## MODULE 2: FOUNDATIONAL CONCEPTS IN SECURITY
## WEEK 2

### Learning Outcomes:

After completing this course you are expected to demonstrate the following:

1. Differentiate authentication and authorization, access control (mandatory vs. discretionary).

### A. Engage

**Did you know?**

1. Confidentiality measures protect information from unauthorized access and misuse.
2. Integrity measures protect information from unauthorized alteration.
3. That there are three main types of threats: natural, unintentional, and intentional threat.

### B. Explore

Video Title: **Access Control Models**
YouTube Link: https://www.youtube.com/watch?v=XQ8GDSUUvPY
Video Module Filename: **Week 2 - Access Control Models**

### C. Explain

**Access controls** authenticate and authorize individuals to access the information they are allowed to see and use.

Moreover, it is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

### D. Elaborate

**Authentication and authorization, access control (Mandatory vs. Discretionary)**

**Authentication and Authorization**

At a high level, access control is a selective restriction of access to data. It consists of two main components: authentication and authorization, says Daniel Crowley, head of research for IBM's X-Force Red, which focuses on data security.

**Authentication** is a technique used to verify that someone is who they claim to be. Authentication isn't sufficient by itself to protect data, Crowley notes. What's needed is an additional layer, **authorization**, which determines whether a user should be allowed to access the data or make the transaction they're attempting.

In simple terms, **authentication** is the process of verifying who a user is, while **authorization** is the process of verifying what they have access to.

## Access Control

Access control is one of the most important cyber security practices. Careful adjustment of users' access rights helps to secure sensitive data and reduces the chance of a successful attack.

## Why is access control important?

Access control regulates which users, applications, and devices can view, edit, add, and delete resources in an organization's environment. Controlling access is one of the key practices to protect sensitive data from theft, misuse, abuse, and any other threats. There are two levels of access control: physical and logical.


**Figure 2.0**

Access control helps to mitigate both inside and outside threats. That's why IT regulations and standards — NIST, HIPAA, PCI DSS, and others — enforce strict physical and logical access control measures. In this article, we discuss models of logical access control.

There are several logical access control models: mandatory, discretionary, role-based, attribute-based, etc. The process of choosing and deploying an access control model looks different for each organization. This choice depends on:

1. The nature of the protected data
2. IT requirements and industry standards
3. The number of employees
4. The cyber security budgets

## What is Mandatory Access Control?

It is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on a need to know basis: users have to prove a need for information before gaining access.

MAC is considered the most secure of all access control models. Access rules are manually defined by system administrators and strictly enforced by the operating system or security kernel. Regular users can't alter security attributes even for data they've created.

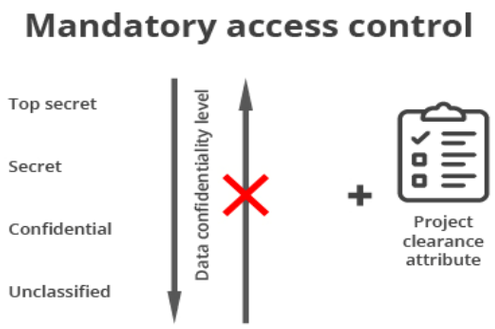


**Figure 2.1**
**Mandatory Access Control Model**

With MAC, the process of gaining access looks like this:

1. The administrator configures access policies and defines security attributes: confidentiality levels, clearances for accessing different projects and types of resources.
2. The administrator assigns each subject (user or resource that accesses data) and object (file, database, port, etc.) a set of attributes.
3. When a subject attempt to access an object, the operating system examines the subject's security attributes and decides whether access can be granted

MAC brings lots of benefits to a cyber security system. But it has several disadvantages to consider.

**What is Discretionary Access Control?**

It is an identity-based access control model that provides users a certain amount of control over their data. Data owners (or any users authorized to control data) can define access permissions for specific users or groups of users.

Access permissions for each piece of data are stored in an **access-control list (ACL)**. This list can be generated automatically when a user grants access to somebody or can be created by an administrator. An ACL includes users and groups that might access data and levels of access they might have. An ACL can also be enforced by a system administrator. In this case, the ACL acts as a security policy and regular users can't edit or overrule it.

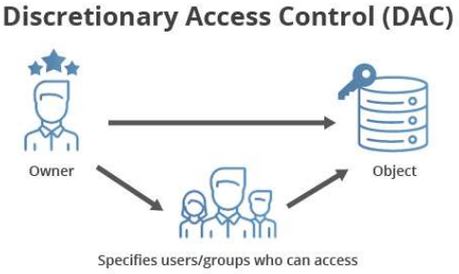


**Figure 2.2**
**Discretionary Access Control Model**

Gaining access in the DAC model works like this:

1. User 1 creates a file and becomes its owner or obtains access rights to an existing file.
2. User 2 requests access to this file.
3. User 1 grants access at their discretion. However, user 1 can't grant access rights that exceed their own. For example, if user 1 can only read a document, they can't allow user 2 to edit it.
4. If there's no contradiction between the ACL created by an administrator and the decision made by user 1, access is granted.

