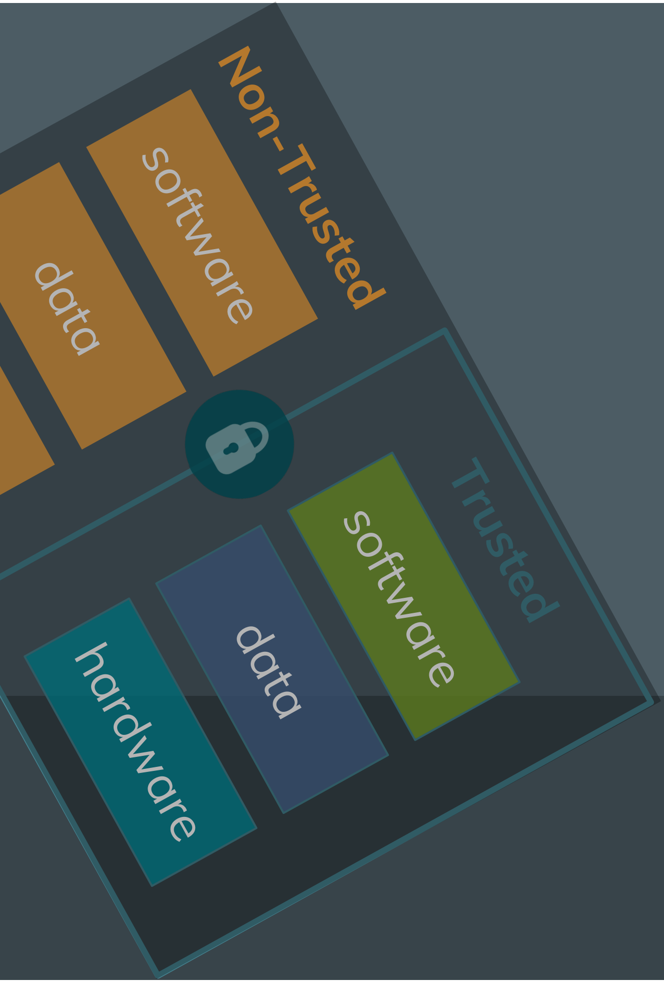


Non-Trusted

software

data

Trusted

software

data

hardware

Open Source Secure World Software

Trusted Firmware

Update October 2018

SPONSORED BY:

arm

HOSTED BY:

