جامـــــعـة المـــــسـتـقـبـل

AL MUSTAQBAL UNIVERSITY

قســـــم الامـــــــــــــــن الـــــــــــــــــــــســيبرانـــــــــــــــــــي

Department of Cyber Security

Subject:

Authentication and access control

Class:

second

Lecturer:

Dr. Suha Alhussieny

Lecture: (7)

Access Control

Authorization

Authorization is the part of access control concerned with restrictions on the actions of authenticated users. authorization deals with the situation where we've already authenticated Alice and we want to enforce restrictions on what she is allowed to do. Note that while authentication is binary (either a user is authenticated or not), authorization can be a much more fine-grained process.

Organizations often struggle to understand the difference between authentication and authorization. Authentication is the process of verifying individuals are who they say they are using biometric identification and MFA. The distributed nature of assets gives organizations many avenues for authenticating an individual.

Authorization is the act of giving individuals the correct data access based on their authenticated identity. One example of where authorization often falls short is if an individual leaves a job but still has access to that company's assets. This creates security holes because the asset the individual used for work -- a smartphone with company software on it, for example -- is still connected to the company's internal infrastructure but is no longer monitored because the individual is no longer with the company. Left unchecked, this can cause major security problems for an organization. If the ex-employee's device were to be hacked, for example, the attacker could gain access to sensitive company data, change passwords or sell the employee's credentials or the company's data.One solution to this problem is strict monitoring and reporting on who has access to protected resources so, when a change occurs, it can be immediately identified and access control lists and permissions can be updated to reflect the change.

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.

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

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

Why is access control important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After high-profile breaches, technology vendors have shifted away from single sign- on systems to unified access management, which offers access controls for on-premises and cloud environments.

How access control works?

Access controls identify an individual or entity, verify the person or application is who or what it claims to be, and authorizes the access level and set of actions associated with the username or IP address. Directory services and protocols, including Lightweight Directory Access Protocol and Security Assertion Markup

Language, provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers. Organizations use different access control models depending on their compliance requirements and the security levels of IT they are trying to protect.

Access Control and Access Control Models

Access control is the process of:

✓ identifying a person doing a specific job

✓ authenticating them by looking at their identification

✓ granting a person only the key to the door or computer that they need access to and nothing more.

In information security, one would look at this as:

✓ granting an individual permission to get onto a network via a username and password

✓ allowing them access to files, computers, or other hardware or software they need

✓ ensuring they have the right level of permission to do their job

So, how does one grant the right level of permission to an individual so that they can perform their duties? This is where access control models come into the picture.

Access Control Models

Access control models have five types:

1. **Mandatory Access Control (MAC)**
2. **Role-Based Access Control (RBAC)**
3. **Discretionary Access Control (DAC)**
4. **Rule-Based Access Control (RBAC or RB-RBAC)**
5. **Attribute-based access control**

1. **Mandatory access control (MAC).** 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

2. **Discretionary access control (DAC).** 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.

3. **Role-based access control (RBAC).** 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.

4. **Rule-based access control.** 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.

5. **Attribute-based access control.** 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.

Authentication – Verifying Identity

Authentication answers the question: **“Who are you?”**

It is the process of proving that a user or device is truly who they claim to be.

Techniques previously studied include:

- Password-based authentication
- Biometric authentication
- Multi-factor authentication (MFA)
- Kerberos authentication
- Digital certificates (X.509)
- TLS/SSL Handshake authentication

Example:

Logging into a system using a password, biometrics, or Kerberos ticket.

2. Authorization – Determining Permissions

Authorization answers the question:
“What are you allowed to do?”

Once a user is authenticated, the system determines:

- Which files they can access
- Which operations they can perform
- Which systems or applications they can use

Authorization policies might include:

- RBAC (Role-Based Access Control)
- DAC (Discretionary Access Control)

- MAC (Mandatory Access Control)
- ABAC (Attribute-Based Access Control)

Example:

A user is authenticated to the company network, but only the HR department is authorized to access salary records.

3. Access Control – Enforcing Restrictions

Access control is the **overall security framework** responsible for enforcing authentication and authorization rules.

It includes:

- Who is allowed to log in
- What resources they can access
- Under what conditions they can access them
- Monitoring and logging user actions

Access control combines the results of authentication and authorization to make access decisions

Principle of Least Privilege (PoLP)

This principle states that users should be granted **only the minimum access necessary** to perform their duties—no more, no less.

Why it's important?

- Reduces attack surface
- Limits insider threats
- Prevents malware from gaining elevated privileges
- Protects sensitive assets

Common Attacks on Access Control Systems (Short Definitions)

1. Privilege Escalation

A type of attack where an attacker gains higher-level permissions than they are supposed to have—such as a normal user gaining admin rights—by exploiting vulnerabilities or misconfigurations.

2. Session Hijacking

An attack where an attacker steals or intercepts a user’s active session token, allowing them to impersonate the user and access the system without logging in.

3. Bypass Attacks

Attacks in which an attacker accesses protected resources by circumventing access control mechanisms—such as directly accessing restricted URLs or APIs without proper authorization checks.

4. Insider Threats

Attacks carried out by someone inside the organization (employee, contractor, partner) who misuses their legitimate access to steal, modify, or damage sensitive information

H.W/

1. What is the primary purpose of authorization in access control?

2. Which of the following best describes authentication?

`3. What is the main goal of access control in security?

4. Which type of access control limits entry to buildings and physical assets?

5. Logical access control includes which of the following?

6. Why is MFA important in access control systems?

7. Authorization answers which question?

8. Which of the following is an example of authorization failure?

9. Mandatory Access Control (MAC) is commonly used in:

10. Which access control model allows resource owners to decide permissions?

11. RBAC assigns permissions based on:

12. Rule-based access control makes decisions based on:

13. Attribute-based access control (ABAC) evaluates:

14. Which principle states users should only receive minimum required access?

15. Privilege escalation occurs when:

16. Session hijacking involves an attacker:

17. Bypass attacks occur when attackers:

18. Insider threats refer to:

19. Which protocol is commonly used for authentication in directories?

20. Access control combines authentication and: