Status of MCUboot alignment

TF-M Tech Forum

Dávid Vincze
11/06/2020
MCUboot + TF-M

Old way of working
- MCUboot fork in TF-M repository
- Code has diverged, features available only in one of the repos
- Occasional code base synchronizations (MCUBoot → TF-M fork)
MCUboot + TF-M

Old way of working
- MCUboot fork in TF-M repository
- Code has diverged, features available only in one of the repos
- Occasional code base synchronizations (MCUBoot → TF-M fork)

“This is the way”
- Support of upstream MCUboot (v1.4.0) from 01/2020
  (MCUBOOT_REPO CMake variable)
  - Joint development in one place..
  - Simulator environment to test new features and regression
## Transition to upstream MCUboot

### TF-M v1.0
(Released in March)

- Support of upstream MCUboot in TF-M with limitations
- Multi-image boot (SWAP and Overwrite-only)
- Available bootloaders:
  - TF-M's fork (default)
  - MCUboot v1.4.0

### TF-M v1.1
(In progress)

- HW Rollback protection
- Boot data sharing (measured boot)
- Hardware key support

- Available bootloaders:
  - MCUboot v1.6.0 (default)
  - TF-M’s fork

### TF-M v1.x

- Single-image boot only:
  - NO_SWAP support (PR #739)
  - RAM_LOADING for Musca-A (in progress)

- Available bootloaders:
  - MCUboot v1.x.x (default)
  - TF-M’s fork

- MCUboot v1.x (default)
- TF-M’s fork
Notes on important differences

- Boot data sharing:
  - Definition of tlv_len in TLV entry header (will be handled in TF-M)
  - boot_save_shared_data() for target specific data
- "NO_SWAP" has been renamed to "direct-xip"
- Using the "official" imgtool package from PyPI
  - Slightly different argument list
  - Usually released at the same time as MCUboot
Future activities

- Enabling new MCUboot features in TF-M:
  - Encrypted image support (in progress)
  - Image update over serial port
  - etc.
- Supporting the multi-image scenario with direct-xip mode?
- Completely remove the MCUBoot fork from the TF-M repo
Thank you