

# 230407.TrustZone.Hypervisor

---

Created: 2023-04-08 18:15:23

## Questions

---

- TCB
  - What are components in TCB?
- Virtualization
  - What are types of virtualization techs?
- Hypervisor
  - What is hypervisor?
  - Is hypervisor a virtual machine manager?
  - Is hypervisor a software or a hardware?
- Hypervisor & Virtualization
  - Please compare hypervisor and virtualization and also summarize them in a table.
  - Is TrustZone a hypervisor or virtualization?
  - Is OP-TEE a hypervisor or virtualization?
  - Does virtualization depend on hypervisor?
  - Are there alternatives of hypervisor?
- VM
  - Does VM require hypervisor?
  - Can a VM contain VMs?
- Hypervisor & TrustZone
  - Please compare TrustZone and Hypervisor and also summarize in a table.
  - Can hypervisor run in secure world?
  - What is difference of running hypervisor in secure world and normal world. Please also summarize it in a table.
- Hypervisor & OP-TEE
  - <https://optee.readthedocs.io/en/latest/architecture/virtualization.html>
  - Does OP-TEE support VMs?
  - Is the technology of OP-TEE supporting VMs mature?

---

## Q & A

---

### TCB

---

Question: What are components in TCB?

Answer:

The Trusted Computing Base (TCB) is the set of all hardware, firmware, and software components critical to the security of a system. These components are responsible for enforcing the security policy and maintaining the system's integrity, confidentiality, and availability. The exact components of a TCB may vary depending on the specific system architecture and implementation. However, some common components in a TCB include:

1. Hardware:
  - Trusted Platform Module (TPM)
  - Secure boot hardware support
  - Hardware security features (e.g., ARM TrustZone, Intel SGX)
  - Hardware-based encryption and key storage

## 2. Firmware:

- Bootloader (e.g., UEFI Secure Boot, Coreboot)
- Trusted firmware (e.g., ARM Trusted Firmware)
- Hardware initialization code
- Firmware for security peripherals (e.g., TPM firmware)

## 3. Operating System (OS) components:

- Security-focused kernel (e.g., seL4, Xen)
- OS security features and policies
- Hypervisor (in virtualized environments)
- Mandatory access control mechanisms (e.g., SELinux, AppArmor)

## 4. Security applications and services:

- Trusted execution environments (e.g., OP-TEE)
- Security-focused libraries and tools (e.g., OpenSSL, GnuPG)
- Cryptographic services
- Authentication and access control services

These components work together to ensure the security of a system and provide a trusted foundation for applications and services. Note that the components listed above are just examples, and the actual TCB components may differ based on the specific system and its security requirements.

---

## Virtualization

---

Question: What are types of virtualization techs?

Answer:

There are various types of virtualization technologies, each targeting a specific layer of computing or specific use cases. Here are some of the major types:

1. **Hardware or Platform Virtualization:** This type of virtualization involves the creation of virtual machines (VMs) that share the physical hardware resources of a host system. Examples of hypervisors that enable this type of virtualization include VMware ESXi, Microsoft Hyper-V, and KVM.
2. **Operating System Virtualization:** This technology involves the creation of isolated environments, or containers, within a single host operating system. Each container shares the host OS's kernel but can have its own file system, libraries, and applications. Examples of containerization platforms include Docker, LXC, and Kubernetes.
3. **Application Virtualization:** This technique enables running applications in isolated environments on a host system without needing to install them. Application virtualization ensures that the application's dependencies do not interfere with the host system or other applications. Examples include Microsoft App-V and VMware ThinApp.
4. **Network Virtualization:** This type of virtualization abstracts the physical network infrastructure, allowing multiple virtual networks to share the same physical hardware. Network virtualization enables better utilization of resources, improved security, and easier network management. Examples include VMware NSX and Cisco ACI.
5. **Storage Virtualization:** Storage virtualization abstracts the physical storage devices, allowing them to be pooled and managed centrally. This enables better resource utilization, improved performance, and easier management. Examples of storage virtualization technologies include software-defined storage (SDS) solutions, such as Ceph and VMware vSAN.
6. **Desktop Virtualization:** This technology enables the delivery of a virtual desktop environment to users over a network. It separates the user's desktop environment from the physical hardware, allowing for centralized management, better resource utilization, and improved security. Examples of desktop virtualization solutions include VMware Horizon and Citrix Virtual Apps and Desktops.

