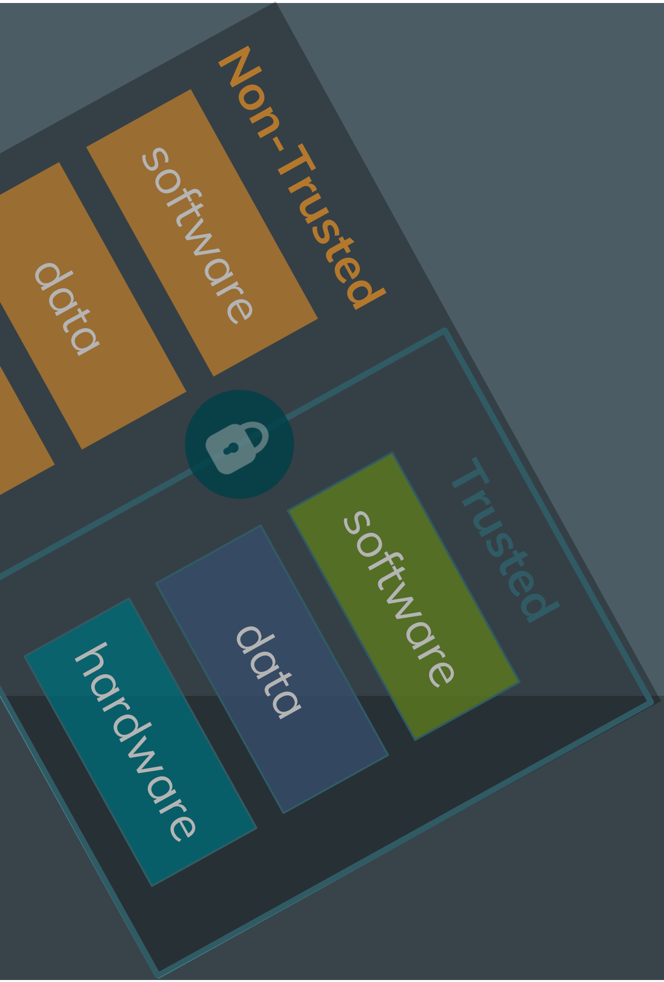


Open Source Secure World Software

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

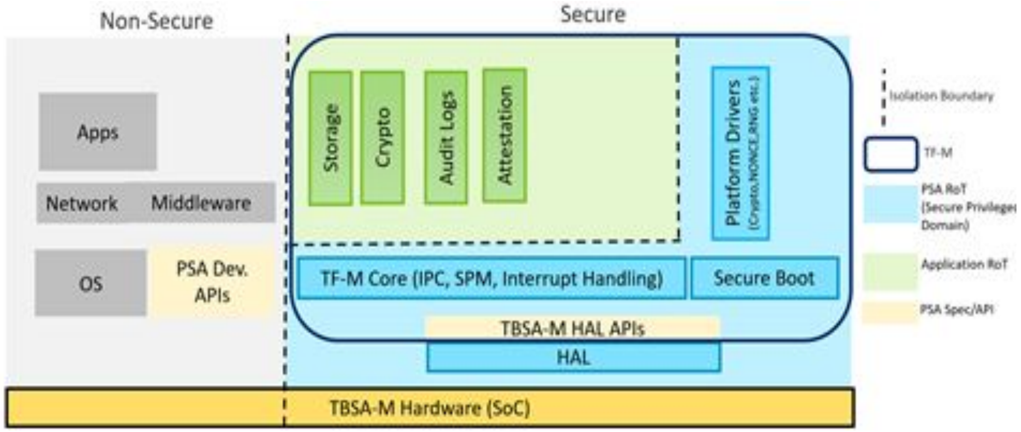
Texas Instruments

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

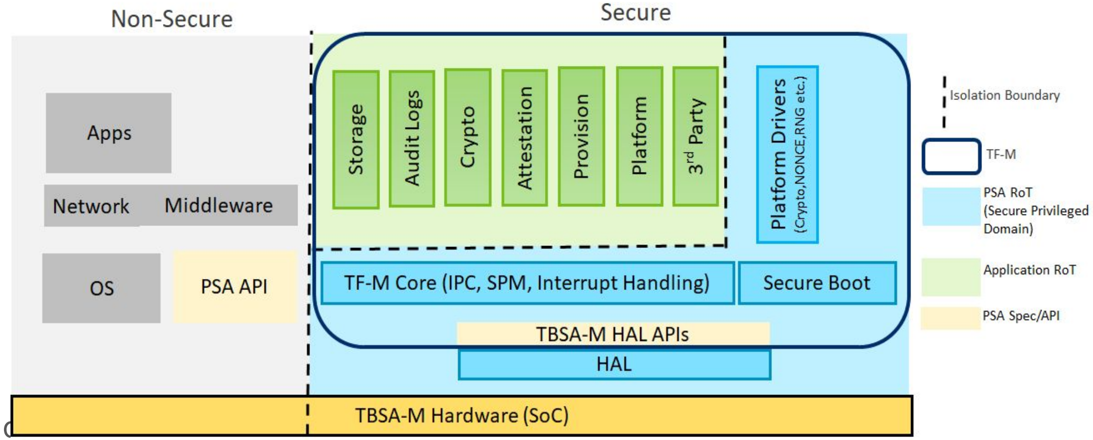
- Initial Implementation of Secure IRQ Handling

