SC3010
Computer Security

Tutorial 5: Operating System Protection

Tianwei Zhang

Q1. Circle the correct answers in the following questions

1. For a reference monitor, which requirement refers to that the reference validation mechanism must be small enough to be analyzed and tested?

A. Function requirement.
B. Security requirement.
C. Assurance requirement.
D. Tamper-proof requirement.

Q1. Circle the correct answers in the following questions

2. Which of the following statement is false about TEE?

A. TEE can provide confidentiality and integrity protection, but not available protection.

B. Intel SGX allows multiple enclaves to exchange data at runtime.

C. In ARM TrustZone, the secure world has less restriction to access the hardware resources than the normal world.

D. In AMD SEV, both the privileged hypervisor and guest OS inside the VM are disallowed to access the protected application's data

Q1. Circle the correct answers in the following questions

3. Which of the following statement is false about virtualization?

A. Hypervisor is more privileged than operating system kernel.

B. Hardware support is required to virtualize and manage the hardware resources and enforce the isolation.

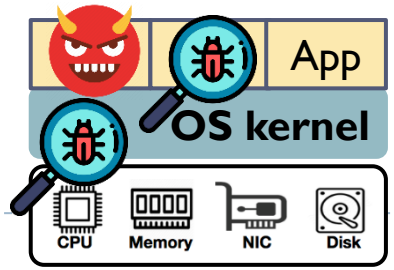
C. It is more challenging to protect the security of a virtualized system due to its more complex implementation.

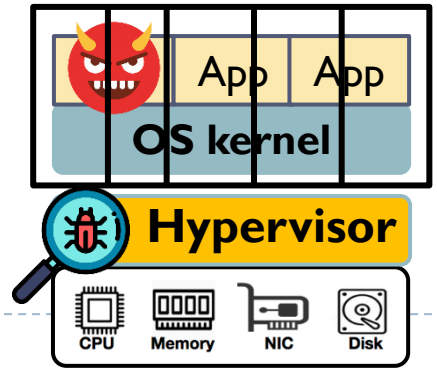
D. Different virtual machines can run different operating systems concurrently on the same physical machine

Q2. Answer the following questions

1. Describe what is the confinement strategy, and why it can be used for malware testing and analysis.

- *Confinement: isolate some components in the system and restrict its impact on other components.*
- *One important application: malware analysis.*
  - *When launching a malware inside the system and analyze its behaviors, the malware can be too strong to compromise the analyzer and the entire system. We can set up an isolated environment for the malware and analyze it from the outside.*
  - *One possible solution: deploy malware inside a virtual machine and analyze it from the hypervisor*





Q2. Answer the following questions

2. List the security functionalities offered by the TPM

- ***Platform integrity***: *building a chain of trust. Establish a secure boot process from the TPM, and continue until the OS has fully booted and applications are running.*

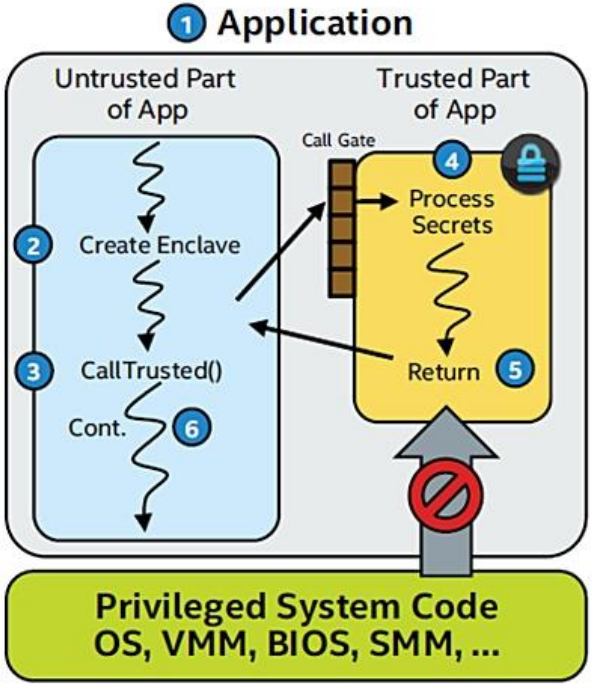
- ***Data encryption***: *encrypt the data with the key in the hardware. TPM can provide platform authentication before data encryption*

