Zephyr and Trusted Execution Environments

Andy Gross
Agenda

Trusted Execution Environments for Microcontrollers

Hardware requirements

Zephyr support for ARMv8M

Multiple Image Complications

Current work items
TEE for Microcontrollers

Current solutions in the ecosystem (or soon to be):

Synopsis Secure Shield™ for ARC

ARM Trusted Firmware for Cortex M (TFM)

Proprietary multi-core solutions with a small designated secure core
Hardware Requirements

Fundamental requirement is to keep from leaking information.

How can this be done?

ARMv8m:
- Separate secure and non-secure environments
- Access control on peripherals and memory space

ARMv7m:
- Multiple cores with separate peripherals and memory space
ARMv8M Specific Hardware

Secure and Non-Secure environment

Privileged and non-privileged modes

Security attribution units (SAU)

Implementation Defined Attribution Unit (IDAU)

Secure and Non-Secure Memory Protection Units
Zephyr Support for ARMv8M

- Zephyr arch support added by Nordic
- Both Baseline (M23) and Mainline (M33) supported
- Memory protection unit and stack limit register
- Supports -mcmse (compiler support for security extensions)
- Optional secure library stub creation
- SDK work in progress
Zephyr and TFM Separation

Non Secure

Zephyr

Secure

SPE SPE SPE SPE

SPM

Level 1
Zephyr and TFM Separation

Non Secure

Zephyr

Secure

SPE

SPE

SPE

SPE

SPM

Level 2
Zephyr and TFM Separation

Non Secure

Zephyr

Secure

SPE SPE SPE SPE

Level 3

SPM
Single Core Implementation

Non Secure

Application Code

Zephyr Secure Service Library

Zephyr v8m Secure Function Call

Secure

SPE
SPE
SPE

SPM
Multicore Implementation
Multiple Image Complications

- May have separate sources (TFM vs Zephyr)
- Multiple binaries
- Bootloader requirements
- Coherent description of hardware and ownership
Current Work Items

• Armv8m targets - Musca and MPS2
• Multi-core v7m and v8m
  • IPC
  • OpenAMP
• Device tree support in TFM
• Single device tree description of secure and non-secure resources
• Modularizing TFM components (secure functions, secure config, etc)
• Integration of TFM and Zephyr
Links to Resources

ARM Platform Security Architecture (PSA):
https://pages.arm.com/psa-resources.html

ARM Trusted Firmware for Cortex M:
https://git.trustedfirmware.org/trusted-firmware-m.git/