These are just a few examples of virtualization technologies, and many more specific solutions and implementations exist in

the industry.

---

## Hypervisor

---

Question: What is hypervisor?

Answer:

A hypervisor, also known as a virtual machine monitor (VMM), is a type of software that enables the creation and management of virtual machines (VMs) on a physical host machine. The hypervisor is responsible for abstracting the underlying hardware resources of the host and allocating them to the virtual machines, allowing multiple VMs to run simultaneously on a single host.

There are two main types of hypervisors:

1. Type 1 hypervisor (Bare-metal): This type of hypervisor runs directly on the host's hardware without the need for an underlying operating system. It provides strong isolation between VMs and efficiently manages hardware resources. Examples of Type 1 hypervisors include VMware ESXi, Microsoft Hyper-V, and Xen.
2. Type 2 hypervisor (Hosted): This type of hypervisor runs on top of an existing operating system, which acts as the host. The VMs are created and managed within the host OS. Type 2 hypervisors typically have higher overhead and lower performance compared to Type 1 hypervisors, but they can be easier to set up and manage. Examples of Type 2 hypervisors include VMware Workstation, Oracle VirtualBox, and Parallels Desktop.

Hypervisors enable efficient use of computing resources, making it possible to run multiple operating systems and applications on the same physical hardware, improving resource utilization, and enabling greater flexibility in managing workloads. They are widely used in data centers, cloud computing environments, and for virtualization in general.

---

Question: Is hypervisor a virtual machine manager?

Answer:

Yes, a hypervisor is often referred to as a virtual machine manager (VMM). A hypervisor is a software or firmware that manages the creation, execution, and management of virtual machines (VMs) on a host system. It allows multiple VMs to run concurrently on the same physical hardware, while providing isolation and resource management between them.

Hypervisors are responsible for abstracting the physical hardware resources and allocating them to the VMs, handling the VMs' requests for resources, and ensuring that the VMs do not interfere with each other or the host system. They play a crucial role in the virtualization process, making it possible to create and manage VMs efficiently and securely.

---

Question: Is hypervisor a software or a hardware?

Answer:

A hypervisor is a software component that enables virtualization, allowing multiple operating systems or environments to run on a single physical host. Hypervisors can be classified into two types:

1. Type-1 hypervisors (bare-metal hypervisors): These hypervisors run directly on the hardware, providing better performance and more efficient resource management. Examples include VMware ESXi, Microsoft Hyper-V, and Xen.
2. Type-2 hypervisors (hosted hypervisors): These hypervisors run on top of a host operating system, sharing the system's resources with the guest operating systems. Examples include VMware Workstation, Oracle VirtualBox, and Parallels Desktop.

In summary, hypervisors are software components that enable virtualization and are not hardware themselves. However, some modern processors have hardware-assisted virtualization features that can improve the performance and security of hypervisors.

---

## Hypervisor & Virtualization

---

Question: Please compare hypervisor and virtualization and also summarize them in a table.

Answer:

Hypervisor and virtualization are related concepts but serve different purposes. Here's a comparison and summary of both in a table:

