University of Oslo
INF3510 Information Security
Spring 2010
Workshop Questions

Lecture 10: Computer Security and Trusted Systems

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

DRM (Digital Rights Management) focuses on principles for enforcing policies for using digital content.

a. What is the main difference between implementing DRM on a specific appliance device (e.g. DVD player) and on a general purpose computing platform (e.g. PC)?
b. How does HDCP (High Definition Content Protection) prevent clear text HD video signals from being exposed withing a computing platform and along the path to the display device during HD content playback?

QUESTION 3

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

a. Describe the three (3) main services of the TPM: *Protected Storage*, *Measurement*, and *Remote Attestation*.
b. *Sealed Storage* can also be considered a main service of the TPM. What is sealed storage, and how can it be supported by the TPM?
c. Describe how it could be possible to control what software runs on a system with a TPM?
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 4

What is the difference between *secure boot* and *authenticated boot*?

QUESTION 5

BitLocker is a technology used by Microsoft for volume encryption.

a. Describe the four (4) protection types used by BitLocker.
b. How can a volume be recovered if the primary key is lost?
c. Describe a situation when an encrypted volume is irrevocably lost because no decryption key can be obtained.

QUESTION 6

The Intel microprocessor has 4 protection rings (0-3) and uses the CPL (Current Privilege Level), the RPL (Requested Privilege Level) and the DPL (Data Privilege Level) to decide whether a process can access a memory segment. 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`

a. What do these levels refer to, and how are they set?
b. A process with CPL=0 requests access to a segment with DPL=2. What are the possible RPLs that would make the processor grant this access?
c. Which levels are used in Microsoft Windows?