Trusted Firmware M: Current Topics

Andy Gross

Overview of Topics

- Build strategies
- Bootloader support
- Device Tree support

Build strategies

- TFM and Zephyr currently built separately
- Final image creation requires extra steps
- What would combined solution look like?

Bootloader support

- TFM uses a snapshot of MCUBoot w/ additional changes

- MCUBoot needs additional feature support
  - Multiple image support
  - Signing/verification of images
  - Ability to copy and execute in other locations for performance

Device Tree Support

- Leverage current device tree support in Zephyr
- Describe both secure and non-secure views of system
  - Secure image may be Zephyr based or TFM based
- Validation of security settings and configuration