Aspect	Hypervisor	Virtualization
Definition	A software layer or firmware that manages and controls virtual machines (VMs).	The process of creating multiple isolated virtual environments on a single physical hardware.
Purpose	Allows multiple VMs to run concurrently on a single hardware platform.	To efficiently utilize hardware resources, improve flexibility, and increase security by isolating workloads.
Types	1. Type 1 (Bare-metal): Runs directly on hardware. Examples: VMware ESXi, Microsoft Hyper-V, Xen, and KVM. 2. Type 2 (Hosted): Runs as a software layer on top of an existing operating system (OS). Examples: VMware Workstation, VirtualBox, and Parallels Desktop.	1. Full Virtualization: VMs have no direct access to the hardware and are managed by a hypervisor. 2. Paravirtualization: VMs are aware of the hypervisor and can make calls to the hypervisor for better performance. 3. OS-level Virtualization: Creates isolated instances (containers) within a single OS kernel, sharing the same OS but having their own file systems and process spaces. Examples: Docker and LXC.
Functionality	Allocates resources such as CPU, memory, storage, and network to VMs, and manages their life cycle.	Separates applications, OSs, and hardware resources, enabling multiple workloads to run simultaneously on a single physical host.
Performance Impact	Hypervisors may introduce some overhead due to resource management and virtual-to-physical resource mapping.	Virtualization may cause a performance impact, depending on the type and extent of virtualization used. However, paravirtualization and OS-level virtualization generally have lower overhead compared to full virtualization.

In summary, a hypervisor is a software layer or firmware that enables and manages virtualization. Virtualization, on the other hand, is the process of creating isolated virtual environments on a single physical hardware platform, allowing for more efficient resource utilization, flexibility, and increased security.

Question: Is TrustZone a hypervisor or virtualization?

Answer:

TrustZone is neither a hypervisor nor virtualization. TrustZone is a hardware-based security technology developed by ARM. It provides an isolated and secure environment called the Trusted Execution Environment (TEE) for running sensitive and security-critical applications, alongside the Rich Execution Environment (REE) where the main operating system and applications run.

TrustZone creates two separate worlds - the secure world and the normal world - by partitioning the hardware resources such as processor, memory, and peripherals. The secure world is designed to protect sensitive data and operations, while the normal world runs the typical operating system and applications. The two worlds are isolated at the hardware level, ensuring that security vulnerabilities in the normal world do not compromise the secure world.

In summary, TrustZone is a security feature designed to provide hardware-level isolation for sensitive operations and data, rather than a hypervisor or virtualization technology.

Question: Is OP-TEE a hypervisor or virtualization?

Answer:

OP-TEE (Open Portable Trusted Execution Environment) is neither a hypervisor nor virtualization. It is a Trusted Execution Environment (TEE) designed to work with ARM TrustZone technology. OP-TEE is an open-source software solution that

provides a secure environment for running security-critical applications.

When used in conjunction with TrustZone, OP-TEE provides the secure operating system and services that run within the secure world created by TrustZone. It manages access to secure resources and protects sensitive data and operations from unauthorized access in the normal world.

In summary, OP-TEE is a TEE solution that works with TrustZone to provide a secure environment for security-critical applications, rather than a hypervisor or virtualization technology.

---

Question: Does virtualization depend on hypervisor?

Answer:

Yes, virtualization typically depends on a hypervisor. A hypervisor is a critical component of virtualization technology, as it is responsible for creating, managing, and running virtual machines (VMs) on a physical host system. The hypervisor manages the distribution of resources, such as CPU, memory, and storage, among the various VMs and provides isolation between them.

There are two types of hypervisors:

1. Type 1 (bare-metal) hypervisors: These hypervisors run directly on the host's hardware, without the need for a host operating system. Examples include VMware ESXi, Microsoft Hyper-V, and Xen.
2. Type 2 (hosted) hypervisors: These hypervisors run on top of a host operating system and manage virtual machines within the host environment. Examples include Oracle VirtualBox, VMware Workstation, and Microsoft Virtual PC.

In both cases, the hypervisor is the key component that enables virtualization, providing the necessary management and isolation between virtual machines running on a single physical host.

---

Question: Are there alternatives of hypervisor?

