Enrico RUSSO

Andrea VALENZA

Università di Genova

Access Control theory

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the
Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided "as is" without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Access Control
- Access Matrix
  - Access Control Lists and Capabilities
- Assigning permission
  - Discretionary and Mandatory access control

Outline

- Access Control
- Access Matrix
  - Access Control Lists and Capabilities
- Assigning permission
  - Discretionary and Mandatory access control

Motivation

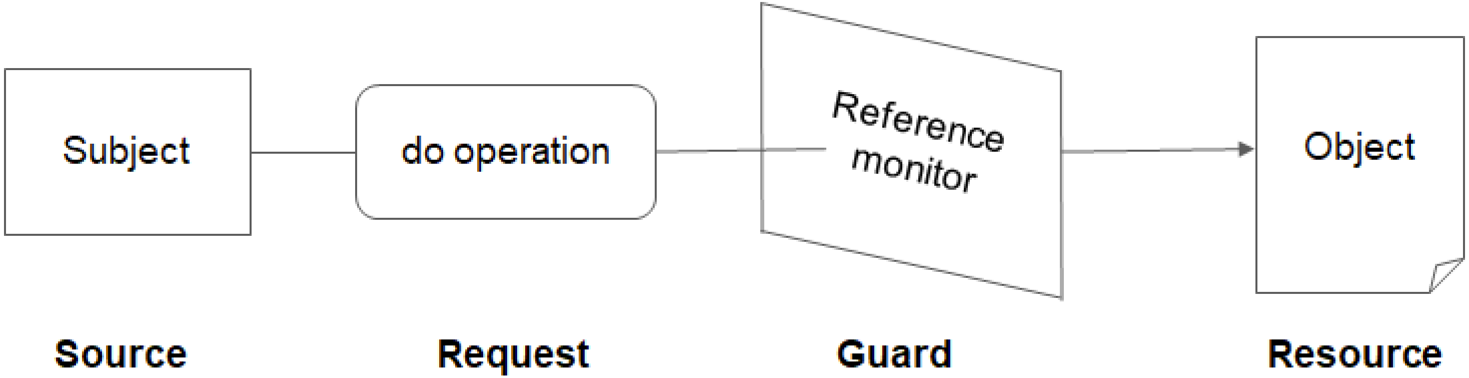
- A prerequisite of any system is protecting its **data** and **resources** against
  - unauthorized disclosure (ensure the **confidentiality**)
  - unauthorized or improper modifications (ensure the **integrity**)
  - unauthorized withholding (ensure the **availability**)

Access Control

- A layer in between (malicious) users and the protected system

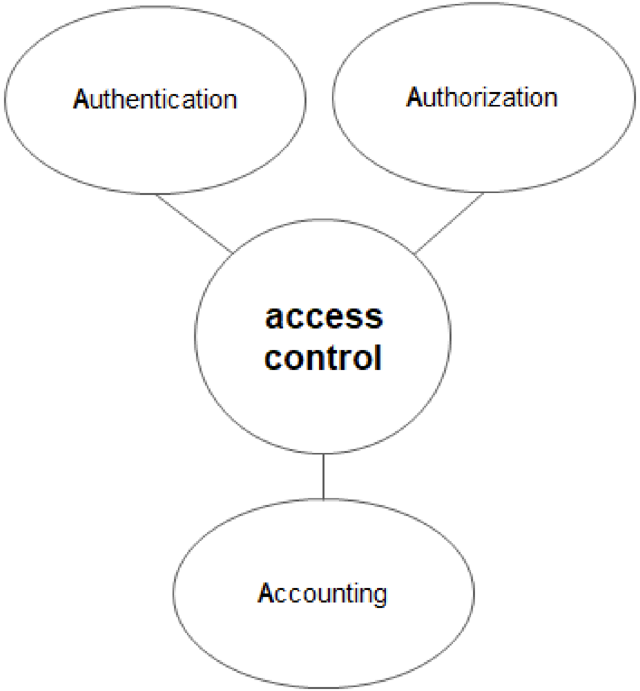
Access control is the process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied.

