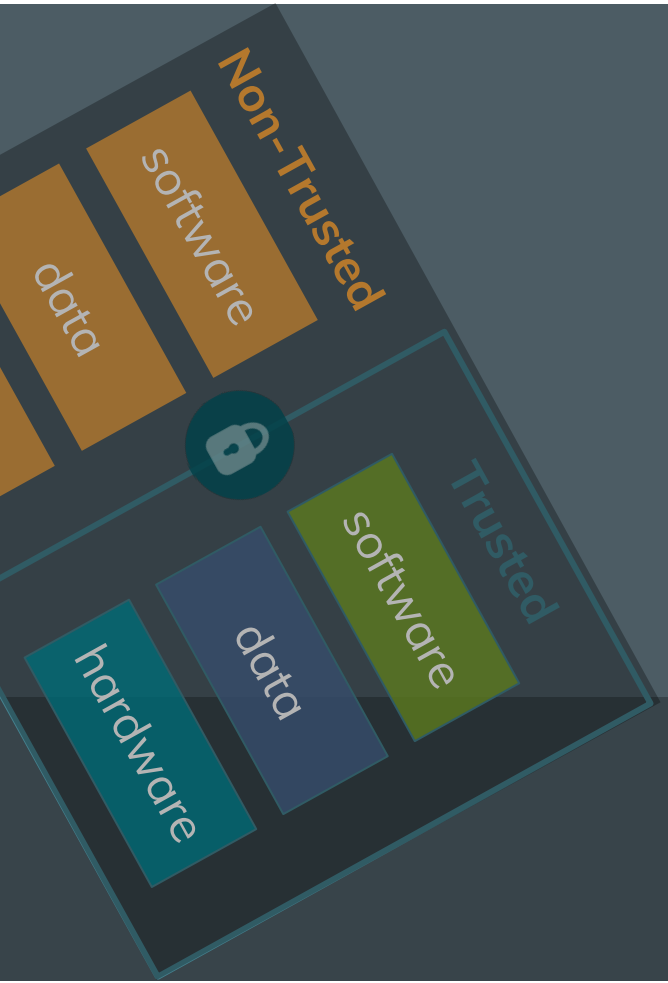


Open Source Secure World Software

Trusted Firmware

Update June 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*

* Subject to the project achieving a viable level of membership

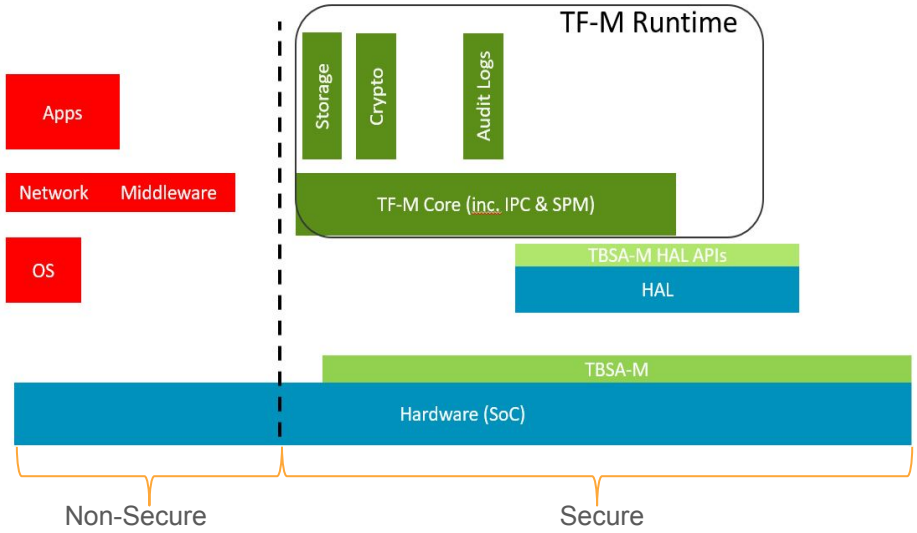
TrustedFirmware.org

Trusted Firmware-M

- Provides Software Components for building a Secure Platform providing
  - Isolated Secure execution environment
  - Secure services invoked from Non-Secure apps
  - Trusted device initialisation and Trusted boot
- Reference Implementation of Arm’s Platform Security Architecture
  - Aimed at Constrained Devices
  - Flexible and Configurable design allowing Partners to adapt to meet their needs
  - Different levels of Isolation
- Launched at HKG’18 Linaro Connect
  - Initial prototype of Secure Boot and Secure Storage

