Open Source Secure World Software

Trusted Firmware

Update January 2019
Trusted Firmware

Trusted Firmware adopted open governance in October 2018

Reference implementation of secure world software for Armv8-A and Armv8-M

Membership of the Trusted Firmware project is open to all

Everyone interested in Trusted Firmware is encouraged to join

Members (January ‘19)

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

- Provides Software Components for building a Secure Platform providing
  - Isolated Secure execution environment for Arm v7-M and v8-M
  - Secure services invoked from Non-Secure apps
  - Trusted device initialisation and Trusted boot
- Reference Implementation of Arm Platform Security Architecture (PSA)
  - Aimed at Constrained Devices
  - Flexible and Configurable design allowing Partners to adapt to meet their needs
  - Different levels of Isolation, Leverages Trustzone in v8-M.
- Initial implementation of Secure Boot, Secure Storage, Crypto, Attestation and Audit Logs available
Trusted Firmware-M – Jan’19

● PSA Firmware Framework IPC implemented. Merging to TF-M master in Progress

● Arm/Cypress Collaboration kicked off to enable TF-M for dual v7-M/pSoC6

● Attestation Service implementing EAT (Entity Attestation Token) Protocol published.

● Aligning Secure Storage, Crypto and Attestation Secure Services to PSA Developer APIs.
● New Arm IoT Reference Platform, MuscaB1e support added
● PSA Level 2 Isolation Design to be available in next few weeks.
## Trusted Firmware-M Plan

### Q1’19 (Jan-Mar’19)
- [TF-M Core] Secure Partition Manager- Level 2 Isolation
- [TF-M Core] Scheduler Design, Interrupt Handling Enhancements
- [Secure Storage] Compatible with PSA Firmware Framework IPC
- Dual v7-M Prototype
- Open Continuous Integration (CI) System

### Q2’19 (Apr-Jun’19)
- [Attestation] EAT Enhancements
- [Platform] Secure Time
- Secure Debug Investigation
- [Provisioning] Initial Investigation/API Prototype
- Dual v7-M Support

### Q2’19 (Apr-Jun’19)
- [TF-M Core] Full Isolation Support, Scheduler Initial Implementation
- [Secure Boot] Rollback Protection, Multiple Image Update
- [Secure Storage] Extended PSA APIs
- [Crypto] Use FF IPC, Hardware Crypto Accelerator
- [Platform] NV Count, Timer, Secure Time

### Q3’19 (Jul-Sep’19)
- [TF-M Core] Scheduler Enhancements
- [Secure Boot] Key Revocation
- [Secure Storage] Lifecycle Management
- [Platform] GPIO, Debug, NONCE
- Secure Debug Prototype
Trusted Firmware-A – January ‘19 Progresses

- v2.1 release planning started
  - Code freeze mid-March
  - Release March/April (around Linaro Connect BKK’19)
- Armv8.5 PSTATE.SSBS enablement completed
- Armv8.3 PAC & Armv8.5 BTI ongoing - Targeting v2.1
- Secure Partitions
  - Reviewing new SPCI version and planning Foundation work (Resource description)
  - Legacy MM based partitions support
- CVE-2018-19440 mitigation against information leakage from one Normal World SMC client to another
- Platforms support:
  - Intel Stratix 10 SoC FPGA
Trusted Firmware-A – Plans for H1/H2 2019

- Secure Partitions
  - Resource Description and Secure Partitions Chain of Trust support
  - Multiple S-EL0, S-EL1 coexistence & TOs integration support (H1/H2.2019)
- Armv8.5 Memory Tagging Extensions at EL3
- Platform Security Requirements investigation
  - Measured Boot, [Discrete/Firmware] TPM & Storage/Crypto interactions
  - Dynamic configuration and Secure world → Normal world information passing
- Trusted Firmware-A migration to new TrustedFirmware.org infrastructure
  - Phase 2 (Q1.2019): TF-A codebase migration from GitHub to Git/Gerrit → Ongoing
  - Phase 3 (~Q2.2019): CI migration - Continuous Build open-source infrastructure
  - Phase 4 (Q2/Q3.2019): CI migration - Continuous Testing on FVPs + LAVA board farm
TrustedFirmware Project Activity