Answer:

Yes, there are alternatives to hypervisors for creating isolated environments. Some of these alternatives include:

1. Containers: Containers are a lightweight form of virtualization that enables the running of multiple isolated applications on the same host without the need for a full-fledged hypervisor. Containers share the host's kernel and can run directly on the host's operating system, leading to less overhead compared to hypervisors. Examples of container technologies include Docker, LXC, and Kubernetes.
2. Paravirtualization: Paravirtualization is an approach to virtualization where the guest operating system is modified to be aware of the virtualized environment and communicates directly with the host's hardware through a thin layer called the paravirtualization interface. This approach can offer better performance than full virtualization, but it requires modifying the guest operating system, which may not always be feasible. Xen is an example of a paravirtualization platform.
3. Application-level virtualization: Application-level virtualization isolates individual applications rather than entire operating systems, allowing them to run in a sandboxed environment. This can provide isolation and security benefits without the overhead of full-system virtualization. Examples of application-level virtualization include Java Virtual Machine (JVM), which runs Java applications in a sandboxed environment, and Microsoft's .NET runtime.
4. OS-level virtualization: OS-level virtualization provides isolated environments by partitioning a single operating system into multiple isolated instances called zones, jails, or namespaces. Each instance has its own file system, network stack, and process space, but they all share the same kernel. Examples of OS-level virtualization technologies include Solaris Zones, FreeBSD Jails, and Linux namespaces.

These alternatives each have their own advantages and trade-offs, and their suitability depends on the specific use case and requirements of the system being virtualized.

---

## VM

---

Question: Does VM require hypervisor?

Answer:

Yes, virtual machines (VMs) typically require a hypervisor to function. A hypervisor is the essential component responsible for creating, managing, and running VMs on a physical host system. It allocates the physical resources, such as CPU, memory, and storage, among the VMs and provides isolation between them. VMs are essentially software-based environments running on the hypervisor, which simulates the hardware and allows multiple VMs with different operating systems to share the same physical hardware resources.

There are alternative virtualization technologies, such as containerization (e.g., Docker), which do not rely on a hypervisor but instead use the host operating system's kernel to isolate and manage containers. However, in the context of traditional virtual machines, a hypervisor is a necessary component for their operation.

---

Question: Can a VM contain VMs?

Answer:

Yes, a virtual machine (VM) can contain other VMs, a concept known as nested virtualization. In nested virtualization, a hypervisor runs inside a virtual machine created by another hypervisor. This creates a hierarchy of virtual machines, where the primary hypervisor manages the first-level virtual machines, and the nested hypervisors manage the second-level virtual machines.

Nested virtualization can be useful in various scenarios, such as:

1. Testing and development: Nested virtualization allows developers to test and experiment with different hypervisors and configurations without needing multiple physical machines.
2. Training: Nested virtualization can be used for educational purposes, providing hands-on experience with different virtualization technologies.
3. Cloud environments: Nested virtualization can help cloud providers support customers who want to use their own hypervisors on top of the cloud provider's infrastructure.

However, nested virtualization can also introduce additional overhead and complexity, which can negatively impact the performance of the nested VMs. Additionally, not all hypervisors support nested virtualization, and hardware virtualization support may be required for acceptable performance.

---

## Hypervisor & TrustZone

---

Question: Please compare TrustZone and Hypervisor and also summarize in a table.

Answer:

TrustZone and hypervisors serve different purposes in providing security and isolation in computer systems, but they can also be complementary. Here's a comparison between the two:

TrustZone:

1. Purpose: Provides hardware-based security and isolation between the secure and non-secure worlds.
2. Scope: Limited to ARM-based systems.
3. Implementation: Built into the ARM processor, enabled by the SoC vendor.
4. Isolation: Creates two separate execution environments (secure world and normal world).
5. Use Cases: Secure boot, key storage, cryptographic operations, and DRM.

Hypervisor:

1. Purpose: Enables the virtualization of multiple operating systems or environments on a single physical host.
2. Scope: Applicable to various processor architectures (x86, ARM, etc.).
3. Implementation: Software-based, can be a Type-1 (bare-metal) or Type-2 (hosted) hypervisor.
4. Isolation: Creates multiple virtual machines (VMs) or containers, each running a separate OS or application.
5. Use Cases: Server consolidation, sandboxing, running multiple OSes on a single device, and cloud computing.

