Linaro OP-TEE Updates

Nov 21

Agenda

- Agenda
  - Focus Areas
  - Previous Cycle Updates
  - Roadmap

Focus areas

- Work with Arm to ensure that OP-TEE works with newer architectures as well as supports older architectures (Armv7).

- Make OP-TEE compatible with FF-A specification. Prepare it so that it can be used in environments with Secure Partitions enabled.

- Support technologies which matter to members eg PKCS#11, SCMI Server, Widevine, Keymaster and Gatekeeper TA's (AOSP) and StMM

- Support other Linaro Projects - Trusted Substrate and Stratos

OP-TEE General Information

- Collaborate Page
  - Latest Roadmap
  - Backlog and Future Version Jira details
  - Repository links

- Monthly Meeting
  - Notes available here
  - Meeting calendar

- Security advisories on git-hub
  - Earlier maintained at optee.org
  - Since June’21 has been shifted to github.

OP-TEE releases

- Quarterly releases
  - Release details

- What devices?
  - Linaro tests all devices at our hands
  - For other devices we rely on external contributors (maintainers)

- Release notes?
  - Latest changes can be read about in the CHANGELOG.md file
  - Follows Semantic Versioning 2.0.0

Previous Cycle (Apr - Oct 2020) Updates

PKCS#11 support in OP-TEE (TS-6)

- TS-5 - PKCS#11 - RSA mechanisms - Reviews mainly - **Completed**
- TS-15 - PKCS#11 - AES mechanisms - **Completed**
- TS-16 - PKCS#11 - HMAC digest family - **Completed**

Asynchronous notification to normal world (TS-8)

- TS-7 - Asynchronous notification to normal world - **In Progress**

Virtualization: Access of single OP-TEE instance from multiple Virtual Machines (TS-13)

- TS-9 - XEN and OPTEE xtests running from DOM0 - **Completed**
- TS-10 - Run xtests from multiple DOMU guests - **Completed**
- TS-11 - PoC to use virtio-rpmb interface with tee-supplicant - **Blocked**

XEN mediator for FF-A and OP-TEE (STR-23)

- STR-22 - XEN mediator for FF-A and OP-TEE - **Completed**

Armv8-A secure side virtualization (TS-100)

- TS-99 - Upstream OP-TEE with a FF-A SPM Core at S-EL2 - **Completed**
- TS-101 - Upstream OP-TEE kernel driver supporting FF-A - **Completed**

PKCS#11

- PKCS#11 API userland library - libckteec
- PKCS#11 TA
- Regression Test Environment - xtest
- Functionality available today
  - Slot and token discovery
  - User session management
  - User authentication (PIN & Linux ACL)
  - Object (session and permanent) creation and generation (AES keys and generic secrets)
  - Key derivation (by AES encryption)
  - AES ciphering (CBC, ECB, CTS, CTR, CMAC)
  - MAC computation (SHA* MAC, HMACs)
  - ECDSA
  - Random number generation
  - Digest

- Functionality available today
  - RSA ciphering and authentication
  - Key Wrap/Unwrap by AES
  - Certificate Support

Demo in LVC'21 - Link here

FF-A and Secure Partition Updates (pre v8.4)

- FF-A S-EL1 SPMC Prototype
  - Using FF-A instead of raw SMC calls as transport carrying the OPTEE_MSG protocol
  - Experimental - Tested with QEMU virt ARMv8
  - Same OP-TEE kernel driver as in next slide (post v8.4)
  - Can be ported to ARMv7 without much effort if desired

- Secure Partition at S-EL0 groundwork to handle SPs
  - This work is driven by Arm, the Linaro work is mainly to review the patches before they can be accepted into OP-TEE OS upstream

