Open Source Secure world software

Trusted Firmware

Update May 2019

SPONSORED BY: arm
HOSTED BY: Linaro
Trusted Firmware

Open governance Community Project since October 2018

Reference implementation of Secure world software for Armv7 & Armv8 architectures (both A/M-Profiles)

Membership of the Trusted Firmware project is open to all

Everyone interested in Trusted Firmware is encouraged to join

Members (May ‘19)

- Arm
- Cypress
- Data I/O
- Google
- Linaro
- Texas Instruments
- STMicroelectronics
Trusted Firmware-M - May 2019 Progress

- TF-M v1.0-RC1 tag created supporting features required for PSA Level2 certification
- New features in the tag
  * PSA Firmware Framework IPC Support
  * Secure Storage, Crypto and Attestation Services working in IPC mode
  * PSA Level2 Isolation
  * mbedcrypto used in the crypto service.
  * Rollback protection in Secure boot.
- Dual CPU enablement in progress -
  https://git.trustedfirmware.org/trusted-firmware-m.git/?h=feature-twincpu
- Continuous Integration Testing of TF-M patches using MPS2 board -
  https://ci.trustedfirmware.org/
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,
- Interrupt Handling

Q3’19
- Secure Storage – Use Hardware Key
- Memory Optimization,
- Multiple Image Update,
- Generic HAL API,
- Dual CPU Support
- PSA API 1.0.0

Q4’19
- Scheduler,
- Crypto Accelerator Integration

Q1’20 +
- Provisioning,
- Secure Debug,
- Platform Services,
- Scheduler
Trusted Firmware-A – May ’19 Progresses

- Architecture enablement under development
  - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  - Armv8.5 Branch Target Identifier (BTI)
  - Armv8.4 Secure EL2 SPM SPCI-based
- Fixed errata for Neoverse-N1 & Cortex-A76
- New platform support: MediaTek mt8183
- 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
TF-A SPM evolution

- **Legacy SP/SPM MM based**
- **S-EL0 Single Partition for UEFI StandaloneMM services based on MM Interface**
- **Building blocks for future use-cases**
- **Client Enterprise Auto/Embed Use-cases**
- **Armv8.4 S-EL2 virtualization extension support with reference SPM implementation SPCI-based**
- **Future architecture support**

Migration path for existing Armv8.2 & v8.3 systems towards Armv8.4+
TrustedFirmware TF-A Project Dashboard

Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>paul.beesley</td>
<td>22</td>
</tr>
<tr>
<td>soby.mathew</td>
<td>16</td>
</tr>
<tr>
<td>john.tsichritzis</td>
<td>13</td>
</tr>
<tr>
<td>sandrine.bailleux</td>
<td>12</td>
</tr>
<tr>
<td>antonio.ninodiaz</td>
<td>6</td>
</tr>
<tr>
<td>leonard.crestez</td>
<td>5</td>
</tr>
<tr>
<td>christophm30</td>
<td>4</td>
</tr>
<tr>
<td>sami.mujawar</td>
<td>4</td>
</tr>
<tr>
<td>alexei.fedorov</td>
<td>4</td>
</tr>
</tbody>
</table>

Commits by domain this month

- arm.com: 81.0%
- baylibre.com: 1.0%
- ti.com: 2.0%
- linaro.org: 3.0%
- gmail.com: 4.0%
- npx.com: 7.0%

Commits vs Month

Commit history

![Graph showing commit count per month from 2018-07 to 2019-03](image-url)
Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>edison.ai</td>
<td>14</td>
</tr>
<tr>
<td>tamas.ban</td>
<td>14</td>
</tr>
<tr>
<td>jamie.fox</td>
<td>13</td>
</tr>
<tr>
<td>david.vincze</td>
<td>10</td>
</tr>
<tr>
<td>antonio.deangelis</td>
<td>10</td>
</tr>
<tr>
<td>chris.brand</td>
<td>9</td>
</tr>
<tr>
<td>mingyang.sun</td>
<td>7</td>
</tr>
<tr>
<td>summer.qin</td>
<td>7</td>
</tr>
<tr>
<td>ashutosh.singh</td>
<td>5</td>
</tr>
</tbody>
</table>

Commits by domain this month

Commit history
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>6</td>
</tr>
<tr>
<td>john.tsichritzis</td>
<td>3</td>
</tr>
</tbody>
</table>

Commits by domain this month (Arm only)

Commits vs Month

Commit history