putting it All Together

ARM Trusted Firmware
EL3
SoC/platform port
Normal World OS
EL1/EL2
Trusted OS
Secure-EL1
Trusted OS Dispatcher

OSS or TEE Vendor

Security Platform Design Documents

TrustZone Media Protection 1 (TZMP1)
System Hardware on ARM®
Document number: ARM DEN 39221 A-9
Copyright ARM Limited 2011-2014

© ARM 2016
GlobalPlatform TEE Certification

- TEE has a Protection Profile Certified by Common Criteria
- Proposed scheme has Security Certification of a Reference Implementation… AND OEM product – looking at the deltas
- Objective is to reduce time to certification by OEM to 2-3 months
- Independent security assessment vs. “Trust Me”
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
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 - 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
Security Foundations for Cortex-M

- Software - 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
TrustZone for ARMv8-A

TrustZone for ARMv8-M

Applications Processors

ARMv8-M Microcontroller

© ARM 2016
## ARM TrustZone Architecture Extensions

<table>
<thead>
<tr>
<th>Feature/Architecture</th>
<th>TrustZone® 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
Security on Next Generation Cortex-M

TrustZone based uVisor is key building block
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
Secure Foundations for Services

Communication
- mbed TLS

Software / OS
- mbed OS, mbed uVisor

Hardware/System
- TrustZone, CryptoCell (Root of Trust), System IP, AMBA 5
Cryptocell acts as a trust anchor and security subsystem for the platform.
Chain of Trust Starts with Initial ROT

- Initial Root of Trust: e.g., CryptoCell Security functions
- Provisioned keys/data at factory
- iROT
- TrustZone
- TEE or uVisor
- Hypervisor (Cortex-A)
- Guest OS
- Apps

OS/App Integrity
- Launch of authenticated Hypervisor
- Extended Root of Trust e.g., TrustZone based TEE
Secure Foundations From Sensor to Servers

Productivity  Security  Connectivity  Management  Efficiency

- mbed OS
- mbed TLS
- mbed OS uVisor
- TrustZone for ARMv8-M
- TrustZone CryptoCell
Summary

- Security is a place where partners can differentiate e.g. certification, provisioning, services…

- ARM provide the building blocks for security on Cortex-A:
  - Security Platform Design Docs
  - Standards e.g. GlobalPlatform
  - Open source e.g. ARM Trusted Firmware, uVisor & Linaro OP-TEE
  - Ecosystem e.g. Trustonic, BeanPod and other commercial TEE providers

- TrustZone for v8-M brings familiar security architecture to lowest cost points
  - TrustZone based uVisor & CMSIS-RTOS provide useful building blocks

- CryptoCell provides Root of Trust to system & a toolbox of security functions
Thank you!

The trademarks featured in this presentation are registered and/or unregistered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

Copyright © 2016 ARM Limited

© ARM 2016