Secure Programming

Practices for Secure Programming_Part2

Dr. Fatma ElSayed

Computer Science Department
fatma.elsayed@fci.bu.edu.eg

Outline

- Access Control
- Access Control Principles
- Access Control Basic Elements
- Access Control Policies

Access Control

Definition: The prevention of unauthorized use of a resource based on *authentication* and *authorization* mechanisms to ensure security goals.

Authentication

- Verifying who a user is (“Who are you?”).

Authorization

- Checking whether a particular user is permitted to perform some action (“What are you allowed to do?”).

- *Authorization depends on authentication, before a system gives permission to access resources, it must first verify the user’s identity.*

Multi-factor Authentication

Definition: is a security measure that requires users to provide multiple forms of identification before gaining access to a system or service ***(Stronger authentication).***

Traditionally, two or more of :

- **Something you have**

  E.g. a smart card, or USB fob 

- **Something you know**

  E.g. a password (or even better, a passphrase)

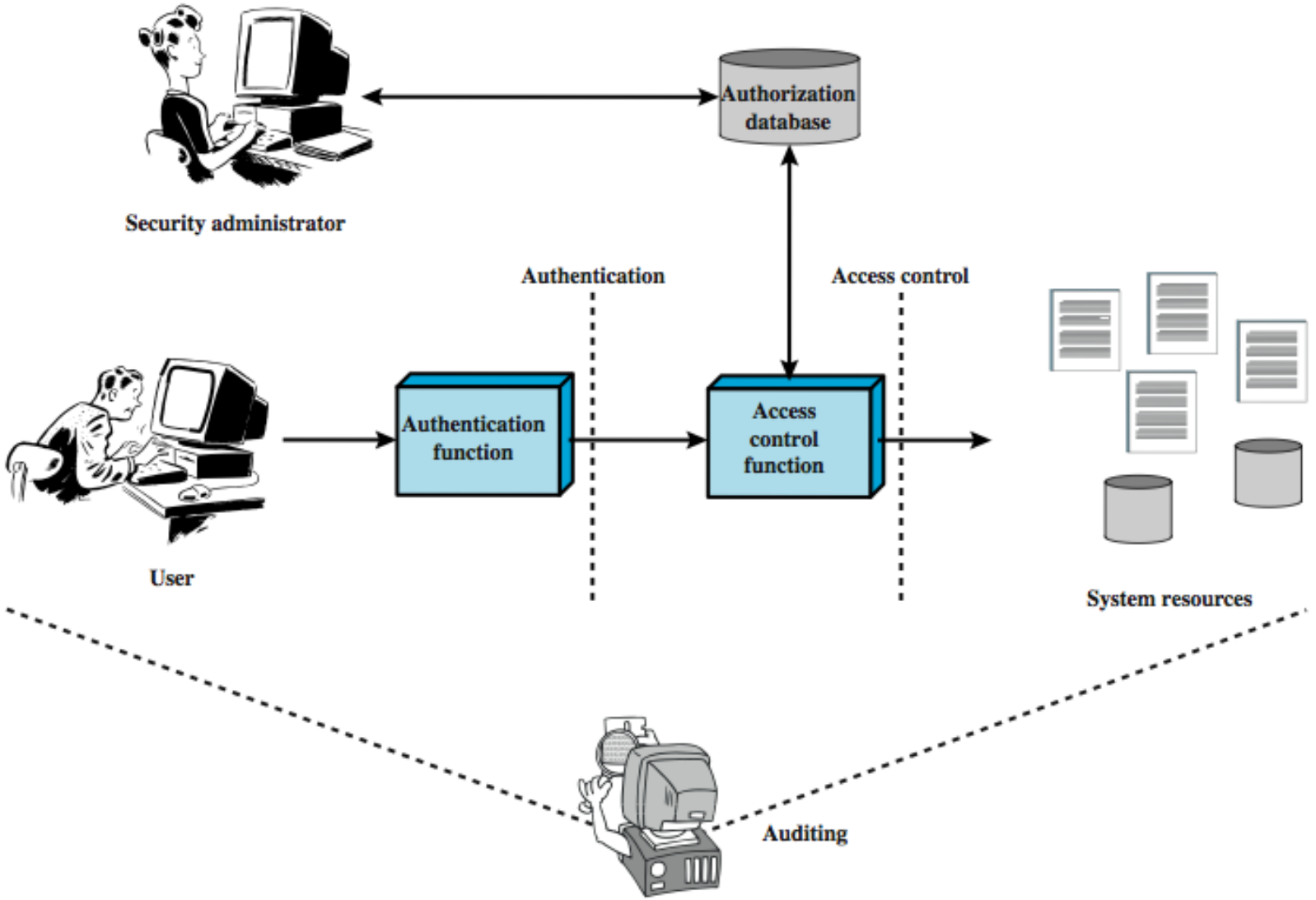
- **Something you are**

  E.g. your fingerprint, retina scan, or face

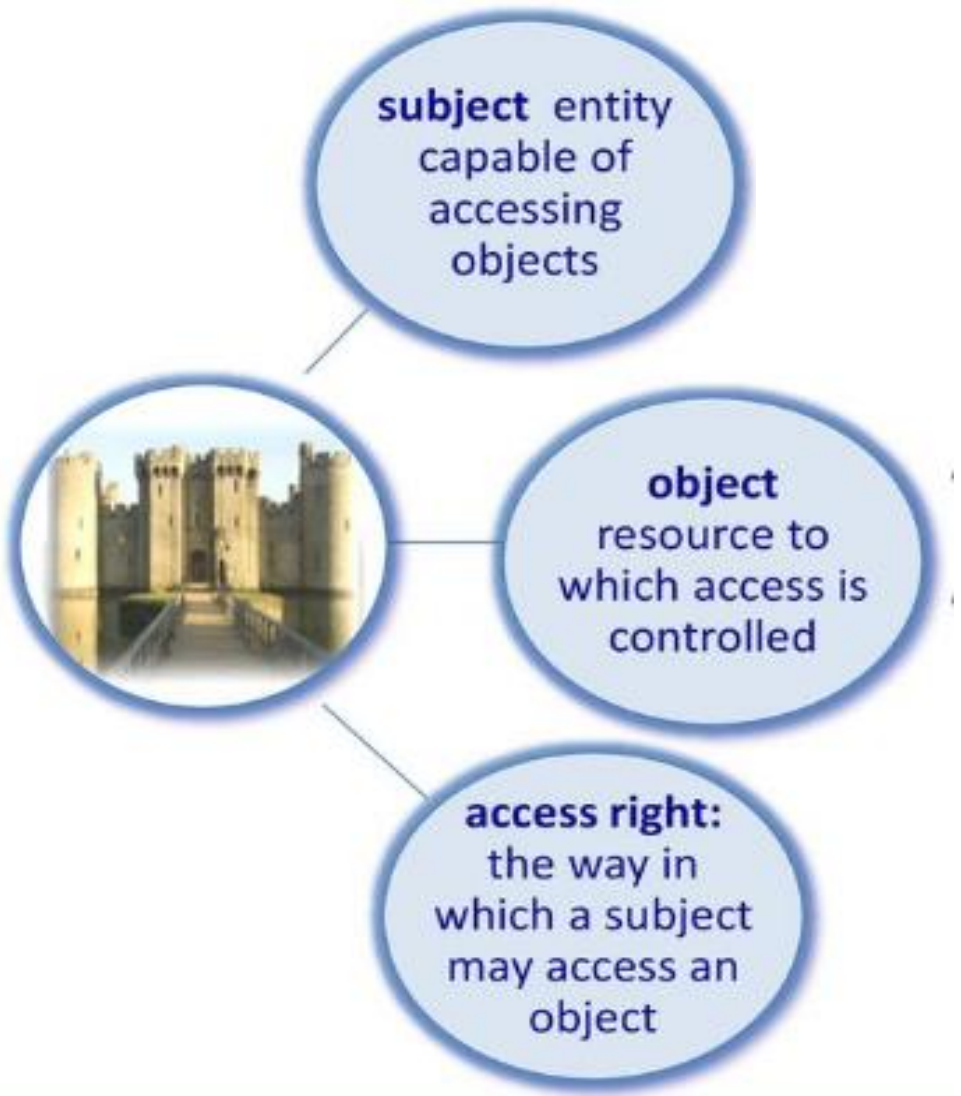
Authentication Best Practices

- Passwords should not be stored as plain text.
- Operating systems (and other software) normally instead store a cryptographic **one-way hash** of the password or passphrase.
- Creating a good password hash algorithm is difficult and error-prone, so it’s best to stick to a known and reliable one.
  - e.g. The default algorithm on many recent Linux distributions is an algorithm called "**yescrypt"**

