230409.FF-A

Created: 2023-04-09 11:26:10

Questions

Q & A

Ch 2 - Introduction

Ch 3 - Software Architecture

Ch 3.1 - Isolation boundaries

Ch 3.2 - Partitions

Ch 3.3 - Partition manager

Question: So SPM and Hypervisor are partition managers. Right?

Answer:

Yes, that's correct. In the context of the Arm Firmware Framework for Arm A-profile, the Secure Partition Manager (SPM) operates in the Secure world, while the Hypervisor operates in the Normal world. Both SPM and Hypervisor are partition managers responsible for creating and managing the physical isolation boundaries of partitions, assigning resources, and enabling inter-partition communication.

Question: What is VMSA?

Answer:

VMSA, or Virtual Memory System Architecture, is a part of the Arm architecture that defines the memory management and address translation mechanisms. It is responsible for managing the address spaces and memory protection features in Arm

systems. VMSA allows for the creation of separate virtual address spaces for each process, providing isolation between processes and the operating system. In the context of the Arm A-profile, the Hypervisor uses the virtualization extension in VMSA to create physical isolation boundaries between different partitions or virtual machines.

Question: Is VMSA a software or a hardware?

Answer:

VMSA (Virtual Memory System Architecture) is not a specific piece of software or hardware, but rather a part of the Arm architecture specification that defines how memory management and address translation should be implemented in Arm-based systems. VMSA provides guidelines for designing hardware and software components that handle memory management, address translation, and access control, allowing for the creation of separate virtual address spaces and ensuring proper isolation between processes and the operating system.

Ch 3.4 Example configurations

Question: Can SPM see SP0 and SP1?

Answer:

Yes, the Secure Partition Manager (SPM) can "see" and manage both SP0 and SP1. The SPM is responsible for creating and managing the physical isolation boundaries of Secure Partitions (SPs) like SP0 and SP1. It uses partition manifests to assign resources, initialize the partitions, and enable discovery of their services. Additionally, the SPM implements FF-A ABIs (Application Binary Interfaces) to enable inter-partition communication for access to partition services. So, while the SPM isolates SP0 and SP1 from each other, it still has visibility and control over both partitions.

Question: Can SP0 or SP1 see SPM?

Answer:

In the ARM Firmware Framework, SP0 and SP1 can communicate with the Secure Partition Manager (SPM) through well-defined interfaces, such as FF-A ABIs (Application Binary Interfaces). While the SPM is physically isolated from SP0 and SP1 in scenarios where they are physical partitions, they can still interact with the SPM using these interfaces for communication, service discovery, and memory management.

However, it is important to note that SP0 and SP1 cannot access the internal workings or the memory of the SPM directly. They can only communicate with the SPM through the defined interfaces, ensuring that the isolation between them is maintained.

Question: Is TrustZone isolation boundary physical isolation or logical isolation?

Answer:

TrustZone isolation boundary is a form of physical isolation. TrustZone is a security extension in ARM architecture that separates the processor's resources, such as memory and peripherals, into two distinct security domains: the Secure world and the Non-secure world. By utilizing hardware-based isolation, TrustZone ensures that sensitive data and functions in the Secure world are protected from unauthorized access by software running in the Non-secure world.

Ch 4.1 - SPM architecture

Question: What is SPMC in the document?

Answer:

In the document "Arm Firmware Framework for Arm A-profile," the SPMC (Secure Partition Manager Core) is a component of the Secure Partition Manager (SPM) responsible for:

1. Initializing and isolating Secure Partitions (SPs) at boot time.
2. Ensuring inter-partition isolation during runtime.
3. Managing inter-partition communication between Secure Endpoints (S-Endpoints) and Non-Secure Endpoints (NS-Endpoints).

The SPMC can co-reside with the SPM Dispatcher (SPMD) in EL3 or reside in adjacent exception levels, such as S-EL1 or S-EL2. It is a part of the Trusted Computing Base and has access to the entire physical address space.

Question: Is SPMC of TrustZone?

Answer:

The SPMC (Secure Partition Manager Core) is part of the Arm Firmware Framework for Arm A-profile, which is built on top of the Arm TrustZone technology. TrustZone provides the underlying hardware support for isolation and security, while the SPMC is responsible for managing partitions and their communication within the Secure world enabled by TrustZone. So, while the SPMC is not TrustZone itself, it is a component that utilizes and operates within the TrustZone technology.