SAN19-121
TF-M remote secure services with Zephyr

Karl Zhang, Kevin Townsend
Agenda

- TF-M + Zephyr
  - Single CM33
  - Multiple-Core
- TF-M Remote Services
  - RPC over openAMP
- PSA certified
TF-M + Zephyr on single CM33

- Library mode
  - Isolation level 1

- TFM IPC mode
  - Asynchronized access
  - Isolation level 2 & 3
TF-M + Zephyr on Multiple-Core

- Secure Island
  - Security managed by TF-M
  - Non-secure cores can be various

- PSA APIs
  - PSA FF compliant
  - Uniform
TF-M Remote Services

- openAMP for Communication
  - Zephyr IPM
  - rpMsg

- eRPC for RPC
  - IDL
  - PSA APIs
IDL for PSA APIs

interface PsaVersionService {
    psa_version(in uint32 sid) -> uint32
}
uint32_t psa_version(uint32_t sid);

interface PsaConnectService {
    psa_connect(in uint32 sid, in uint32 minor_version) ->
    psa_handle_t
}
psa_handle_t psa_connect(uint32_t sid, uint32_t
minor_version);

interface PsaCallService {
    psa_call(in psa_handle_t handle, in uint32 in_vec, in uint32
in_len, in uint32 out_vec, in uint32 out_len) -> psa_status_t
}
psa_status_t psa_call(psa_handle_t handle,
uint32_t in_vec, uint32_t in_len, uint32_t
out_vec, uint32_t out_len);
Status update

Supported

- Single M33 supported for TFM + Zephyr
  - TFM integrated

- Dual Zephyr on dual core
  - MHU IPM/openAMP
  - PR 17553

In Progress

- TFM + Zephyr on dual core
  - openAMP
  - eRPC

Demo Friday
What is ‘PSA Certified’?

- Indicates compliance with Arm’s PSA
- Independently evaluated suite of security tests and requirements
- Results in a unique ID associated with a chip, RTOS release, or OEM product
PSA Certified Levels

- There are currently three ‘PSA Certified’ levels:

  - PSA Certified Level 1
    Based on a security questionnaire filled out by the chip vendor, RTOS vendor or OEM. Minimal baseline of security best practices. ~1 day lab time.

  - PSA Certified Level 2
    Lab-based penetration testing against specific threats and risks. Aimed at chip vendors. ~25 days lab time.

  - PSA Certified Level 3
    In development, but will cover extensive device penetration testing.
Level 1 Questionnaire

- Questionnaire can be downloaded at https://www.psacertified.org/resources/
- Self-completed by
  - Chip vendors
  - RTOS vendors
  - OEMs.
- Questionnaire submitted to lab for verification

### 5 Assessment Questionnaire – For RTOS Vendors

For Chip Vendors or OEMs, skip this Section.

#### 5.1 Code Integrity

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Response</th>
<th>Yes</th>
<th>Part.</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1.1</td>
<td>The RTOS and updateable PSA-RoT supports firmware update, either from local connectivity (such as USB or removable media) or from remote servers. N.B: Verification of integrity and authenticity for local update is not mandatory for the first products that will be evaluated in 2019. If the RTOS supports updates from remote servers, all updates received from remote servers are validated locally to check integrity and authenticity prior installation. This includes manifest, executable code and any related data, such as configuration data. (Describe how updates are validated, including the cryptographic algorithms used, and where are stored the cryptographic keys used for validation) Example of response for Yes: The RTOS relies on TF-M firmware upgrade based on swapping method. The new firmware image is downloaded from RTOS on stored in bootloader slot 1 (slot 0 is the active firmware) and marked for update. At the next boot, the bootloader measures and validates the update and swaps slot 1 and slot 0.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R1.2</td>
<td>The update mechanism shall prevent firmware downgrade and protect current firmware version in a secure storage, such as anti-rollback counter in protected flash or OTP. N.B: This requirement is not mandatory for the first products that will be evaluated in 2019. (Describe the firmware versioning information used to detect firmware downgrade and how it is protected in integrity and against decrease and overflow) Example of response for Yes: In the process described in answer for R1.1, the RTOS verifies firmware version before storing the new image in slot 1. The current version of firmware is stored using secure storage service from TF-M.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Certification Outcomes

- Certification ID issued by test lab
- Device/RTOS listed on psacertified.org
Current Status of PSA Certified Level 1 Zephyr

- Sample PSA Certified Level 1 application available (Zephyr PR 18185)
  - Merge pending changes upstream to TF-M repo
  - Integrates upstream TF-M repo into Zephyr build system
  - Uses BL2 Secure Bootloader (BL2, fork of mcuboot)
    - Single Core
    - Dual Core with a single flash image
    - Dual MCU not currently handled on NS side
- RTOS vendor questionnaire will be provided as a reference
- Verification in progress with independent lab
Thank you

Join Linaro to accelerate deployment of your Arm-based solutions through collaboration

contactus@linaro.org