Linaro

Trusted Firmware with Open Governance

Membership of the Trusted Firmware project is open to all

Governance overseen by a board of member representatives

Stakeholders in Trusted Firmware are encouraged to join

Arm’s Trusted Firmware is adopting Open Governance

Public announcement on Oct 16th and first Board meeting on Oct 31st

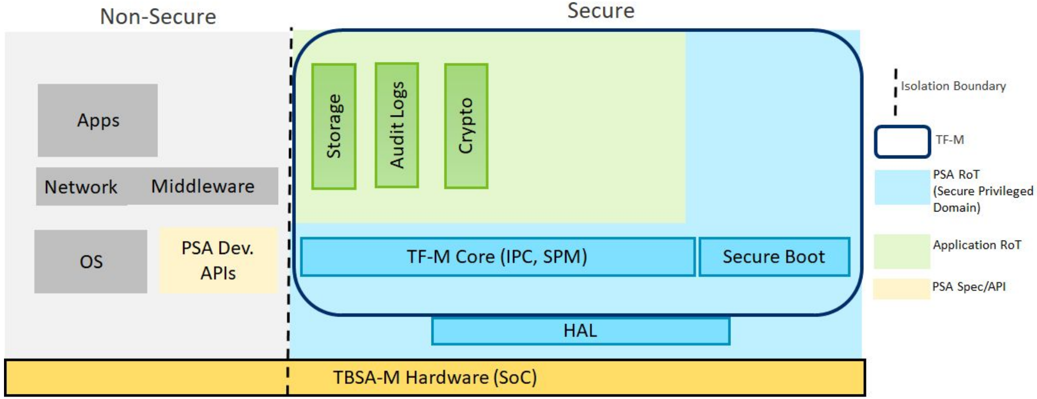
TrustedFirmware .org

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 and Audit Logs available

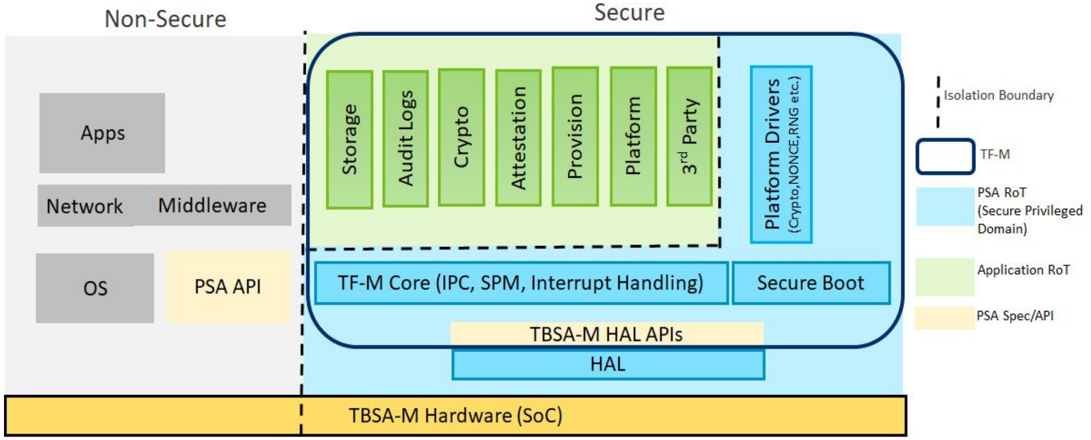
Trusted Firmware-M – Progress since June 2018

- IPC Prototype in TF-M Core
  - Based on PSA Firmware Framework
- Crypto Secure Service
  - PSA APIs
  - PSK-TLS Support
- Secure Storage
  - Key Diversification
- Audit Logs
  - Enhancements to API and implementation
- Secure Boot
  - Rollback protection
  - External Storage



Trusted Firmware-M Plan

- Q4 2018
  - Attestation - Initial PSA API and Initial Attestation Service
  - IRQ Handling
  - 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 – Progress since June 2018

- v1.6 and v2.0 recently released!
    - See detailed blogpost & new TF-A Release Information page
- v1.6 (Sept 21st) highlights:
    - Support for v8.2 RAS extensions (ESB) and v8.4 RAS extensions (Fault Injection)
    - v8.4 MPAM (Memory Partitioning And Monitoring) EL3 enablement
    - CVE-2018-3639 workaround
    - Arm Cortex-A cores support: Cortex-Ares, Cortex-A76, Cortex-Deimos, Cortex-Helios
    - Add dynamic configurations for BL31, BL32 and BL33 and support for Chain of Trust
    - Platforms support:
        - Arm SGI-575 & Arm SGM-775,
        - Allwinner, NXP, TI, Socionext, Marvell and STM platforms support
- v2.0 (Oct, 2nd) highlights:
    - Removal of deprecated APIs
    - Checkout new TF-A Platform compatibility policy & Trusted Firmware-A Porting Guide

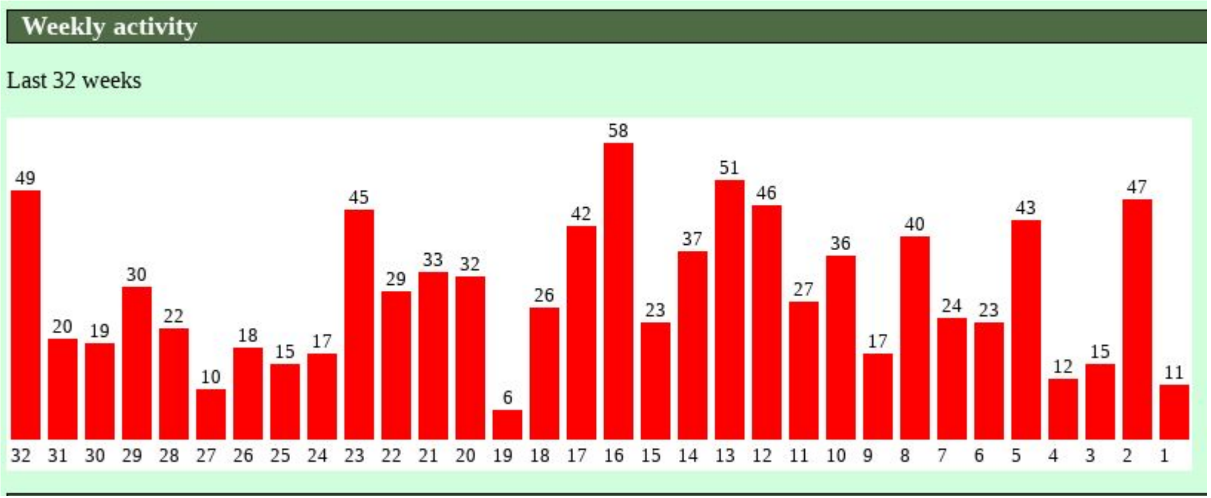
Trusted Firmware-A – Plans for Q4 2018 / H1 2019