Model of access control



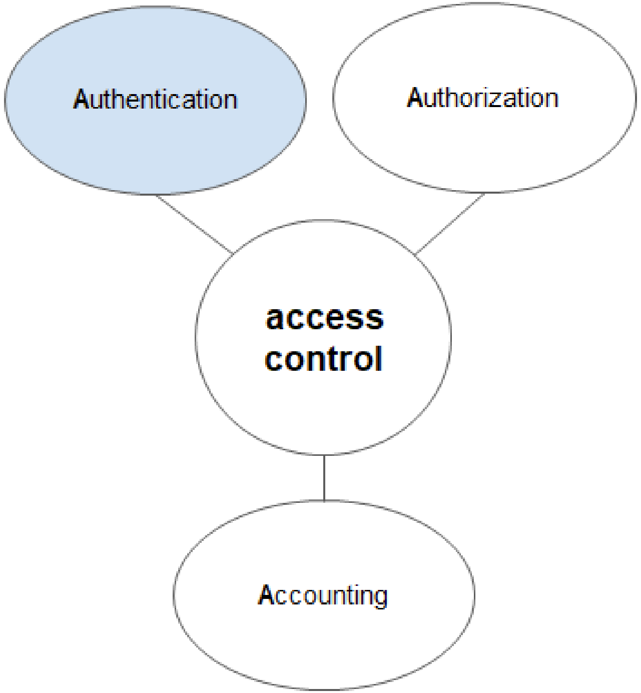
An active entity (subject) accessing a passive object (resource) with some specific operation while a reference monitor (guard) grants or denies access.

Access control systems



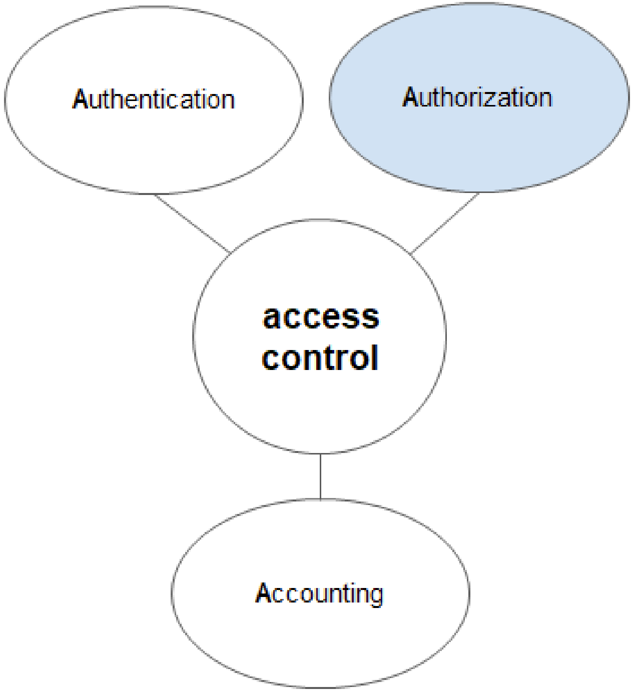
- Authentication, authorization, and accounting (AAA) represent the three pillars of access control.

Access control systems



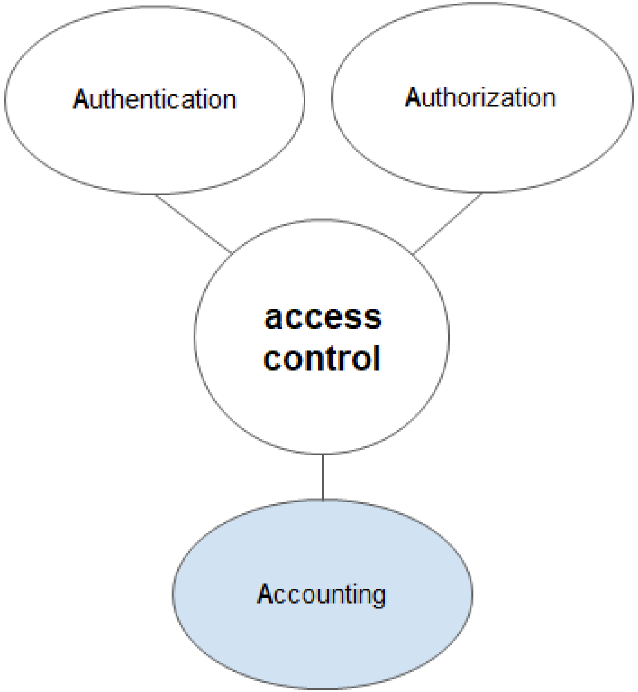
- **Authentication** is the process by which a system verifies the identity of a user who wishes to access resources and data
  - The secure establishment of identities represents the fundamental prerequisite for the integrity and soundness of any access control system.

