University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions and Answers

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.

Answer

a. A trusted system is a system that you (the user) have decided to depend on for a certain usage or application. A trustworthy system is a system that is objectively reliable and that can be objectively depended upon without risk for a certain usage or application. You never really know with 100% certainty whether a system is trustworthy, but you can decide for yourself whether a system is trusted. Thus, a totally untrustworthy system can be a trusted system, but it would require you (the user) to be foolish or ignorant.

b. 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

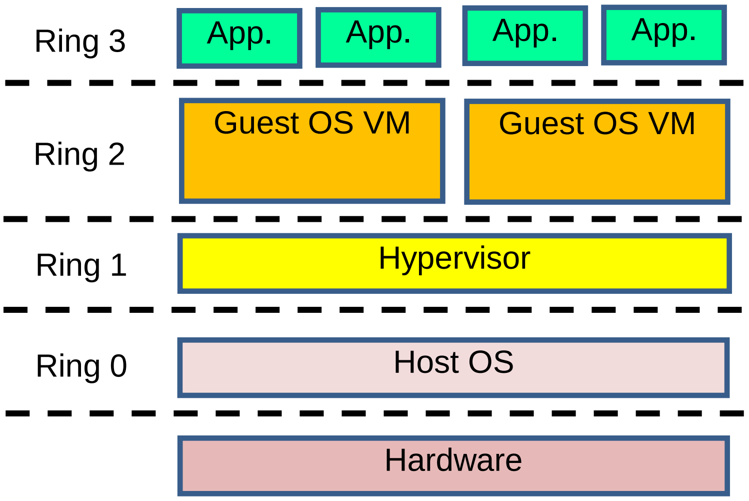
What is the difference between secure boot and authenticated/measured boot?

Suggested answer:

a. 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.
b. 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 privileged instructions (that are forbidden in Ring 1 or 2) in order to execute them on behalf of the guest OS. The same would apply to the hypervisor which needs to execute privileged 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

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 ?

Suggested answer:

c. There have been several attacks where malicious drivers could exploit virtualisation to corrupt the OS execution and take control over the whole platform. Since virtualization exploitation attacks are impossible when virtualization is disabled, vendors often ship computers with virtualisation disabled so that the default configuration is more secure.

d. Virtualisation enables additional hardware instructions in the CPU, which can give a penalty on performance. The smaller the instruction set the more efficient the CPU runs. Having virtualization disabled reduces the instruction set and allows the CPU to cache fewer instruction and thereby run faster.

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 ?

Suggested answer:

a. Intel ME is a small, low-power computer subsystem which is integrated with Intel CPUs. Intel ME runs its own operating system called MINIX, and is active when the main operating system (Windows, Linux, MacOS, hypervisor) is asleep, booting up, and running normally. Intel ME has full access to system hardware, including the system memory, display, keyboard, camera, microphone, peripherals and network.
b. According to Intel, the Intel ME “performs various tasks”, but Intel provides few details about what these tasks are. Intel AMT is e.g. a service provided by ME. https://www.intel.com/content/www/us/en/support/articles/000005974/software/chipset-software.html
c. MINIX is a microkernel operating system. MINIX is small in size and has a very limited set of functions, which allows it to have low power consumption and small footprint (physical size) in embedded systems. Intel ME runs MINIX. http://www.cs.vu.nl/~ast/intel/
d. Intel AMT is a remote CPU management service implemented in Intel ME. It can be used on servers, desktops, laptops, and tablets that run Intel CPUs. Target users are typically large organizations, not home users. AMT must be actively enabled in the BIOS/UEFI, and is disabled by default when servers are shipped. AMT can be used to remotely power on, configure, control, or wipe computers running Intel CPUs. Unlike typical platform management solutions, AMT works even if no operating system (Windows, Linux, MacOS, hypervisor) is installed.
e. Intel ME has full control over Intel CPUs, and is therefore the most privileged function of a computer platform. AMT allows this function to be remote controlled. Relevant threat scenarios are e.g. that attackers manage to take control over ME, e.g. via remote access based on AMT. Real attacks have been reported: https://www.intel.com/content/www/us/en/support/products/34227/software/chipset-software/intel-management-engine.html