Access Control Principles



Access Control Basic Elements



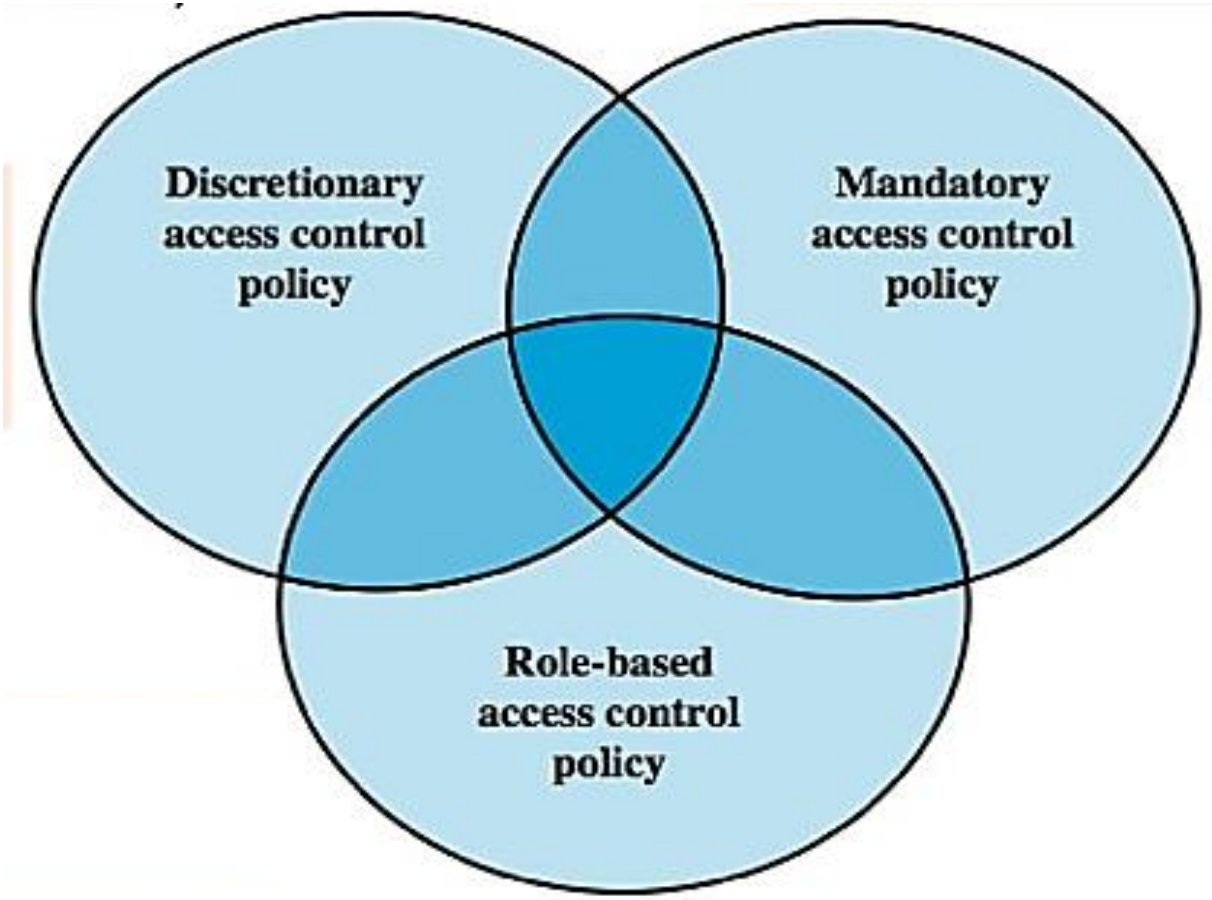
- **Subject:** entity that can access objects
- A process representing user/application
- Often have 3 classes: owner, group, world

- **Object:** Something we want to protect
  e.g. files, directories, records, programs, etc.
- Number/type depends on the environment

- **Access right:** a way in which the subject accesses an object
  e.g. read, write, execute, delete, create, search

Access Control Policies

Policy: decides which **subject** can perform what **operations** on which **object**.



