New ARM technologies for a more secure IoT

Neil Parris
Director of Marketing, Interconnect Products

ARM Tech Symposia
November 2016
Agenda

- IoT security
- Implementing secure embedded systems
- CoreLink SIE-200 – System IP for Embedded ARMv8-M designs
- TrustZone CryptoCell-312
- CoreLink SSE-200 – TrustZone enabled SubSystem for Embedded
IoT security
Different Types of Security

**Lifecycle security**
- Device management
- Monitoring

**Communications security**
- Link encryption
- Authentication
- Anonymity/Confidentiality

**Device security**
- Device integrity
- Asset protection
- Data Security
- Physical Security
- Future-proofing
Implementing secure embedded systems
## TrustZone: A comprehensive security foundation

**Security separation with TrustZone**
- Isolate trusted resources from non-trusted
- Reduce attack surface of key components

**Security throughout the system**
- Software, CPU, interconnect, memory and peripherals

**Trusted hardware**
- Fortified security for entire device lifecycle

<table>
<thead>
<tr>
<th>Trusted software</th>
<th>Trusted hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto</td>
<td>Secure system</td>
</tr>
<tr>
<td></td>
<td>Secure storage</td>
</tr>
<tr>
<td></td>
<td>TRNG</td>
</tr>
</tbody>
</table>
Bringing TrustZone protection to the system

- Secure the system, secure the processor
  - Hardware separation and isolation
  - Protect memories, peripherals, legacy IP

- AMBA 5 AHB5 bus protocol
  - Signals security through the interconnect
  - Complementary to ARMv8-M

- Optimized for embedded systems
  - Fewer wires saves area and power
  - Hardware protection simplifies software
CoreLink SIE-200
System IP for Embedded
CoreLink SIE-200: Extending security to the system

Simplify the design of a secure system
- Designed and verified with latest ARMv8-M processors

Library of AMBA 5 AHB5 components
- Implements system wide hardware security
- Configurable to enabled tailored IoT solutions

Reduce design time with IP re-use
- Secure existing AHB and APB peripherals

Accelerate deployment of ARMv8-M SoCs with TrustZone compatible system IP
CoreLink SIE-200: System IP for embedded

Library of AHB5 IP
- Lightweight & low latency

Scalable and configurable
- Full AHB5 support
- Parallel transactions for highest performance

Protect code and data
- Protect software IP
- Programmable regions for multiple applications

Integrate legacy IP
- Re-use and secure existing IP in AHB5 systems

Minimize power
- Flexible clock and power domains save energy

Protect peripherals
- Re-use existing peripherals
- Programmable at run-time

Library of AHB5 IP
- Lightweight & low latency

Scalable and configurable
- Full AHB5 support
- Parallel transactions for highest performance

Protect code and data
- Protect software IP
- Programmable regions for multiple applications

Integrate legacy IP
- Re-use and secure existing IP in AHB5 systems

Minimize power
- Flexible clock and power domains save energy

Protect peripherals
- Re-use existing peripherals
- Programmable at run-time
TrustZone AHB5 memory protection controller

- Programmable
  - Dynamic allocation of trusted and non-trusted regions
- Configurable protection block sizes
  - From 32B to 1MB
- Provides device security
  - Asset protection – data and code
  - Data security and privacy
- Programmable response on illegal access
  - Decode error response
  - Secure error interrupt

![Diagram of TrustZone AHB5 memory protection controller]
TrustZone CryptoCell-312
TrustZone CryptoCell-312: Fortified device security

Enabling a full set of security services over deeply embedded form factors

Easy to integrate, silicon proven. Software and tools included

10x faster cryptography* performance drives improved energy efficiency

* when compared to SW only operations on cryptography tasks
CoreLink SSE-200

TrustZone enabled Subsystem for Embedded
CoreLink SSE-200: A complete HW/SW subsystem

- A foundation you can trust
  - Integrated hardware and software system
  - Fully verified
  - Configurable and extendable
The fastest and lowest-risk path to secure silicon

- A validated subsystem
  - Security architecture
  - Optimized for low power

- Easy to integrate with your own IP

- Development support
  - Fast model for SW
  - FPGA platform
  - Socrates tools for system expansion
CoreLink SSE-200 subsystem block diagram

- Secure debug
- Cortex-M33
- Instruction cache
- Cortex-M33
- Instruction cache
- TrustZone filters
- Always-on domain
- Multi-layer AHB5 interconnect
- TrustZone protection
- SRAM Control
- TrustZone protection
- System SRAM
- TrustZone protection
- TrustZone CryptoCell
- TrustZone protection
- Cordio radio (digital part)
- Cordio RF
- Options
- AHB5 expansion ports
- Master/Slave
- Non-ARM IP
- ARM CoreLink SSE-200 IP
- Other ARM IP

- DMA
- HW acceleration
- Other radios
- Peripherals
- ADC/DACs
- Interfaces (SPI, I²C, SDIO,...)
- ...
A ready-to-use software framework

- Integration of
  - Libraries, drivers
  - Protocol stack
  - mbed OS

- Verification at the system level

- Different targets
  - Fast Model
  - FPGA board

- Distributed as open-source
Fast track to mbed OS ecosystem

**mbed OS Connectivity**
- Ethernet
- WiFi
- Bluetooth

**mbed OS Core**
- Peripheral drivers
- Peripheral HAL

**mbed OS API**
- Sockets
- Profiles
- Cloud client infrastructure
- Connect client
- Provision client
- Update client

**mbed OS Communication Security**
- BLE stack
- mbed Transport Layer Security

**Security APIs**
- Provision trusted library
- Update trusted library
- Secure storage
- Crypto trusted library
- Trusted drivers
- Trusted HAL
- mbed uVisor

**Hardware interfaces**
- Peripherals
- Radio
- Sensors
- ARM CoreLink SSE-200

**mbed OS components**
- TrustZone for ARMv8-M

ARM mbed
IoT device platform

mbed OS
200K developers
2016

60K developers
2014

CoreLink SSE-200
software integration

Partner components/ports
Build your ARMv8-M system on FPGA

- Evaluation and prototyping
  - IoT subsystem on FPGA
  - Rapid software and hardware development

- Used by software and tools ecosystem partners

- Expandable
  - Large FPGA for user logic
  - Arduino shield adapter
  - IO expansion
  - Debug connectors

Demo on ARM booth!
Tackling the security challenges of IoT

- Lifecycle security
  - mbed Cloud and mbed Cloud client
  - CryptoCell lifecycle management

- Communications security
  - mbed TLS
  - CryptoCell encryption/authentication

- Device security
  - TrustZone technology
  - Subsystem and system IP to build secure SoCs
  - mbed uVisor
  - CryptoCell secure storage
Creating a secure IoT is everyone’s responsibility

- Need to get security foundation right
  - Secure processor
  - Secure system
  - Secure software

- ARM IP is available to implement it
  - TrustZone technology
  - TrustZone CryptoCell
  - CoreLink System IP and Subsystem
  - mbed OS

- ARM solution helps you get to market fast