Open Source Secure world software

Trusted Firmware

Update June 2019
Following TF-M v1.0-RC1 tag created end of May’19 for PSA Level2 certification, following have been merged:
- SPE Preemption by NSPE
- Secure IRQ Support
- Updates for mbedcrypto 1.1.0

Added support for MPS3 AN524 FPGA platform.

Dual CPU support with Level1 Isolation made available in feature-twincpu branch.

Design posted in mailing list for Internal Trusted Storage and HW key usage in secure boot.
TF-M Roadmap

Q1’19
- Library Mode,
- L1 Isolation, Cert.
- PSA APIs, IPC

Q2’19
- L2 Isolation, Cert,
- Secure Boot Roll Back protection,
- IPC Compatibility,
- mbedcrypto,
- NS Interrupt,
- Dual v7-M feature branch

Q3’19
- Memory Opt.,
- Mul. Image Update,
- Generic HAL API,
- Dual v7-M

Q4’19
- Scheduler,
- Crypto HW,
- PSA API 1.0.0

Q1’20 +
- Provisioning,
- Secure Debug,
- Platform Services,
- Scheduler,
- Crypto HW,
- PSA API 1.1,
- Secure Boot Std.
Trusted Firmware-A – June ’19 Progresses

- Architecture enablement under development
  - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  - Armv8.4 Secure EL2 SPM SPCI-based investigation
- Armv8.5 Branch Target Identifier (BTI) support completed (needs GCC>9)
- GICv3 Driver updates for multi socket GIC redistributor discovery
- Platform Security Requirements under development
  - Attestation and Measured Boot reference flow
  - Multiple Signing Domains and separate Chain of Trust
- Investigations in other areas
  - PSA for IoT A-class devices
  - New I/O Layer support
  - New Build system
TF-A SPM evolution

- **Legacy SP/SPM MM based**
  - S-EL0 Single Partition for UEFI Standalone MM services based (Legacy MM)

- **Building blocks for future use-cases**
  - S-EL2 SPM DI
    - Resource description
    - CoT update / Multiple Signing domains

- **Client Enterprise Auto/Embed Use-cases**
  - S-EL2 SPM SPCI-based SMMU support
    - Pre-8.4: SPCI
    - OP-TEE + PSA TAs
    - Secure Firmware Update

- **Architecture Secure virtualization**
  - New Arch support

Timeline:
- 2018
- 2019
- 2020
- 2021+
Open Source Firmware Conference

- Trusted Firmware sponsoring the **OSFC** Conference
  - 3-6 September 2019 - @Google/Facebook premises
  - [https://osfc.io/sponsors/trusted-firmware](https://osfc.io/sponsors/trusted-firmware)

- Trusted Firmware & standardised open source Firmware on Arm talk scheduled on Tuesday 3rd Sept, 5:15pm

- Trusted Firmware sponsoring the **ELC, Lyon** (Oct 28-30, 2019)
TrustedFirmware TF-A Project Dashboard

Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>marek.vasut+renesas</td>
<td>74</td>
</tr>
<tr>
<td>john.tsichritzis</td>
<td>21</td>
</tr>
<tr>
<td>yann.gautier</td>
<td>12</td>
</tr>
<tr>
<td>ambroise.vincent</td>
<td>8</td>
</tr>
<tr>
<td>paul.beesley</td>
<td>7</td>
</tr>
<tr>
<td>soby.mathew</td>
<td>7</td>
</tr>
<tr>
<td>muhammad.hadi</td>
<td>4</td>
</tr>
<tr>
<td>afd</td>
<td>3</td>
</tr>
<tr>
<td>samuel</td>
<td>2</td>
</tr>
</tbody>
</table>

Commits by domain this month

- gmail.com: 50.7%
- arm.com: 32.0%
- st.com: 8.9%
- aholland.org: 1.3%
- intel.com: 2.7%
- ti.com: 2.0%

Commit history

Commits vs Month

- 2018-09: 150
- 2018-11: 100
- 2019-01: 200
- 2019-03: 100
- 2019-05: 100
TrustedFirmware TF-M Project Dashboard

Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>david.hu</td>
<td>13</td>
</tr>
<tr>
<td>jamie.fox</td>
<td>7</td>
</tr>
<tr>
<td>mate.toth-pal</td>
<td>7</td>
</tr>
<tr>
<td>ainhs</td>
<td>5</td>
</tr>
<tr>
<td>antonio.deangelis</td>
<td>4</td>
</tr>
<tr>
<td>chris.brand</td>
<td>4</td>
</tr>
<tr>
<td>edison.ai</td>
<td>3</td>
</tr>
<tr>
<td>tamas.ban</td>
<td>2</td>
</tr>
<tr>
<td>lgl</td>
<td>2</td>
</tr>
</tbody>
</table>

Commits by domain this month

Commit history

Commits vs Month

Month


Commits
TrustedFirmware TF-A Tests Project Dashboard

Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>sandrine.bailleux</td>
<td>8</td>
</tr>
<tr>
<td>soby.mathew</td>
<td>1</td>
</tr>
<tr>
<td>john.tsichritzis</td>
<td>1</td>
</tr>
<tr>
<td>madhukar.pappireddy</td>
<td>1</td>
</tr>
<tr>
<td>ambroise.vincent</td>
<td>1</td>
</tr>
</tbody>
</table>

Commits by domain this month (Arm only)

Commits vs Month

Commit history