2023-04-08

Created: 2023-04-29 22:44:53

Questions

- 2020 Demystifying TEE Client API `(230406.Papers.OP-TEE.txt)`
  - `[11:30]` Paper: Demystifying ARM TrustZone TEE Client API using OP-TEE `(Papers.OP-TEE.0406.md)`
- Virtualization `(230327.OP-TEE.txt)`
  - `[23:11]` The following article are from the website https://optee.readthedocs.io/en/latest/architecture/virtualization.html `(OP-TEE.0327.md)`
  - `[23:15]` Does the hypervisor relied on OP-TEE run in normal world or secure world? `(OP-TEE.0327.md)`
  - `[23:19]` Does a TA run in a VM described in the article? `(OP-TEE.0327.md)`

Q & A

2020 Demystifying TEE Client API `(230406.Papers.OP-TEE.txt)`

Question: `[11:30]` Paper: Demystifying ARM TrustZone TEE Client API using OP-TEE `(Papers.OP-TEE.0406.md)`

Answer:

Title: Demystifying ARM TrustZone TEE Client API using OP-TEE

Abstract: With the increased use of mobile devices for various purposes, such as payment systems, the need for secure storage of critical data has become more important. Trusted Execution Environment (TEE) technology has emerged as a solution to provide a secure execution environment for sensitive data. ARM TrustZone technology, primarily used in mobile devices, divides a physical processor into the Normal World and Secure World, ensuring a safer execution environment. While various manufacturers have adopted TrustZone technology, existing commercial TEEs have limitations in conducting security research using TrustZone.

This paper introduces OP-TEE, an open-source project for implementing ARM TrustZone technology, and the TEE Client API that enables communication with Trusted Applications within the TrustZone Secure World. To demystify the TEE Client API, the authors also implemented a simple trusted application for communication between the Normal World and Secure World in the OP-TEE OS using the QEMU emulator. This research aims to make the TEE Client API more accessible and easier to understand for researchers and developers working with ARM TrustZone technology.

Virtualization `(230327.OP-TEE.txt)`

Question: `[23:11]` The following article are from the website https://optee.readthedocs.io/en/latest/architecture/virtualization.html `(OP-TEE.0327.md)`

Answer:

The following is a summary of OP-TEE's experimental virtualization support, as described in the article:

- One OP-TEE instance can run TAs from multiple virtual machines, isolating all VM-related states to prevent one VM from affecting another.
- OP-TEE relies on a hypervisor (e.g., Xen) to determine which VM is calling it, and the hypervisor must inform OP-TEE about the creation and destruction of VMs.
- OP-TEE cannot translate intermediate physical addresses (IPAs) to physical addresses (PAs), so the hypervisor is responsible for this translation.
- Virtualization support is enabled with the CFG_VIRTUALIZATION configuration option, and the maximum number of

supported VMs is controlled by CFG_VIRT_GUEST_COUNT.

- Hypervisors must be aware of OP-TEE, handle SMCs from virtual guests, perform IPA<->PA address translation, and manage memory pages shared between VMs and OP-TEE.
- Limitations of the experimental virtualization support include platform support (only Armv8 is supported and tested on QEMU-V8), static VM guest count and memory allocation, sharing hardware resources and PTAs, compatibility with "normal" mode, and the experimental state of the technology.
- The implementation details of OP-TEE virtualization support involve splitting OP-TEE into "nexus" (core part) and TEE (handles requests and runs TAs). There is one nexus instance and multiple TEE instances, one for each registered VM. Banked memory sections are used for TEE/VM instances, and the nexus and TEE have separate heaps.

This summary provides an overview of OP-TEE's experimental virtualization support, but it is essential to refer to the original documentation for a complete understanding of the technology, its requirements, and its limitations.

Question: `[23:15]` Does the hypervisor relied on OP-TEE run in normal world or secure world? (`OP-TEE.0327.md`)

Answer:

The hypervisor that OP-TEE relies on runs in the normal world. It is responsible for managing multiple virtual machines and handling the communication between the normal world and OP-TEE in the secure world. The hypervisor must be aware of OP-TEE, handle SMCs from virtual guests, perform IPA <-> PA address translation, and manage memory pages shared between VMs and OP-TEE.

Question: `[23:19]` Does a TA run in a VM described in the article? (`OP-TEE.0327.md`)

Answer:

No, a Trusted Application (TA) does not run inside a Virtual Machine (VM) as described in the article. Instead, the TA runs in the secure world within the OP-TEE environment. The hypervisor manages the VMs in the normal world and is responsible for handling the communication between the normal world and OP-TEE in the secure world. When OP-TEE has virtualization support enabled, it allows multiple VMs to utilize a single OP-TEE instance for running TAs while maintaining isolation between the VM-related states.