Trusted Firmware-M training

Outline

PSA and Trusted Firmware-M for Arm microcontrollers

This course introduces trainees to the Platform Security Architecture and how Trusted Firmware-M can be used to implement the architecture on Arm microcontrollers, especially for Armv8-M devices that include TrustZone technology.

This is a four module course, equivalent to approximately two days face-to-face training. It is suited to both face to face and remote delivery.

Trainees must have a good general knowledge of microcontroller development and of the C language. Prior experience working on secure or networked products is useful but not mandatory. Trainees will learn how Trusted Firmware-M implements the relevant PSA specifications alongside gaining practical experience on topics such as configuration and porting.

Platform Security Architecture

This session describes the relationship between the PSA and Trusted Firmware-M. To help understand PSA in concrete rather than abstract terms trainees will study the different ways secure hardware can be implemented using Arm microcontrollers before studying the main PSA concepts and principles.

- Overview
    - Platform Security Architecture
    - Trusted Firmware-M
    - PSA Certification
- Secure Hardware
    - Trustzone for Armv8-M
    - Secure physical cores
- Platform Security Architecture
    - Security model
        - Goals
        - Device and isolation models
        - PSA Root-of-trust
        - Applications
    - Firmware Framework for M
        - Goals
        - Secure partitions
        - Secure partition manager
        - Isolation levels

- Lab: ?TF-M build and boot?

Secure boot

This session is entirely dedicated to secure boot. It covers the relevant PSA specification together with a summary of the root-of-trust requirements the specification imposes on the hardware. Trainees will also learn about mcuboot, the reference secure boot implementation included as part of TF-M.

- Platform Security Boot Guide
- First stage bootloader requirements
- Mcuboot
    - Overview
    - Slots and flash map
    - Upgrade strategy
    - Anti-rollback protection
- Lab: ?SPE image upgrade: delivery and flashing?

Trusted Firmware-M: Core and services

In this session we will examine all the runtime components of TF-M, from its core features to the services it can be configured to provide.

- TF-M Core
    - Secure partition manager
    - Secure call flow
    - Interrupt model and handling
        - Library model
        - IPC model
    - NSPE client identification
- Services
    - Crypto
    - Internal Trusted Storage
    - Attestation
- Application services
    - Protected Storage
- Lab: ?Applications and providing services to NSPE?

Porting Trusted Firmware-M

In this final session trainees will move past theory into the pragmatic issues trainees are likely to face when porting TF-M to their platforms.

- Source structure
- TF-M HAL
- Profiles
    - Small

    - Medium
    - Large? (not yet documented)
- NSPE OS integration
- Debugging
- TF-M Organization, governance and licensing
- Contributing to TF-M
- Lab: ?Extending the HAL?