- ***Remote attestation***: *provide unforgeable evidence about the security of its software to the remote client.*

Q2. Answer the following questions

3. Describe the lifecycle of an SGX enclave application.

1. *The target application is divided into two parts: trusted and untrusted.*
2. *The untrusted part creates an enclave, and loads the code/data into this enclave.*
3. *During the execution, when the application needs to run the trusted code, the untrusted part calls an API to enter the enclave.*
4. *The trusted code is executed in the enclave.*
5. *After the trusted code is finished, it exits the enclave and returns to the untrusted code.*
6. *The untrusted code can continue the execution, and repeat steps 3-5 when trusted code needs to be executed again.*



Q3

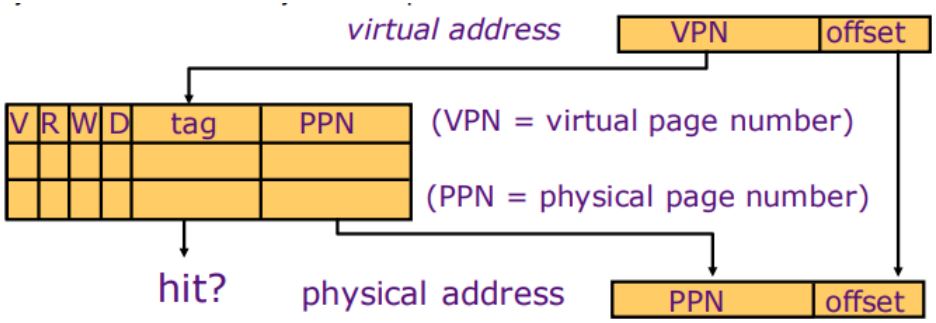
Early Intel processors (e.g., the 8086) did not provide hardware support for dual-mode operation (i.e., support for a separate user mode and kernel mode). If a system is implemented on such processors to support the multi-programming scenario, describe one confidentiality, integrity and availability threat respectively in this system, due to the lack of hardware support.

If there is no hardware support for different modes, then every component (user programs, kernel functions and services) has the same privilege. Then a malicious program can easily affect other processes, services and then the entire system. For instance:

- *Confidentiality threat: any malicious program can read the memory data of other processes and kernel as there is no memory access control restrictions.*
- *Integrity threat: any malicious program can modify the code of other processes and kernel as there is no memory access control restrictions.*
- *Availability threat: any malicious program can disable the interrupts, and avoid getting re-scheduled. Then it will occupy the CPU permanently while other processes can never be scheduled.*

Q4

Translation Lookaside Buffer (TLB) is a small hardware component that caches the recent translations of virtual memory to physical memory. It can help accelerate the memory access of programs. When a program wants to access the data with the specific virtual memory address, the system will check if there is an entry of this address in the TLB, and if the program has the access permission to this address. If both checks pass, then the corresponding physical address will be generated, and the access is allowed. Otherwise, a hardware interrupt will be triggered. The following figure shows the mechanism of the TLB. Note that the TLB can be updated only when the CPU is in the kernel mode.



Solution

a. The TLB can be regarded as one type of hardware-based reference monitor. Please list the requirements for a reference monitor.

Reference monitor: a security mechanism that monitors and mediates requests from the protected targets at runtime

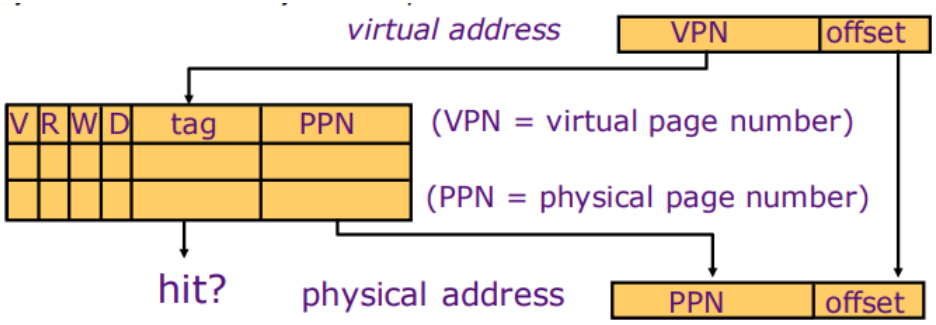
- *Enforce some security policies, e.g., confinement*
- *When any security policy is violated, RM can deny the request*

Requirements of RM:

- ***Function requirement**: the reference validation mechanism must always be invoked, i.e., it can observe all the requests and deny any malicious ones*
- ***Security requirement**: the reference validation mechanism must be tamper-proof*
- ***Assurance requirement**: the reference validation mechanism must be small enough to be analyzed and tested.*

Solution

b. Analyze if the TLB can satisfy these three requirements.



