

Cybersecurity: Technology and Governance

Audun Jøsang
1st edition 2024
Springer Nature



Exercises

Chapter 1: Basic security concepts

Task 1: Access authorization

- X.800 is a standard for security services in OSI (Open Systems Interconnection). Search and find the X.800 standard, or visit <https://www.itu.int/rec/T-REC-X.800-199103-I/en>
Read the definitions of confidentiality, integrity, and authorization in X.800. Are the definitions of confidentiality and integrity from X. 800 meaningful in relation to how authorization is defined? Why or why not?
- How is authorization defined on Wikipedia? <https://en.wikipedia.org/wiki/Authorization>
- Explain whether the definitions of confidentiality, integrity, and availability (KIT) in the X.800 and ISO/IEC 27000 standards make sense based on Wikipedia's definition of authorization.

Task 2: Examples of attacks that can result in a breach of the KIT

Describe examples of attacks that can cause security breaches for each KIT security target, and possible actions that can prevent the attacks. The attack descriptions must be very abstract, such as. *"A hacker steals a password and takes over another person's account."*

- Confidentiality
- Integrity
- Accessibility

Task 3: Threats to IAM (Identity and Access Management)

A simple method to identify threats is to ask "What could go wrong?" or "How can this be attacked?".

- Mention relevant threats to (the steps in) the configuration phase of IAM (identity and access management).
- Mention relevant threats to (the steps in) the use phase of IAM (identity and access management).

Task 4: User authentication and data authentication

A user has authenticated to a website on the Internet at the start of a session and is using services on the web server via the client computer. Explain possible scenarios that cause the website/web server to receive false data from the client computer during the session, i.e. data that **is not** authentically sent by the user, despite the user being correctly authenticated.

Task 5: Personal Laptop Security Policy

Articulate a simple (2-3 sentence) security policy for your personal laptop, stating who is or who may be authorized to use the laptop while you own it.

Task 6: ISO/IEC 27000 ISMS – Overview

Look at the ISO/IEC 27000 Information security management systems — Overview and vocabulary standard;

https://www.mn.uio.no/ifi/forskning/grupper/sec/sikkerhetsledelse/iso_iec_27000_2018.pdf

- a. What is the difference between a *security incident* and a *security event*?
- b. What is an Information Security Management System (ISMS)?
- c. Give an interpretation of the term "information asset"?
- d. Explain whether the CIA for information assets is adequate as a general information security objective? Propose an alternative general information security objective.
- e. Explain meanings of the terms "information asset" and "digital asset".