University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions and Answers

Lecture 4: Computer Security

Question 1

Explain the meaning of the proposition: *"a trusted system or component is one that can break your security policy"* that is typically used to define trusted systems.

Answer

If the system is trusted, then it is relied upon to enforce the security policy. So there can be a breach of security policy when the trusted system does not work as expected. A non-trusted system on the other hand is not relied upon to enforce the security policy, so when it breakes it does not lead to a breach of security policy.

Question 2

Attempts of physical attacks against hardware components of a computer system can not be prevented when the system is physically accessible to attackers. However, such physical tampering can be frustrated with tamper resistant devices.

a. Describe the mechanisms implemented in the IBM 4764 Secure Coprocessor aimed at resisting tampering.
b. Mention some other mechanisms that could be used to frustrate tampering.

Answer

a. Hard shield around the semiconductor components. Environmental monitoring of temperature, power and structural integrity. Zeroization (resetting all memory to zero) of critical secret memory when tampering is detected.
b. Tamper resistant screws. Remote reporting. Security by obscurity e.g. in the form of confused chip architecture. Make it illegal to tamper with security hardware.

Question 3

TPM (Trusted Platform Module) is specified by the TCG (Trusted Computing Group).

a. Explain the three main services that the TPM supports: 1) Secure/authenticated boot, 2) Remote attestation, 3) Sealed storage.
b. Which TPM mechanism is used by the Bitlocker disk encryption applicaiton ?
c. Which security threat to Bitlocker does the TPM mechanism address?
d. Each TPM has a unique pair of public-private keys called *Endorsement Keys* (EK). How can an external party authenticate a particular TPM (and thereby a particular computer) based on the EK?

Answer

a. 1) Secure boot: Only boot when software has integrity, Authenticated boot: Boot anyway, and report the integrity of the software. 2) Remote Attestation: reporting to an external

party the integrity status of software and data. 3) Sealed storage: decryption with secret keys only with correct integrity
b. Bitlocker uses sealed storage.
c. The threat that an attacker removes an encrypted harddrive from a computer. It will not decrypt outside the original computer, even with password or USB key, because TPM is missing.
d. The external party can verify the authenticity of the public EK by means of a public-key certificate issued by the TPM manufacturer. Then the external party can authenticate the TPM based on the public EK.

Question 4

A detailed description of the protection mechanisms in the Intel microprocessors is given in the Intel microprocessor manual available from
`http://www.intel.com/design/processor/manuals/253668.pdf`
The Intel microprocessor provides 4 protection rings (0-3).

a. What is the main principle for allowing a process running in ring *m* to access a memory segment specified as ring *n*.
b. Which protection rings are actually used in Linux and Microsoft Windows?
c. What is the correspondence between protection rings and user/supervisor modes in Linux/Windows?

Answer

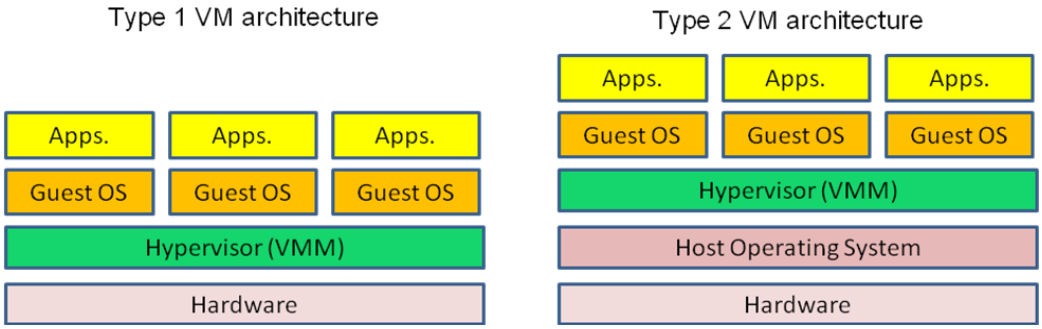
a. A process running in ring m can directly access a memory segment in ring n only if m ≤ n. Otherwise it must call an OS gate (OS function). Privileged instructions (e.g. setting values in specific register) can only be executed by processes running in ring 0.
b. Only ring 0 and 3 are normally used. Ring 0 for Kernel, OS and Drivers. Ring 3 for applications.
c. Processes in user mode run as ring 3, processes in supervisor mode run in ring 0.