TLB can satisfy all the three requirements of RM:

- *Function requirement: all the memory accesses from all the program must go through the TLB. When the TLB denies this memory request, the program is not able to access the data*
- *Security requirement: any user-level program cannot change any entries in the TLB. Only the kernel has the privilege to do so*
- *Assurance requirement: the TLB is relatively a small hardware unit and is intensively verified. Hardware is usually more trusted compared to software components.*

Q5

Trusted Computing Base (TCB) is an important concept in computer security. It refers to the set of components (e.g., hardware, software, firmware, etc.) that must be trusted in order to guarantee the security of the entire system. Well protection of the TCB can defend the system against the threats from outside the TCB.

Solution

a. As a system designer, do we expect to have a larger TCB or smaller TCB? Why?

Smaller TCB is preferred.

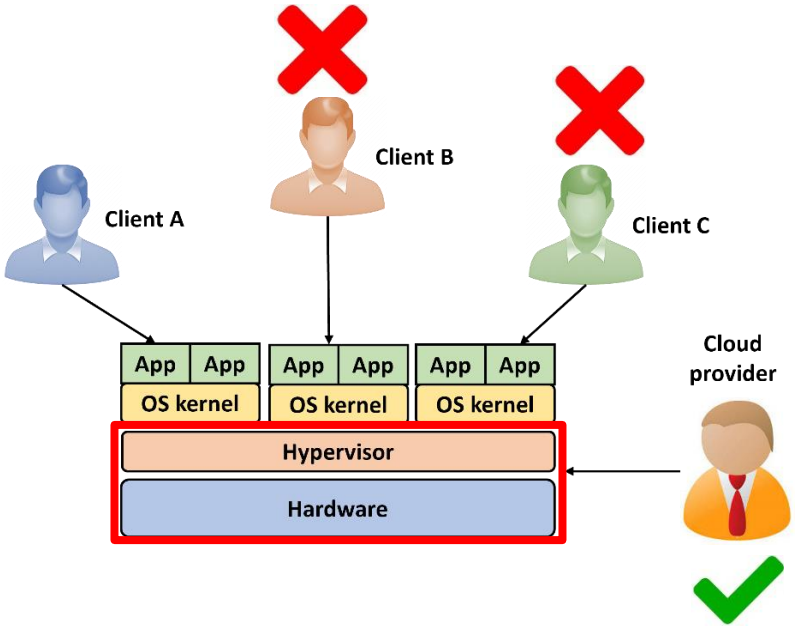
The components inside the TCB must guarantee to be trusted. When designing a system, it is more challenging to make more, and larger components trusted. An ideal secure system is to have a minimal TCB, which can defeat any threats from any components outside the TCB.

Solution

b. Consider a conventional cloud computing scenario, where you launch a virtual machine in a cloud service provider (e.g., Amazon). The following figure shows the system architecture of a cloud server running your virtual machines together with other users' virtual machines. Please specify which components are included in the TCB, and what entities and components are considered untrusted.

TCB: hardware and hypervisor in each cloud server. The cloud provider must be trusted.

The virtual machines from other clients can be untrusted. Even they contain malware, the hypervisor can provide isolation, and prevent the malware from compromising other virtual machines.



Solution

c. Assume the cloud provider adopts the TEE solution – AMD SEV processors to protect the users' virtual machines. In this case, specify which components are included in the TCB. Discuss how SEV processors can protect the virtual machines from untrusted components outside of the TCB.

TCB: only the hardware with the SEV feature in each cloud server. The hypervisor can be malicious, and the cloud provider does not need to be trusted.

The virtual machines from other clients can also be untrusted. The hardware provides protection and isolation from the hypervisor and other virtual machines.

- *Virtual memory encryption*
- *Remote attestation.*