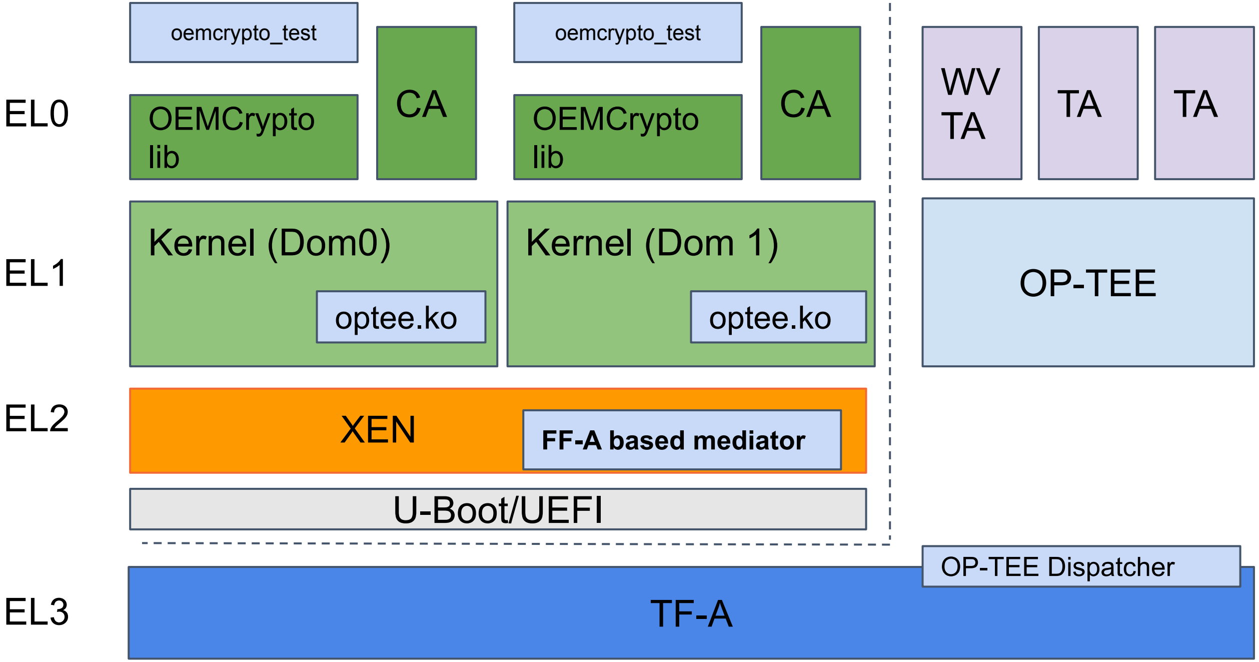
FF-A and Secure Partition Updates (post v8.4)

- OP-TEE as SP at S-EL1 is progressing
    - Using FF-A instead of raw SMC calls as transport carrying the OPTEE_MSG protocol
    - OP-TEE as SP at S-EL1 - Patches Merged in OP-TEE OS
        - The OP-TEE ABI will become stable once the kernel driver is upstream
    - FF-A support in OP-TEE driver - Pull request accepted by Arnd.
    - Based on
        - FF-A v1.0 specification
        - Linux FF-A driver patches
        - **With Hafnium at S-EL2 as SPMC (secure hypervisor)**

OP-TEE and Virtualization

- To demonstrate and cover most of the things we are targeting to run oemcrypto-tests (Widevine DRM test suite) from VM's.
- Steps being done to demonstrate the same are :
    - xtests successfully running from XEN Dom0 and DomUs on QEMU and integrated with build repos upstream - **Completed**
    - Secure storage virtualization - Access of RPMB from multiple guests - **Backlog** (TS-12)
    - Sharing of large dma buffers (ion unmapped heap) between virtual guests and secure world
    - Demo OEMCrypto tests from VM's
- FF-A
    - FF-A based generic mediator