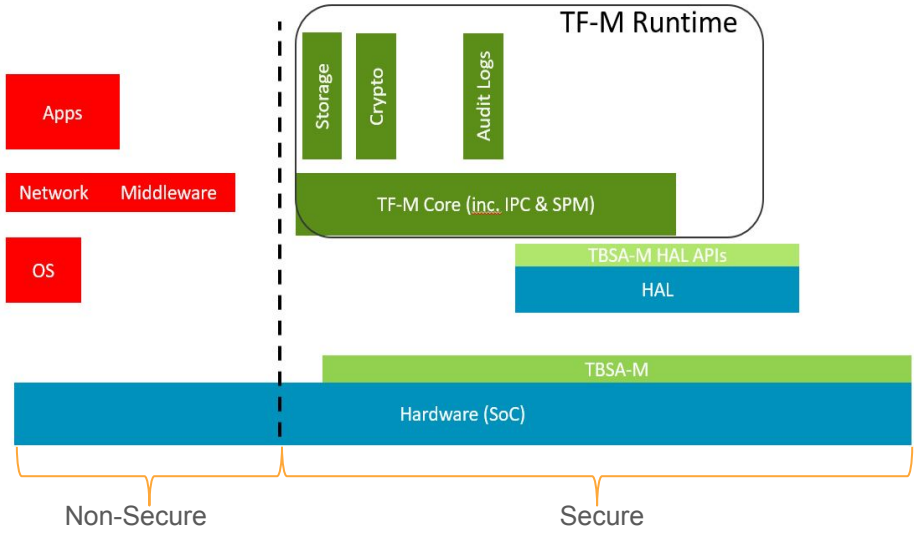
Trusted Firmware-M – Progress since HKG'18

- Secure Boot Enhancements
  - Avoid image swapping during upgrade
  - Position Independent Boot
- TF-M Core
  - Secure Partition Manager Enhancements
- Secure Storage
  - Use CMSIS Flash Driver for Storage
  - Integration Guide & Test Improvements
- Audit Logs
  - Initial implementation allowing secure partitions to log their security critical events
- Crypto
  - Initial Investigation



Trusted Firmware-M Plan - Q4’18

- Secure Boot Enhancements
  - Secure and Non-Secure image update separately
- TF-M Core
  - IPC Support
- Secure Storage
  - Key Diversification
  - Rollback protection
- Audit Logs
  - Encryption and Secure Storage of Logs
- Crypto
  - Initial Prototype supporting TLS
- Attestation
  - Initial Support - GP Token
- Provisioning
  - Initial Prototype
- TBSA Platform
  - Timer, Debug, GPIO



Trusted Firmware-A – Progress since HKG'18

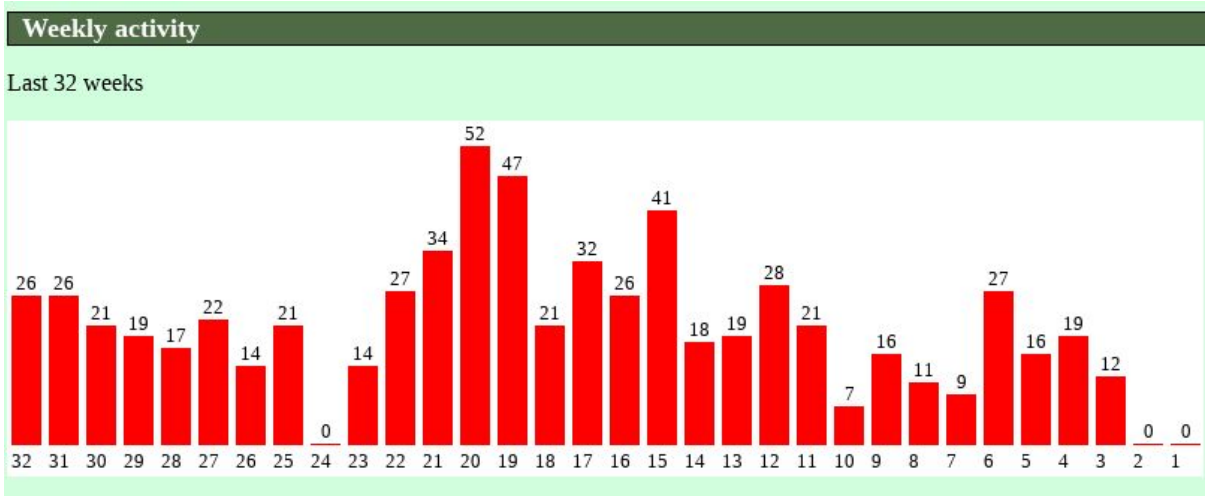
- Arm Cortex-A76 and Cortex-Ares support
- Dynamic Configuration updates
  - Firmware configs are now supported for BL31, BL32 and BL33 within the Chain of Trust
  - Dynamic disable of authentication during boot for development purposes
- RAS support
  - External aborts and RAS EL3 handling
- Functional Safety
  - Additional fixes of MISRA non-compliances
- Google Project Zero: CVE-2018-3639 workaround for affected Arm Cortex cores
- Partners update: NXP i.MX8QX SoC support

