**Lecturer notes**

# Authorization policies.

**Introduction to Authorization policies**

**Definition of terms:**

**Authorization** is any right or ability a user has anywhere or It is a process by which a server determines if the client has permission to use a resource or access a file.

It is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.

Example:

In a multi-user system, the system administrator uses the authorization mechanism to define permissions for each user or group of users. Once a user is logged in, via a process called authentication, the system determines which resources should be available to them during their session.

So the term authorization can have two related meanings:

- Allocation of privileges to users by the system administrator
- Granting access to users at runtime according to predetermined permissions

## Authentication vs Authorization

Authentication is the process of verifying a user's identity—making sure they are who they say they are. Most common method for identity authentication was a password. If the username provided by a user matched the password credentials, the identity was determined valid and the user was granted access.

Authorization comes into action after the user's identity has been verified through authentication. It provides full or partial access to resources such as devices, files, applications, specific operations or data.

To take a simple example:

- A user logs into a business application, providing their company username and password.
- The application authenticates the user and verifies the password.
- The application checks what permissions are allocated to that username and grants access to the relevant data and features.

Every organization should have a security policy that specifies who is allowed to access which resources and what they are allowed to do with these resources.

**Authorization policies** can be affected by anything from privacy concerns to regulatory compliance.

## Types of Authorization policies/ Models

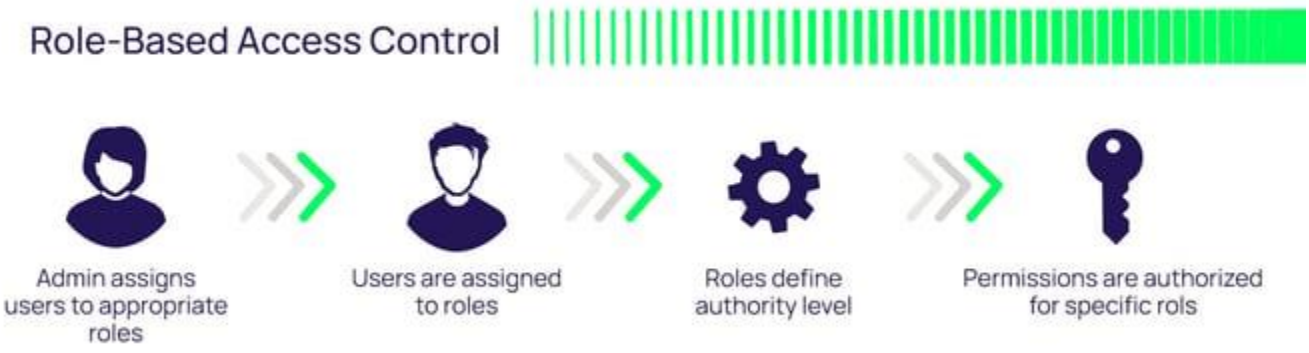
**Access policies**: Authorization policies are defined based on the organization's security requirements and are typically managed through frameworks or **Models** like

1. Role-Based Access Control (RBAC),
2. Attribute-Based Access Control (ABAC), or
3. Mandatory Access Control (MAC)
4. Discretionary Access Control (DAC)
5. Rule-Based Access Control (RBAC or RB-RBAC)

### 1. Role-Based Access Control (RBAC)

RBAC mechanisms allow or restrict access to users according to their roles within the organization. It provides users with access to data and applications required to perform their jobs while minimizing the risk of unauthorized activities like access to sensitive data.

Organizations can use RBAC to define how each user can interact with data. For example, it lets you allow read/write or read-only access to specific roles to limit a user's ability to perform unauthorized actions, such as data deletion and commands execution




