University of Oslo
INF3510 Information Security
Spring 2017
Workshop Questions and Answers

Lecture 6: Computer Security

Question 1

"A trusted system or component is one that can break your security policy".
Explain the meaning of this proposition.

Answer

If the system is trusted, then it is relied upon to enforce the security policy. So the security policy will be broken when the trusted system does **not** work as expected. A non-trusted system on the other hand is not relied upon to enforce the security policy, so when it breaks it does not lead to a breach of security policy.

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.

Answer

a. Reasons for self-destruction of the IBM 4765 Secure Coprocessor are:
    - The on-board batteries have run out of power without timely replacement.
    - A too high or too low temperature has been detected.
    - A too high or too low voltage has been detected.
    - Physical damage to the shield has been detected.
b. Tamper resistant screws. Hard shield. Remote reporting. Security by obscurity e.g. in the form of confused chip architecture. Make tampering illegal.

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 ?

Answer

a. 1) Authenticated boot: Report the integrity status of the software when booting.
   2) Sealed storage: decryption with secret keys only with correct integrity,
   3) Remote Attestation: reporting to an external party the integrity status of software and data.
b. Bitlocker uses sealed storage.
c. Bitlocker with TPM can protect against the following threats:
   - A harddrive removed from computer will not decrypt outside the original computer, even with password or USB key, because the TPM is missing.
   - The loss of integrity of specific software or data files on the computer, determined by non-match of the corresponding measurement values with the values stored in the PCR registers.

   These threats are not very relevant. So Bitlocker with TPM is rather meaningless. It is not necessary to run Bitlocker with TPM, it works fine without.
d. TPM does not protect against zero-day infection during runtime, because it only protects the boot process. A zero-day malware infection in a software module protected by secure boot will be detected next time the computer boots. A zero-day malware infection in a software module not covered by secure boot will not be detected by secure boot, and will by definition not be detected by anti-malware.

Question 4

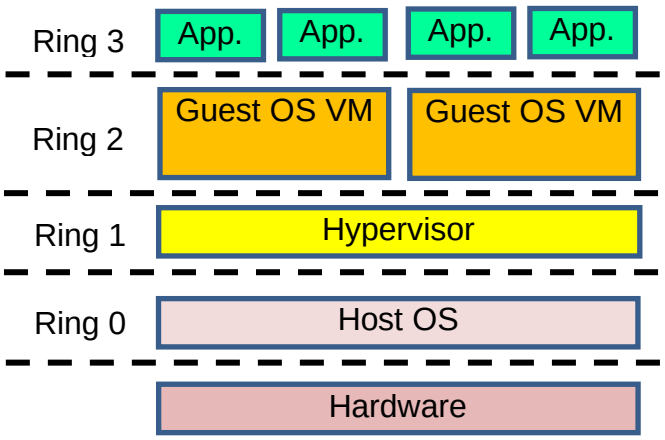
What is the difference between secure boot and authenticated/measured boot?

Suggested answer:

- Secure boot means that the digital signatures on boot loader, kernel and drivers must be correct for the boot sequence to complete. This is supported by UEFI.
- Authenticated/measured boot means that the boot sequence will not be halted, but the measures of software modules will be reported to the user or to remote parties. This is supported by the TPM.

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.

Answer

This is similar to Type 2 VM architecture (hosted). The main problem is that OSs expect to be able to execute privileged microprocessor instructions that are only available in Ring 0.Running guest OSs in ring 1 or 2 causes the Host OS to intercept calls to forbidden instructions and execute them on behalf of the guest OS. The same would apply to the hypervisor which needs to execute instructions that are forbidden in Ring 1. Every time a process tries to execute a forbidden instruction the exception handler is called so that the host OS will determine what to do. This would cause significant execution delays.

Question 6

a) Imagine that your company plans to develop a system to be sold to government and military customers. The system will be used in high security environments and will contain important security functions, and hence the government/military customers will only consider buying systems with certified security evaluation. Describe the main steps that your company must go through in order to get the required security evaluation certification for the system.

b) Imagine that your company is already producing a security product, but it has no security evaluation certification. Which is the highest assurance level that this product can be certified for? Explain why.

Answer:

a) The main steps are:
   1. Find out which protection profile and the required assurance level that the system must comply with.
   2. If the assurance level is 5 or higher, then prepare for producing R@D assurance documentation.
   3. Collect and produce detailed system specification.
   4. Contact the security evaluation authority to request evaluation.
   5. Submit system with documentation to evaluation laboratory.
   6. Reply to request for additional information from evaluation laboratory

b) Assurance level 4 is the highest if the system has already been developed. Assurance levels 5 and higher require documentation of the R&D process, so it's too late if the system has already been developed.