Open Source Secure World Software

Trusted Firmware

Update April 2019

SPONSORED BY:
HOSTED BY:
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 (April ‘19)

- Arm
- Cypress
- Data I/O
- Google
- Huawei
- Linaro
- Texas Instruments
- STMicroelectronics
Linaro Connect BKK19

Check out the Project presentation update held at Linaro Connect BKK19 in early April

https://connect.linaro.org/resources/bkk19/bkk19-216/

TF-M 1st Birthday Cake!
Trusted Firmware-M - April 2019 Progress

- Celebrated first birthday at Linaro Connect BKK’19
- Initial PSA Level 2 Isolation enabled
- PSA Firmware framework IPC Support for Protected Storage merged, IPC support for Attestation Service under review
- Attestation EAT support completed
- Design proposal for Secure Boot Rollback protection and Non-Secure Interrupt support posted
- Dual CPU enablement in progress
- Open CI Rollout - Jenkins job to create build artifact based on gerrit submissions in place - [https://ci.trustedfirmware.org/](https://ci.trustedfirmware.org/). Next step is to run the build on MPS2 board
TF-M Roadmap

- **Q1’19**: Library Mode, L1 Isolation, Cert, PSA APIs, IPC
- **Q2’19**: L2 Isolation, Cert, Roll Back protection, IPC Compatibility, mbedcrypto, NS Interrupt, Dual v7-M feature branch
- **Q3’19**: Scheduler, HAL API, Crypto HW, Crypto Binding
- **Q4’19**: Provisioning, Secure Debug, Platform Services
Trusted Firmware-A – April 2019 Progresses

● v2.1 TF-A & TF-A-Tests release highlights (read full article)
  ○ Armv8.3 Pointer Authentication enabled for Normal world
  ○ Armv8.4 Data Independent Timing and Small Translation Tables support
  ○ Armv8.5 PSTATE.SSBS Speculation Store Bypass Safe (on Cortex-A76 & Neoverse-N1)
  ○ New Arm Platforms support
    ■ Neoverse N1 Edge (RD-N1-Edge) FVP & N1SDP HW Platform
    ■ Neoverse E1 Edge (RD-E1-Edge) FVP
    ■ Neoverse Zeus core initial support
  ○ Dynamic Configuration – Position Independent Executable support for BL31

● TF-A now fully migrated to new Git/Gerrit infrastructure:
  ○ https://git.trustedfirmware.org/TF-A/trusted-firmware-a.git/about/
  ○ https://review.trustedfirmware.org/
Trusted Firmware-A – What’s on

- Architecture enablement
  - Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  - Armv8.5 Branch Target Identifier (BTI)

- Platform Security Requirements
  - Attestation and Measured Boot reference flow
  - Multiple Signing Domains and separate Chain of Trust

- Investigations in other areas
  - PSA for IoT A-class devices
  - Debug Certificates and Arm Debug IPs support
  - Functional Safety requirements
TF-A SPM evolution

- **Legacy SP/SPM MM based**
- S-EL0 Single Partition for UEFI StandaloneMM services based on MM Interface
- Resource description
- CoT update / Multiple Signing domains
- Architecture
- Secure virtualization
- Multiple S-EL0 and S-EL1 (with TOS migration)
- Secure Partitions SPCI-based
- Migration path for existing Armv8.2 & v8.3 systems towards Armv8.4+
- Building blocks for future use-cases
- Enterprise IoT/Edge Auto/Embed Use-cases
- Armv8.4 S-EL2 virtualization extension support with reference SPM implementation
TrustedFirmware TF-A Project Dashboard

Top Authors this month

- antonio.ninodiaz: 33
- afd: 13
- heiko: 11
- marek.vasut+renesas: 9
- ambroise.vincent: 9
- soby.mathew: 7
- joel.hutton: 7
- louis.mayencourt: 6

Commits by domain this month

Commit history

Commits vs Month

Month

- 2018-05
- 2018-07
- 2018-09
- 2018-11
- 2019-01
- 2019-03
TrustedFirmware TF-M Project Dashboard

Top Authors this month

<table>
<thead>
<tr>
<th>Author</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>edison.ai</td>
<td>19</td>
</tr>
<tr>
<td>tamas.ban</td>
<td>7</td>
</tr>
<tr>
<td>hugues.devalon</td>
<td>7</td>
</tr>
<tr>
<td>ken.liu</td>
<td>6</td>
</tr>
<tr>
<td>lgl</td>
<td>5</td>
</tr>
<tr>
<td>antonio.deangelis</td>
<td>5</td>
</tr>
<tr>
<td>summer.qin</td>
<td>4</td>
</tr>
<tr>
<td>jamie.fox</td>
<td>3</td>
</tr>
<tr>
<td>kevin.peng</td>
<td>3</td>
</tr>
</tbody>
</table>

Commits by domain this month

commit history

Commits vs Month

Commit history

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>antonio.ninodiaz</td>
<td>7</td>
</tr>
<tr>
<td>joel.hutton</td>
<td>2</td>
</tr>
<tr>
<td>sandrine.bailleux</td>
<td>2</td>
</tr>
</tbody>
</table>

Commits by domain this month (Arm only)

Commits vs Month

Commit history
How to Get Involved

Become a project member

Platinum Board (voting) members define the mission and strategy: $50K/year

General members receive project updates, make requests to the board and may attend monthly calls: $2.5-25K*/year

Maintainers to be appointed from members

* Fee according to company size and type

Contact:

enquiries@TrustedFirmware.org

for more information