CE4062/CZ4062 Computer Security

Tutorial 6 – Operating System Security (2)

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

   b. List the security functionalities offered by the TPM.

   c. Describe the lifecycle of an SGX enclave application.

2. 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.

3. 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. Figure Q3 shows the mechanism of the TLB. Note that the TLB can be updated only when the CPU is in the kernel mode.
   a. The TLB can be regarded as one type of hardware-based reference monitor. Please list the requirements for a reference monitor.

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

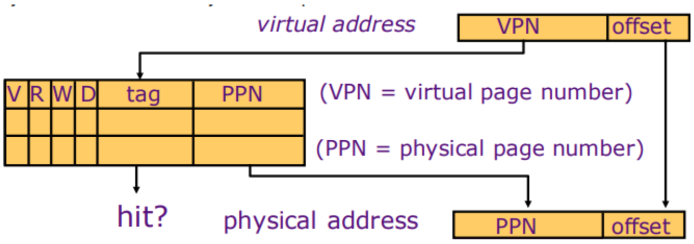

Figure Q3

4. 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). Figure Q4 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.

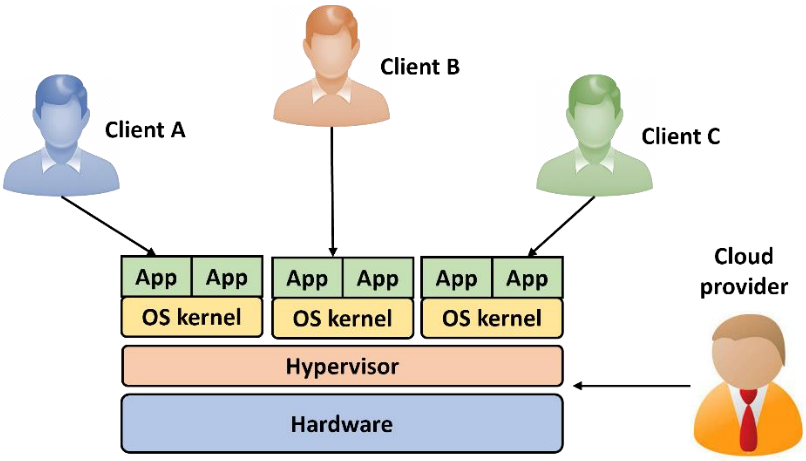

Figure Q4