Agenda

- Trusted Firmware Community Project update
- Trusted Firmware-A updates
- Trusted Firmware-M updates
- How to get involved
Trusted Firmware Community Project
Welcome OP-TEE into TrustedFirmware.org!
TrustedFirmware.org: Secure world software and Secure services reference implementation

All Arm-based systems

Easily portable to many other trusted software implementations
Current members
All market segments

Devices
IoT/Mobile/Auto/Laptop
Embedded
Edge
Cloud
Server
Trusted Firmware-A Updates
2019 Stats...and counting!

- **Half of commits** now coming from partners
- 30+ partners Platforms supported upstream
- 16+ different vendors (not counting Arm Ltd platforms)
- Collaboration dramatically increased in the past 2 years!

**Partners commits over years**

- **2013** to **2014**
- **2015**
- **2016**
- **2017**
- **2018**
- **2019**

- 2019 (Jan-Jun)
  - **49%** Arm
  - **51%** Partners

- +600% in 3yrs (2019 projections)
v2.2 release highlights (October 2019)

- Armv8.3 Pointer Authentication use in Secure world (EL3 and lower S-ELs)
- Armv8.5 Branch Target Identifier (BTI)
- Armv8.5 Memory Tagging Extension (MTE) enabled for Normal world
- GICv3 Driver updates for multi socket GIC redistributor discovery (tentative)
- RSA-3072 support as per latest versions of TBSA/TBFU
- Arm Cores/Platform support:
  - Fixed errata for Neoverse-N1 & Cortex-A76
  - Hercules & Hercules-AE (tentative)
  - Cortex-A65 & Cortex-A65AE (tentative)
  - Enable AMU for Zeus & Hercules
What’s on

- Architecture enablement
  - Armv8.5 Memory Tagging Extension (MTE) use at EL3
- Platform Security Requirements
  - Attestation and Measured Boot with TPM APIs
  - Multiple Signing Domains and separate CoT
  - Secure Firmware Update
- New build environment (cmake based)
- New Documentation: https://trustedfirmware-a.readthedocs.io/
- Open CI
  - Continuous Build open-source infrastructure
  - Continuous Testing on Juno (LAVA Board Farm)
  - Continuous Testing on Arm FVPs
WHAT IS THE SPM COOKING TODAY?
Secure world software architecture today (TOS)

**Normal world**
- Client Application
- Client Library
- Operating System Kernel
- Trusted OS Driver
- Hypervisor (optional)
- SIP Extension
- Trusted OS DD / OEM Ext

**Secure world**
- Client Application
- Client Library
- Trusted Application
- TA Library
- Trusted OS
- Trusted hardware resource drivers
- App TOS Dispatcher
- Platform Firmware
- Trusted Firmware

**Secure services:**
- DRM
- Secure payment
- Secure storage
- Crypto

**Platform services:**
- Trusted boot
- Power management (PSCI)
- Silicon vendor services
- Errata management
Secure world software architecture today

Secure services:
• DRM
• Secure payment
• Secure storage
• Crypto

Platform services:
• Trusted boot
• Power management (PSCI)
• Silicon vendor services
• Errata management
Secure world software architecture goal

- **Normal world**
  - Client Application
  - Client Library
  - Operating System Kernel
  - Hypervisor (optional)

- **Secure world**
  - Secure Services
  - Platform Services

**Secure services:**
- DRM
- Secure payment
- Secure storage
- Crypto

**Platform services:**
- Silicon vendor services
- Errata management
- BMC communication

**Standard services:**
- Trusted boot
- Power (PSCI, SCMI)
- SMCCC/SPCI

**Configuration files (DT-based):**
- Trusted Firmware.org
- Silicon Vendor specific software
- Application provider specific
- Application trusted OS specific
- Generic software

Legend:
- Standard/Generic
- Silicom Vendor specific software
- TrustedFirmware.org
- Application provider specific
- Application trusted OS specific
Single Secure Partition (MM-based)

Normal world

- Client Application
- Client Library
- Operating System Kernel
- Hypervisor (optional)

Secure world

- StandaloneMM Service
- MM Secure Partition
- Secure Partition Manager
- Generic Firmware

TrustZone Isolation Boundary

svc to smc shim

Available upstream now

Single uniprocessor partition (MM spec)

Execute a UEFI image with StandaloneMM service

Run to completion model
Multiple Secure Partitions (SPCI-based)

- **Normal world**
  - EL0
    - Client Application
    - Client Library
  - EL1
    - Operating System Kernel
    - Trusted OS / OP-TEE Driver
    - Hypervisor (optional)
    - SiP/ODM Extension
  - EL2
    - SPCI
  - EL3
- **Secure world**
  - (PSA) Trusted Application
  - TA Library
  - StandaloneMM Service
  - SPCI
  - Trusted OS (OP-TEE)
  - SPM
  - Secure Partition Manager
  - Generic Firmware

- **Isolation Boundary**
  - TrustZone Isolation Boundary

- **Application**
  - Application trusted OS specific
  - Application provider specific
  - Generic software
  - TrustedFirmware.org
  - Silicon Vendor specific software

- **Multiple SPs (SPCI spec)**
- **Migration path towards Armv8.4 Secure EL2**
- **Ongoing work now within TF.org**
Armv8.4 Secure EL2 Virtualization extension

Isolation through virtualization in the Secure world

Coupled with new SMMU and GIC, system-wide isolation

Future development within TF.org
TF-A Roadmap

- Legacy SP/SPM MM based
- S-EL0 Single Partition for UEFI StandaloneMM services based (Legacy MM)
- Building blocks for future use-cases
- Resource description
- CoT update / Multiple Signing domains
- Measured Boot
- Pre-8.4: SPCI OP-TEE + StandaloneMM SPs + PSA TAs
- Secure Firmware Update
- TrustedOS software-based isolation & PSA services
- Armv8.4 S-EL2 Secure Partition Manager (SPCI-based)
- Isolation through Secure virtualization Use-cases

Today

H2 2019

H1 2020

H2 2020+
Trusted Firmware-M Updates
To Secure Trillion Connected Devices
Growing up as a Toddler....

