Building A Secure IoT Device

Ashutosh Singh
Aug 23, 2019
Agenda

• Security challenges in building an IoT device
• Common security functions across use-cases
• Introduction to Platform Security Architecture (PSA)
• Introduction to Trusted Firmware M
Security Challenges
Complex Supply Chain

- Silicon Vendor
- Protected Secrets

- Trusted OS Applet
- Protected Secrets

- OEM 1
- OEM 2
- …

- OS Vendor
- OS Vendor
Security Challenges

- Trusted OS Injection
- Secure Device Provisioning
- OS Vendor
- OEM 1
- OEM 2
- ...
Common Usage Patterns

Connectivity
- Device to Cloud
- Device to Device

Data Management
- Sensor Data Handling
- Payment Processing
- DRM Content
- Biometric data

Multi Vendor Supply Chain
- Silicon Vendor, OEM, OS Vendors
- APP Vendors
- IP Protection

Device Management
- Device Configuration
  - Feature certificates
  - Firmware Update
  - Incident Mgmt
Security Challenges

• Trust Establishment
  • Secure Communication

• Multi Vendor Assets
  • Secure Firmware Updates

• Secure Device Provisioning
  • IP Protection
  • Complex Licensing Models

• Secure Data Management
  • Content License Management

Connectivity

Data Management

Multi Vendor Supply Chain

Device Management
Security Building Blocks
Common Security Functions

- Immutable Root of Trust
- Chain of Trust & SW Integrity
- Principle of Least Privilege
- Software Updateability
- Device identification and Authentication
- Lifecycle Management
Root of Trust and Chain of Trust

**Immutable RoT**
- ROM Code
- Key signing Pub key
- Likely to be part of RTL
- Authentication of updateable bootloader
- Assist in factory floor device provisioning

**Updateable Bootloader**
- Hardware Unique Key
- RNG
- Image signing Pub key
- Monotonic counter
- Runtime SW authentication
- Firmware update process
- Key derivation tree and boot seed
- Boot signature measurements

**Runtime Software**
- RNG
- Use-case keys
- Crypto accelerator
- Business use-case
- Secure communication
- Firmware update support
- Compartmentalization
Principle of Least Privilege

- SW and HW compartmentalization
- Cryptographic key hygiene
- Multivendor scenarios with mutual distrust
Firmware Update

- SW/HW vulnerability fixes
- Multivendor software updates
- Certificate based image authentication
- Rollback Protection
Device Identification and Authentication

- Immutable Unique Identity
- Certificate based authentication
- Device attestation
Lifecycle Management

Silicon Manufacturing
- RTL Key
- Feature control
  - Secure device provisioning
  - Feature subscription licensing models

OEM/OS Vendors/ APP Vendors
- Key provisioning
- Firmware Provisioning
  - Secure device provisioning
  - SW Integration

Field Deployment
- Keys
- Subscription Certs
- HUK
  - Multiple vendor (apps, firmware fragments) management
  - Device Recall
Hardware Building Blocks

- Immutable Root of Trust
- Device Identity
- Hardware Unique Key
- NV Counters
- Hardware isolation support
- Crypto Accelerator
- Lifecycle management
- Root of Trust Keys
Supply Chain Challenge
A Scalable Solution

- OEM provisioningKey
- Lifecycle change

Silicon Vendor

OS Vendor

OEM 1

- OS signing/update key
- Lifecycle change

OEM 2

OS Vendor

...
Platform Security Architecture and Trusted Firmware M
Platform Security Architecture

3 Parts to PSA

Analyze
Threat models & security analysis

Architect
Hardware & firmware architecture specifications

Implement
Firmware source code

Device identity
Trusted boot sequence

Secure over-the-air software update
Certificate based authentication

Common principles across multiple use cases

Software architecture
Hardware requirements

Architecture & Specifications
How to get involved

trustedfirmware.org

Open Source, Open Governance Secure World Software
Launched in 2018