Why is getting security right for IoT so important?

When our “everyday appliances” become connected, our most private moments become at risk of getting exposed


Or even that our “appliances” could become “malicious”

“….100,000 malicious endpoints. We are able to confirm that a significant volume of attack traffic originated from Mirai-based botnets.” (Dyn, Attack analysis)
How can ARM help?

▪ ARM has deep system understanding of HW security which enables us to provide solutions that address full end-to-end security of a connected system

▪ Enable you to get security right and to focus on your differentiation

▪ Saving development costs and time-to market
Applying the Lessons From 20 Years of Mobile to IOT:
Initial Root of Trust & Chain of Trust

**Initial Root of Trust & Chain of Trust**

- **Initial Root of Trust:** Dependable Security functions
- **Extended Root of Trust (TEE)**
- **Trusted Apps/Libs**
- **Provisioned keys/certs**

- **Keys**
- **CryptoCell**
- **TrustZone**
- **uVisor**
- **Trusted Software**
- **OS**
- **Apps**
Security on Cortex-A systems

GlobalPlatform standardization

TrustZone based TEE

Common foundation

Initial ROT & security subsystem

Normal world code

Trusted software

Apps EL0
- Apps/user
- Comms stack

EL1
- Device Drivers
- Rich OS

EL2
- Hypervisor

EL3
- SMCCC
- PSCI
- Payload Dispatcher
- Trusted Boot

Hardware Interfaces

ARM Cortex-A
SoC System
Physical IP
CryptoCell Platform Security Services

Search for - Webinar: How to build trust into your embedded device
Security on ARMv8-M systems

Unprivileged
- Apps/user
- Comms stack

Privileged
- RTOS
- Device drivers

Hardware Interfaces

Normal world code

Trusted software

TLS/Crypto libs

CMSIS API

TrustZone based ARM uVisor

Initial ROT & Security subsystem

Search for - Webinar: ARM TrustZone – Understanding system security
TrustZone CryptoCell: a comprehensive security solution

Host direct operation (REE, TEE)

Control interface
- Slave Bus interface
- Decode
- Queuing

Security resources
- Lifecycle State
- RoT management
- RNG
- Key Slots (policies)
- Provisioning

Asymmetric cryptography
- SW image validation
- IP Protection
- Secure Debug / DFT
- Data protection
- Feature enablement

Symmetric cryptography
- PKA
- ALU

Data interface
- Master Bus Interface DMA
- FIFOs

Persistent roots of trust
- Always On

Lifecycle State
RoT management
RNG
Key Slots (policies)
Provisioning
Arbitration
IP Protection
Secure Debug / DFT
Arbitration
Scheme control
PKA
ALU
Tasks submission
Crypto
DMAs
Data protection
Feature enablement
System memory
Host direct operation (REE, TEE)
How can ARM help?

- ARM has deep system understanding of HW security which enables us to provide solutions that address full end-to-end security of a connected system.

- Enable you to get security right and to focus on your differentiation.

- Saving development costs and time-to market.
Threat model identification

Cost/effort to attack

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

Cost/effort to secure
Selecting the right security solution for your design

Isolation of the Execution Environment

- App CPU
- Separated (TrustZone, standalone CPU)
- Tamper resistant and separated (SecurCore)

Robustness of the platform security means

- SW only
- HW-based
- Tamper resistant HW based

Considerations like addressed threat model, power, performance, area and certification target are the ones determining the right combination of execution environment and platform security means.
Selecting the right security solution for your design

Isolation of the Execution Environment

- App CPU
- Separated (TrustZone, standalone CPU)
- Tamper resistant and separated (SecurCore)

Robustness of the platform security means

- SW only
- HW-based: CryptoCell
- HW-based: CryptoCell with SCA CMs
- Tamper resistant

Considerations like addressed threat model, power, performance, area and certification target are the ones determining the right combination of execution environment and platform security means.
HW protection level: **optional** Power Analysis countermeasures

ARM offers products in which selected logic gets its power from (on-die) Capacitors – not from the SoC’s power supply, making power analysis attacks impossible.
Selecting the right security solution for your design

Isolation of the Execution Environment

- App CPU
- Separated (TrustZone, standalone CPU)
- Tamper resistant and separated (SecurCore)

Robustness of the platform security means

- SW only
- HW-based
- Tamper resistant HW based

Considerations like addressed threat model, power, performance, area and certification target are the ones determining the right combination of execution environment and platform security means
Portfolio of security IP solutions

- **CryptoCell** - a HW/SW/Tools package
  - “External” SW execution
  - No specific app stack
- **Security Enclaves** - Security “subsystems” providing a highly isolated and robust execution environment for security tasks
  - Blackbox model (ARM provided functionality) or Whitebox model (where non-ARM code can be added in a secure manner)
- **Solutions family** – security enclave plus application layer (3rd party SW stack)
  - A specific vertical SW stack (or several stacks) integrated (and certified when appropriate)

---

**Platform security services**

- **TEE**
- **CryptoCell family**
- **Security Enclaves family**
- **Solutions family**

---

**Integration Level**

- **CryptoCell 3xx, 7xx**
- **CryptoCell 3xx, 7xx**
- **CryptoCell 3xx, 7xx**
- **Trusted App (e.g. Payment)**
How can ARM help?

▪ ARM has deep system understanding of HW security which enables us to provide solutions that address full end-to-end security of a connected system

▪ Enable you to get security right and to focus on your differentiation

▪ Saving development costs and time-to market
Shortening TTM with a comprehensive BoM

<table>
<thead>
<tr>
<th>CryptoCell-312 - Bill of Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Factory Tools</strong></td>
</tr>
<tr>
<td>OTP population tools for the chip vendor and for the device maker</td>
</tr>
<tr>
<td><strong>Off-line Tools</strong></td>
</tr>
<tr>
<td>Code signing &amp; encryption, Debug certificates generation, Authorization of 3rd parties to introduce code and do Debug, Asset provisioning,</td>
</tr>
<tr>
<td><strong>Middleware</strong></td>
</tr>
<tr>
<td>Optional HomeKit Crypto library</td>
</tr>
<tr>
<td>Optional Thread Crypto library</td>
</tr>
<tr>
<td><strong>Firmware/Drivers</strong></td>
</tr>
<tr>
<td>Boot lib</td>
</tr>
<tr>
<td>Runtime (mbed TLS)</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
</tr>
<tr>
<td>Verilog RTL sources</td>
</tr>
</tbody>
</table>
In summary:

- As an IoT SoC designer, you can take advantage of ARM’s vast experience in security

- ARM delivers a range of security IP solutions and you can choose (with our help) the one which fits your needs

- Integrating ARM’s security IPs saves TTM as each comes as a comprehensive package
Questions?

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 © 2017 ARM Limited

©ARM 2017