COM-402 exercises 2024, session 5: Access control and authentication

Exercise 5.1

- Explain what is the most important principle for access control in IT systems.

Exercise 5.2

- What is the difference between ACLs and capabilities?

Exercise 5.3

- Describe an advantage and a disadvantage of RBAC.

Exercise 5.4

Linux systems store password hashes and other information about user accounts in a file called `shadow`. The file has the following access rights:

- `There is a program called unix_chkpwd that is owned by the user root and the group shadow. It has the setgid bit set:`

  `What could be the reason for the setgid to be set?`

Exercise 5.5

When mandatory access control (MAC) is used to protect the integrity of a system:

- Can a subject write to objects on levels above or below it (write-up or write-down)? Explain.
- Give an example of how an operating system can use MAC to protect its integrity.

Exercise 5.6

Consider the Universal 2nd Factor (U2F) authentication system.

- Explain why the name of the visited website is added to the information signed by U2F.
- Explain why a U2F second factor is better than an OATH based one time password (OTP).

Exercise 5.7

- Is a biometric authentication system with a false acceptance rate of 0.01% a good system?

Exercise 5.8

What is the role of the AS and TGS in Kerberos? Why are they separate?

Exercise 5.9

- When you change your password on the website of Twitter, you can still access Twitter from you smartphone, without giving the new password. How is this possible?