- 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 Upd
  - 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



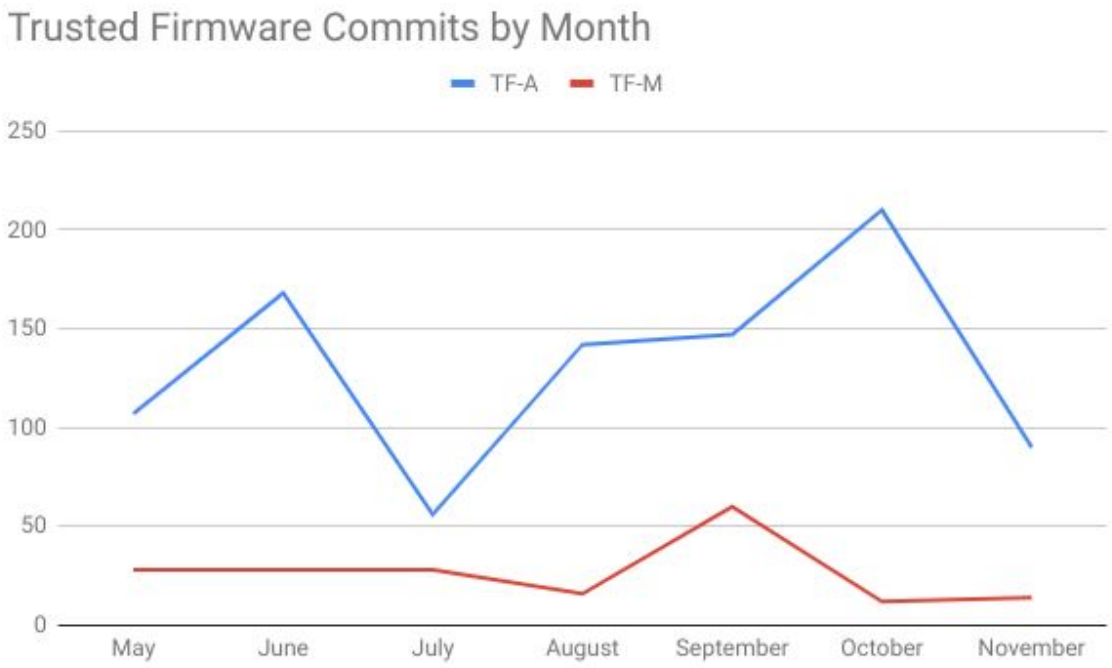
Trusted Firmware-A – Nov/Dec ‘18 Progresses

- 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



* To November 30

TrustedFirmware TF-A Project Activity

Domains by Commits for November - December 15

Domains	Commits
arm.com	118
st.com	12
gmail.com	12
marvell.com	10
chromium.org	6
linaro.org	5
nxp.com	3
akeo.ie	3
semihalf.com	2
edited.us	2

Generated 2018-12-17

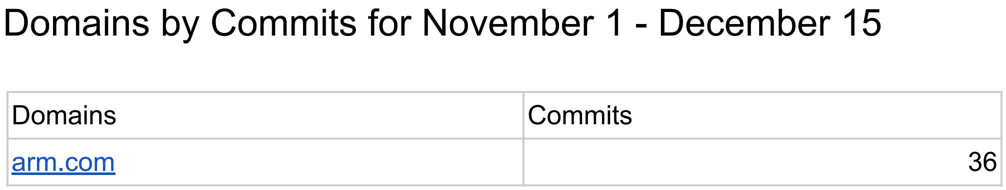
- Total Files: 1909
- Total Lines of Code: 318721 (504574 added, 185853 removed)
- Total Commits: 4476 (average 3.8 commits per active day, 2.4 per all days)
- Total Authors: 181 (average 24.7 commits per author)

TrustedFirmware TF-A Project Activity

Top 10 authors for November 1 - December 15

Author	Email	Commits
Antonio Nino Diaz	antonio.ninodiaz@arm.com	37
Antonio Niño Díaz	antonio.ninodiaz@arm.com	34
Soby Mathew	soby.mathew@arm.com	14
Yann Gautier	yann.gautier@st.com	12
Chandni Cherukuri	chandni.cherukuri@arm.com	10
Marek Vasut	marek.vasut+renesas@gmail.com	9
Konstantin Porotchkin	kostap@marvell.com	6
Julius Werner	jwerner@chromium.org	6
Sathees Balya	sathees.balya@arm.com	4
Sandrine Bailleux	sandrine.bailleux@arm.com	4

TrustedFirmware TF-M Project Activity



Domains by Commits for November 1 - December 15

Domains	Commits
arm.com	36

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)

TrustedFirmware TF-M Project Activity

Top 10 authors for November 1 - December 15

Author	Email	Commits
Tamas Ban	tamas.ban@arm.com	15
Marc Moreno Berengue	marc.morenoberengue@arm.com	11
Jamie Fox	jamie.fox@arm.com	3
Antonio de Angelis	antonio.deangelis@arm.com	3
Miklos Balint	miklos.balint@arm.com	2
Mate Toth-Pal	mate.toth-pal@arm.com	1
Avinash Mehta	avinash.mehta@arm.com	1

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

Contact:

board@TrustedFirmware.org

for more information

* Fee according to company size and type

TrustedFirmware
.org