Chapter 4: Access Control

Access Control:

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Logical access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers, biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

Three Elements of Access Control:

- Identification: For access control to be effective, it must provide some way to identify an individual. The weakest identification capabilities will simply identify someone as part of a vague, poorly defined group of users who should have access to the system. Your username, a PGP e-mail signature, or even the key to the server closet provides some form of identification.
- Authentication: Identification requires authentication. This is the process of ensuring that the identity in use is authentic — that it’s being used by the right person. In its most common form in IT security, authentication involves validating a password linked to a username. Other forms of authentication also exist, such as fingerprints, smartcards, and encryption keys.
- Authorization: The set of actions allowed to a particular identity makes up the meat of authorization. On a computer, authorization typically takes the form of read, write, and execution permissions tied to a username.

Types of access control/ Access control Models:

Discretionary Access Control (DAC)

With a discretionary access control system (DAC) the owner of the company can decide how many people have access to a specific location. Each access control point has a list of authorised users. Every time a keycard is swiped, a PIN is punched, or a fingerprint is scanned, the system checks the credential against the list and either allows or denies access based on the previously set allowances.

DAC is defined as an access control policy enforced over all subjects and objects granting information access that allows the subject to:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes of subjects, object, systems, or system components
- Choose security attributes associated with newly-created or revised objects
- Change rules governing access control

A good example of DAC would be giving someone Editor privileges for a folder in Google Drive. That person can share information, give the same privileges to others, change other users' ability to edit/read information, and choose security attributes for any other assets in the folder.

This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

DAC systems are considered to be the most flexible and offer the highest number of allowances compared to other types of access control. Because it's the most flexible, it's also not as secure as some other types, especially mandatory access control systems. Since one person has total control over the system, he or she might grant access to someone who shouldn't have it. Discretionary access control systems are best for companies that expect the most ease of use and flexibility.

Mandatory Access Control (MAC)

On the other end of the spectrum, mandatory access control systems (MAC) are the most secure type of access control. Only owners and custodians have access to the systems. All the access control settings are preset by the system administrator and can't be changed or removed without his or her permission.

This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel. MAC grants or denies access to resource objects based on the information security clearance of the user or device. For example, Security-Enhanced Linux is an implementation of MAC on Linux.

MAC as an access control policy uniformly enforced across all subjects and objects, ultimately placing restrictions on DAC. MAC controls limit a subject's access by preventing:

- Passing the information to unauthorized subjects or objects
- Giving its privileges to others
- Changing security attributes on subjects, object, systems, or system components
- Changing access control rules

Instead of creating an access list on each individual entry point like in a DAC system, a MAC system works by classifying all the users and grants them access to areas based on the system's programming. If you have 150 employees, you're going to need 150 user permissions set up in the system.

Mandatory access control systems are the strictest and most secure type of access control, but they're also the most inflexible. In order to change permissions, the administrator has to reprogram the specific user's access, not just the security lists at the entry point. MAC systems are primarily used by companies and agencies that require the utmost levels of security.

Role-Based Access Control (RBAC)

Role-based access control (RBAC) is quickly becoming the most popular type of access control. Instead of assigning permissions to individual users like in a MAC system, an RBAC system works by assigning permissions to a specific job title. It cuts down on the time required to set up or change user access.

This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.

RBAC collects all the access permissions a user needs to complete their job function, both explicitly outlined and implicitly needed, and maybe inherited through a hierarchy. A single role may apply to one user or a group of users.

Under RBAC, you assign users access based on their job functions. Therefore, people in the marketing department have access to the networks, systems, and applications they need to do their jobs. This might include your customer relationship management (CRM) application, corporate blog, social media accounts, folders that marketing uses in a shared drive, and your collaboration tool. Additionally, not everyone on the marketing team will have the same access to resources. Your social media manager may be the only person with access to those accounts but does not have access to your corporate blog or CRM.

Additionally, you also need to remember that departments may need to have similar access to resources for different reasons. Your sales team might need access to your CRM and some of the same folders in a shared drive.

As the company's application ecosystem grows, managing access becomes more challenging.

For example, if you have 20 salespeople, two managers, and three accountants, you wouldn’t have to create 25 individual security profiles in the system. You’d only have to create three: one for each separate job title. When employees gets promoted, just give them credentials that fit the new role and they’re good to go.

Rule-Based Access Control

Not to be confused with the other “RBAC,” rule-based access control is commonly used as an add-on to the other types of access control. In addition to whatever type of access control you choose, rule-based access control can change the permissions based on a specific set of rules created by the administrator.

This is a security model in which the system administrator defines the rules that govern access to resource objects. These rules are often based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.

If your business closes at 5 p.m., there’s no need for anyone to have access to your main office, even managers, after closing. With rule-based access control, you can set a rule to deny access to everyone from 5 p.m. to 9 a.m. the next morning. Rules can be created for just about any occasion.

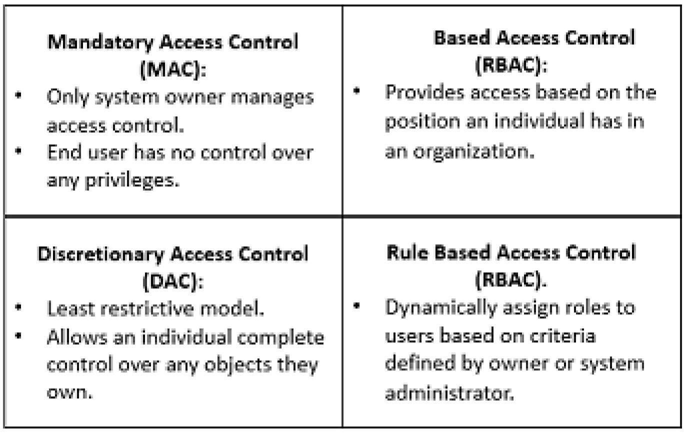
Attribute-based access control (ABAC)

In this dynamic method, access is based on a set of attributes and environmental conditions, such as time of day and location, assigned to both users and resources. This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

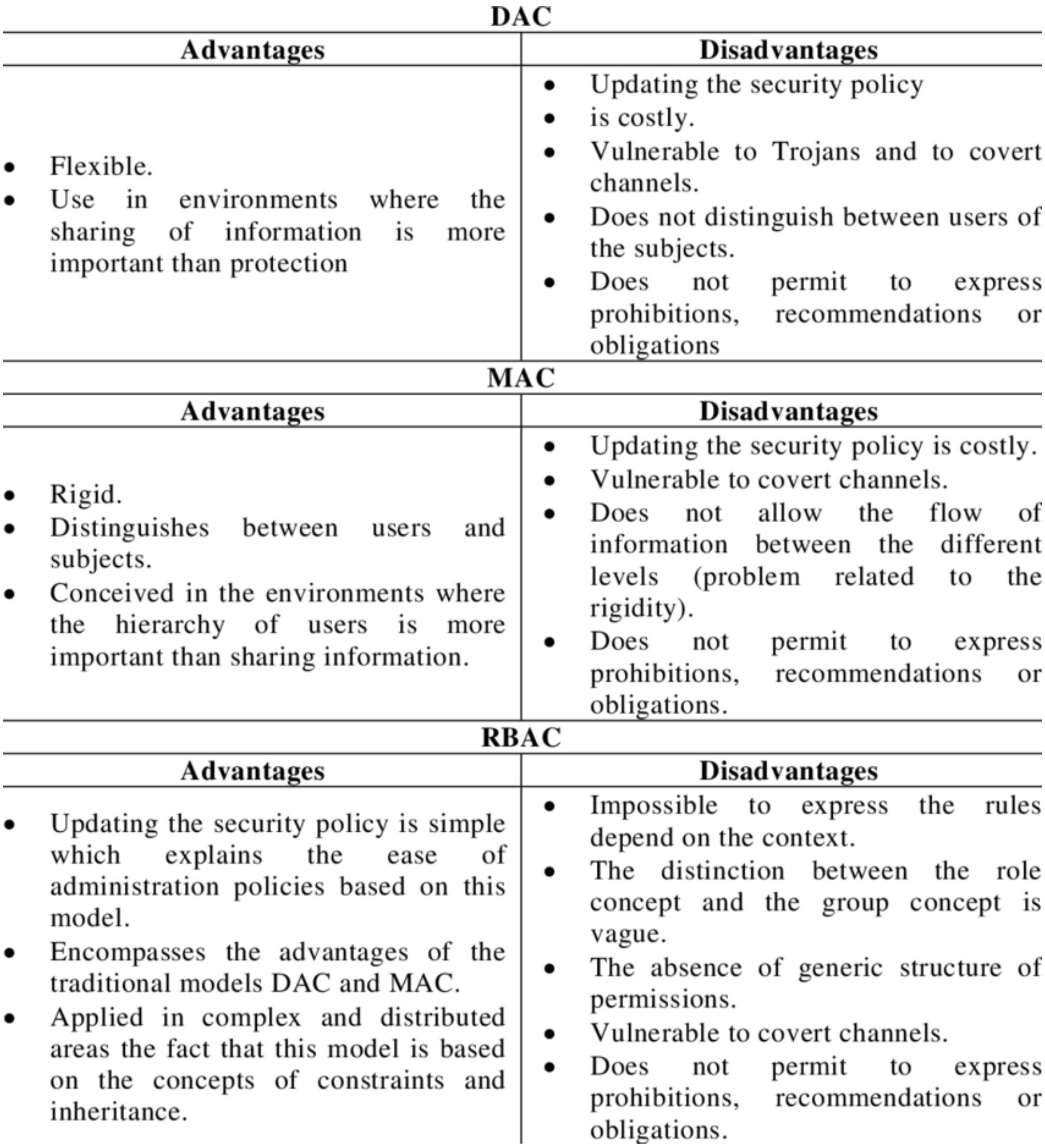
ABAC is a policy that restricts system access using a combination of:

- Organizational attributes, like job function
- Action attributes, like read, write, and delete
- Environmental attributes, like time of day and geolocation
- Resource attributes, like data type or application

ABAC enables organizations to set privileges and dynamically grant access, making it useful in dynamic cloud environments.



Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.



DAC

Advantages	Disadvantages
• Flexible. • Use in environments where the sharing of information is more important than protection	• Updating the security policy • is costly. • Vulnerable to Trojans and to covert channels. • Does not distinguish between users of the subjects. • Does not permit to express prohibitions, recommendations or obligations

MAC

Advantages	Disadvantages
• Rigid. • Distinguishes between users and subjects. • Conceived in the environments where the hierarchy of users is more important than sharing information.	• Updating the security policy is costly. • Vulnerable to covert channels. • Does not allow the flow of information between the different levels (problem related to the rigidity). • Does not permit to express prohibitions, recommendations or obligations.

RBAC

Advantages	Disadvantages
• Updating the security policy is simple which explains the ease of administration policies based on this model. • Encompasses the advantages of the traditional models DAC and MAC. • Applied in complex and distributed areas the fact that this model is based on the concepts of constraints and inheritance.	• Impossible to express the rules depend on the context. • The distinction between the role concept and the group concept is vague. • The absence of generic structure of permissions. • Vulnerable to covert channels. • Does not permit to express prohibitions, recommendations or obligations.

Note: This document is for reference purpose.

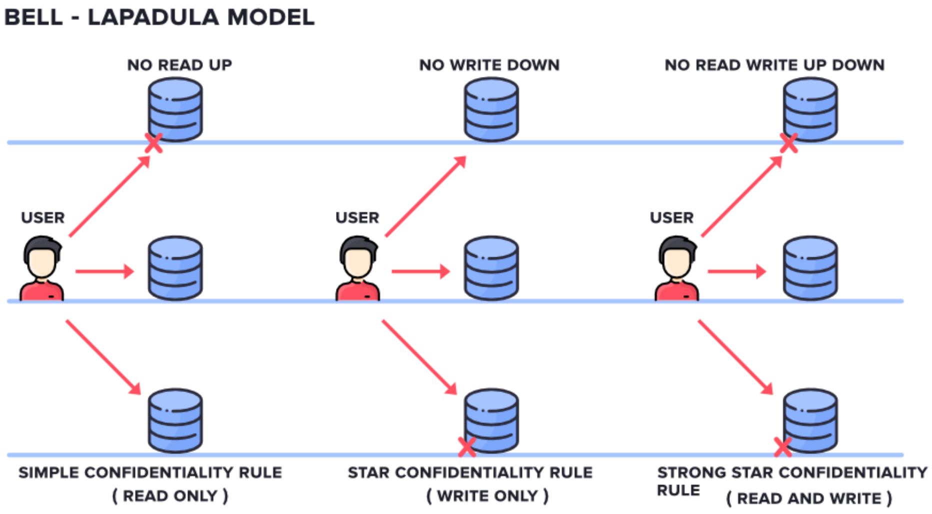
Classic Security Models

These models are used for maintaining goals of security, i.e. Confidentiality, Integrity, and Availability. In simple words, it deals with CIA Triad maintenance. There are 3 main types of Classic Security Models.

- Bell-LaPadula
- Biba
- Clarke Wilson Security Model

1. Bell-LaPadula

This Model was invented by Scientists David Elliot Bell and Leonard .J. LaPadula.Thus this model is called the Bell-LaPadula Model. This is used to maintain the Confidentiality of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy.



