2.1 Confinement strategy restricts the impact of a compromised component on other components. It can be used for malware analysis as a malware has the potential to compromise the entire system. A virtual machine creates an ideal environment so that the malware cannot cause damages outside of the VM and the malware's behaviour can be observed from the host OS

Solution: deploy malware inside virtual machine and analyse it from the hypervisor

SC3010 Computer Security

Tutorial 5 – Operating System Protection

1. 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.

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

   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.

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

   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.

target application divided into trusted and untrusted parts

2. Answer the following questions.
   1) Describe what is the confinement strategy, and why it can be used for malware testing and analysis.

      2.2 Platform integrity, Data Encryption and Remote Attestation

   2) List the security functionalities offered by the TPM.

   3) Describe the lifecycle of an SGX enclave application.

2.3 The untrusted part of the application creates an enclave and puts the trusted part into it. When the trusted code needs to be executed, the processor enters the enclave and only the trusted code can be executed and access the data. After code is completed, processor exits the enclave

untrusted code continue execution and repeat steps when trusted code to be executed again

3. 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.

4. 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

3. SQL Injection Vulnerability: A compromised input can include 1=1 which is always true, selecting the entire client data base and violating confidentiality.
Scripting Vulnerability: |rm -rf / can be added to an input and compromise it, causing all files in the script has permission to delete to be deleted, violating availability.
Format String vulnerability: important program flags that control access privileges are overwritten together with return addresses on the stack and function pointers.

If there is no hardware support for different modes, then every component has the same privilege. A malicious program can easily affect other processes, services and the entire system. For example, Confidentiality threat: any malicious program can read the memory data of 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. Avaiability threat: any malicious program can disable the interrupts and avoid getting rescheduled. It will occupy CPU permanently while other processes can never be scheduled.

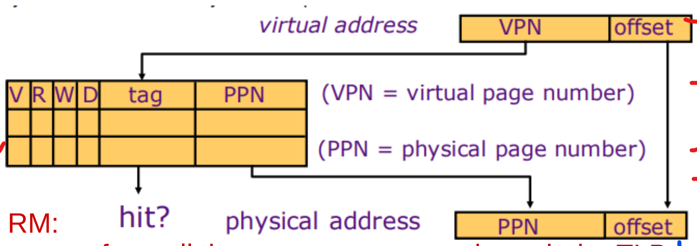
programs. When a program wants to access the data with the specific virtual memory address, the system will check if there is an entry of this address in the TLB, and if the program has the access permission to this address. If both checks pass, then the corresponding physical address will be generated, 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.

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

2) Analyze if the TLB can satisfy these three requirements.

4.1 Function requirement: reference validation mechanism always be invoked, reference monitor can observe all the requests and deny malicious requests
Security requirement: reference validation mechanism is tamper proof.
Assurance requirement: reference validation mechanism is small enough to be analysed and tested

4.2 Each process has a dedicated virtual memory address with the hardware responsible for checking each memory access. There are distinct user and kernel modes where the CPU can be in one mode at any time. Privileged instructions can only be issued in kernel mode. When user execute these functions, it switches to kernel mode for execution and goes back to user mode when finished.



TLB satisfy all three requirements of RM:
Function requirement: all memory accesses from all the program must go through the TLB
When TLB denies the memory request program not able to access the data
Security requirement: any user level program cannot change any entries in the TLB. Onyl the kernel has the privilege to do so.
Assurance requirement: the TLB is relatively small hardware and is intensively verified. Hardware is usually more trusted compared to software components

5. 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.

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

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.

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.

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

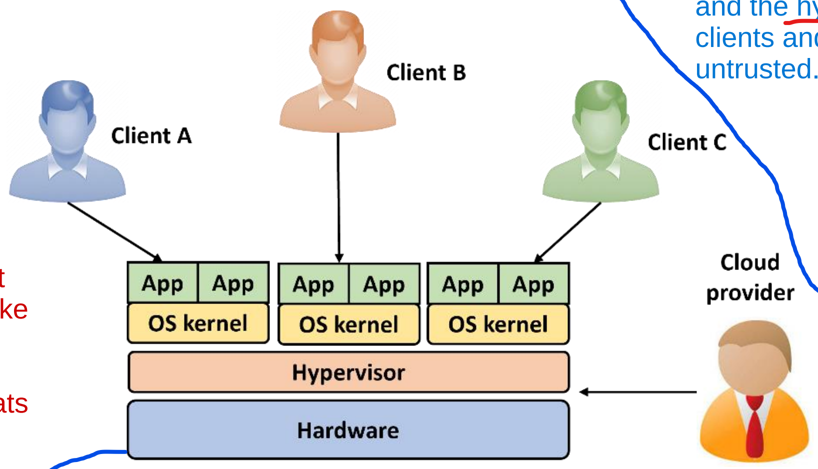
enforce security policies. When violated, RM can deny request

cloud provider must be trusted

5.2 The TCB composes of hardware and the hypervisor. The OS kernel, clients and apps are considered untrusted.

5.1 We expect a smaller TCB as it is hard to ensure the security of privileged software which contains lots of vulnerabilities. So the smaller the TCB, the better the security.

Components inside TCB must be trusted. Challenging to make more and largert components trusted. Best to have minimal TCB that can defeat any threats from any components outside TCB



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

VMs from other clients can be untrusted. Protection done with virtual memory encryption and remote attestation

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

5.3 The components included in the TCB are the hardware, ~~hypervisor~~ and the ~~OS kernels~~. The SEV processors introduce new hardware to protect apps from untrusted OS or hypervisor which support execution of apps but cannot compromise them. The data of apps cannot be read and the code of apps cannot be changed. Virtual machines are protected against the hypervisor and other virtual machines. The processor encrypts the data of guest virtual machines so hypervisor is not allowed to access the data.