Goal of an Access Control Policy

- Policy partitions system states into:
  - **Authorized (secure)**

    These are states the system can enter.
  - **Unauthorized (nonsecure)**

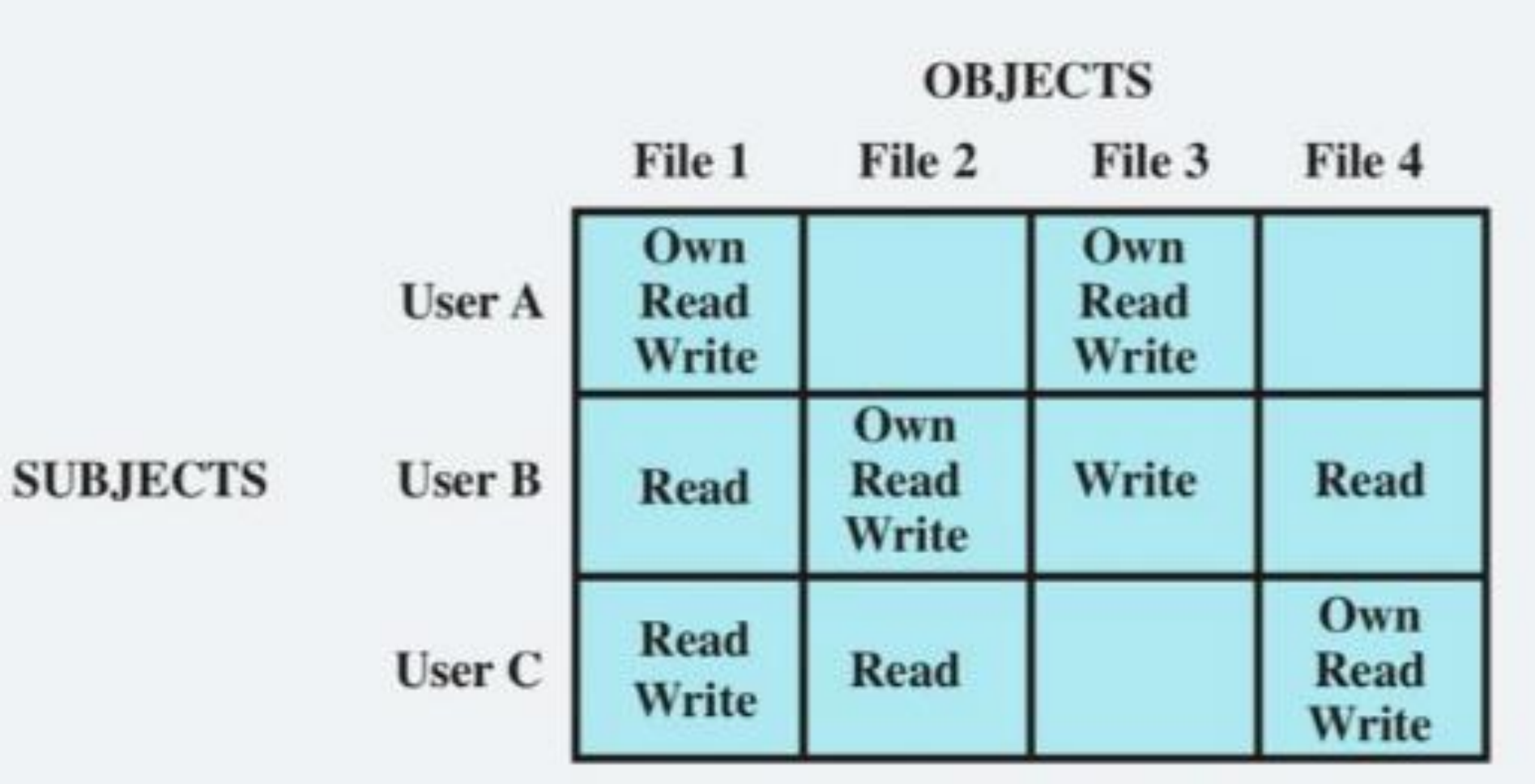
    If the system enters any of these states, it’s a security violation.
- Secure system
  - Starts in authorized state.
  - Never enters unauthorized state.