Access control systems



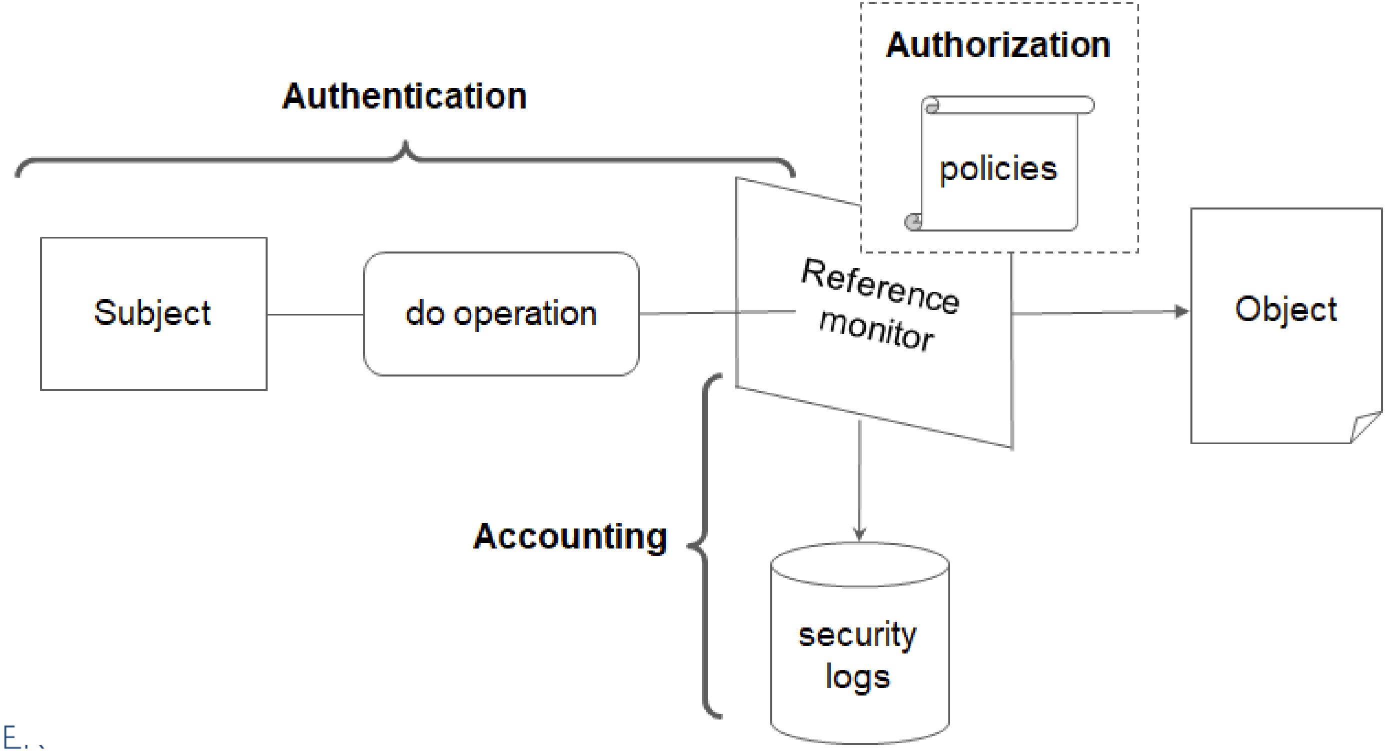
- **Authorization** is the function of specifying access rights/privileges (*policies*) to resources and data.
  - Access control represents the methods we use to enforce such policies.

Access control systems



- **Accounting** (or **Audit**) consists of logging security-related events, analyzing them for potential breaches, and notifying concerned parties.
  - Auditing is a key security element for monitoring threats: it maintains evidence of attempts to compromise the access controls put in place by an organization.