With a Lot of Friends and Toys!!!
Trusted Firmware-M: Open Source Implementation of PSA

- Analyze
  - Threat models & security analyses

- Architect
  - Hardware & firmware architect specifications

- Implement
  - Firmware source code

- Certify
  - psaCertified™
TF-Mv1.0-RC1: Enabling L1,2 and Functional API Certification

- F.INITIALIZATION
- F.FIRMWARE_UPDATE
- F.ISOLATION
- F.SECURE_STORAGE
- F.SECURE_CRYPTO
- F.SECURE_ATTESTATION
- F.SECURE_AUDIT
- F.SECURE_STATE
- PSA Dev. APIs

Non-Secure

Secure/TF-M

PSA Test Suite*

PSA Storage API
PSA Crypto APIs
PSA Attestation APIs
Audit APIs
Secure Boot

TF-M Core (IPC, SPM, Interrupt Handling)

TBSA-M HAL

HAL

TBSA-M Hardware

RTOS

TBSA-M Hardware

PSA Dev APIs

• F.SECURE_STORAGE
• F.SECURE_CRYPTO
• F.SECURE_ATTESTATION
• F.SECURE_AUDIT
• F.SECURE_STATE
• PSA Dev. APIs
Open Continuous Integration System

https://ci.trustedfirmware.org

Gerrit
review.trustedfirmware.org

Jenkins
ci.trustedfirmware.org

Artifacts

MPS2 FPGA Board

Trigger

2

Push

1

 TF-M Patch
/ TF-A Patch

Result +1

Jenkins

Trigger

3

LAVA
validation.linaro.org

Build Slaves

Coming Soon

Juno Board

TrustedFirmware.org
More TF-M Enabled Platforms

Musca-A, B1e  AN5xx on MPS2  NXP LPC55S69  Cypress pSoC6

Design Start Cortex-M33 based FPGA platform on AWS Marketplace
- Add HW accelerator/peripherals
- Use for HW/SW co-development
Enablement in RTOSes

- mbedOS 5.12 (March’19) onwards integrated TF-M
  - PSA Level1 and Functional API certified
  - Several PSA Level1 certified platforms supported

- Zephyr PR integrating TF-M
  - For MuscaA, B1e and AN521 on MPS2
  - Aiming to get PSA certified

- Integration of FreeRTOS 10.2.1 and TF-M under evaluation by FreeRTOS team
  - Investigating how best TF-M can integrate with Amazon: FreeRTOS

- Collaboration kicked off with RT-Thread on integration
What’s Coming...
PSA Level2 Certification for TF-M Platforms

- TF-Mv1.0-RC1 tag created end of May including PSA Level2 Certification requirements

- Riscure (one of the PSA Labs.) performed a brief Level2 security evaluation/pipecleaning during July/August

- TF-Mv1.0-RC2 planned in October addressing observations made during the evaluation

- Enabling platforms to use TF-M as PSA RoT for Level2 certification.
Integrating with Crypto Hardware

- **Crypto Hardware**
  - Increased Performance, Security

- **Example integration on MuscaB1e**
  - Cortex-M33 Cryptocell-312

- **Secure Boot**
  - Key Hash in OTP, Authentication

- **Crypto Acceleration**
  - Leverage Crypto Hardware

- **Secure Storage**
  - Use Key derived from Hardware Unique Key (HUK)

- **Attestation**
  - Use Key in OTP for signing Attestation Token
TF-M Roadmap

Today
- Library, IPC Mode, L1,L2 Isolation, PSA APIs mbedcrypto

H2 2019
- L2 Cert., PSA 1.0.0

H1 2020
- Enabling L2 Certification, Dual v7-M, PSA 1.0.0, Crypto HW
- Crypto HW, TF-M Profiles, Level3 Isolation, TF-M in CI

H2 2020+
- Provisioning, Secure Debug, Platform Services, PSA API 1.1
- More Secure Services
- TF-M Profiles, Level3 Isolation

PSA APIs, L1 Cert.
TF-M Developer Workshop

- Oct 31st, Nov 1st - Lyon, France
- Workshop open to all TF-M collaborators
- Covering various technical topics

ELC, Lyon

- Oct 28-30th - Lyon, France
- Hosting Booth with Trusted Firmware demos
How to get involved
Build Security Collaboratively

- Security by Scale
- Shared Ownership
- Complexity solved once for all
- Faster TTM & Reduced Cost
- Less Individual Maintenance & Minimised TCO
How to Get Involved

- Contribute to the open source codebase!
- Join the project mailing lists!
- Evaluate adopting Trusted Firmware for your new products!

...and last but not the least: **become a project member!**
(enquiries@trustedfirmware.org)

- Own the strategic and technical direction of the project
- Have your board supported and maintained by the open CI
- Become a Trusted Firmware ambassador!
• Join us in welcoming OP-TEE to Trustedfirmware.org family

• Inviting everyone to TF-M’s 2\textsuperscript{nd} Birthday celebrations at next Linaro Connect
Thank you

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

contactus@linaro.org