Trusted Firmware
Central Engineering - Open Source Software
Matteo Carlini, Shebu Varghese Kuriakose, James King

Linaro Connect – Vancouver
September 2018
Contents

• Update on Open Source Project
• Update on TF-A
• Update on TF-M
• A small celebration 😊
TRUSTED Firmware
OPEN SOURCE SECURE WORLD SOFTWARE

Learn More
## Trusted Firmware for M profile Arm CPUs

### Files

<table>
<thead>
<tr>
<th>Mode</th>
<th>Name</th>
<th>Size</th>
<th>Log</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>r-w-</td>
<td>.gitignore</td>
<td>243</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-</td>
<td>BuildMbedTLS.cmake</td>
<td>4100</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-</td>
<td>CMakeLists.txt</td>
<td>513</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-x-r-x</td>
<td>CommonConfig.cmake</td>
<td>7446</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>ConfigCoreTest.cmake</td>
<td>1265</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-x-r-x</td>
<td>ConfigDefault.cmake</td>
<td>1408</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-x-r-x</td>
<td>ConfigRegression.cmake</td>
<td>1392</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>app</td>
<td>241</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>bl2/ext/mcubOOT</td>
<td>38</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>cmake</td>
<td>103</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>contributing.md</td>
<td>1686</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>dco.txt</td>
<td>1421</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>docs</td>
<td>81</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>glossary.md</td>
<td>2227</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>interface</td>
<td>66</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>license.md</td>
<td>1763</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>log.bat</td>
<td>326</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-x-r-x</td>
<td>log.sh</td>
<td>565</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-w-r-</td>
<td>maintainers.md</td>
<td>1052</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>platform</td>
<td>101</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>r-x-r-x</td>
<td>readme.md</td>
<td>4981</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>secure.txt</td>
<td>176</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>test</td>
<td>193</td>
<td>log</td>
<td>plain</td>
</tr>
<tr>
<td>d----</td>
<td>tools</td>
<td>387</td>
<td>log</td>
<td>plain</td>
</tr>
</tbody>
</table>

Generated by cgit v1.0-122-ghee09 (git 2.18.0) at 2018-09-16 11:09:35 +0000
Roadmap

TF-M has been under active development since it was launched in Q1’18. It is being designed to include

1. **Secure boot** ensuring integrity of runtime images and responsible for firmware upgrade.
2. Runtime firmware consisting of **TF-M Core** responsible for secure isolation, execution and communication aspects, and a set of Secure Services providing services to the Non-Secure and Secure Applications. The secure services currently planned to be supported are **Secure Storage, Cryptography, Audit Logs, Attestation, Provisioning and Platform Services**

Roadmap below shows when the services are getting supported and then enhanced.

Currently Supported Features

- Secure Boot
- Secure Storage
- Audit Logs

Q3’18 (July-Sept’18)

- [TF-M Core] Inter Process Communication (IPC)
- [Secure Boot] Enhancements
- [Secure Storage] Rollback Protection
- [Cryptography] PSK TLS
- [Attestation] Initial Attestation Service

Q4’18 (Oct-Dec’18)
Project Status

• Almost at official kick-off…

• Everything is working for partners wanting to use trustedfirmware in their product
  • Member benefits still to come:
  • OpenCI
  • Platforms and board farm
  • Project member backlog and roadmap

• We welcome interest and input from all Arm SoC segments
  • IoT, Automotive, Mobile, Infrastructure, etc…
  • Secure firmware is important for all products!
Trusted Firmware-A
A long time ago in a Connect far, far away...

commit 4f6ad66ae9fcc8bcb3b0fcee10b7ab1ffcaf1a56
Author: Achin Gupta <achin.gupta@arm.com>
Date:   Fri Oct 25 09:08:21 2013 +0100

ARMv8 Trusted Firmware release v0.2

Feb 13  Conception    Arm has idea of providing reference EL3 firmware for Armv8-A to help defragment the Arm Software ecosystem
Jul 13  Communication Discussions with partners at LCE13
Sep 13  Implementation v0.1 binaries in Linaro AArch64 release
Oct 13  Introduction   v0.2 source code at GitHub and LCU13 announcement
## 5 successful years since then!