- Trusted Firmware-A celebrates 5 years of open source presence on GitHub on October 25th 2018 - see Linaro Connect presentation

- Plans for Q4 2018 / H1 2019:
    - TF-A-Tests open source
    - Secure Partitions
        - Enhanced Secure Partition Manager for Multiple S-EL0 partitions
        - SPCI/SPRT specifications support
    - Dynamic Configuration
        - Advanced configuration options / Position Independent Executables
    - Trusted Firmware-A migration to new TF.org infrastructure
    - SCMIv2 specification support
    - Armv8.x architectural features support
    - v2.1 Release (March 2019)

TrustedFirmware TF-A Project Activity

Generated 2018-10-02



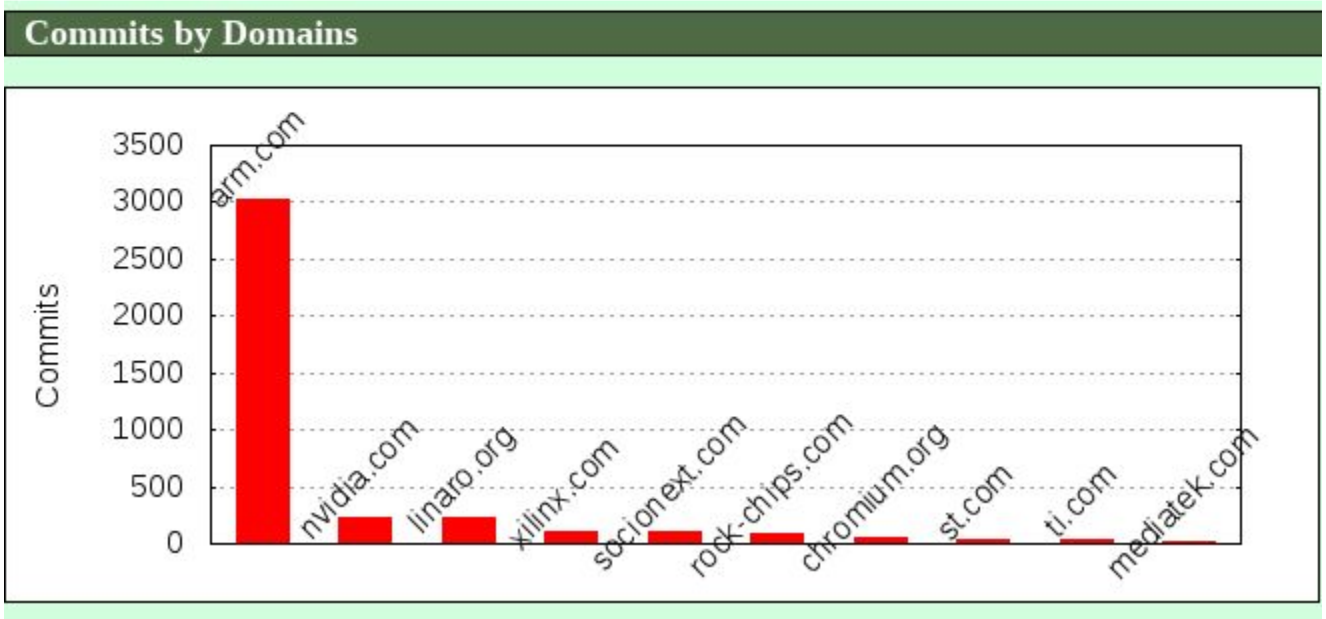
Weekly activity

Last 32 weeks

- Total Files
  1600
- Total Lines of Code
  251108 (426681 added, 175573 removed)
- Total Commits
  4081 (average 3.7 commits per active day, 2.3 per all days)
- Authors
  165 (average 24.7 commits per author)