Discretionary access control is quite a popular model because it allows a lot of freedom for users and doesn't cause administrative overhead. However, it has several considerable limitations.

## Comparing the Two Approaches

Let's review the key characteristics of these two access control models:

**Table 1.0**
**Comparison of MAC vs. DAC**

| Characteristic | MAC | DAC |
|---|---|---|
| Access control enforced by | Administrators and operating system | Administrators and users |
| Flexibility | – | ✓ |
| Scalability | – | ✓ |
| Simplicity | – | ✓ |
| Maintenance | Hard | Easy |
| Implementation cost | High | Low |
| Granularity | High (admins adjust clearances for each user and object manually) | High (users can assign access rights for any other user or group) |
| Easy to use | – | ✓ |
| Security level | High | Low |
| Useful for | Government, military, law enforcement | Small and medium-sized companies |

MAC and DAC are very different access control models, suitable for different kinds of organizations. DAC works well for organizations that require flexibility and user-friendly workflows. On the other hand, MAC is more efficient for organizations that work with highly sensitive data.

## What is Role-Based Access Control (RBAC)?

It is an access control method based on defining employee roles and corresponding privileges within the organization. The idea of this model is that every employee is assigned a role. Every role has a collection of permissions and restrictions. An employee can access objects and execute operations only if their role in the system has the relevant permissions.

Let's consider the main components of the role-based approach to access control:

1. **User** – an individual (with UID) with access to a system
2. **Role** – a named job function (indicates the level of authority)
3. **Permission** – equivalent to access rights
4. **Session** – a mapping between a user and a set of roles to which the user is assigned in the context of a working time
5. **Object** – a system resource that requires permission to access
6. **Operation** – any action in the protected network

**What is Attribute-Based Access Control (ABAC)?**

It is a model that evolved from RBAC. This model is based on establishing a set of attributes for any element of your system. A central policy defines which combinations of user and object attributes are required to perform any action.

Let's consider the main components of the ABAC model according to NIST:

1. **Attribute** – a characteristic of any element in the network. An attribute can define:
2. **User characteristics** – employee position, department, IP address, clearance level, etc.
3. **Object characteristics** – type, creator, sensitivity, required clearance level, etc.
4. **Type of action** – read, write, edit, copy, paste, etc.
5. **Environment characteristics** – time, day of the week, location, etc.
6. **Subject** – any user or resource that can perform actions in the network; a subject is assigned attributes in order to define its clearance level
7. **Object** – any data stored in the network; objects are assigned attributes in order to describe and identify them
8. **Operation** – any action taken by any subject in the network
9. **Policy** – a set of rules allowing or restricting any action in your information retrieval system; rules are "IF/THEN" statements based on attributes of any element (user, resource, environment)

## Concept of Trust and Trustworthiness

Given recent breaches and the activity surrounding the regulation and usage of data, there is one important aspect to our online lives that is being overlooked, and that is the role of trust in our relationships.

***Trust*** and ***trustworthiness*** go hand in hand. **Trust** has been defined as a relationship between a trustor and a trustee. A **trustor** shows 'the willingness to be vulnerable to another party' [1] and has a confident expectation [2] that the **trustee** will not take advantage of this vulnerability. **Trustworthiness** is the complement to trust, whereby the relationship between the two parties is predicated upon the trustee being (literally) worthy of trusting. **Trustworthiness** means that the trustee will work on behalf of the trustor to fulfil their confident expectation without taking advantage of the vulnerability of the trustor by acting in an opportunistic manner.

## E. Evaluate

**ASSESSMENT:**
**Instructions**: You may write your answer on the Answer Sheet (AS) provided in this module.

**CONTENT FOR ASSESSMENT:**

For 2-points each:

1. Defined as a relationship between a trustor and a trustee.
2. An identity-based access control model that provides users a certain amount of control over their data.
3. The process of verifying who a user is.
4. Authenticate and authorize individuals to access the information they are allowed to see and use.
5. The complement to trust, whereby the relationship between the two parties is predicated upon the trustee being (literally) worthy of trusting.

**References:**

1. *https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html*
2. *https://auth0.com/docs/authorization/concepts/authz-and-authn*
3. *https://www.ekransystem.com/en/blog/mac-vs-dac*
4. *https://www.ekransystem.com/en/blog/rbac-vs-abac*
5. *https://informationwithinsight.com/2018/05/04/trust-trustworthiness-and-data-sharing/*

| **Facilitated By:** | | |
|---|---|---|
| Name | : | |
| MS Teams Account (email) | : | |
| Smart Phone Number | : | |