Question 5

a. Describe the typical virtual machine architecture(s).
b. Mention advantages of running a virtual machine.
c. When used for security protection, a virtual machine must take advantage of the protection ring structure of the microprocessor. What is the danger when Guest OS kernels are allowed to run in ring 0?
d. Discuss options for allocating protection rings to the Host OS kernel, to the Hypervisor and to the Guest OS kernels in a way that provides meaningful security.

Answer

a. Virtual machine architecture is a layered structure. Two main types:



b. Advantages:
- Allows multiple OSs on same hardware
  - improved security because processes in different OSs are separated
  - improved management and resource utilization
  - reduced energy consumption (green hype)
- Take a snapshot of the current state of the OS
  - Use this later on to reset the system to that state
- Distribute applications bundled with OS
  - Allows optimal combination of OS and application
- Safe testing and analysis of malware
  - Malware can only infect the VM (guest OS)

c. A Guest OS in ring 0 can subvert the Hypervisor and/or the Host OS kernel.

d. Options for allocating protection rings are:

- Let the Guest OS kernels run in ring 1, so that only the Host OS kernel and the hypervisor run in ring 0. This requires the Guest OS to be recompiled as Guest OS.
- Use specialized hardware, e.g. Intel VT (Virtualization Technology) or AMD-V (Virtualization) that offer an additional ring -1, so that the Host OS and the Hypervisor run in ring -1, and the guest OS kernel can run in ring 0 as before. This requires the Host OS and the Hypervisor to be specially designed and compiled to run in ring -1.

Question 6

a) Assume that an attacker has found a way to produce input data that crashes a program due to a buffer overflow error. The input could e.g. be a particular MSWord Document in MSOffice. Roughly explain what is needed to exploit this bug to create an attack.

b) What is the name of the technique used to find bugs that cause program crashes which potentially can be used to create exploits?

Answer:

a) The attacker must determine the structure of the stack frame where the input arguments are stored in memory, and craft the input arguments in such a way that they overwrite the EIP (Extended Instruction Pointer) with a specific address which points to a memory location where the attacker has placed malicious code.
b) Fuzzing or Fuzz Testing, which consist of generating many different random inputs to applications in order to make them crash, which could indicate a buffer overflow bug.

Question 7

The CC (Common Criteria) has replaced TCSEC and ITSEC as framework for security evaluation of IT products.

a. Describe the meaning of the following terms used by the CC:
   - TOE (Target of Evaluation)
   - ST (Security Target)
   - PP (Protection Profile)
   - EAL (Evaluation Assurance Level)
   - SFR (Security Functional Requirement)
   - SAR (Security Assurance Requirement)
b. Investigate the PP CAPP (Controlled Access Protection Profile). What is the EAL specified in the PP CAPP? How does this assurance level compare to that of a system with the same functionality that is evaluated under TCSEC?
c. Which of the following security systems would it be meaningful to evaluate under TCSEC and under CC?
   i) A data diode (a hardware device for interconnecting two networks that guarantees that data can only flow on one direction).
   ii) A system that provides discretionary access control only.
   iii) A system that provides labelled multilevel security only.
   iv) A system that provides both discretionary and labelled multilevel security.
   v) The encryption software package PGP (Pretty Good Privacy).

Answer:

a. Terms used by the CC:
   - TOE: The system to be evaluated.
   - ST: A document that provides a system-specific description of the security objectives, threat environment, the SFRs, the SARs and the EAL.
   - PP: A document that provides a system-independent description of security objectives, threat environment, SFRs, SARs and the EAL.
   - EAL: A numerical grade (1-7) assigned following the completion of a CC security evaluation. Increasing EAL reflects added assurance requirements. Higher EAL provides higher confidence that the system's security features are reliably implemented. The EAL level does not measure the security of the system itself, it simply states at what level the system was assessed/tested.
   - SFR: consists of 11 Classes, each class consists of a set of families, each family consists of a set of components.
   - SAR: consists of 6 Classes, each class consists of a set of families, each family consists of a set of components.
b. The assurance level of CAPP is higher than that of a C2 system.
c. TCSEC: Yes to ii) and iv). CC: Yes to all.