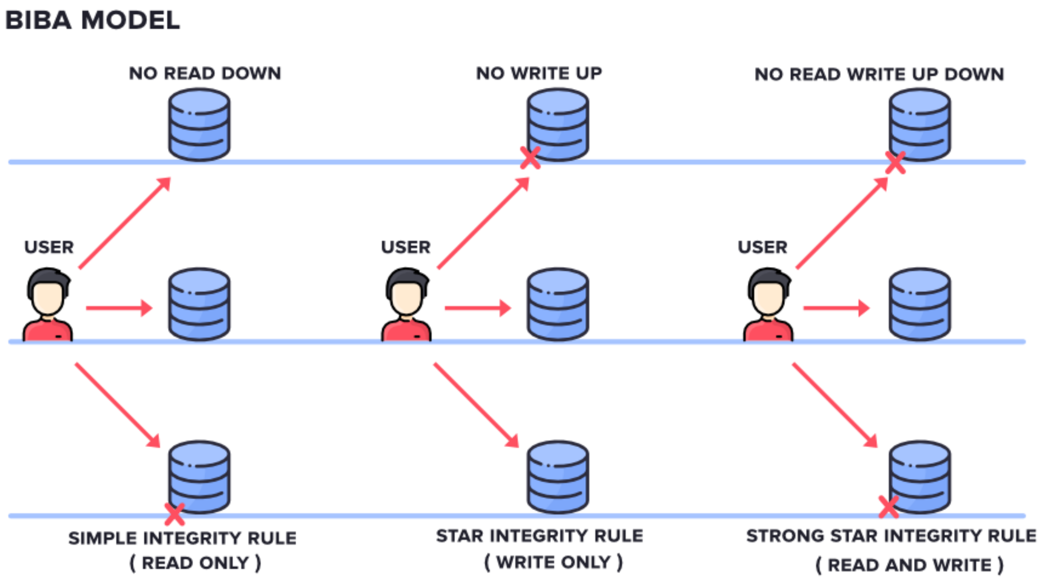
It has mainly 3 Rules:

- SIMPLE CONFIDENTIALITY RULE: Simple Confidentiality Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO READ-UP
- STAR CONFIDENTIALITY RULE: Star Confidentiality Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO WRITE-DOWN
- STRONG STAR CONFIDENTIALITY RULE: Strong Star Confidentiality Rule is highly secured and strongest which states that the Subject can Read and Write the files on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as NO READ WRITE UP DOWN

2. Biba

This Model was invented by Scientist Kenneth .J. Biba. Thus this model is called Biba Model. This is used to maintain the Integrity of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy. This works the exact reverse of the Bell-LaPadula Model.

Note: This document is for reference purpose.

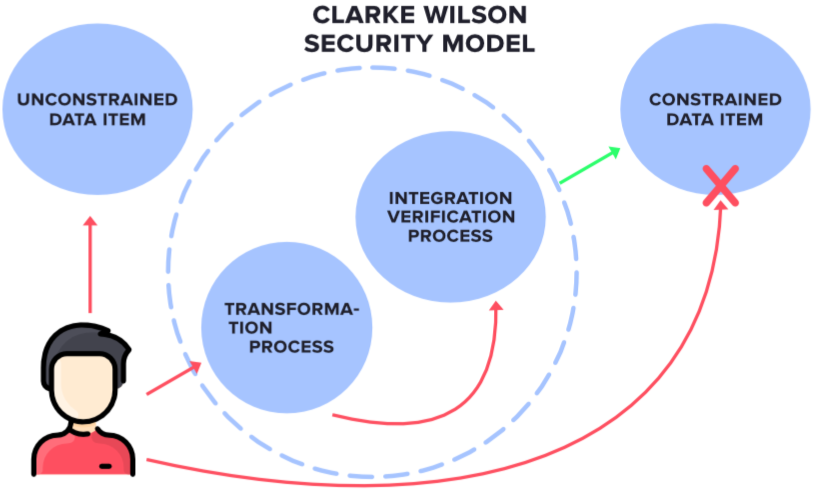


It has mainly 3 Rules:

- SIMPLE INTEGRITY RULE: Simple Integrity Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO READ DOWN
- STAR INTEGRITY RULE: Star Integrity Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO WRITE-UP
- STRONG STAR INTEGRITY RULE

3. Clarke Wilson Security Model

This Model is a highly secured model. It has the following entities.



SUBJECT: It is any user who is requesting for Data Items.

CONSTRAINED DATA ITEMS: It cannot be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model

Note: This document is for reference purpose.

UNCONSTRAINED DATA ITEMS: It can be accessed directly by the Subject.

The Components of Clarke Wilson Security Model

TRANSFORMATION PROCESS: Here, the Subject's request to access the Constrained Data Items is handled by the Transformation process which then converts it into permissions and then forwards it to Integration Verification Process

INTEGRATION VERIFICATION PROCESS: The Integration Verification Process will perform Authentication and Authorization. If that is successful, then the Subject is given access to Constrained Data Items.

Access Control List

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

- Inbound access lists –
  When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

- Outbound access lists –
  When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.
  - **Types of ACL –**

  There are two main different types of Access-list namely:

  Standard Access-list –

  These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

Extended Access-list –

These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Also, there are two categories of access-list:

Numbered access-list – These are the access list that cannot be deleted specifically once created i.e if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

Named access list – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

Rules for ACL –

- The standard Access-list is generally applied close to the destination (but not always).
- The extended Access-list is generally applied close to the source (but not always).
- We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
- We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then the whole ACL will be removed. If we are using named access lists then we can delete a specific rule.
- Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
- As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
- Standard access lists and extended access lists cannot have the same name.

Advantages of ACL –

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.