Trusted Firmware-A – Plans for H2 2018

- Dynamic Configuration
  - Advanced configuration options
  - Position Independent Executables
- Secure Partitions
  - Enhanced Secure Partition Manager for Multiple S-EL0 partitions
  - SPCI/SPRT specifications support
- Functional Safety
  - Additional fixes of MISRA non-compliances

TrustedFirmware TF-A Project Activity

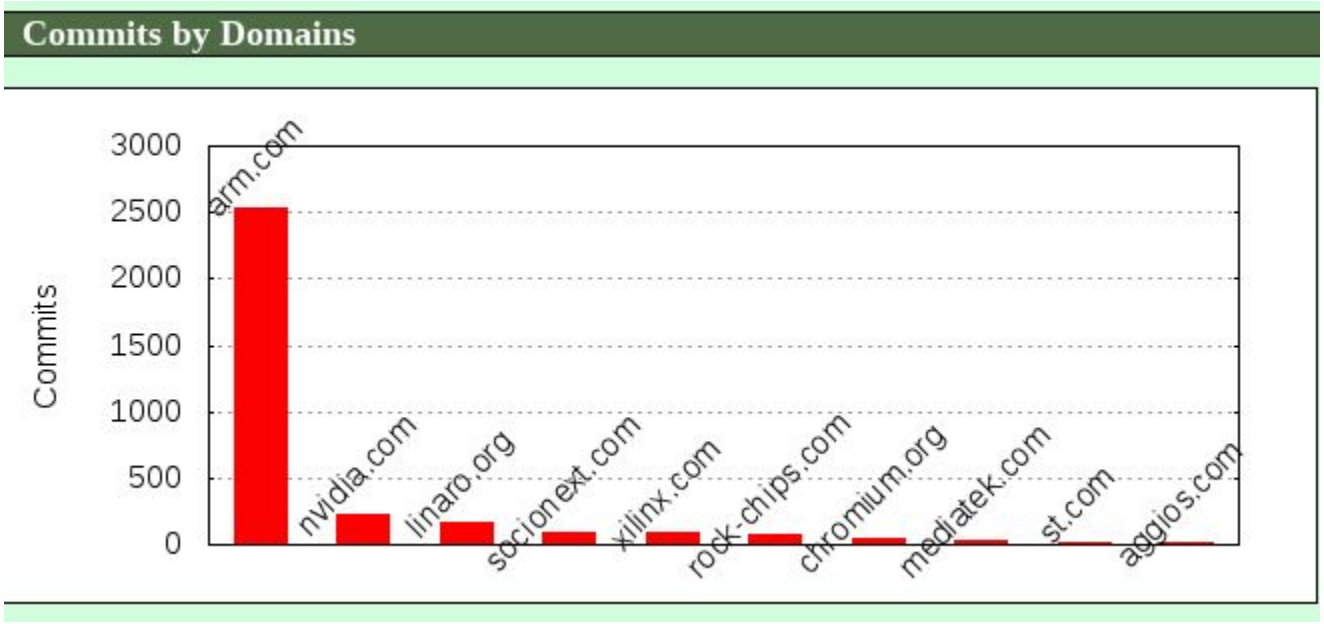
Generated 2018-06-01



- Total Files
  1251
- Total Lines of Code
  204011 (352560 added, 148549 removed)
- Total Commits
  3369 (average 3.4 commits per active day, 2.0 per all days)
- Authors
  137 (average 24.6 commits per author)