Model of access control [2]



Access control is pervasive

Level	Subject	Action	Guard	Protected System
Hardware	OS Process	Write memory	CPU	CPU and memory
Network	Host	Send packets	Firewall	Intranet
Database	User	SELECT query	DBMS	Database
Operating System	User	Read file	OS Kernel	Filesystem
Application	User	Update personal information	Application code	Application data

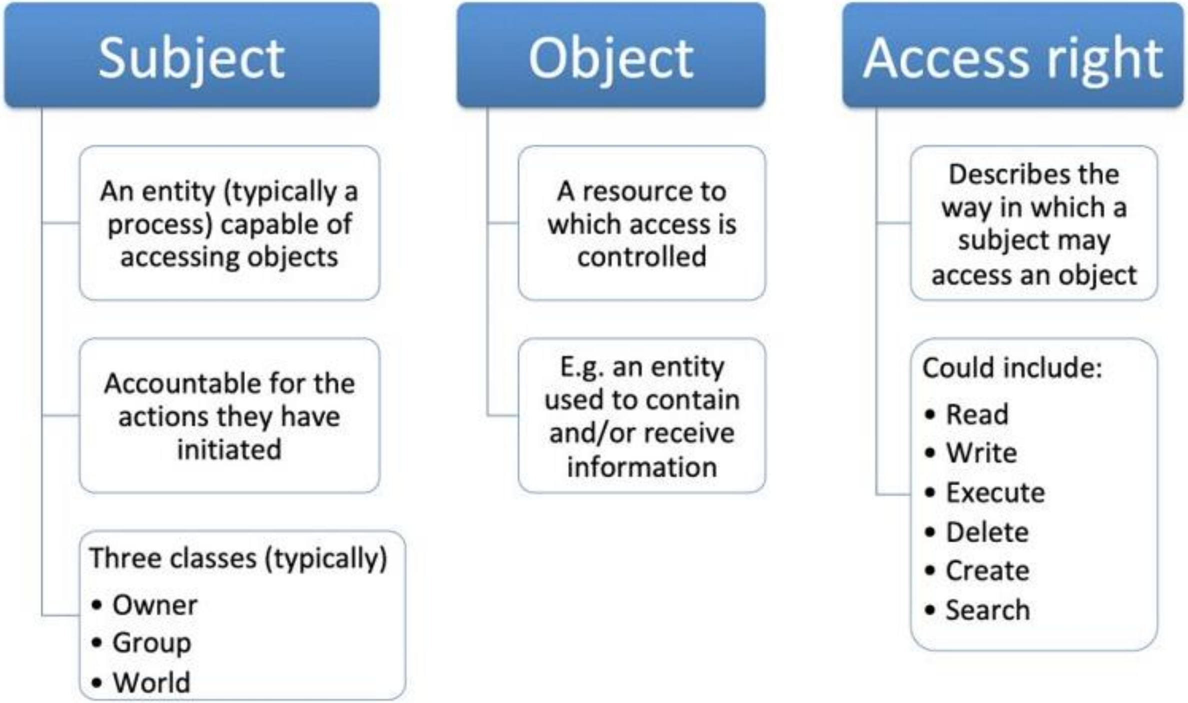
Outline

- Access Control
- Access Matrix
  - Access Control Lists and Capabilities
- Assigning permission
  - Discretionary and Mandatory access control

Security Policies

- A **security policy** from an access-control perspective is the set of rules adopted to determine who can have access to which resource.
- It describes acceptable **protection states** in an access control system.

Basic elements of Access Control



Subject

An entity (typically a process) capable of accessing objects

Accountable for the actions they have initiated

Three classes (typically)

- Owner
- Group
- World

Object

A resource to which access is controlled

E.g. an entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:

- Read
- Write
- Execute
- Delete
- Create
- Search

Access Control policies

- Discretionary (DAC) (authorization-based) policies control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed to do.
- Mandatory (MAC) policies control access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate if system entities are eligible to access certain resources)
- Role-based (RBAC) policies control access depending on the roles that users have within the system and on rules specifying the accesses allowed to users in given roles.
- Attribute-based (ABAC) policies control access based on attributes of the user, the resource to be accessed, and current environmental conditions, and on access rules

