Agenda

- Trusted Firmware Open Governance Project update
- Trusted Firmware-A updates
- Trusted Firmware-M updates
- A small celebration (oh yes...again!)
Trusted Firmware.org Project update

- Open Governance Community project
- Officially announced on October 16th 2018
- 6 founding members:
  - Arm
  - Cypress
  - Data I/O
  - Google
  - Linaro
  - Texas Instruments
- STMicroelectronics and Huawei recently joined!
- Membership open to all & Project charter publicly available

enquiries@trustedfirmware.org
Trusted Firmware.org – What is it

- Reference implementation of secure world software for Armv7-A, Armv8-A, Armv7-M and Armv8-M architectures
- Reference implementation of the Arm Platform Security Architecture (PSA) for Arm-based IoT devices
- Covering all types of market segments: IoT, Embedded, Automotive, Edge, Networking, Client, Mobile, Infrastructure, Cloud
- Trusted codebase providing standard implementation of relevant Arm system architecture specifications
- Quick and easy porting to modern chips and platforms
- Foundations of Trusted Execution Environment (TEE) on application processors, or the Secure Processing Environment (SPE) of microcontrollers
Trusted Firmware.org – Why joining

- Appetite for open, collaborative, cross-industry Security collaboration
- Participate in effort to cater for whole ecosystem’s security requirements and to secure the foundation software of trillions of connected devices
- Be part of an open collaboration space for partners across the vast array of Arm-based systems from all different market segments
- Achieve cost-effectiveness by leveraging Open CI & Public Board Farm
- Contribute and influence the strategic and technical directions of the project for existing and future architectures
- Help guiding the whole security community towards a common reference code base and implementation best practices
- Take shared ownership of a project you depend on
Trusted Firmware.org – Available Resources

● Monthly Project status updates:
  ○ On the blog: https://www.trustedfirmware.org/blog/
  ○ On the wiki: https://developer.trustedfirmware.org/w/resources/

● Board meeting minutes:
  ○ https://developer.trustedfirmware.org/w/resources/board-minutes/

● Project Dashboards
  ○ TF-A: https://developer.trustedfirmware.org/project/profile/1/
  ○ TF-M: https://developer.trustedfirmware.org/dashboard/view/5/

● Wiki Pages:
  ○ https://developer.trustedfirmware.org/w/

● Mailing Lists (see https://www.trustedfirmware.org/contact/)  
  ○ TF-A: https://lists.trustedfirmware.org/mailman/listinfo/tf-a  
  ○ TF-M: https://lists.trustedfirmware.org/mailman/listinfo/tf-m  
Trusted Firmware-A Updates

Foundation of Arm TrustZone technology
A long time ago in a Connect far, far away...

ARM Trusted Firmware

5 successful years since then!

Jun 14 Adoption
Early adopters port v0.4 to silicon

Aug 14 Celebration
v1.0 released, including Juno port

Feb 15 Evolution
OP-TEE support at v1.1 completes mainboard Trusted Board Book

Dec 15 Acceleration
v1.2 provides minimal upstreaming of NCI

Oct 16 Extension
v1.3 adds AArch32/64, dropped CLA, secure boot

Jun 17 Optimisation
v1.4 adds Dynamic PSCI with OP-TEE

Mar 18 Expansion
v1.5 introduces RA

Oct 18 Open Governance
Upcoming v1.6/v2

Show me the numbers!

5780 Commits overall

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+ Linaro Connect presentations
5 UEFI Plugfest appearances
2 Open Source Firmware Conference (OSFC) Talks*

Vancouver 2018 – 5 years old Celebrations!
Vancouver 2018 ➔ Bangkok 2019

- Trusted Firmware-A Tests (TF-A-Tests) first open-source release
  - BSD-3-clause and contributions accepted under DCO as parent TF-A project
  - Code and documentation [https://git.trustedfirmware.org/TF-A/tf-a-tests.git/about/](https://git.trustedfirmware.org/TF-A/tf-a-tests.git/about/)

- Updated stats October 2018 – March 2019

### Partners commits

<table>
<thead>
<tr>
<th></th>
<th>2018-Q1</th>
<th>2018-Q2</th>
<th>2018-Q3</th>
<th>2018-Q4</th>
<th>2019-Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 new partners platforms upstream!</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Making now 30 partners platforms officially supported upstream!</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Highlights TF-A & TF-A-Tests v2.1 release