TrustedFirmware TF-A Commits by Domain

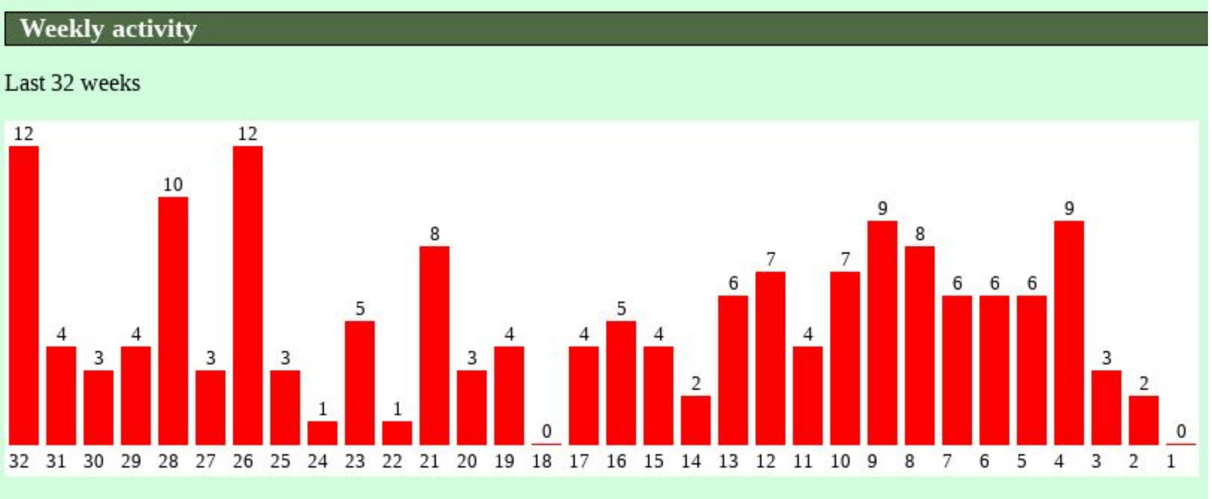
Generated 2018-10-02



Commits by Domains

TrustedFirmware TF-M Project Activity

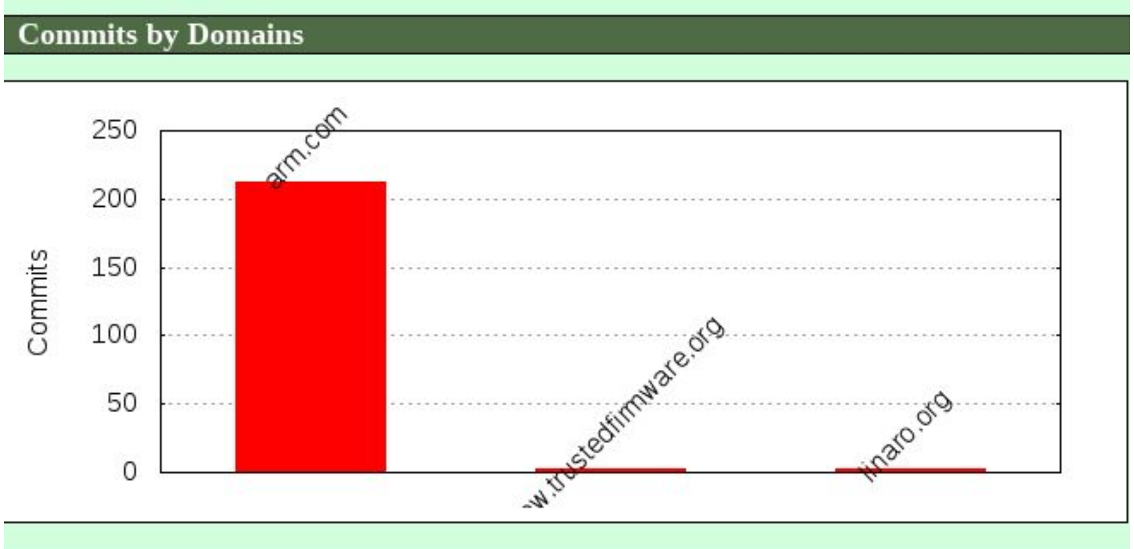
Generated 2018-10-02



- Total Files
  432
- Total Lines of Code
  96432 (138190 added, 41758 removed)
- Total Commits
  216 (average 2.0 commits per active day, 0.7 per all days)
- Authors
  16 (average 13.5 commits per author)

TrustedFirmware TF-M Commits by Domain

Generated 2018-10-02



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