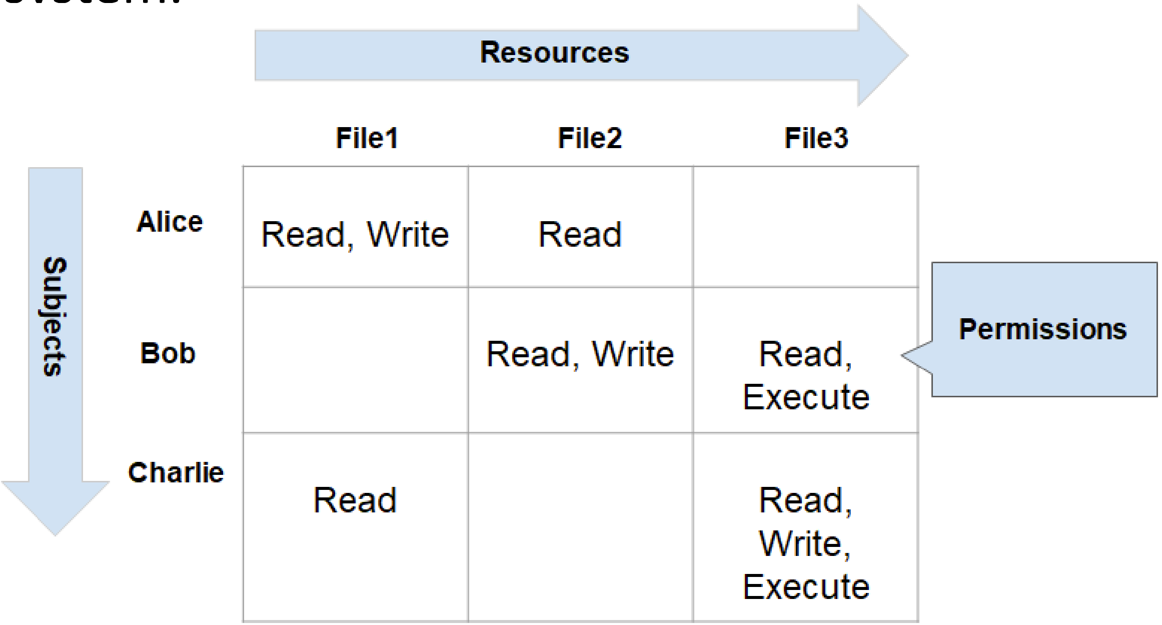
Access Control policies

- DAC is the traditional method of implementing access control
  - An entity enables other entities to access some resource
- MAC evolved out of requirements for military information security
  - An entity that has clearance to access a resource may not enable another entity to access that resource
- RBAC and ABAC are becoming increasingly popular

- These four policies are not mutually exclusive
  - Employ two or more of these policies to cover different classes of system resources

Access Matrix Model

- It provides a framework for describing protection states in an access control system.

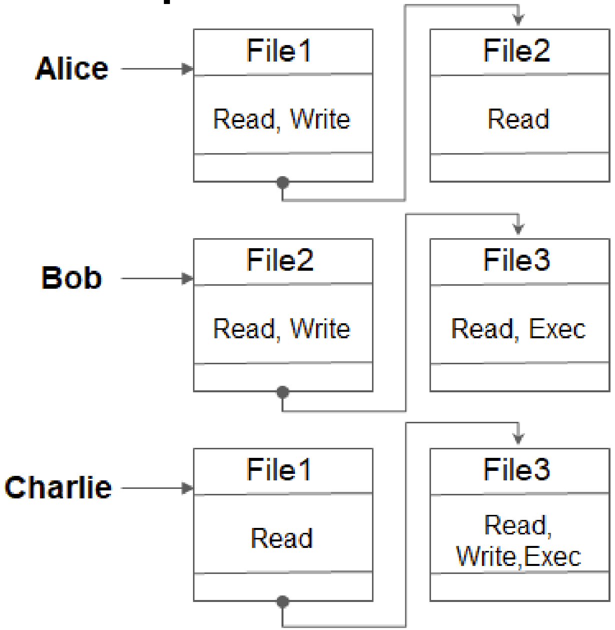


	File1	File2	File3
Alice	Read, Write	Read	
Bob		Read, Write	Read, Execute
Charlie	Read		Read, Write, Execute

Capabilities

Capabilities represent a dual technique for ACLs.

- A subject's capability enumerates the list of resources accessible to the subject.
- Each entry identifies an object along with the set of access rights conferred on the subject.
- Capabilities correspond to the rows of an access matrix.