OP-TEE and Virtualization

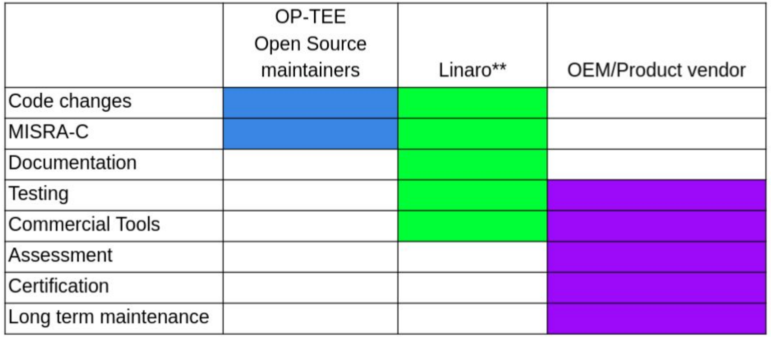


RUST, OP-TEE, TeaClave

- Apache Teaclave (incubating) is an open source universal secure computing platform, making computation on privacy-sensitive data safe and simple.
- Teaclave provides 2 rust crates:
  - optee-teec (Rust crate for GPD TEE Client API)
  - optee-utee (Rust crate for GPD TEE Internal Core API)
- Teaclave trustzone-sdk also proposes examples of Client and Trusted applications:
  - linaro-swg/optee_examples.git CAs (host/) and TAs, re-written in Rust
  - few other useful common modules: serde (serialization) and a message passing interface (interfaces with protobuf).
- Presentation by Baidu recently on the same in LOC meeting. Details here.
- Baidu has officially integrated it in OP-TEE 3.15.0. Details here.

Functional Safety Updates

- Change in direction
  - Initially the focus was at making OP-TEE itself safety ready
    - MISRA first level analysis was done on OP-TEE code.
  - But after talking to Tier 1’s it looks like they are more interested in the “freedom of interference” i.e OP-TEE should not affect domains running software that already has been safety certified.
- Specifications
  - IEC 61508 is very old and a new version is expected 2023(?) i.e a long time to wait.
  - ISO26262 is also old, but more up-to-date then IEC 61508



	OP-TEE Open Source maintainers	Linaro**	OEM/Product vendor
Code changes	🟦	🟩	
MISRA-C	🟦	🟩	
Documentation		🟩	
Testing		🟩	🟪
Commercial Tools		🟩	🟪
Assessment			🟪
Certification			🟪
Long term maintenance			🟪

Asynchronous Notification

- Patches in review
  - Kernel patchset
  - OP-TEE patchset

- Documentation at https://optee.readthedocs.io/en/latest/architecture/core.html#notifications

- Can be summarized as a way of waking up a thread sleeping in the kernel driver from a non-secure interrupt handler
  - This includes a top half and bottom half device driver in secure world, this is demonstrated in the optee_os pull request above
  - Required to support SCMII server use case in OP-TEE