Discretionary Access Control

Discretionary Access Control (DAC)

- Scheme in which access is determined by the **resource owner**. This sort of "ownership" grants the ability to **add or remove rights**.
- An entity may enable another entity to access some resource.
- Often provided using an **access matrix**
  - One **dimension** consists of identified **subjects** that may attempt data access to the resources,
  - The other **dimension** lists the **objects** that may be accessed
- Each **entry** in the matrix indicates the **access rights** of a particular subject for a particular object

Access Matrix

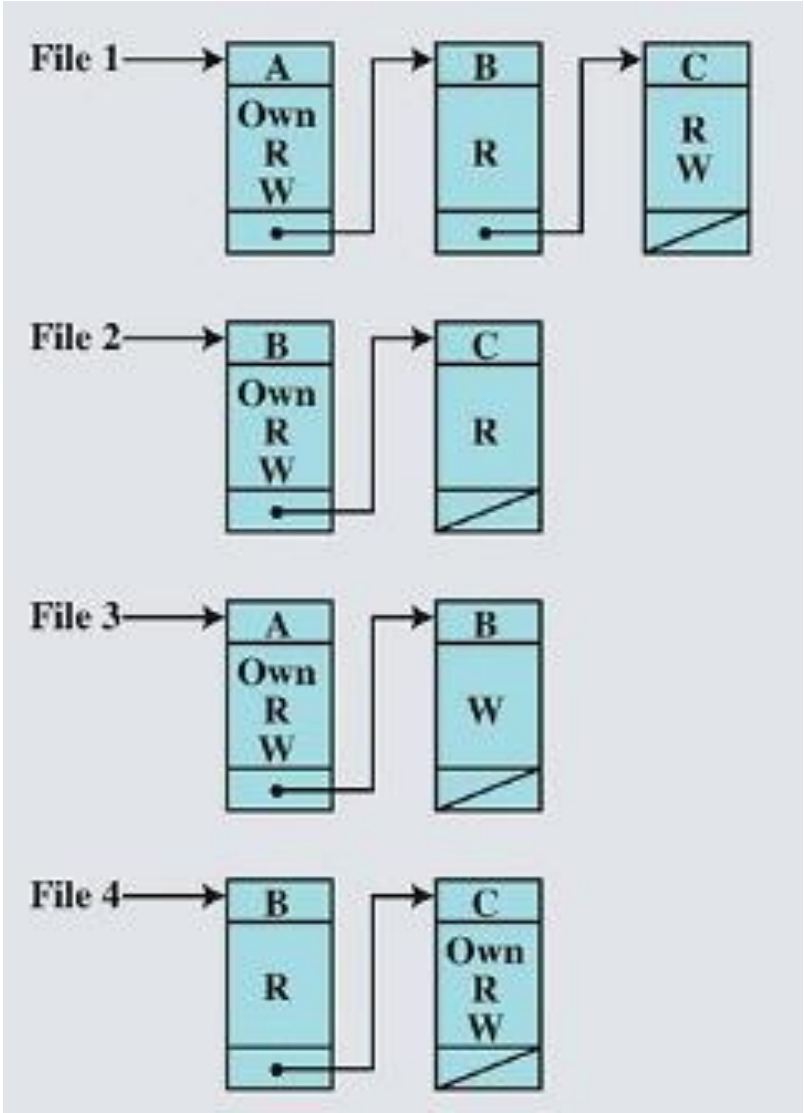


