University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 7: Computer Security

Question 1

a. Why do Operating Systems use Virtual Address Space and Virtual addressing instead of physical addresses for the running processes?
b. What is the advantage and disadvantage of using Virtual Address Space?

Question 2

a. What is "Data Execution Prevention" and what is the purpose of it?
b. What is ASLR (Address Space Layout Randomization) and what is the purpose of it?

Question 3

a. What is the difference between the following concepts?
   - *"a trusted system"*
   - *"a trustworthy system"*
b. Explain the meaning of the following statement:
   - *"A trusted system can break information security"*.

Question 4

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

a. Explain the three main TPM supported services: i) authenticated boot, ii) Sealed storage, iii) Remote attestation.
b. Which TPM service is used by the Windows Bitlocker disk encryption application?
c. Assume that a computer has a zero-day vulnerability used by an exploit to take control of the computer. Answer Yes/No to whether the TPM can protect against this threat, and explain why / why not.

Question 5

What is the difference between secure boot and authenticated/measured boot?

Question 6

In order to run virtualization on a computer it is necessary that ‘hardware virtualization’ is enabled in the BIOS. Why is hardware virtualization often disabled in new computers, so that users manually have to enable it when they want to run a hypervisor on the machine ?

Question 7

a. What is Intel ME (Management Engine) ?
b. What is the purpose of Intel ME ?
c. What is MINIX ?
d. What is Intel AMT (Active Management Technology) ?
e. In what way does Intel ME and AMT expose computers to cyberthreats ?

Question 8

Supposed you want to implement a “root of trust of measurement” based on TPM.

a. Where would you decide to store your program?
b. Where would you not store it?
c. Discuss why and why not, with reference to a) and b) above.

Question 9

a. Explain the principle of secure boot based on UEFI (Unified Extensible Firmware Interface).
b. Why is it not an example of trusted computing boot process?