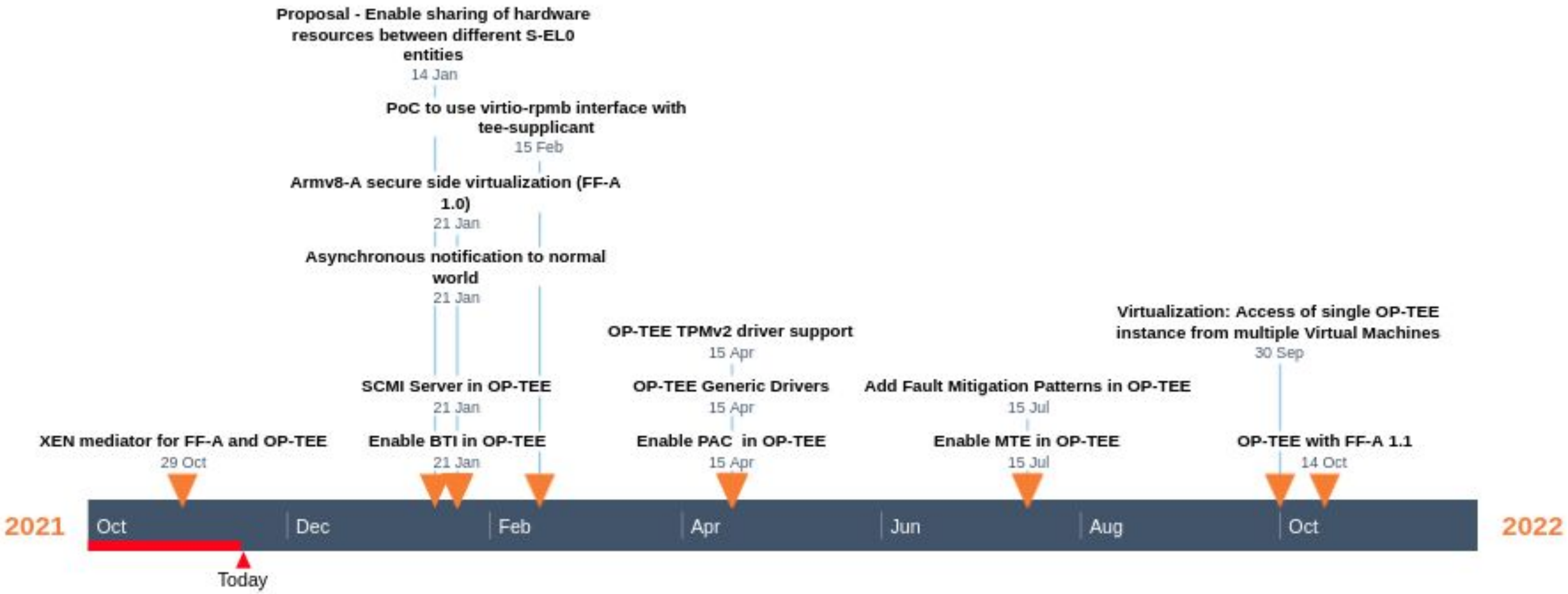
Sharing of h/w resources in secure world

- Draft Proposal available - Proposal - Sharing of hardware resources in secure world - 211101
- A walkthrough of the proposal will be done in upcoming monthly meeting on Nov 25.

Roadmap - Details

- Arm and FF-A
    - Armv8-A secure side virtualization (FF-A 1.0) TS-100
    - ARMv8-A FF-A 1.1 support - TS-103
    - Enable sharing of hardware resources between different S-EL0 entities (TS-109)
- Generic features
    - Enable BTI in OP-TEE- TS-105
    - Enable PAC in OP-TEE - TS-152
    - Enable MTE in OP-TEE - TS-153
    - OS Runtime Integrity checking from OP-TEE - TS-120
    - Addition of Fault Mitigation Patterns in OP-TEE - TS-111
    - Asynchronous notification to normal world TS-8
    - TPM driver in OP-TEE - TS-53
    - OP-TEE Generic Driver Support - TS-165
- Virtualization: Access of single OP-TEE instance from multiple Virtual Machines (TS-13)
- SCMI Server in OP-TEE - TS-122

Roadmap



XEN mediator for FF-A and OP-TEE
29 Oct

Proposal - Enable sharing of hardware resources between different S-EL0 entities
14 Jan

Armv8-A secure side virtualization (FF-A 1.0)
21 Jan

Asynchronous notification to normal world
21 Jan

SCMI Server in OP-TEE
21 Jan

Enable BTI in OP-TEE
21 Jan

PoC to use virtio-rpmb interface with tee-supplicant
15 Feb

OP-TEE TPMv2 driver support
15 Apr

OP-TEE Generic Drivers
15 Apr

Enable PAC in OP-TEE
15 Apr

Add Fault Mitigation Patterns in OP-TEE
15 Jul

Enable MTE in OP-TEE
15 Jul

Virtualization: Access of single OP-TEE instance from multiple Virtual Machines
30 Sep

OP-TEE with FF-A 1.1
14 Oct

Thank you

Linaro