Trusted Firmware: Build Security Collaboratively

Open Governance Community Project

Reference open source implementation of Secure software for Arm processors across all market segments

Membership open to all

Board

Technical Steering Committee
Current members

Diamond Members
arm  Google  ST

Platinum Members
CYPRESS  Linaro  NXP  Renesas

General Members
FUTUREWEI  NXM

Partners
bugSeng
<table>
<thead>
<tr>
<th>Member Benefits: Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>🏛️ Governing Board seat driving strategic direction and investments</td>
</tr>
<tr>
<td>(Budget, Marketing Initiatives, explore new investment areas)</td>
</tr>
<tr>
<td>✔️ Part of Technical Steering Committee driving technical direction of project</td>
</tr>
<tr>
<td>(Define Release process, Security Incident Handling process, Roadmaps reviews &amp; influence)</td>
</tr>
<tr>
<td>🐴 Add and maintain platforms in Open CI (<a href="#">Refer to the “Open CI &amp; Board Farm” slide</a>)</td>
</tr>
<tr>
<td>👯‍♀️ Opportunity for close engineering collaboration with other members</td>
</tr>
<tr>
<td>🏦 Refer “Membership Structure” slide for details on membership tiers and benefits</td>
</tr>
</tbody>
</table>
The Virtuous Circle Of Collaboration!

- Mailing Lists
- Tech Forums
- Workshop
- Open Collaboration
- Open Reviews
- Open Source
- Open CI

Links:
- https://www.trustedfirmware.org/meetings/
- https://git.trustedfirmware.org/
- https://ci.trustedfirmware.org/
- https://review.trustedfirmware.org/
- https://www.trustedfirmware.org/blog/
Current Projects

- TF-A
- OP-TEE
- Hafnium

- TF-M
- Mbed TLS
- Trusted Services
Build Security Collaboratively

- Security by Scale
- Complexity solved once for all
- Shared Ownership
- Faster TTM & Reduced Cost
- Less Individual Maintenance & Minimised TCO
All market segments

- Devices
- IoT/Mobile/Auto/Laptop
- Embedded
- Edge
- Cloud
- Server
Open CI & Board Farm

Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

LAVA
validation.linaro.org

Push 1

TF.org Patch

Trigger 2

Trigger 3

Artifacts

Jenkins

Build Slaves

Result +1

MPS2

Juno

Member boards

https://tf.validation.linaro.org/scheduler/device_types
Trusted Firmware Security Center

New centralized Security incident process

https://developer.trustedfirmware.org/w/collaboration/security_center/

● Have you found a security vulnerability in Trusted Firmware?
  → Report it here: security@lists.trustedfirmware.org

● Coordinated disclosure with Trusted Stakeholders and ESS
  ○ https://developer.trustedfirmware.org/w/collaboration/security_center/trusted_stakeholder_registration/

● Per-project security email aliases
  ○ https://developer.trustedfirmware.org/w/collaboration/security_center/mailing_aliases/
Trusted Firmware-A

Secure world reference software for all Arm Cortex-A & Neoverse processors across all market segments.

Trusted boot flow and runtime firmware providing standard implementation of Arm specifications:

- SMCCC (SMC Calling Convention)
- TBBR (Trusted Board Boot Requirements)
- PSCI (Power State Coordination Interface)
- SCMI (System Control & Management Interface)
- FF-A (Firmware Framework for A-Profile)
TF-A-Tests

https://trustedfirmware-a-tests.readthedocs.io/en/latest/

A suite of bare-metal functional tests to exercise TF-A features from the Normal World, without dependencies on a Rich OS.

It provides a strong basis for TF-A developers to validate their own platform ports and add their own test cases, interacting with TF-A through its SMC interface.

Features currently tested include:

- SMC Calling Convention
- Power State Coordination Interface (PSCI)
- Software Delegated Exception Interface (SDEI)
- Performance Measurement Framework (PMF)
- Trusted Board Boot Requirements (TBBR)
- Secure Partition Manager (SPM) … and lots more!
Trusted Firmware-M

Implements the Secure Processing Environment (SPE) for Armv8-M, Armv8.1-M architectures. It is the platform security architecture reference implementation aligning with PSA Certified guidelines.

It consists of Secure Boot and a set of Secure Services such as Secure Storage, Crypto, Attestation, Firmware update, for Applications accessible via PSA Functional APIs.
OP-TEE

A reference implementation of a Trusted Execution Environment (TEE), designed as companion to a non-secure Linux kernel running on Arm Cortex-A cores using the TrustZone technology.

Implements TEE Internal Core API v1.1.x and the TEE Client API v1.0, as defined in the GlobalPlatform API specifications.
**Mbed TLS**

- Portable, highly modular, easy-to-use TLS and X.509 library
- Extensively used in various market segments
- Distributed under Apache2.0 License
- Components –
  - Cryptography
  - Protocol (TLS, DTLS)
  - Certificates (X.509, PKI)
- PSA Crypto (Mbed Crypto), derived from Mbed TLS library, brings together Crypto primitives and makes them available via PSA Crypto APIs.
- PSA Crypto also support driver interfaces to integrate with Secure Elements and Crypto Accelerators.
Trusted Services

- Framework to develop Security related Services

- Deployable over range of Isolated Processing Environments (e.g., Secure EL0 Partitions under OP-TEE, Secure Partition under Hafnium.)

- Applications access Trusted Services for Security Operations via a standardized service layer

- Includes PSA Trusted Services for Cryptography, Storage and Attestation
Arm CCA: Open Source Software enablement

https://connect.linaro.org/resources/arm-cca/

Brand new open source component

Dynamic Secure memory support
Arm CCA: More resources

- Introducing the TF-A Monitor code for the Arm CCA architecture
- CCA Awakens on Arm’s Modelling Platform
- LVC21F-311 Overview of Firmware Architecture for Arm CCA
## Membership Structure

<table>
<thead>
<tr>
<th></th>
<th>Diamond</th>
<th>Platinum</th>
<th>General</th>
<th>Community (Uni/Non-profit)</th>
<th>Individual (invite only)</th>
<th>Non-Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Access, Review Participation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical Forums</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Logo and marketing recognition (scaled per tier)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Technical Steering Committee (TSC) seat + vote</td>
<td>Yes (2 votes each)</td>
<td>Yes (1 vote each)</td>
<td>Yes (1 vote every 5)</td>
<td>Yes (1 vote every 5)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Governing Board seat + vote</td>
<td>Yes (2 votes each)</td>
<td>Yes (1 vote each)</td>
<td>Yes* (1 vote every 5)*</td>
<td>Yes (1 vote every 5)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Boards in Open CI</td>
<td>2 new / year</td>
<td>1 new / year</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Fees</td>
<td>$100k</td>
<td>$50k</td>
<td>G1: $2.5K G2: $10K G3: $25k</td>
<td>$2.5K</td>
<td>$500</td>
<td>No</td>
</tr>
</tbody>
</table>

*: Only for G2 & G3 General members
G1: $2.5K (0 to 50 empl. only)
G2: $10k (0-499)
G3: $25k (500+)

Additional benefits will be evaluated and revisited for future investment topics (MISRA, LTSs, …) when it happens
Adopt Trusted Firmware to build your next secure platform

Visit www.TrustedFirmware.org or email enquiries@trustedfirmware.org for more information

Thank you