



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.

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.

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

Question 3

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

- Explain the three main services that the TPM supports: 1) Secure/authenticated boot, 2) Remote attestation, 3) Sealed storage.
- Which TPM mechanism is used by the Bitlocker disk encryption application?
- Which security threat to Bitlocker does the TPM mechanism address?
- 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?

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).

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

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.

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?

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).