Open Source Secure World Software

Trusted Firmware

Update November 2018
Trusted Firmware

Arm’s Trusted Firmware is adopting open governance

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

Initial Members

Arm
Cypress
Data I/O
Google
Linaro
Texas Instruments
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 and Audit Logs available
Trusted Firmware-M – Progress since YVR’18

- PSA Firmware Framework
  - IPC Implementation being done

- Initial Attestation Service
  - PSA API under review

- Secure IRQ Handling
  - Initial Implementation

- Support for latest Arm IoT Reference platform - Musca-B1

- PoC with mbedOS/Pelion Cloud and Zephyr/Google Cloud shown at ELC-E

- Presentations at ELC-E
Trusted Firmware-M Plan

- **Q4 2018**
  - Attestation - Initial Attestation Service
  - Scheduler Design
  - Crypto Service Enhancements
  - IPC Enhancements
  - Open Continuous Integration (CI)

- **Q1 2019**
  - Full Isolation (Level 2 & 3)
  - Scheduler Initial Implementation
  - Secure Boot - Multiple Image Update
  - Platform APIs - NVCount, Timer
  - Provisioning - Initial Investigation/API Prototype

- **Q2 2019**
  - Scheduler Enhancements
  - [Secure Boot] Key Revocation
  - [Secure Storage] Lifecycle Management
  - [Audit Logs] Secure Storage, Crypto Binding
  - [Platform] GPIO, Debug, NONCE
Trusted Firmware-A – Progresses since YVR’18

- Trusted Firmware-A Tests first open source release (v2.0)!
  - See detailed blogpost & project landing page on TF-A-Tests Git repository
  - BSD 3-clause license and contributions accepted under DCO as parent TF-A project

- TF-A codebase recent progresses:
  - Dynamic Configuration
    - Position Independent Executable (PIE) support for BL31 (enabled for FVPs)
  - Added option to jump straight to Linux Kernel in AArch32 mode without the need for an intermediate BL33 boot-loader (option already present in AArch64 mode)
  - Platforms support
    - Arm NeoVerse N1 System Development (N1SDP)
    - Arm SGI-Clark.Ares
    - Renesas R-Car Gen3
    - Amlogic Meson S905
    - Armada 3700
Trusted Firmware-A – Plans for Q4 2018 / H1 2019

- Plans for Q4 2018 / H1 2019:
  - Secure Partitions
    - Enhanced Secure Partition Manager for Multiple S-EL0 partitions
    - SPCI/SPRT Alpha/Beta specifications support
  - Trusted Firmware-A migration to new TrustedFirmware.org infrastructure
    - **Phase 1:** TF-A-Tests go live announcement under Git/Gerrit
      @trustedfirmware.org
    - Phase 2: TF-A codebase migration from GitHub to Git/Gerrit @trustedfirmware.org
    - Phase 3: CI migration from internal Arm infrastructure to trustedfirmware.org
  - SCMIv2 specification support
  - Armv8.x architectural features support
  - v2.1 Release (March 2019)
TrustedFirmware Project Activity

Trusted Firmware Commits by Month

- TF-A
- TF-M

May | June | July | August | September | October
TrustedFirmware TF-A Project Activity

Domains by Commits for October

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>163</td>
</tr>
<tr>
<td>baylibre.com</td>
<td>17</td>
</tr>
<tr>
<td>marvell.com</td>
<td>9</td>
</tr>
<tr>
<td>st.com</td>
<td>7</td>
</tr>
<tr>
<td>ti.com</td>
<td>4</td>
</tr>
<tr>
<td>linaro.org</td>
<td>4</td>
</tr>
<tr>
<td>socionext.com</td>
<td>2</td>
</tr>
<tr>
<td>semihalf.com</td>
<td>2</td>
</tr>
<tr>
<td>siemens.com</td>
<td>1</td>
</tr>
<tr>
<td>nvidia.com</td>
<td>1</td>
</tr>
</tbody>
</table>

Generated 2018-11-07

- Total Files: 1833
- Total Lines of Code: 309340 (491099 added, 181759 removed)
- Total Commits: 4308 (average 3.8 commits per active day, 2.3 per all days)
- Total Authors: 171 (average 25.2 commits per author)
## TrustedFirmware TF-A Project Activity

### Top 10 authors for October

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soby Mathew</td>
<td><a href="mailto:soby.mathew@arm.com">soby.mathew@arm.com</a></td>
<td>47</td>
</tr>
<tr>
<td>Antonio Nino Diaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>36</td>
</tr>
<tr>
<td>Andre Przywara</td>
<td><a href="mailto:andre.przywara@arm.com">andre.przywara@arm.com</a></td>
<td>21</td>
</tr>
<tr>
<td>Antonio Niño Díaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>18</td>
</tr>
<tr>
<td>Jorge Ramirez-Ortiz</td>
<td><a href="mailto:jramirez@baylibre.com">jramirez@baylibre.com</a></td>
<td>17</td>
</tr>
<tr>
<td>Konstantin Porotchkin</td>
<td><a href="mailto:kostap@marvell.com">kostap@marvell.com</a></td>
<td>9</td>
</tr>
<tr>
<td>Daniel Boulby</td>
<td><a href="mailto:daniel.boulby@arm.com">daniel.boulby@arm.com</a></td>
<td>9</td>
</tr>
<tr>
<td>Chandni Cherukuri</td>
<td><a href="mailto:chandni.cherukuri@arm.com">chandni.cherukuri@arm.com</a></td>
<td>9</td>
</tr>
<tr>
<td>Yann Gautier</td>
<td><a href="mailto:yann.gautier@st.com">yann.gautier@st.com</a></td>
<td>7</td>
</tr>
<tr>
<td>Dimitris Papastamos</td>
<td><a href="mailto:dimitris.papastamos@arm.com">dimitris.papastamos@arm.com</a></td>
<td>7</td>
</tr>
</tbody>
</table>
TrustedFirmware TF-M Project Activity

Domains by Commits for October

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>11</td>
</tr>
<tr>
<td>linaro.org</td>
<td>1</td>
</tr>
</tbody>
</table>

- Total Files: 511
- Total Lines of Code: 115461 (157417 added, 41956 removed)
- Total Commits: 227 (average 2.0 commits per active day, 0.7 per all days)
- Total Authors: 18 (average 12.6 commits per author)

Generated 2018-11-07
## TrustedFirmware TF-M Project Activity

### Top 10 authors for October

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antonio de Angelis</td>
<td><a href="mailto:antonio.deangelis@arm.com">antonio.deangelis@arm.com</a></td>
<td>4</td>
</tr>
<tr>
<td>David Vincze</td>
<td><a href="mailto:david.vincze@arm.com">david.vincze@arm.com</a></td>
<td>3</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>Marc Moreno Berengue</td>
<td><a href="mailto:marc.morenoberengue@arm.com">marc.morenoberengue@arm.com</a></td>
<td>1</td>
</tr>
<tr>
<td>Karl Zhang</td>
<td><a href="mailto:karl.zhang@linaro.org">karl.zhang@linaro.org</a></td>
<td>1</td>
</tr>
<tr>
<td>Alexander Zilberkant</td>
<td><a href="mailto:alexander.zilberkant@arm.com">alexander.zilberkant@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