Scalable IoT Security - Trusted Firmware-M Profiles

David Wang
Shebu V. Kuriakose
Arm Ltd.
Trillion Connected Devices

*IoT take up gaining traction in the coronavirus crisis*

Source: verdict.co.uk
Trillion Connected Devices: Are They Secure?

Since the emergence of COVID-19, IoT adoption is swiftly and necessarily on the rise. The increasingly technology driven enterprise must architect around multi-layered security to protect their IoT device estates.

Source: Economist, The IoT Business Index 2020
Trusted Firmware-M: Providing Platform Security

- **Analyze**: Threat models & security analyses
  - Methodically developed

- **Architect**: Hardware & firmware architect specifications
  - Open architecture

- **Implement**: Firmware source code
  - Open Source (TF-M & TF-A)

- **Certify**: Independently tested
  - Enabling trust

Open Source (TF-M & TF-A) Enabling trust
Trusted Firmware-M
Secure Processing Environment For Cortex-M
How Can IoT Applications Use TF-M?
TF-M: Available on Several PSA Certified Devices
TF-M: Upstream Integration in RTOSes

The diagram illustrates the integration of TF-M with RTOSes, showing the interaction between non-secure and secure processing environments. Key components include:

- TF-M Core (IPC, SPM, Interrupt Handling)
- Secure Boot
- TBSA-M HAL
- HAL
- TBSA-M Hardware

The diagram highlights the integration of Trusted Firmware-M (TF-M) with PSA Functional APIs within the secure processing environment, alongside PSA Root of Trust (PSA-RoT) and PSA Functional APIs within the non-secure environment. The overall goal is to provide a secure and efficient integration of TF-M into existing RTOS architectures.
PKCS#11 To PSA Functional API Shim in FreeRTOS
TF-M Profiles
Very Different IoT Devices, Very Different Security
TF-M Profiles: Aligning with PSA Certification

Scalable Security To Meet Diverse Security Requirements
Profile Small

- For Ultra Constrained Devices, Simple Applications
- Connection with Edge Gateway and IoT Cloud Services with symmetric cryptography
- Aligns with PSA Level1 Certification Requirements
Profile Medium

- For Constrained Devices
- Connect devices to IoT Cloud Services directly with asymmetric cipher support
- Secure world and normal world are managed by different vendors
- Aligns with PSA Level2 Certification Requirements
Profile Large (Under Design)

- Less Constrained devices
- Multiple vendors, Secure applications which don’t trust each other
- Need to mitigate against higher attack potentials
Profile Small Demo
Demo Overview

AWS IoT Cloud

Gateway – RPi 3B

Attestation TLS-PSK

Temperature/Humidity Data logging

Attestation TLS-PSK

Temperature
Humidity

NXP – LPC55S69
FreeRTOS + TF-M Profile Small

Arm – Musca B1
FreeRTOS + TF-M Profile Small

ST – STM32L5
FreeRTOS + TF-M Profile Small
Demo workflow
Demo Video
Thank you

Accelerating deployment in the Arm Ecosystem