		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

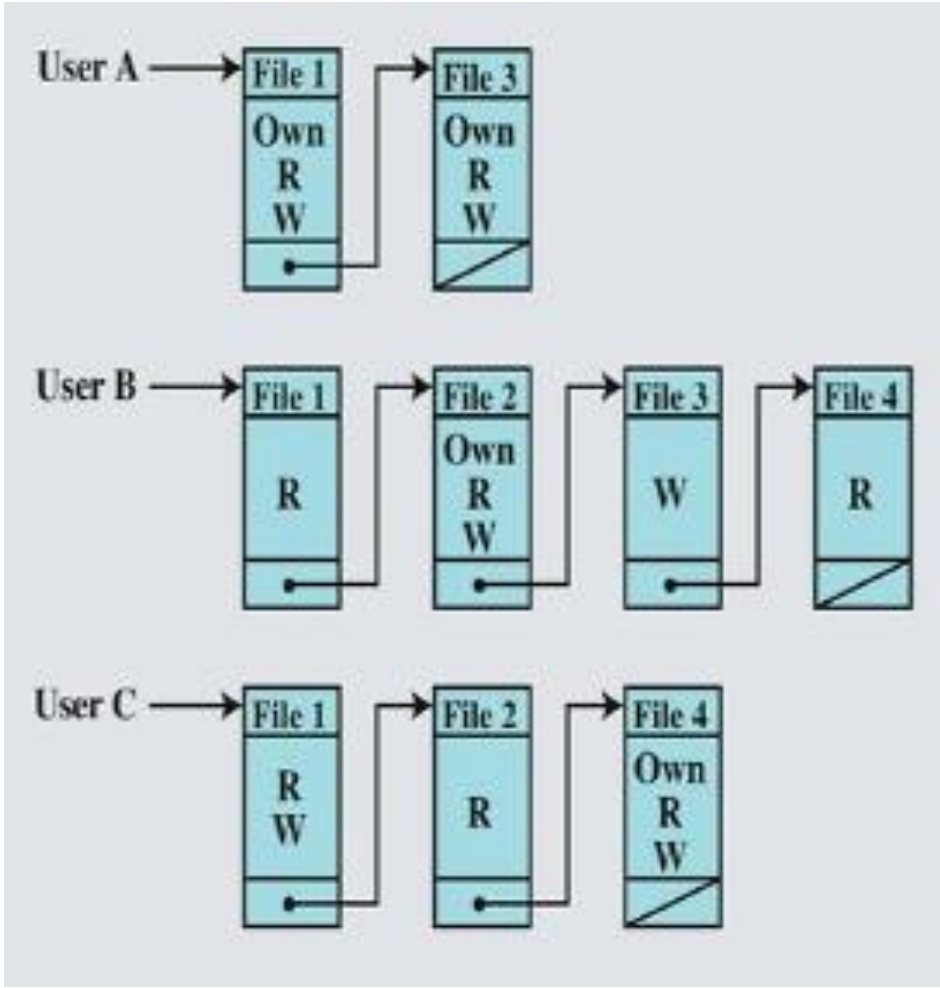
Access Matrix

Example of Access Control Structures

Access control list for files

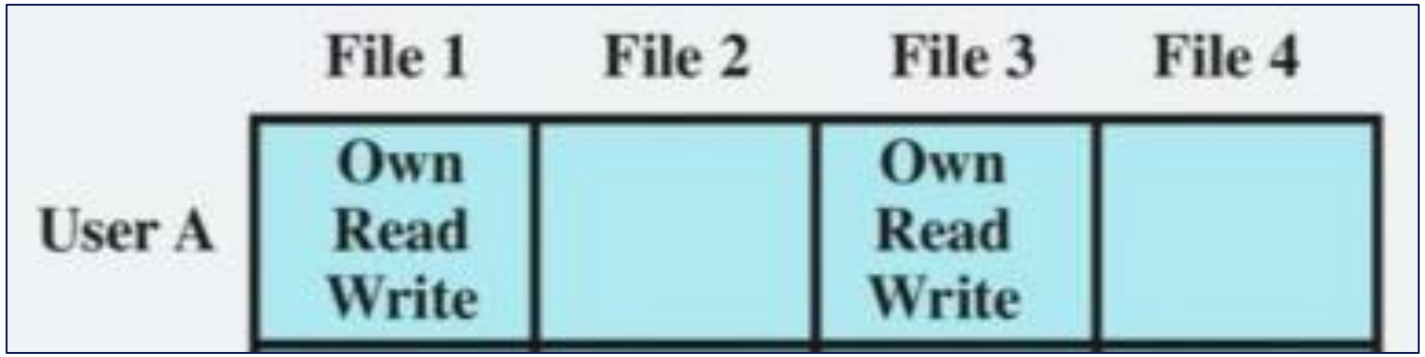


Capability lists for files



Protection Domains

- **Definition:** set of objects together with access rights to those objects.
- In terms of the access matrix, a **row** defines a protection domain.



- Each user has a protection domain, and any process initiated by the user has the same access rights defined by that protection domain.
    - E.g. If a user can read a file but not write to it, any program they run will have the same restriction.