Summary in a table:

Feature	TrustZone	Hypervisor
Purpose	Hardware-based security	Virtualization
Scope	ARM-based systems	Multiple platforms
Implementation	Built into ARM processor	Software-based
Isolation	Secure and normal worlds	Virtual machines/containers
Use Cases	Secure boot, key storage, crypto operations, DRM	Server consolidation, sandboxing, multiple OSes, cloud computing

Keep in mind that TrustZone and hypervisors can be used together in some cases to enhance the overall security of a system. For example, a TrustZone-enabled secure world can host a secure hypervisor to further isolate and protect sensitive applications.

Question: Can hypervisor run in secure world?

Answer:

Yes, a hypervisor can run in the secure world, but it is less common. Typically, hypervisors run in the normal world, and they manage VMs in the normal world while ensuring their isolation. However, there are secure world hypervisors, like ARM TrustZone-based hypervisors, which are designed to run in the secure world and manage secure partitions or secure VMs.

A secure world hypervisor manages the secure partitions, including OP-TEE, and ensures their isolation from each other and the normal world. In this configuration, OP-TEE acts as one of the secure partitions managed by the secure world hypervisor. This approach allows multiple secure services to coexist in the secure world, each running in its own isolated partition or secure VM.

It's worth mentioning that having a hypervisor in the secure world adds complexity to the system, and its implementation must ensure that it does not introduce vulnerabilities or weaken the security guarantees provided by the secure world.

Question: What is difference of running hypervisor in secure world and normal world. Please also summarize it in a table.

Answer:

Aspect	Secure World Hypervisor	Normal World Hypervisor
1. Security	Enhanced security and isolation	Less secure environment
2. Trust boundaries	Well-defined trust boundaries for secure services	Trust boundaries managed within the normal world
3. Resource allocation	Resource constraints due to limited secure world size	More resources available for the hypervisor
4. Complexity	Increased development and maintenance complexity	Simpler development and maintenance process
5. Attack surface	Smaller attack surface due to isolation	Potentially larger attack surface
6. Isolation	Strong isolation between secure and normal world	Less strict isolation between guest OSs and hypervisor

## Hypervisor & OP-TEE

Question: <https://optee.readthedocs.io/en/latest/architecture/virtualization.html>

Answer:

The link you provided points to the official OP-TEE documentation on virtualization. According to the documentation, OP-TEE

does support virtualization in the sense that it can work with virtualized environments managed by a hypervisor. The hypervisor is responsible for managing VMs running in the normal world, while OP-TEE provides secure services in the secure world.

The documentation also mentions that OP-TEE has been tested with Xen on ARM, and there are ongoing efforts to test it with KVM on ARM. This indicates that OP-TEE can be used in conjunction with virtualization solutions like Xen and KVM to provide secure services to multiple VMs running on the same hardware platform.

However, it is crucial to ensure that the hypervisor is correctly configured to maintain the secure world's isolation from the normal world and that proper access control policies are in place to prevent unauthorized access to sensitive resources.

---

Question: Does OP-TEE support VMs?

Answer:

Yes, OP-TEE supports working with virtual machines (VMs) in the sense that it can operate in a virtualized environment managed by a hypervisor. The hypervisor is responsible for managing VMs running in the normal world, while OP-TEE provides secure services in the secure world.

In a virtualized environment, OP-TEE works in conjunction with a hypervisor, like Xen or KVM on ARM, to provide secure services to multiple VMs running on the same hardware platform. The hypervisor ensures the secure world's isolation from the normal world and enforces proper access control policies to prevent unauthorized access to sensitive resources.

However, it is important to note that OP-TEE itself does not directly manage the VMs; it works with a hypervisor that is responsible for managing the VMs in the normal world.

---

Question: Is the technology of OP-TEE supporting VMs mature?

Answer:

The technology of OP-TEE supporting VMs is maturing but may not be considered fully mature yet. There have been significant efforts put into enabling OP-TEE to work with virtual machines and hypervisors. OP-TEE does provide support for virtualization, as described in its documentation, and some projects, such as XEN Project, have been working on integrating OP-TEE with their hypervisors.

However, the maturity of this technology can vary depending on the specific use cases, hardware platforms, and hypervisors in question. It is advisable to assess the maturity of the technology on a case-by-case basis and consult with experts or the community to ensure that the chosen solution meets the required security and performance needs.

---