- Armv8.3 Pointer Authentication enabled for Normal world
- Armv8.4-DIT Data Independent Timing
- Armv8.4-TTST Small translation tables
- Armv8.5 PSTATE.SSBS Speculation Store Bypass Safe (on Cortex-A76 & Neoverse-N1)
- New Arm Cores/Platform support:
  - Neoverse N1, Neoverse N1 Edge (RD-N1-Edge) FVP & N1SDP HW Platform
  - Neoverse E1, Neoverse E1 Edge (RD-E1-Edge) FVP
  - Neoverse Zeus preliminary support
- RomLib support: Allow patching of romlib functions
- Dynamic Configuration
  - Position Independent Executable (PIE) support for BL31 (enabled on FVPs)
- CVE-2018-19440 mitigation against information leakage from one Normal world SMC client to another
What’s on

● Architecture enablement
  ○ Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
  ○ Armv8.5 Branch Target Identifier (BTI)

● Platform Security Requirements
  ○ Attestation and Measured Boot with TPM interactions (discrete, fTPM)
  ○ Multiple Signing Domains and separate CoT
  ○ Dynamic Firmware configuration and S/N world information passing
    → Don’t miss BKK19-513 on Friday 11:30!

● Investigations in other areas
  ○ PSA for IoT A-class devices
  ○ Debug Certificates and Arm Debug IPs support
  ○ Functional Safety requirements
Migration Plans Update

Trusted Firmware-A migration steps (see detailed plan)

- **Phase 0 (Q4.2018): TF-A-Tests go live announcement under Git/Gerrit**
  - Completed

- **Phase 1 (Q1.2019): TF-A codebase migration from GitHub to Git/Gerrit**
  - Live after v2.1 release

- Phase 2: Public CI - Continuous Build open-source infrastructure
- Phase 3: Public CI - Continuous Testing on Arm FVPs
- Phase 4: Public CI - Continuous Testing on LAVA Board Farm
Where is the SPM?
Secure world & SPM evolution

- Building blocks for future use-cases
  - S-EL0 Single Partition for UEFI Standalone MM services based on MM Interface
  - Resource description CoT update / Multiple Signing domains
  - Migration path for existing Armv8.2 & v8.3 systems towards Armv8.4+

- Enterprise IoT/Edge Auto/Embed Use-cases
  - Multiple S-EL0 and S-EL1 (with TOS migration) Secure Partitions SPCI-based

- Architecture Secure virtualization
  - Armv8.4 S-EL2 virtualization extension support with reference SPM implementation

Legacy SP/SPM MM based

Timeline:
- 2018
- 2019
- 2020+
Trusted Firmware-M Updates
To Secure Trillion Connected Devices
As TF-M Turns 1....
Platform Security Architecture
A complete security offering independently tested
Trusted Firmware-M Framework
Secure Boot, Isolation, Secure Partition

Non-Secure Processing Environment

Secure Processing Environment

Non-secure Partition
- Application firmware
- OS libraries
- OS kernel

TF-M Core
- Secure call API and routing
- Partition Manager
- Scheduling
- Secure isolation

Secure Partition
- Secure function
- Secure function
- Secure function
- Partition-private code

Trusted Partition
- Trusted Function
- Crash handling
- Secure Drivers
- Secure IRQ
- Secure Debug
What Have I been upto?

- Growing Up
- Starting To Listen and Speak
- Making Friends
Growing Up: TF-M v1.0-Beta

- Secure Boot - mcuboot
- Level 1 Isolation
- Secure Storage
- Crypto Functions
- Attestation following EAT (Entity Attestation Token)
- PSA Certification
PSA Certified™ Embedded World!

- TF-M as PSA RoT
- PSA Certification of Silicon Platforms and RTOS
- See psacertified.org
Listen and Speak: Building TF-M Community

- Public Mailing list
- Open Design and Implementation Reviews
- Open CI – Initial Version Going Live this week
- Hacking Session Thursday, Secure Payment Demo on Friday

Messages in TF-M Mailing List
Making Friends in the Ecosystem

- mbedOS 5.12 contains TF-M
- CMSIS Packs
- Standardized PSA APIs
- Standard HAL Interface
- Multiple Toolchains
What’s Coming...
2019 – What’s Coming

• PSA FF IPC
• Level 2 Isolation
• Secure Boot Enhancements
• mbedCrypto
• SST, Crypto, Attestation
  • IPC mode
• Dual CPU Enablement
• Scheduler
  • Multiple Secure Context
  • Pre-emption
• Boot and Runtime – Crypto HW Integration
PSA Launched

Q3’2017

TF-M v0.1

Q1’2018

PSA Specs, TF.org

Q4’2018

v1.0-Beta, Mailing List, Ecosystem

Today

TF-M v1.0 L2 Certified

2019
Trusted Firmware-M now 1 year old.

Join trustedfirmware.org in celebrating
Thank you

Join Linaro to accelerate deployment of your Arm-based solutions through collaboration

contactus@linaro.org