Trusted Firmware Commits by Month

* To January 31, 2019
TrustedFirmware TF-A Project Activity

Domains by Commits for January 2019

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>102</td>
</tr>
<tr>
<td>nvidia.com</td>
<td>83</td>
</tr>
<tr>
<td>gmail.com</td>
<td>35</td>
</tr>
<tr>
<td>xilinx.com</td>
<td>29</td>
</tr>
<tr>
<td>nxp.com</td>
<td>15</td>
</tr>
<tr>
<td>st.com</td>
<td>13</td>
</tr>
<tr>
<td>linaro.org</td>
<td>12</td>
</tr>
<tr>
<td>ti.com</td>
<td>8</td>
</tr>
<tr>
<td>Arm.com</td>
<td>4</td>
</tr>
<tr>
<td>debian.org</td>
<td>2</td>
</tr>
</tbody>
</table>

Generated 2019-02-05

- Total Files: 1983
- Total Lines of Code: 334392 (542996 added, 208604 removed)
- Total Commits: 4844 (average 4.0 commits per active day, 2.5 per all days)
- Total Authors: 199 (average 24.3 commits per author)
### Top 10 authors for January 2019

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antonio Niño Díaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>57</td>
</tr>
<tr>
<td>Varun Wadekar</td>
<td><a href="mailto:vwadekar@nvidia.com">vwadekar@nvidia.com</a></td>
<td>38</td>
</tr>
<tr>
<td>Marek Vasut</td>
<td><a href="mailto:marek.vasut+renesas@gmail.com">marek.vasut+renesas@gmail.com</a></td>
<td>32</td>
</tr>
<tr>
<td>Jolly Shah</td>
<td><a href="mailto:jollys@xilinx.com">jollys@xilinx.com</a></td>
<td>29</td>
</tr>
<tr>
<td>Antonio Nino Diaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>24</td>
</tr>
<tr>
<td>Anthony Zhou</td>
<td><a href="mailto:anzhou@nvidia.com">anzhou@nvidia.com</a></td>
<td>20</td>
</tr>
<tr>
<td>Anson Huang</td>
<td><a href="mailto:Anson.Huang@nxp.com">Anson.Huang@nxp.com</a></td>
<td>14</td>
</tr>
<tr>
<td>Yann Gautier</td>
<td><a href="mailto:yann.gautier@st.com">yann.gautier@st.com</a></td>
<td>13</td>
</tr>
<tr>
<td>Paul Beesley</td>
<td><a href="mailto:paul.beesley@arm.com">paul.beesley@arm.com</a></td>
<td>11</td>
</tr>
<tr>
<td>Harvey Hsieh</td>
<td><a href="mailto:hhsieh@nvidia.com">hhsieh@nvidia.com</a></td>
<td>7</td>
</tr>
</tbody>
</table>
TrustedFirmware TF-A-Tests Project Activity

Domains by Commits for January 2019

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>29</td>
</tr>
</tbody>
</table>

Generated 2019-02-05

- Total Files: 429
- Total Lines of Code: 51395 (55971 added, 4576 removed)
- Total Commits: 107 (average 2.3 commits per active day, 0.5 per all days)
- Total Authors: 7 (average 15.3 commits per author)
trustedfirmware TF-A-Tests project activity

Top 10 authors for January 2019

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandrine Bailleux</td>
<td><a href="mailto:sandrine.bailleux@arm.com">sandrine.bailleux@arm.com</a></td>
<td>21</td>
</tr>
<tr>
<td>John Tsichritzis</td>
<td><a href="mailto:john.tsichritzis@arm.com">john.tsichritzis@arm.com</a></td>
<td>4</td>
</tr>
<tr>
<td>Antonio Nino Diaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>4</td>
</tr>
</tbody>
</table>
Domains by Commits for January 2019

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>15</td>
</tr>
</tbody>
</table>

- **Total Files:** 572
- **Total Lines of Code:** 126715 (173167 added, 46452 removed)
- **Total Commits:** 289 (average 2.1 commits per active day, 0.7 per all days)
- **Total Authors:** 19 (average 15.2 commits per author)
TrustedFirmware TF-M Project Activity

Top 10 authors for January 2019

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mate Toth-Pal</td>
<td><a href="mailto:mate.toth-pal@arm.com">mate.toth-pal@arm.com</a></td>
<td>11</td>
</tr>
<tr>
<td>Jamie Fox</td>
<td><a href="mailto:jamie.fox@arm.com">jamie.fox@arm.com</a></td>
<td>2</td>
</tr>
<tr>
<td>Miklos Balint</td>
<td><a href="mailto:miklos.balint@arm.com">miklos.balint@arm.com</a></td>
<td>1</td>
</tr>
<tr>
<td>David Vincze</td>
<td><a href="mailto:david.vincze@arm.com">david.vincze@arm.com</a></td>
<td>1</td>
</tr>
</tbody>
</table>
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:

board@TrustedFirmware.org

for more information