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 14</td>
<td>Adoption</td>
<td>Early adopters port v0.4 to silicon</td>
</tr>
<tr>
<td>Aug 14</td>
<td>Celebration</td>
<td>v1.0 released, including Juno port OP-TEE support at LCU14</td>
</tr>
<tr>
<td>Feb 15</td>
<td>Evolution</td>
<td>v1.1 completes mandatory PSCI v1.0 Trusted Board Boot prototype</td>
</tr>
<tr>
<td>Dec 15</td>
<td>Acceleration</td>
<td>v1.2 provides minimally complete TBB Upstreaming of Non-Arm platforms</td>
</tr>
<tr>
<td>Oct 16</td>
<td>Extension</td>
<td>v1.3 adds AArch32 PSCI Dropped CLA, security hardening</td>
</tr>
<tr>
<td>Jun 17</td>
<td>Optimisation</td>
<td>v1.4 adds DynamIQ, GIC-600, SCMI, PSCI with OP-TEE, HiKey/HiKey960</td>
</tr>
<tr>
<td>Mar 18</td>
<td>Expansion</td>
<td>v1.5 introduces RAS &amp; Secure Partitions, Dynamic Configuration, Armv7 support</td>
</tr>
<tr>
<td>Oct 18</td>
<td>Open Governance</td>
<td>Upcoming v1.6/v2.0 and TF.org migration</td>
</tr>
</tbody>
</table>
Show me the numbers!

5780 Commits overall

- 20% Arm
- 80% Partners

- 2015: 6%
- 2016: 14%
- 2017: 26%
- 2018: 34%

25+ companies contributing
20+ partners platforms supported
- 10+ added in the last year!
- 5+ in the last 3 months!

All Armv8-A market segments:
Mobile, Clamshell, Automotive,
Server, Networking/Edge, Embedded

10 official releases

Partners commits over years

10+ Linaro Connect presentations
5 UEFI PlugFest appearances
2 Open Source Firmware Conference (OSFC) talks

Data as of Sept, 10th 2018
Upcoming v1.6/v2.0 release (October 2018)

v1.6:

RAS & Secure Partitions:

- Secure Partition Manager – Single Partition enhancements
- v8.2 RAS Extension (ESB), v8.4 Fault Injection support, & Double Fault handling

CVE-2018-3639 workaround (Spectre Variant 4 – Static & Dynamic mitigation)

Arm Cortex-A76 and new cores support

Armv8.4 MPAM enablement support

Functional Safety: Coverity MISRA Required fixes

Dynamic Configuration – BL31, BL32 & BL33 extension

New HW support:

- Arm SGI-575, Arm SGM-775
- 6 new Platforms from Partners

v2.0 (just after v1.6)

Remove support for deprecated interfaces from Trusted Firmware-A codebase

New baseline for all subsequent TF-A developments and releases within trustedfirmware.org
A look to the future

Trusted Firmware-A Tests (TF-A-Tests)

Secure Partitions evolutions:

- Multiple S-EL0 partitions
- S-EL2 introduction, secure virtualization and coexistence of multiple isolated TEEs

Arm IPs, specifications and architecture evolution

Publicly announced regular release cadence

End-to-end secure boot and secure firmware update

Security assessments and threat modelling

Public Board Farm and CI (trustedfirmwareci.org?)

Single Firmware vision: “1 Firmware to support them all” (boards, partners, features)

Join us to make it even more successful in the next 5 years!
Trusted Firmware-M
TF-M: To Secure a Trillion Connected Devices

• Launched at HKG’18

• Isolated Trusted Execution Environment for v7-M and v8-M Devices

• Trusted Boot and Secure Services invoked from Non-Secure Applications.

• Highly Configurable to suit Target Application

• Reference Implementation of Arm Platform Security Architecture (PSA)
Platform Security Architecture
A recipe for building a secure system & a reference implementation

1. Analyze
   - Threat models & security analysis

2. Architect
   - Hardware & firmware architecture specifications

3. Implement
   - Firmware source code

4. Common principles across multiple use cases
   - Device identity
   - Trusted boot sequence
   - Secure over-the-air software update
   - Certificate based authentication

5. Software architecture
6. Hardware requirements

3 Parts to PSA
Integrating into IoT Open Source Ecosystem....

Beyond Feature Development

- **Enablement on IoT Platforms**
  - TF-M enablement on several v8-M based platforms underway

- **Secure Counterpart of RTOSes**
  - mbedOS upstream support in Q4’18
  - LITE Team Demo of Google Cloud Client + Zephyr + TF-M
  - FreeRTOS

- **Open Design Documents, Roadmaps, Code**
Growing up Fast - Be Part of the Journey

Open Design, Code Review, Presentations, Blogs, Infrastructure

HKG’18
Secure Boot, Secure Storage
43 Commits

YVR’18
Secure Boot, Secure Storage, Audit Logs, Crypto APIs, Zephyr Demo
GCC Support
Early Ecosystem Engagements
175 Commits

2019
Secure Services Implemented
PSA APIs
Integrated with RTOSes
Platform Support
As Trusted Firmware-A (Arm Trusted Firmware) is now 5 years old.

• We’d like you to join us in celebrating
• Ask now (or after the presentation)
• Email board@trustedfirmware.org
Thank You!
Danke!
Merci!
谢谢!
ありがとうございます!
Gracias!
Kiitos!