Securing the Future of IoT

ARM

Joseph Yiu
Senior Embedded Technology Manager, ARM

China
July 2016

Connectivity in all aspects of modern life

© ARM 2016
ARM

The Need for Security

Communication Protection

- Cryptography, authentication

Data Protection

- Secret data (keys, personal information)

Firmware Protection

- IP theft, reverse engineering

Operation Protection

- Maintaining service and revenue

Anti-tamper Protection

- Protection against physical attack

© ARM 2016
ARM

TrustZone Concepts

Separation

- Isolate trusted resources from non-trusted
- Isolate non-trusted software
- Reduce attack surface of key components

Trusted Software

- Provision of security services
- Small, well reviewed code

Trusted Hardware

- Hardware assist for cryptography
- Secure access validation built into SoC

© ARM 2016
ARM

Security Domains and Protection

- 1st level : Cryptography and authentication (communication protection)

- Simple…
- But a single software component being compromised can lead to the loss of the whole device

© ARM 2016
ARM

Security Domains and Protection

- 1st level : Cryptography and authentication
- 2nd level : Privileged levels and memory protection

- Available today…
- But no separate barrier for on-chip firmware

© ARM 2016
ARM

Security Domains and Protection

- 1st level : Cryptography and authentication
- 2nd level : Privilege levels and memory protection
- 3rd level : ARM TrustZone

© ARM 2016
ARM

ARM Architecture: For Diverse Embedded Processing Needs

Cortex - A

Highest performance

Optimised for
rich operating systems

Cortex - R

Fast response

Optimised for
high performance,
hard real-time applications

Cortex - M

Smallest/lowest power

Optimised for
discrete processing and
microcontrollers

© ARM 2016
ARM

Cortex-A: Wide Portfolio for Diverse Embedded Markets

© ARM 2016
ARM

TrustZone on Cortex-A Processors

- 4 Execution Levels
  - Level transitions using system calls instructions : SVC, HVC and SMC

© ARM 2016
ARM

Cortex-A32 - ARM's Most Efficient Cortex-A Processor

Optimized for 32-bit ARMv8-A

>25% Higher efficiency than Cortex-A7
More performance and less power

Scalability for diverse embedded applications

© ARM 2016

Performance and power compared to Cortex-A7 for same CPU configuration, same frequency and iso-process (28nm)

Cortex-A32: Extreme Scalability for Diverse Applications

Performance optimized configuration
>1.0 GHz

Less than 75mW/core at 1 GHz

Smallest area configuration
<0.25 mm^2

Less than 4mW at 100 MHz

© ARM 2016

Total Dhrystone power reported at typical operating conditions, Process – 28HPC

ARM

New Architectural Features for Rich Embedded 32-bit Applications

© ARM 2016
ARM

Cortex-A32: Boosts 32-bit Performance and Efficiency

- Higher performance than Cortex-A5 and Cortex-A7
- Same performance as Cortex-A35

Efficiency Improvement

>25% vs. Cortex-A7

>30% vs. Cortex-A5

>10% vs. Cortex-A35

Efficiency defined as integer performance/power (Performance/mW)
Iso-process (28HPC), Iso-frequency, comparisons, identical processor configurations (32KB L1 caches, NEON, 1MB L2)

© ARM 2016
ARM

ARMv8-M: Taking Embedded to the Next Level

© ARM 2016
ARM

ARMv8-M Sub-profiles

Scalable architecture

- ARMv8-M ***Baseline***:
  - Lowest cost, smallest, ARMv8-M implementations.
- ARMv8-M ***Mainline***:
  - For general purpose microcontroller products
  - Highly scalable
  - Optional DSP and floating-point extensions.
- Similar to ARMv6-M / ARMv7-M
  - 32-bit architecture, architectural memory map
  - Nested Vectored Interrupt Controller (NVIC)
  - Architecturally defined sleep modes

© ARM 2016
ARM

ARMv8-M Additional States

Existing handler and thread modes mirrored with secure and non-secure states

- Secure and Non-Secure code run on a single CPU
  - For efficient embedded implementation.
- Secure state for trusted code
  - New Secure stack pointers for robust operation
  - Addition of stack-limit checking.
- Dedicated resources for isolation between domains
  - Separate memory protection units for Secure and Non-secure
  - Private SysTick timer for each state.
- Secure side can configure target domain of interrupts.

© ARM 2016
ARM

High Performance Cross-Domain Calls

Efficient microcontroller focussed implementation

- Security inferred from instruction address
  - Secure memory considered to hold Secure code.
- Direct function calls across boundary
  - High performance and high security
  - Multiple entry points
  - No need to go via "monitor" for transitions.
- Uses Secure Gateway instruction "SG"
  - Only permitted in special Secure memory with Non-secure-callable attribute (NSC).

© ARM 2016
ARM

TrustZone for ARMv8-A

TrustZone for ARMv8-M

Secure transitions handled by the processor to maintain embedded class latency

© ARM 2016
ARM

Virtualization (ARMv8-R)

Enables consolidation of multiple systems into one system.

TrustZone for ARMv8-M

Enables security protection with very low overhead:
Execution cycles, memory footprint

© ARM 2016
ARM

Communication Protection

- TrustZone CryptoCell
  - Platform level security solutions

- mbedTLS library
  - Enables cryptographic and SSL/TLS capabilities in the connected embedded products
  - Available as standalone version, and also as part of mbedOS

© ARM 2016
ARM

SecurCore - Security Against Physical Attacks

- **SC300**
  - ARMv7-M architecture
  - Similar feature set as Cortex-M3 processor
  - Configurable Anti-tampering features

- **SC000**
  - ARMv6-M architecture
  - Similar feature set as Cortex-M0 processor
    - Support optional privileged/unprivileged levels
    - Support optional MPU
  - Configurable Anti-tampering features

© ARM 2016
ARM

ARM TrustZone Covers Multiple Security Requirements

Data Protection

- Secure data is protected from Non-Secure access

Firmware Protection

- Protects firmware while allowing interactions

Operation Protection

- Secure interrupts can have higher priority

Additional protection technology:

- Communication from ARM TrustZone CryptoCell
- Anti-tampering from ARM SecurCore processors

© ARM 2016
ARM

ARM Security Solutions for Embedded and IoT

Thank you

ARM

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