Secure IoT devices at scale

Neil Parris, Director of Product, IoT Device IP, Arm

IOTSF
5th December 2017
World changing inventions

1000+ partners
Insecurity of things
Our Digital Social Contract

Security Manifesto
In IoT security cannot be optional
Security at the core of every device
Arm secure IP: Helping to protect billions of devices

<table>
<thead>
<tr>
<th>Year</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000+</td>
<td>SecurCore</td>
<td>Smart Card for payment</td>
</tr>
<tr>
<td>2005+</td>
<td></td>
<td>Apps processors gain TrustZone</td>
</tr>
<tr>
<td>2010+</td>
<td></td>
<td>Enablement of premium content streaming &amp; mobile payment</td>
</tr>
<tr>
<td>2015+</td>
<td>Mbed, CryptoCell, Cortex-M33, CryptIsland</td>
<td>Trusted Execution Environment (TEE) for Cortex-A</td>
</tr>
<tr>
<td>Today</td>
<td></td>
<td>TrustZone for Cortex-A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TrustZone for Armv8-M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform Security Architecture &amp; Security enclave</td>
</tr>
</tbody>
</table>

©2017 Arm Limited
Arm: The industry’s architecture of choice

- 50 billion chips shipped
- 50 billion chips shipped
- 100 billion chips expected to ship

- 22 years
- 4 years
- 4 years

1991 2013 2017 2021

2016 80% microcontrollers
Arm vision: A trillion securely connected devices

Security across entire value chain

Scalable security to the smallest, low-cost devices

Secure connection and management of devices

From device to cloud
The diversity of device types needs common ground-rules.
Platform Security Architecture

From principles to architecture

3 Parts to PSA

Analyze

- Threat models & security analysis

Architect

- Hardware & firmware architecture specifications

Device identity

Trusted boot sequence

Secure over-the-air software update

Certificate based authentication

Implement

- Firmware source code

Software architecture

Hardware requirements

Architecture & Specifications

Common principles across multiple use cases
Security starts with analysis
Analysis leads to requirements

- System description
  - Assets
  - Threats
  - Security Objectives
  - Security Requirements

Example
- Asset: metering data to be protected in integrity & confidentiality
- Threat: Remote SW attacks
- Security Objective: Strong Crypto
- Security Requirement: Hardware based key store

Arm will deliver representative IoT device security analyses & requirements
Platform Security Architecture deliverables

Security architecture derived from principles

IoT Security analyses
- Wireless meter
- Asset tracker
- Connected camera

Firmware specifications
- Firmware framework
- Secure update
- Boot sequence

Hardware requirements
- Random Number Generator
- Secure storage
- Crypto
Open source code to accelerate adoption
Freely available reference implementation

Trusted Firmware-M (TF-M)

- Reference firmware for the architecture specification
- Initially targeting Armv8-M
- In development now – public availability first quarter 2018

Arm Mbed OS will provide an implementation of PSA

- Integrated with Mbed TLS and Mbed Cloud Client
- Targeting all Cortex-M processors
- Available in subsequent releases of Mbed OS
Platform Security Architecture – Isolation

Designed to secure low cost IoT devices
• Where a full Trusted Execution Environment would not be appropriate.

PSA protects sensitive assets
• keys, credentials and firmware
• separates assets from application firmware and hardware.

Defined Secure Processing Environment (SPE)
• Protected data, code & trusted hardware resources

PSA is architecture neutral
• Cortex-M, Cortex-R & Cortex-A
• The focus is Cortex-M based devices
### Platform Security Architecture - Standardized Interfaces

PSA specifies interfaces to decouple components.

- Enables reuse of components in other device platforms
- Reduces integration effort

Partners can provide alternative implementations.

- Necessary to address different cost, footprint, regulatory or security needs

PSA provides an architectural specification

- Hardware, firmware, process requirements & interfaces

<table>
<thead>
<tr>
<th>Non-secure processing environment</th>
<th>Secure processing environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Trusted Functions</td>
</tr>
<tr>
<td>RTOS</td>
<td>Secure partition API</td>
</tr>
<tr>
<td>Secure IPC</td>
<td>Secure partition manager</td>
</tr>
<tr>
<td>Platform hardware</td>
<td>Boot firmware</td>
</tr>
<tr>
<td>Secure hardware requirements</td>
<td>Root of Trust keys</td>
</tr>
</tbody>
</table>
Example IoT Device Implementation

OEMs can choose their preferred implementations.

Arm Trusted Firmware-M will be a new OSS project.

- To reduce rework across our partners
- To speed up device or component validation against standards such as Common Criteria EAL

Open to any RTOS and other partners

Will be implemented in Mbed OS
PSA framework for real results

BEFORE PSA

• Metering data exposed resulting in theft of electricity

• Default passwords left in device

• Unable to fix a vulnerability in deployed devices

AFTER PSA

• Designed-in security identity and data logging

• Devices use certificate based authentication

• Over-the-air update mechanism built in by default
Arm Secure Connected IoT Device

- TrustZone processor
- Secure debug channel protects firmware
- Secure system building blocks
- Example PSA compliant system
- Low power management built in
- Secure enclave for on-die security services
- Connectivity to the cloud e.g. NB-IoT

Diagram:
- TrustZone aware Interconnect
  - TrustZone filters
  - Flash controller
  - Flash (internal/external)
- CryptolIsland
  - Isolating I/F
  - Secure CPU
  - Boot ROM
  - Secure RAM
  - Cryptography
  - LCS Manager
  - Secure Always On
  - Alarms
  - Roots of Trust
  - Debug control
- Cortex-M Host CPU
  - System SRAM
  - SRAM control
  - TrustZone filters
- Power Control
- Secure SoC
- Radio & IO
- Secure debug channel protects firmware
- Roots of Trust
- Isolating I/F
- Secure CPU
- Boot ROM
- Secure RAM
- Cryptography
- LCS Manager
- Secure Always On
- Alarms
- Roots of Trust
- Debug control
Shifting the economics of security

Platform Security Architecture: A common framework for securing the next trillion connected devices

Devices must be born secure; security is no longer optional

Arm is architecting end-to-end IoT security from device to cloud

Arm reducing cost and helping scale by contributing PSA specifications and Trusted Firmware-M source code

https://developer.arm.com/products/architecture/platform-security-architecture
Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!
The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks