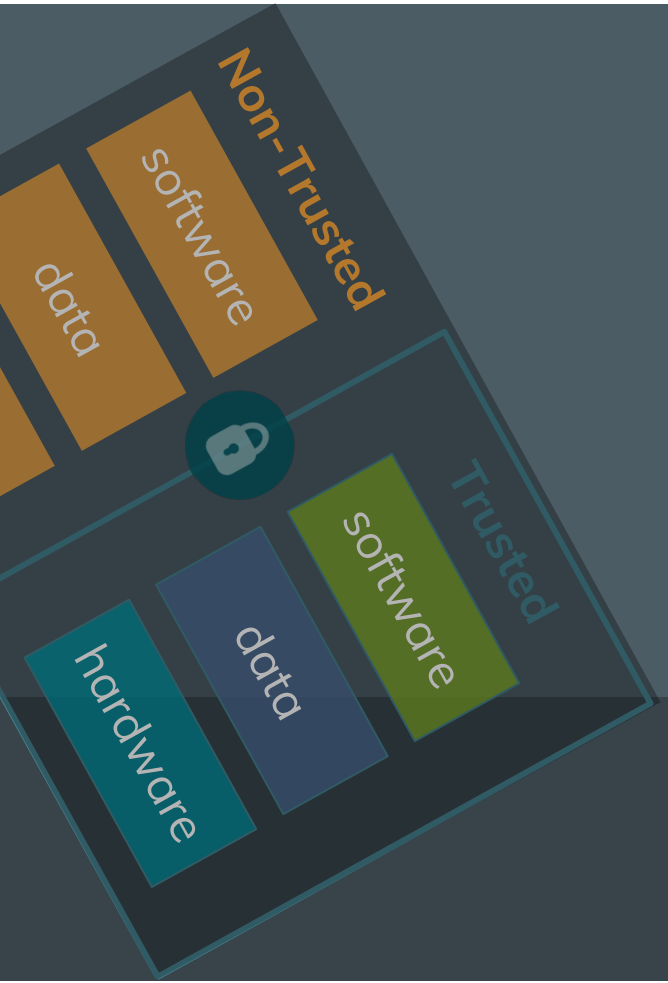


Open Source Secure World Software

Trusted Firmware

Update January 2019

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 (January ‘19)

Arm

Cypress

Data I/O

Google

Linaro

Texas Instruments

STMicroelectronics

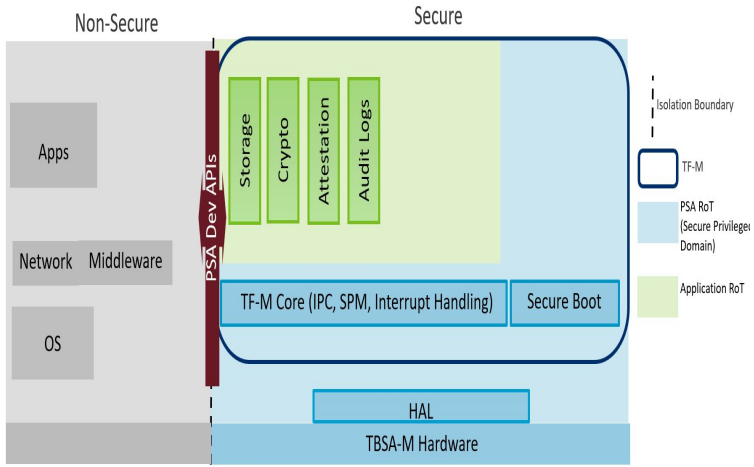
TrustedFirmware.org

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)

- [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

Q2'19 (Apr-Jun'19)

- [Attestation] EAT Enhancements
- [Platform] Secure Time
- Secure Debug Investigation
- [Provisioning] Initial Investigation/API Prototype
- Dual v7-M Support

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

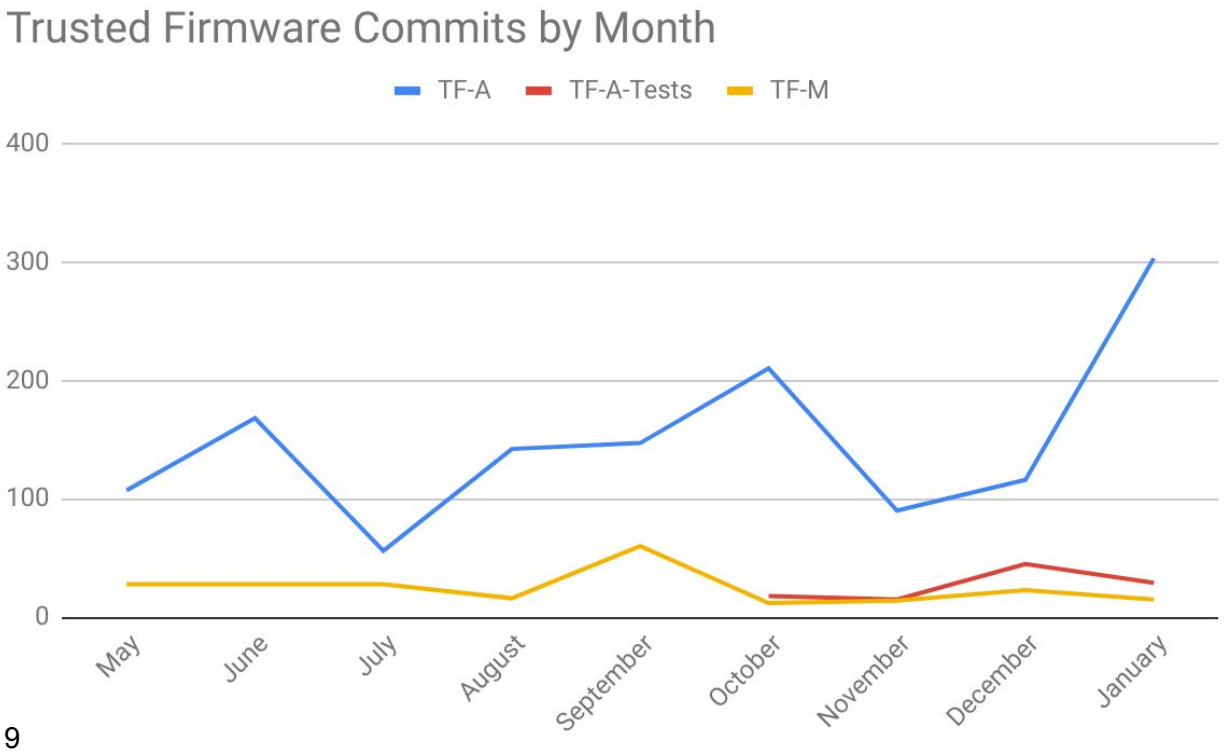
Trusted Firmware-A – January ‘19 Progresses

- 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 1 (Q4.2018): TF-A-Tests go live announcement under Git/Gerrit → Completed**
  - **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



* To January 31, 2019

TrustedFirmware TF-A Project Activity

Domains by Commits for January 2019

Domains	Commits
arm.com	102
nvidia.com	83
gmail.com	35
xilinx.com	29
nxp.com	15
st.com	13
linaro.org	12
ti.com	8
Arm.com	4
debian.org	2

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)

TrustedFirmware TF-A Project Activity

Top 10 authors for January 2019

Author	Email	Commits
Antonio Niño Díaz	antonio.ninodiaz@arm.com	57
Varun Wadekar	vwadekar@nvidia.com	38
Marek Vasut	marek.vasut+renesas@gmail.com	32
Jolly Shah	jollys@xilinx.com	29
Antonio Nino Diaz	antonio.ninodiaz@arm.com	24
Anthony Zhou	anzhou@nvidia.com	20
Anson Huang	Anson.Huang@nxp.com	14
Yann Gautier	yann.gautier@st.com	13
Paul Beesley	paul.beesley@arm.com	11
Harvey Hsieh	hhsieh@nvidia.com	7

TrustedFirmware TF-A-Tests Project Activity

Domains by Commits for January 2019

Domains	Commits
arm.com	29

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

Author	Email	Commits
Sandrine Bailleux	sandrine.bailleux@arm.com	21
John Tsichritzis	john.tsichritzis@arm.com	4
Antonio Nino Diaz	antonio.ninodiaz@arm.com	4

TrustedFirmware TF-M Project Activity

Domains by Commits for January 2019

Domains	Commits
arm.com	15

Generated 2019-02-05

- 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

Author	Email	Commits
Mate Toth-Pal	mate.toth-pal@arm.com	11
Jamie Fox	jamie.fox@arm.com	2
Miklos Balint	miklos.balint@arm.com	1
David Vincze	david.vincze@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

* Fee according to company size and type

Contact:

board@TrustedFirmware.org

for more information

TrustedFirmware.org