

Cybersecurity: Technology and Governance

Audun Jøsang
1st edition 2024
Springer Nature



Exercises

Chapter 3: System Security

Task 1: Trust Anchor

What is meant by the term "trust anchor" in system security?

Task 2: Virtualization

- What is the difference between a general "system" and a "virtual system"?
- What is a virtual machine when talking about computers?
- How can virtualization support security?

Task 3: Privilege Levels

Watch the YouTube video *Replace Your Exploit-Ridden Firmware with Linux*

<https://www.youtube.com/watch?v=iffTJ1vPCSo>

- Assume VM architecture Type 1 (native/direct): What privilege levels do processes have for (i) a user in a VM, (ii) administrator/root in a VM, and (iii) hypervisor?
- Assume VM architecture Type 2 (hosted/hosted): What privilege levels do processes have for (i) a user in a VM, (ii) administrator/root in a VM, and (iii) hypervisor?
- Technically, microprocessors support the privilege levels from -1 to 3. Informally, there is also talk that the privilege levels -2 and -3 exist. What is meant by these levels?
- What is Intel ME (Management Engine)?
- What is Intel AMT (Active Management Technology)?
- In what way can it be said that Intel ME and AMT pose vulnerabilities?

Task 4: Prevent cell phone tracking

Just like with regular computers, the microprocessor in a smartphone is active as long as the phone has power. Threat actors with sufficient expertise can exploit this to track a mobile phone even when it is completely turned off. Suggest measures that prevent a mobile phone from being tracked in this way.

Task 5: Protecting Memory

- a. Many processes run simultaneously on a computer. Explain why a user process (with privilege level 3) cannot access the memory space (data and code) to other processes.
- b. What is stack canaries and what is its purpose?
- c. What is Address Space Layout Randomization (ASLR) and what is its purpose?

Task 6: Trusted Platform Module (TPM)

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

- a. Explain the three main TPM-supported services: i) Authenticated/Secure Boot, ii) Sealed Storage, iii) Remote Attestation.
- b. What TPM service is used by the Windows Bitlocker disk encryption application?
- c. Suppose a computer has a zero-day vulnerability that an exploit exploits to take control of the computer. Can TPM protect against this threat? Explain why/why not.