### 2. Attribute-Based Access Control (ABAC)

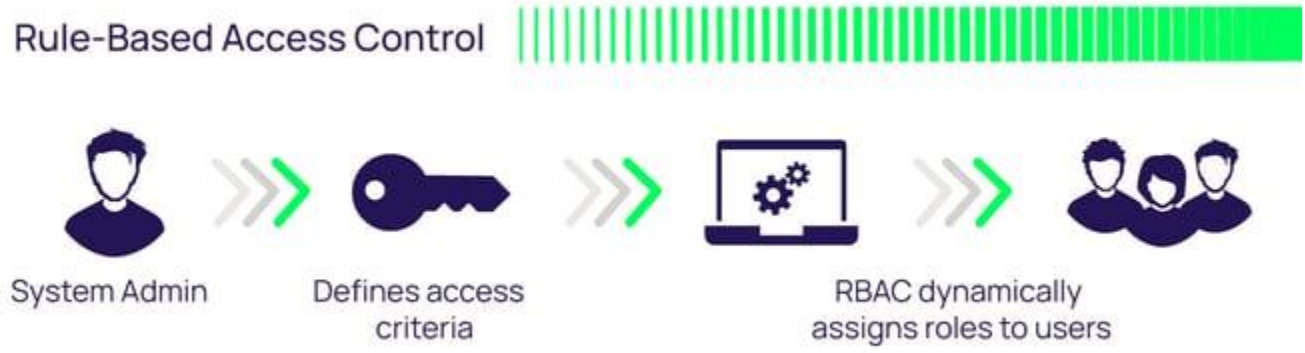
ABAC lets you define access and privileges based on attributes (or characteristics) instead of roles. It helps protect objects such as network devices, IT resources, and data from unauthorized actions and users that do not have the approved characteristics defined by the organization's security policies.

ABAC evolved from simple access control lists to a form of logical access control. It was initially endorsed in 2011 by the Federal Chief Information Officers Council to help federal organizations improve access control architectures. The council recommended ABAC to help organizations safely share information.

## 3. Rule-Based Access Control, RBAC or RB-RBAC.

**Rule-Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator. For example, if someone is only allowed access to files during certain hours of the day, Rule-Based Access Control would be the tool of choice.**

**The additional "rules" of Rule-Based Access Control requiring implementation may need to be "programmed" into the network by the custodian or system administrator in the form of code versus "checking the box."**




## 4. The Mandatory Access Control, or MAC,

This model gives only the owner and custodian management of the access controls. This means the end-user has no control over any settings that provide any privileges to anyone. Now, there are two security models associated with MAC: **Biba and Bell-LaPadula.**

The **Biba** model is focused on the integrity of information, whereas the Bell-LaPadula model is focused on the confidentiality of information.

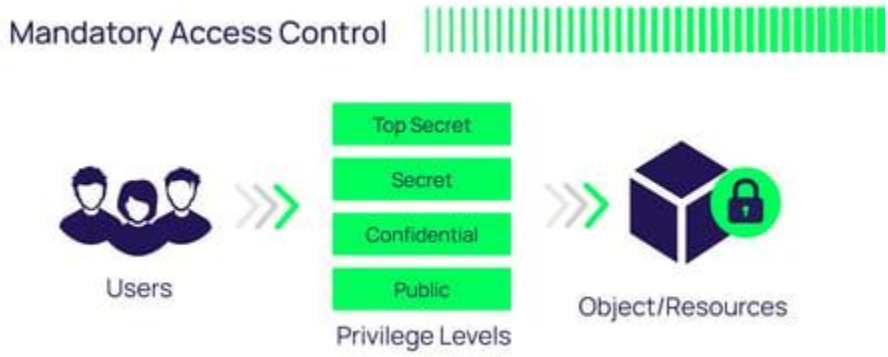
Biba is a setup where a user with low-level clearance can read higher-level information (called "read up") and a user with high-level clearance can write for lower levels of clearance (called "write down").

The Biba model is typically utilized in businesses where employees at lower levels can read higher-level information and executives can write to inform the lower-level employees.

**Bell-LaPadula**, on the other hand, is a setup where a user at a higher level (i.e. Top Secret) can only write at that level and no lower (called “write up”), but can also read at lower levels (called “read down”).

Bell-LaPadula was developed for governmental and/or military purposes where if one does not have the correct clearance level and does not need to know certain information, they have no business with the information.

MAC is the highest access control there is and is utilized in military and/or government settings utilizing the classifications of Classified, Secret, and Unclassified in place of the numbering system previously mentioned.