Mandatory Access Control (MAC)

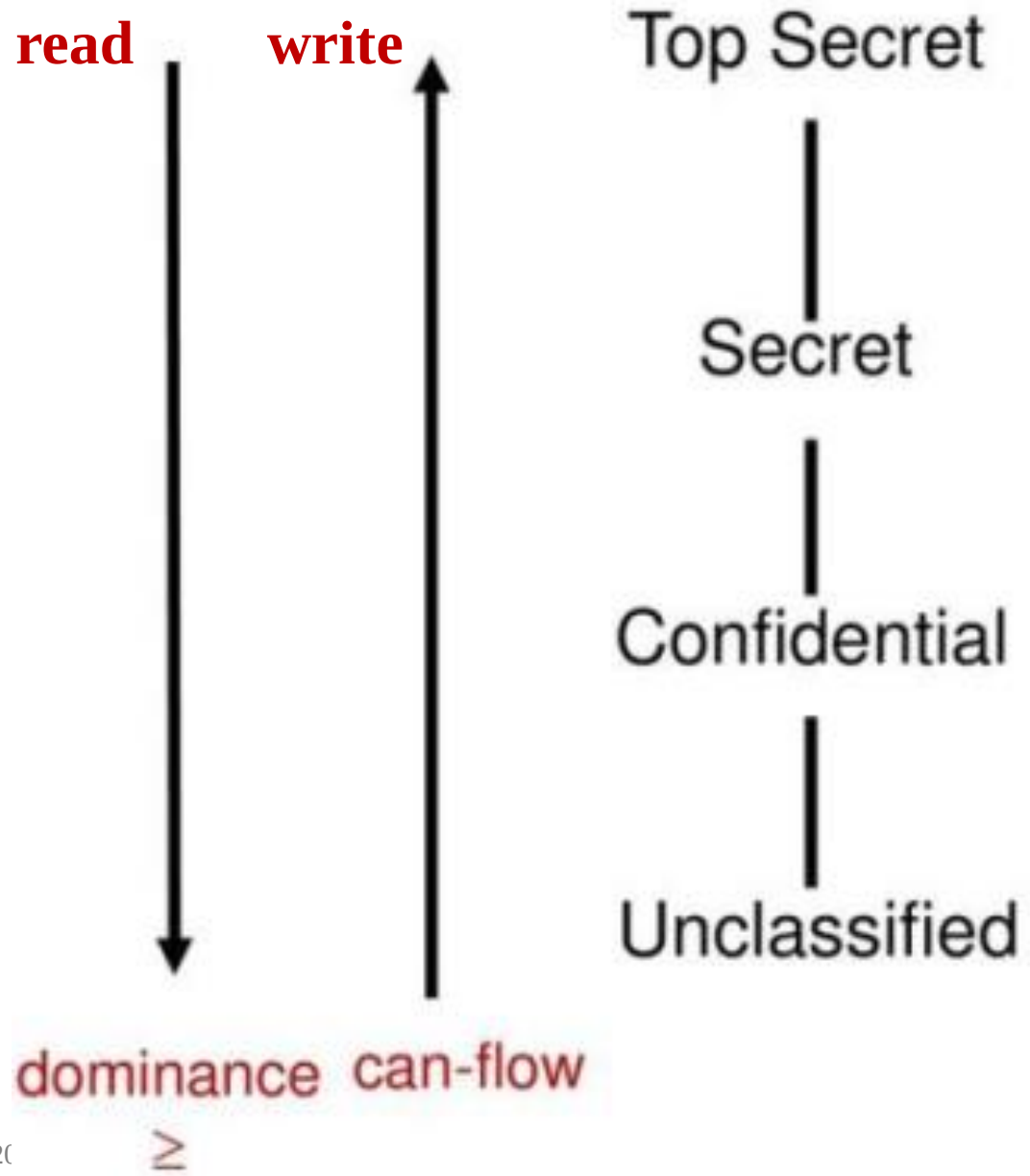
Mandatory Access Control (MAC)

- **Definition:** A system-wide policy determines who is allowed to have access; individual users **cannot alter** that access.
  - Relies on the **system** to control access *(Enforced by the OS)*.
  - Appropriate for e.g. Dept of Defense systems *(military or government environments)*
  - Implies that super users / system administrators don't have ultimate control.

Examples:

- The law allows a court to access driving records without the owners' permission.

