University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions

Lecture 6: Computer Security

Question 1

a. What is the difference between *"a trusted system"* and *"a trustworthy system"* ?
b. *"A trusted system or component is one that can break your security policy"*. Explain the meaning of this proposition.

Question 2

Attempts of physical attacks against security hardware components of a computer system can not be prevented when the system is physically accessible to attackers. However, such physical tampering can be prevented with tamper proof devices. Look at the specification for the IBM 4765 Secure Coprocessor at
https://www-03.ibm.com/security/cryptocards/pciecc/pdf/PCIe_Spec_Sheet.pdf

a. In which situations will the IBM 4765 Secure Coprocessor self-destruct, i.e. zeroize memory and permanently disable itself?
b. Suggest mechanisms for tamper resistance of security hardware.

Question 3

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

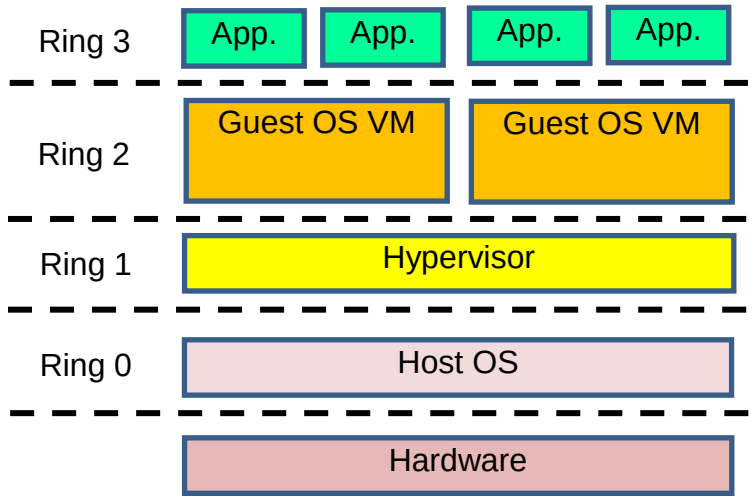
a. Explain the three main TPM supported services: 1) authenticated boot, 2) Sealed storage, 3) Remote attestation.
b. Which TPM service is used by the Windows Bitlocker disk encryption application?
c. Which security threat to Bitlocker does the TPM mechanism address?
d. Assume that a computer is exposed to a zero-day vulnerability that potentially could be exploited to take control of the computer. Say Yes/No whether the TPM can protect against this threat, and explain why / why not ?

Question 4

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

Question 5

An alternative to introducing Ring -1 for virtualization could have been to instead use Ring 1 and 2 as illustrated in the diagram below.



Discuss how practical or meaningful this would have been.

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 ?