## 5. The Discretionary Access Control, or DAC,

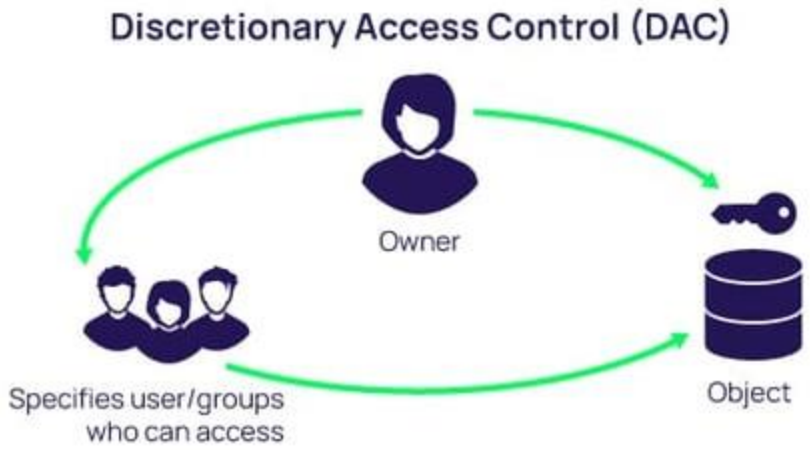
This model is the least restrictive model compared to the most restrictive MAC model.

DAC allows an individual complete control over any objects they own along with the programs associated with those objects.

This gives DAC two major weaknesses. First, it gives the end-user complete control to set security level settings for other users which could result in users having higher privileges than they’re supposed to.

Secondly, and worse, the permissions that the end-user has are inherited into other programs they execute.

This means the end-user can execute malware without knowing it and the malware could take advantage of the potentially high-level privileges the end-user possesses.




## Logical access control methods

Logical access control is done via access control lists (ACLs),

**ACLs (Access Control Lists)**

Examples are**; A group policies, passwords, and account restrictions**.

Let's see how each list provide control to resources

**Access Control Lists (ACLs)** are permissions attached to an object (i.e. spreadsheet file) that a system will check to allow or deny control to that object.

These permissions range from full control to read-only to "access denied." When it comes to the various operating systems (i.e. Windows®, Linux, Mac OS X®), the entries in the ACLs are named "access control entry," or ACE, and are configured via four pieces of information:

i. A security identifier (SID),
ii. An access mask,
iii. A flag for operations that can be performed on the object, and
iv. Another set of flags to determine inherited permissions of the object.

So, as one can see, ACLs provide detailed access control for objects. However, they can become cumbersome when changes occur frequently, and one needs to manage many objects.

1. **Group policies** are part of the Windows® environment and allow for centralized management of access control to a network of computers utilizing the directory services of Microsoft called Active Directory.

This eliminates the need to go to each computer and configure access control. These settings are stored in Group Policy Objects (GPOs) which make it convenient for the system administrator to be able to configure settings. Although convenient, a determined cybercriminal can get around these group policies and make life miserable for the system administrator or custodian.

**2. Passwords** are “the most common logical access control, sometimes referred to as a logical token”

Passwords need to be tough to hack in order to provide an essential level of access control.

If one makes the password easy to guess or uses a word in the dictionary, they can be subject to brute-force attacks, dictionary attacks, or other attacks using rainbow tables.

In addition, ensuring patches are accomplished regularly, deleting, or disabling unnecessary accounts, making the BIOS password-protected, ensuring the computer only boots from the hard drive, and keeping your door locked with your computer behind it will help ensure your passwords are protected.

**3. Account restrictions**

They are the last logical access control method in the list.