Mandatory Access Control (MAC)



Labeling Mechanism is used

Prevent any illegal flow of information through the enforcement of multilevel security

Military Security

Require a strict classification of subjects and objects in security levels

Drawback of being too rigid

Applicable only to very few environments

Mandatory Access Control (MAC)

Hierarchy of Security Levels

- Data and resources are classified into **hierarchical** security levels *(labels)*: *Unclassified, Confidential, Secret, and Top Secret.*

Dominance Rule (No Read Up - "≤")

- A subject (user) can **only read data** at their **level or lower.**
- *Example: A user with Secret clearance can read Confidential and Unclassified data but not Top Secret data.*

Can-Flow Rule (No Write Down - "≥")

- A subject **cannot write to a lower** level to prevent data leakage.
- Example: A Top Secret user cannot write a document labeled "Confidential" because it may expose sensitive information to lower-clearance users.

Classification & Clearance

- **Classification:** indicates the **level of sensitivity** associated with some information, and **who** can access it.
  - **Format:** <rank; compartments>
  - **Rank:** Defines the security level
  - **Compartments:** Further restrict access to specific groups or subjects
- **Clearance:** indicates the **level of trust** given to a person to access information up to a certain level of sensitivity
  - <rank; compartments> → Clearance of a subject

Example

- Information classified as <secret; {Sweden}>

Which of the following subject clearances can read the above information?

1. <top secret; {Sweden}>
2. <secret; {Sweden, crypto}>
3. <top secret; {crypto}>
4. <confidential; {Sweden}>
5. <secret; {France}>

Example

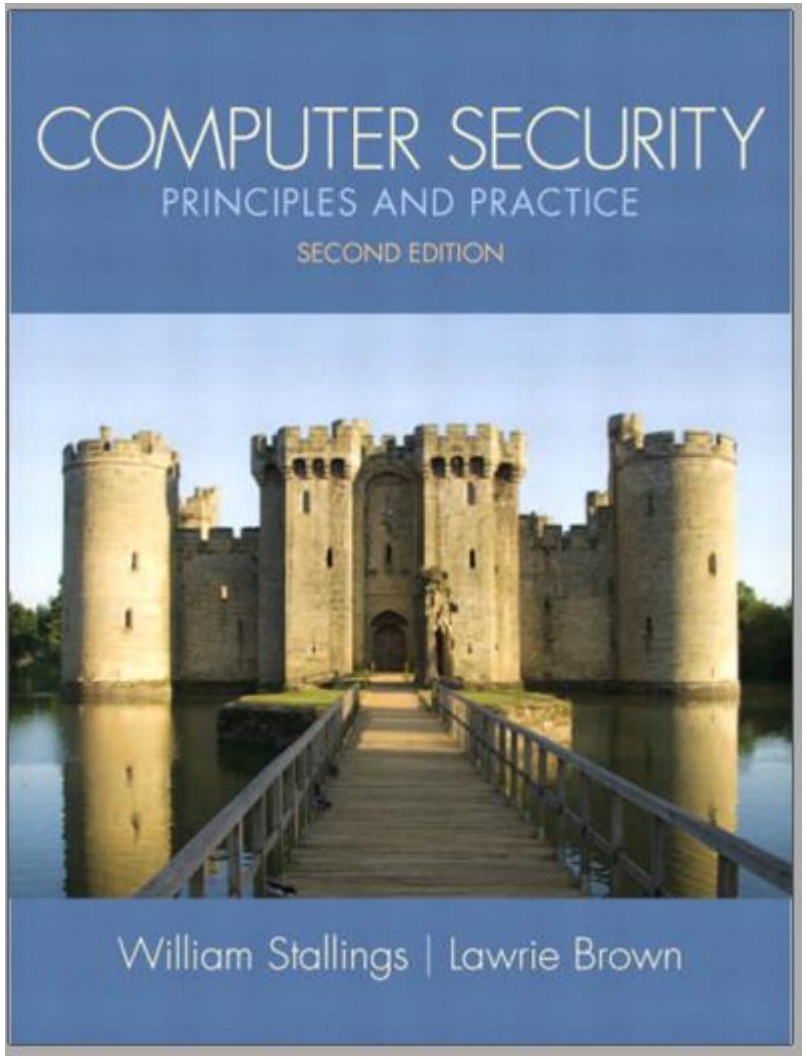
- Information classified as <secret; {Sweden}>

Which of the following subject clearances can read the above information?

1. <top secret; {Sweden}>
2. <secret; {Sweden, crypto}>
3. <top secret; {crypto}>
4. <confidential; {Sweden}>
5. <secret; {France}>

References

- Computer Security: Principles and Practice, William Stallings, 2nd Edition.
- ***Chapter 4: access control***



THANK YOU