COM-301 Computer Security
Exercise sheet: Computer security principles

Note: Some of these exercises could have multiple acceptable answers. The answers we provide are jut one example. If you have another answer and would like to check, use the forum or send us an email or ask us during the exercise sessions or ask for student hours.

1. A company publishes the design of its security software product in a manual that accompanies the executable software. In what ways does this satisfy the principle of open design? In what ways does it not?

2. A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts. Discuss how this technique might prevent legitimate users from accessing the system. Why is this situation a violation of the principle of least common mechanism?

3. Explain, in terms of the security principles, why it is not a good idea to revert the execution of a program that writes in memory regions that was not allocated for this program to reserve more memory. What is a better option than reverting in terms of security ?

4. The IC Building elevator requires card key access to go to the 4th floor. The door connecting the stairs and the 4th floor opens without a card. Which of the following security principles is missing in this design?

   (a) Fail-safe defaults

   (b) Complete mediation

   (c) Separation of privilege

5. You are building a system and following the Compromised Recording principle you decide to create a log to register accesses to a very sensitive file `ImportantStuff` to detect if someone non authorized has accessed the file. Are the following good or bad ideas to make sure that this log fulfills its goal (justify your answer in terms of security principles):

   (a) Store the log in the same folder as the `ImportantStuff` file.

   (b) Keep two copies of the log on the same machine as `ImportantStuff` file. to the log.

(c) If you detect an suspicious access, stop every user from accessing `ImportantStuff`

(d) Store in this log information about other file `LessImportantThings`.