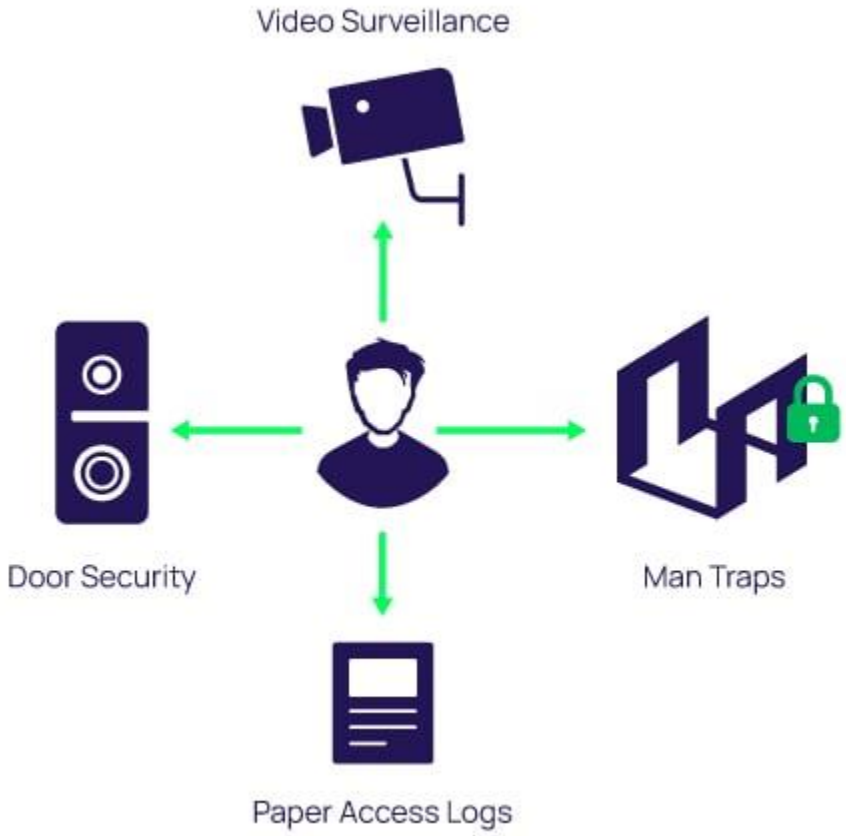
The two most common account restrictions are

1. Time-of-day restrictions and
2. Account expiration

Time of day restrictions can ensure that a user has access to certain records only during certain hours. This would make it so that administrators could update records at night without interference from other users.

Account expirations are needed to ensure unused accounts are no longer available so cybercriminals cannot possibly utilize them for any “dirty work.”

## Types of physical access control




---

## Explanation:

Physical access control is utilizing physical barriers which can help prevent unauthorized users from accessing systems. It also allows authorized users to access systems keeping physical security in mind. This type of control includes keeping the computer secure by securing the door which provides access to the system; using a paper access log; performing video surveillance with closed-circuit television; and in extreme situations, having "mantraps."

Securing the computer consists of disabling hardware so that if a bad guy were to gain access, they can't do any damage to the computer due to disabled USB ports, CD or DVD drives, or even a password-protected BIOS. Again, this just reduces the risk of malicious code being loaded onto the system and possibly spreading to other parts of a network.

**Door security** can be very basic or it can utilize electronic devices such as keyed dead-bolt locks on the door, cipher locks, or physical tokens. A keyed dead-bolt lock is the same as one would use for a house lock.

The cipher lock only allows access if one knows the code to unlock the door. Physical tokens will typically consist of an ID badge which can either be swiped for access, or they may instead contain a radio frequency identification tag (RFID) that contains information on it identifying the individual needing access to the door.

**Paper access logs** are common in many places for physical security. This allows a company to log a person in with name, company, phone number, time in, and time out. It can also document the employee who escorted the person during the time they were there. Paper access logs, filled out accurately, will complement video surveillance.

**Video surveillance** on closed-circuit television allows for the recording of people who pass through a security checkpoint. This type of door security allows one to observe the individuals going through the checkpoint, as well as the date and time, which can be useful when trying to catch bad guys. Video surveillance can also be utilized in mantraps.

**Mantraps** take door security to another level. This type of security can be seen in military and government settings, among others when entering very high-security areas. A person will present their identification to the security attendant and the attendant will allow the person to enter the first door into a room. Only if the individual's identification credentials are valid will they be allowed to pass through the room and go through the second door; if not, mantrap! They can only get out of the room by going back through the first door they came in.