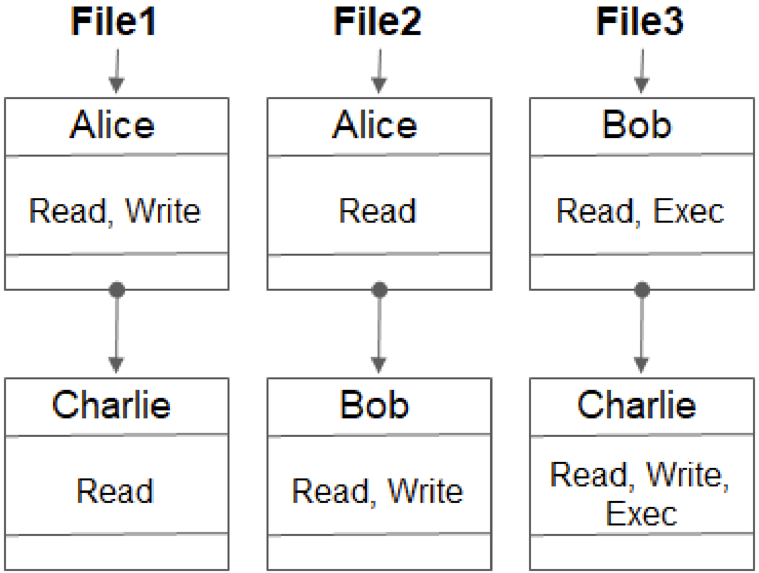


Access Control Lists (ACL)

Access control lists (ACLs) are commonly used in implementing an access matrix.

- An ACL is a data structure that associates a resource identifier with the list of subjects that have access to it (the list is qualified by the access rights available to it).

- An ACL corresponds to a **column** of the access matrix with the empty entries removed.



ACLs vs Capabilities

- Alexis wishes to keep all his valuables in a safe deposit box in the Bank. On occasions, he would like one or more trustworthy friends to make deposits or withdrawals. Two solutions for controlling accesses.
  - The Bank maintains a list of people authorized (**ACLs**).
  - The Bank gives Alexis one or more keys (**capabilities**) for the safe deposit box.

ACLs vs Capabilities [2]

	ACL approach	Capabilities approach
Bank	store the list of authorized users and authenticate	need not to be involved
Forging access right	safeguard the list of authorized users	requires unforgeability of the keys
Add a new person	owner visits the bank	the key can be transferred to a new person (requires control of propagation)
Delegation	authorization can not be extended	
Revoke	owner can remove authorized users	owner can ask for the key back, but not to be possible to know if the friend has made a copy

ACLs vs Capabilities [3]

Access Control Lists are based on an object view of AC matrix :

- Use lists to express view of each object *o*: *i*-th entry in the list gives the name of a subject s_i and the rights r_i in $M(s_i, o)$ of the access-matrix.
- Owner has the sole authority to grant, revoke or decrease access rights to *F* to other users.
- ACLs are used in UNIX/Linux operating system.

Capability Lists are based on a subject view of AC matrix.

- Not compatible with object oriented view.
- Difficult to get an overview of who has permissions on an object.
- Difficult to revoke a capability.
- Used in distributed (e.g., mobile agent) setting: Users are endowed with credentials (e.g., from a credential server) that they present to network objects.

Outline

- Access Control
- Access Matrix
  - Access Control Lists and Capabilities
- Assigning permission
  - Discretionary and Mandatory access control

Assigning permissions

- In general two approaches.
  - Discretionary Access Control (DAC): by subject themselves.
  - Mandatory Access Control (MAC): by central authority.

Discretionary Access Control

- Permissions are set at the discretion of the resource owner.
  - Highly flexible policy where permission can be transferred.
  - Lack of central control makes revocation or changes difficult.
- Discretionary Access Control in use
  - Controlling access to files (e.g., Linux filesystem).
  - Controlling the sharing of personal information (e.g., Social networks).

Mandatory Access Control

- Permissions are assigned by a central authority according to a central policy.
  - Finest solution to implement organization-wide security policies.
  - Low flexibility and high management overhead.
- Mandatory Access Control in use
  - Multi-level security systems (e.g., military applications)
  - Modern Operating System (e.g., SELinux)

Enrico RUSSO

Andrea VALENZA

Università di Genova

Access Control theory

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it