Open Source Secure World Software

Trusted Firmware

Update December 2018

SPONSORED BY: arm
HOSTED BY: Linaro
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 (December ‘18)

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 – Nov/Dec’18

- PSA Firmware Framework
  - Initial implementation getting merged to feature-ipc

- Initial Attestation Service
  - PSA API merged
  - CBOR required for EAT in review

- Initial Implementation of Secure IRQ Handling

- Adding support for GCC7.3

- Demo with mbedOS/Pelion Cloud and Zephyr/Google Cloud shown at ELC-E posted here
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 – Nov/Dec ‘18 Progresses

- Trusted Firmware-A copyright headers updated to allow contributors using their own company/individual name in copyright notices (for new files or significant changes to existing files) - See announcement [here](#)

- Secure Partition Manager for Multiple S-EL0 partitions
  - Initial prototype for multiple S-EL0 partitions posted as a basis for further developments
  - Not to be used as-is, since not compliant yet with SPCI/SPRT specifications

- CVE_2018_3639 mitigation with Armv8.5 PSTATE.SSBS architectural feature

- CVE-2017-5753 initial mitigation to address potential speculative data leak found in PSCI code

- **Exception handling framework** and **RAS** documentation now available

- **Platforms support**
  - Arm SGI-Clark.Helios (multi-threaded platforms support)
  - NXP i.MX8MQ, Xilinx Versal ACAP
Trusted Firmware-A – Plans for 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
- Armv8.x architectural features support
- SCMIv2 specification support
- v2.1 Release (March 2019)
TrustedFirmware Project Activity

Trusted Firmware Commits by Month

* To November 30
TrustedFirmware TF-A Project Activity

Domains by Commits for November - December 15

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>118</td>
</tr>
<tr>
<td>st.com</td>
<td>12</td>
</tr>
<tr>
<td>gmail.com</td>
<td>12</td>
</tr>
<tr>
<td>marvell.com</td>
<td>10</td>
</tr>
<tr>
<td>chromium.org</td>
<td>6</td>
</tr>
<tr>
<td>linaro.org</td>
<td>5</td>
</tr>
<tr>
<td>nxp.com</td>
<td>3</td>
</tr>
<tr>
<td>akeo.ie</td>
<td>3</td>
</tr>
<tr>
<td>semihalf.com</td>
<td>2</td>
</tr>
<tr>
<td>edited.us</td>
<td>2</td>
</tr>
</tbody>
</table>

- Total Files: 1909
- Total Lines of Code: 318721 (504574 added, 185853 removed)
- Total Commits: 4476 (average 3.8 commits per active day, 2.4 per all days)
- Total Authors: 181 (average 24.7 commits per author)
# TrustedFirmware TF-A Project Activity

## Top 10 authors for November 1 - December 15

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antonio Nino Diaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>37</td>
</tr>
<tr>
<td>Antonio Niño Diaz</td>
<td><a href="mailto:antonio.ninodiaz@arm.com">antonio.ninodiaz@arm.com</a></td>
<td>34</td>
</tr>
<tr>
<td>Soby Mathew</td>
<td><a href="mailto:soby.mathew@arm.com">soby.mathew@arm.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>12</td>
</tr>
<tr>
<td>Chandni Cherukuri</td>
<td><a href="mailto:chandni.cherukuri@arm.com">chandni.cherukuri@arm.com</a></td>
<td>10</td>
</tr>
<tr>
<td>Marek Vasut</td>
<td><a href="mailto:marek.vasut+renesas@gmail.com">marek.vasut+renesas@gmail.com</a></td>
<td>9</td>
</tr>
<tr>
<td>Konstantin Porotchkin</td>
<td><a href="mailto:kostap@marvell.com">kostap@marvell.com</a></td>
<td>6</td>
</tr>
<tr>
<td>Julius Werner</td>
<td><a href="mailto:jwerner@chromium.org">jwerner@chromium.org</a></td>
<td>6</td>
</tr>
<tr>
<td>Sathees Balya</td>
<td><a href="mailto:sathees.balya@arm.com">sathees.balya@arm.com</a></td>
<td>4</td>
</tr>
<tr>
<td>Sandrine Bailleux</td>
<td><a href="mailto:sandrine.bailleux@arm.com">sandrine.bailleux@arm.com</a></td>
<td>4</td>
</tr>
</tbody>
</table>
TrustedFirmware TF-M Project Activity

Domains by Commits for November 1 - December 15

<table>
<thead>
<tr>
<th>Domains</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>arm.com</td>
<td>36</td>
</tr>
</tbody>
</table>

Generated 2018-12-17

- Total Files: 562
- Total Lines of Code: 120113 (163808 added, 43695 removed)
- Total Commits: 262 (average 2.1 commits per active day, 0.7 per all days)
- Total Authors: 18 (average 14.6 commits per author)
Top 10 authors for November 1 - December 15

<table>
<thead>
<tr>
<th>Author</th>
<th>Email</th>
<th>Commits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamas Ban</td>
<td><a href="mailto:tamas.ban@arm.com">tamas.ban@arm.com</a></td>
<td>15</td>
</tr>
<tr>
<td>Marc Moreno Berengue</td>
<td><a href="mailto:marc.morenoberengue@arm.com">marc.morenoberengue@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>3</td>
</tr>
<tr>
<td>Antonio de Angelis</td>
<td><a href="mailto:antonio.deangelis@arm.com">antonio.deangelis@arm.com</a></td>
<td>3</td>
</tr>
<tr>
<td>Miklos Balint</td>
<td><a href="mailto:miklos.balint@arm.com">miklos.balint@arm.com</a></td>
<td>2</td>
</tr>
<tr>
<td>Mate Toth-Pal</td>
<td><a href="mailto:mate.toth-pal@arm.com">mate.toth-pal@arm.com</a></td>
<td>1</td>
</tr>
<tr>
<td>Avinash Mehta</td>
<td><a href="mailto:avinash.mehta@arm.com">avinash.mehta@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