Arm Secure Foundations

Speed-up your next IoT design

December 2018
Build secure IoT systems
Arm’s Vision For IoT Security
Making Security Easier to Implement

Key IoT security considerations

1. Security needs to be built-in from the ground up

2. A collective industry responsibility

3. Security needs to be simple, with seamless integration

Platform Security Architecture (PSA) is the perfect starting point

Providing a framework to ensure consistent security
Platform Security Architecture (PSA)
A recipe for building a secure system & a reference implementation

<table>
<thead>
<tr>
<th>Analyze</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat models &amp; security analysis</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Architect</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware &amp; firmware architecture specifications</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware source code</td>
<td></td>
</tr>
</tbody>
</table>

3 parts to PSA

<table>
<thead>
<tr>
<th>Security Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Goals</td>
</tr>
</tbody>
</table>

Common principles across multiple use cases

<table>
<thead>
<tr>
<th>Software architecture</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hardware requirements</th>
</tr>
</thead>
</table>

Architecture & Specifications
Designing Secure IoT Systems

1. Identify threats
2. Define secure architecture
3. Acquire security IP
4. Design secure hardware
5. Design secure software
6. Integrate cloud security
7. Integrate system
Designing Secure IoT Systems with Arm Secure Foundation

- Identify threats
- Define secure architecture
- Acquire security IP
- Design secure hardware
- Design secure software
- Integrate cloud security
- Integrate system

- Identify threats
- Use Arm secure foundation
- Integrate system
Arm Secure Foundation Solutions
Arm secure foundation solutions

Extendable for differentiation & diversity

- Corstone foundation IP
  - Pre-integrated processor & security IP
  - Pre-verified, modifiable subsystems
- Corstone ready software
  - Standardized interfaces and architecture
  - Mbed OS and Mbed Linux
- Tools
  - Arm and 3rd party development tools
  - FPGA, fast models, test chip boards

Note: Arm Corstone replaces Arm System Design Kits (SDK)
Different Classes of Devices have Different Requirements

Rich IoT nodes & gateways
- Data processing at the edge
- Decision making
- Machine learning
- Gateway to cloud

Mainstream
- Balancing performance and cost
- Moderate data / audio processing
- High power efficiency

Constrained
- Ultra-low-cost, sensors or beacons
- Often battery powered
- Connecting to gateway or cloud
Corstone Foundation IP

Definition

• Corstone foundation IP
  • A Licensable package that gives access to
    – Example Subsystems
    – System IP
    – Scripts
    – Basic Testbench
    – Supporting Documentation

• Supported by Corstone Ready Software

*Corstone is the new brand name that replaces System Design Kit (SDK)*
A Family of Solutions

Nested Doll Principle

- Corstone-700 includes Corstone-100 & 200 components
- Corstone-200 includes Corstone-100 components
Corstone foundation IP – Subsystem for Embedded (SSE)

A range of subsystems available with security

Rich nodes / gateways

SSE-700 + Media / AI
- Cortex-A + Cortex-M
- Cortex-A + Cortex-M

SSE-700
- Cortex-A + Cortex-M
- TrustZone
- Secure enclave
- Firewalls
- Protected multi-domains debug support
- Isolated domains

Mainstream

SSE-200
- Cortex-M33
- TrustZone
- CryptoCell pre-integrated
- Secure debug

Constrained

SSE-123
- Cortex-M23
- TrustZone
Constrained Subsystem - SSE-123 example subsystem

- **Cortex-M23**
- **IDAU**
- **Always-on domain**
- **Power Control**
- **Multi-layer AHB5 interconnect**
  - **AHB5 code interface**
  - **TrustZone Filters**
  - **SRAM Cntl**
  - **APB Bridge**
  - **APB Peripherals**
- **System SRAM**
- **Flash Controller**
- **Embedded Flash or External Flash**
- **Cryptocell**
- **AHB5 expansion ports** (Master/Slave)
- **JTAG or SW**

**Non-Arm IP**
- Corstone-201 Foundation IP
- Other Arm IP

- DMA
- HW acceleration
- Radios
- Peripherals
- ADC/DACs
- Interfaces (SPI, I²C, SDIO,...)
- ...

- Embedded Flash or External Flash
- System SRAM
- APB Bridge
- APB Peripherals
- Always-on domain
- Power Control
- Multi-layer AHB5 interconnect
- Cortex-M23
SSE-200 Subsystem

- Secure Debug
- CoreSight SoC
- Cortex-M33 (with ETM)
- Instruction Cache
- Cortex-M33 (with ETM)
- Instruction Cache
- Local SRAM
- Always-on domain
- Multi-layer AHB5 interconnect
- Power Control
- TrustZone Filters
- SRAM Cntl
- System SRAM
- CryptoCell
- APB Bridge
- APB Peripherals
- Flash Controller
- Embedded Flash or External Flash
- AHB5 code interface

Non-Arm IP
- Corstone-201 foundation IP
- Other Arm IP

Rest of the system

Option
Corstone-Ready Software for 100 and 200 Series

Essential elements

• Keil MDK pack supports any RTOS
  • Largest RTOS choice

• Trusted Firmware (TF-M)
  • Implementation of PSA APIs

Application and RTOS support

• Mbed OS
  • Support out of the box
  • Integrated with TF-M in Mbed OS 5.12 (December)

• Other RTOS support
  • E.g. Zephyr, FreeRTOS

• Example applications
Trusted Firmware-M (TF-M)

Open-source reference implementation of PSA

Non-Secure

Apps
Network
Middleware
OS
PSA API

Secure

Storage
Crypto
Attestation
Audit Logs
Provision
Platform
3rd Party

Platform Drivers

TF-M Core
Secure Boot

TBSA-M HAL APIs
HAL

TBSA-M Hardware (SoC)

USPS Spec/API
Application RoT
PSA RoT
TF-M
Isolation

www.trustedfirmware.org
Some Ways Arm is Promoting Security

- Thought-leadership & education: Security manifesto, surveys and events
- Platform Security Architecture: Offering an industry best practice framework
- Providing security elements: TF-M, PSA ready systems, security IP
- Develop the ecosystem: Musca test chip program
Musca-A Test Chip

SSE-200 Proven In Silicon

- SSE-200
- Cortex-M33

Distributed to the ecosystem

- SW developers
  - Target for TF-M
  - Develop secure software

- SoC developers
  - Evaluate the IP
  - Understand security architecture

100s of companies already use a Musca board

Ask for a free loan!
Conclusion

• Arm invests in secure IoT solutions
  • For all IoT segments (constrained, mainstream, rich nodes / gateways)
  • System approach – HW, SW, services, tools
  • Corstone foundation IP

• Benefit for users
  • Reduced cost, faster TTM, focusing on differentiation
  • Security in line with PSA principles
  • Architecture alignment ➔ Ecosystem
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