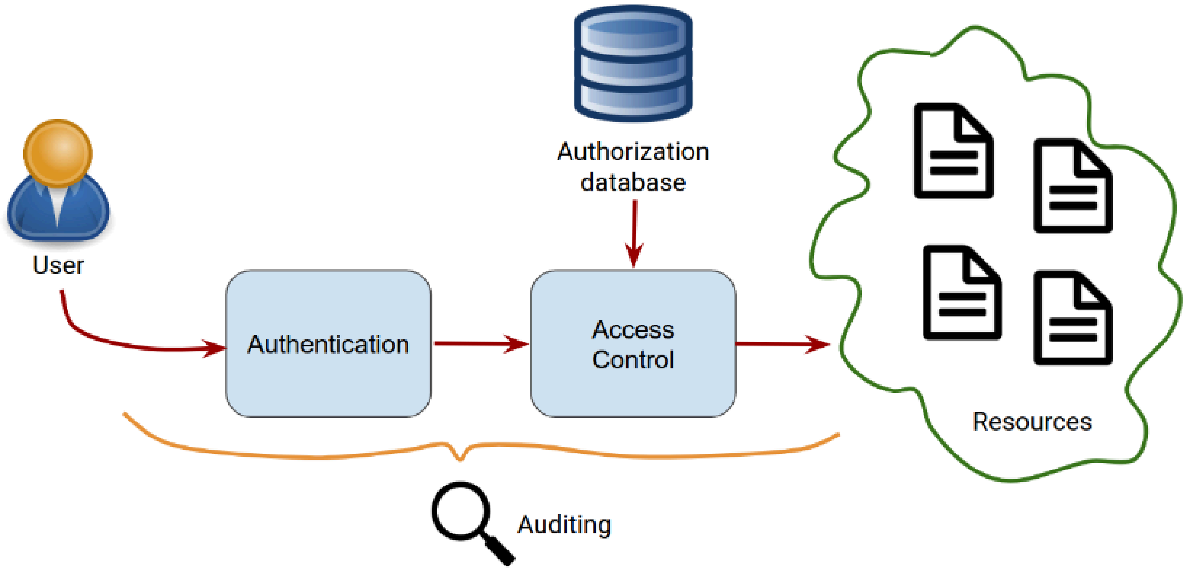
Lezione7

Access Control

Definition

From RFC 4949:
Protection of system resources against unauthorized access.

This is basically the process that regulates the **system resources** according to a **security policy**.
According to the previous policy, access is permitted only by authorized entities (users, . . .).



Where:

- Authentication: Verification of system entity (e.g. user) credentials are valid.
- Authorization: **Granting of a permission/right** to a system entity to access a system resource. This determines *who's trusted for that purpose*.
- Audit: **Independent review** and examination of system records and activities to:
  - Test for adequacy of controls
  - Ensure compliance with the policy
  - Detect breaches in security and change the environment accordingly.
- Subject: The entity capable of accessing resources.
- Object: the resource to which access is controlled.

Access rights

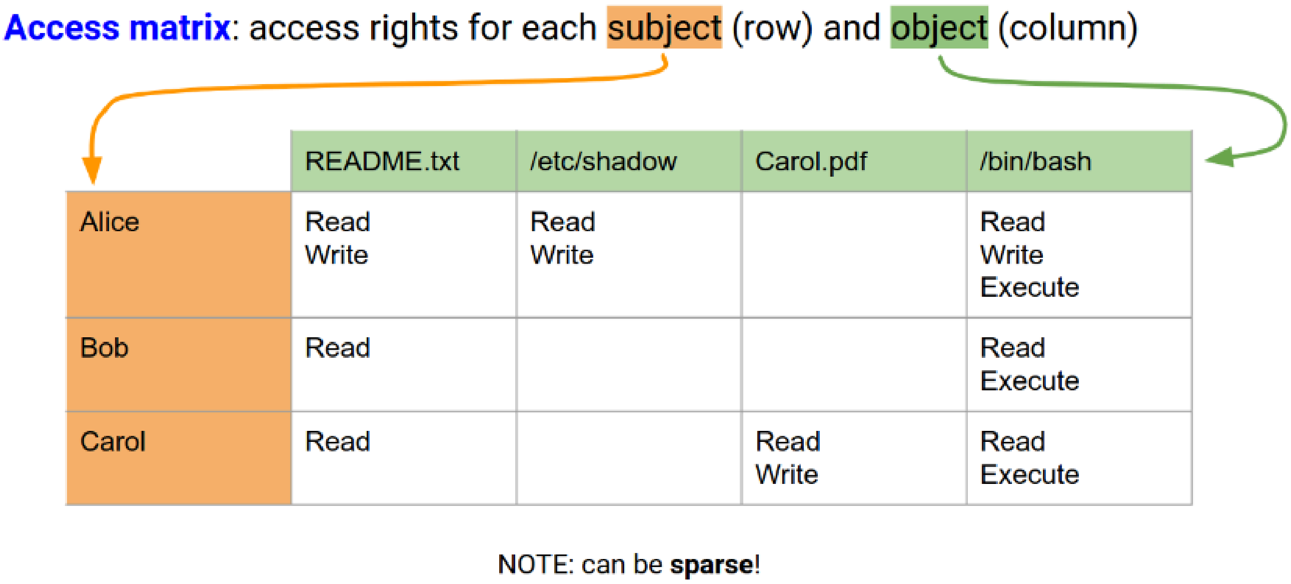
- Read: Viewing information in an object (Confidentiality)
- Write: Add, modify, delete data in a object (Integrity)
- Execute: Execute the object.
- Delete: Delete the object.
- Create: Create the object.
- Search: Search into the object.

Access control policies

Discretionary Access Control (DAC)

Access matrix

Access right for each subject and object



Access matrix: access rights for each subject (row) and object (column)

	README.txt	/etc/shadow	Carol.pdf	/bin/bash
Alice	Read Write	Read Write		Read Write Execute
Bob	Read			Read Execute
Carol	Read		Read Write	Read Execute

NOTE: can be **sparse**!

This type of access control is theoretical only, not efficient in practice because there are tons of files and users and creating this kind of table is inefficient.

Access Control List (ACL)

For each object lists subjects and their permission rights. (Check access matrix by column)
e.g.
README.txt:
- A: R,W
- B: R
- C: R,W,X
Pros:
Easy to find which subjects have access to a given object.

Cons:
Hard to find the access rights for a certain subject.

Capabilities

For each subject, list object and access rights to them (Check access matrix by row).
Pros:
Easy to find access rights for a given subject.
Cons:
Hard to find all subjects that have access to a certain object.

So, can we have the pros of both?
Yes, using the authorization table:
For each row there will be [Subject, Access Rights, Object]
Depending on which parameter you query, you get either capabilities or ACL.

A subject can give different accesses (read, write, ...) to other subjects if he owns the objects.

If a malicious object (program) is executed by a subject, it can leak privileges by giving read access to other subjects.
Or simply, the subject can mistakenly give access to other subjects.

Mandatory Access Control (MAC)

Rules that the subjects **cannot** change.
For example: A subject has a clearance "secret", that allows him to access secret file but does not allow those files to be accessed by "public" subjects.
This prevents two things:

- Leakage due to malware execution: the malware would run with the same privileges as the subject.
- Leakage due to subject error: every new object is created with the same privileges as the subject.

Security levels

They define the level of security with reference to a certain property.

Bell - La Padula

- Subjects have a security level called **clearence**.

- Object have a security level called **classification**.