DM510 Operating Systems
Spring 2026

Exercise Sheet 9

Complete before tutorial on Thursday, April 23th

Learning goals

Be able to

- name the four layers of security.
- explain buffer overflows and how to prevent them.
- explain functionality of symmetric and asymmetric encryption
- explain protection domains, capability list, access-control matrix
- understand and use Unix file protection notation
- execute Unix superuser
- explain principle of least priviledge, need-to-know principle and principle of compartmentalization

Exam preparation

Exercise 1. Take a look at the instructions and old exams at https://larsrohwedder.com/teaching/dm510-26/res and https://larsrohwedder.com/teaching/dm510-26/plan. If time permits in the exercise session (possibly also next week), recap course materials by discussing exercises in the old exams.

Chapter 16

Exercise 2. Give three examples where protection mechanisms in some layer of security can be circumvent by a breach of another security layer.

Exercise 3. Discuss the following approaches to protect against buffer overflow attacks:

- Which better programming practices can help against buffer overflows?
- Some compilers write "canary words" after the end of a buffer. These are specific values that should not be modified by a correctly working program. The compiler also needs to insert checks for whether the canary words have been modified. Where should this occur?

- How can a hardware bit in the page table, which indicates that a page is executable code or not, help against buffer overflow attacks?

Exercise 4. What is the purpose of using a "salt" along with a user-provided password? Where should the salt be stored, and how should it be used?

Exercise 5. A denial-of-service (DOS) attack may try to make a website unavailable by initiating more HTTP requests than the website can handle. what makes it difficult to protect against such an attack? discuss aspects that can make a DOS attack more effective and counter-measures.

Exercise 6. An encrypted TCP/IP connection typically uses symmetric encryption, but asymmetric encryption is still required for the initial key exchange.

- Explain how this key exchange can be performed
- Suppose you connect to a website via HTTPs (HTTP inside an encrypted TCP connection) for the first time and your computer does not have a copy of the website's public key. If you would simply download the public key from this website before establishing the encrypted connection, what kind of security problems might occur?
- The previous problem is usually solved using trusted authorities. Imagine there is an authority and every computer is delivered with this authority's public key. Websites can request from the authority to confirm (using digital signature) that their public keys belongs to their host name (for example, that key 123 is the correct public key for larsrohwedder.com). Explain the procedure in detail and how it resolves the previous problem.

Chapter 17

Exercise 7. In some systems, when a sensitive file is deleted, its storage area is overwritten by some random bits. What is the purpose of such a scheme?

Exercise 8. Consider a computing environment where a process is given the privilege of accessing an object only n times. Suggest a scheme for implementing this policy.

Exercise 9. Capability lists are usually kept within the address space of the user. How can the system ensure that the user cannot modify the contents of the list?

Exercise 10. The access-control matrix can be used to determine whether a process can switch from, say, domain A to domain B and enjoy the access privileges of domain B. Is this approach equivalent to including the access privileges of domain B in those of domain A?

Exercise 11. Give a real-world example each for:

- the principle of least priviledge
- need-to-know principle

- principle of compartmentalization

Exercise 12. In Linux, you can execute programs as the "superuser" with elevated priviledges by running `sudo <command>`. You can also switch permanently to the superuser by typing `sudo su`. Since it can be cumbersome to always remember to type `sudo`, would it be a good idea to always switch to the superuser in the terminal?

Exercise 13. Explain the following Unix protection settings and translate them into the other (decimal or rwx) notation

- `rwxr--r--`
- 755
- `rwxr-x---`