University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 4: Computer Security

Question 1

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.

Question 2

The 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. What mechanism is used by the TPM to verify the integrity of software and data?
c. Describe how the TPM could be used to control what software users must use?
d. Each TPM has a unique pair of public-private keys called *Endorsement Keys* (EK). How can an external party authenticate a particular TPM based on the EK?

Question 3

BitLocker is a technology used by Vista and Windows 7 for disc encryption.

a. Describe the four (4) protection alternatives that BitLocker offers.
b. How can a volume be recovered if the primary key is lost?
c. Describe a situation when an encrypted volume is irrevocably lost, i.e. when BitLocker will refuse to decrypt.

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 used in Linux and Microsoft Windows?
c. What is the correspondence between protection rings and user/supervisor modes in Linux/Windows?

Question 5

a. Describe the typical architecture of a virtual machine.
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

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).