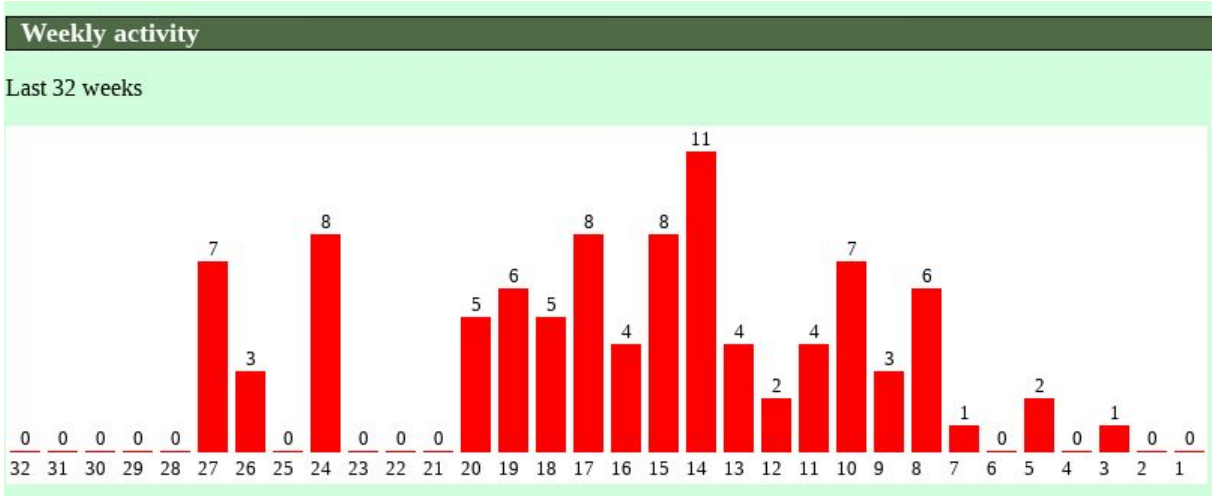
TrustedFirmware TF-A Commits by Domain

Generated 2018-06-01



TrustedFirmware TF-M Project Activity

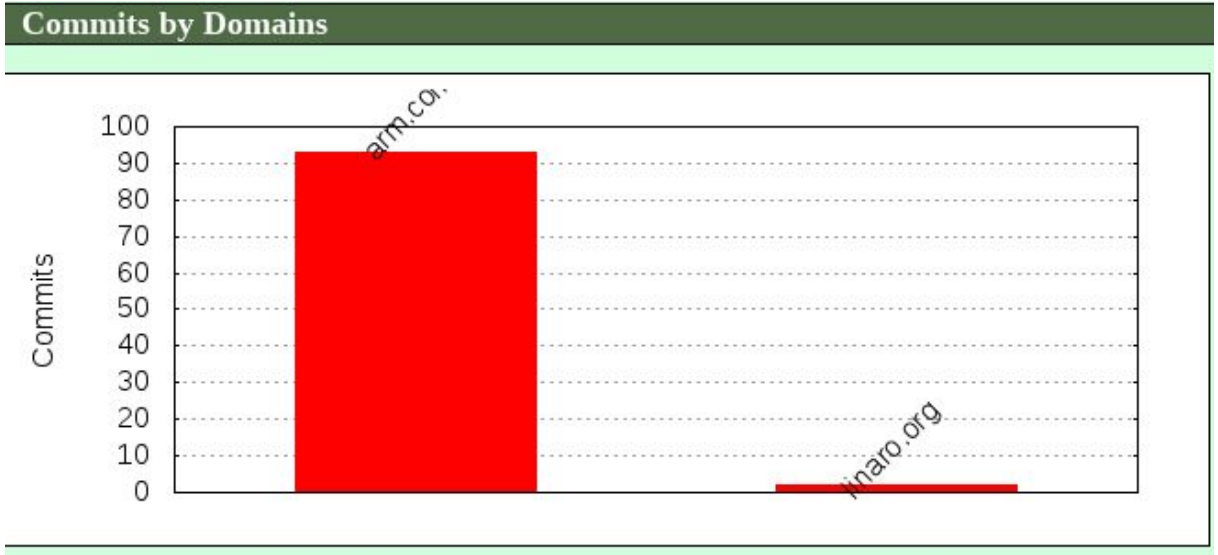
Generated 2018-06-01



- Total Files
  343
- Total Lines of Code
  73340 (91627 added, 18287 removed)
- Total Commits
  95 (average 1.9 commits per active day, 0.6 per all days)
- Authors
  11 (average 8.6 commits per author)

TrustedFirmware TF-M Commits by Domain

Generated 2018-06-01



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