Module 5: Homework 5

Harsh Siddhapura

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

September 20, 2023

Review Questions

1. **Explain the difference between authorization, authentication, and access control.**

   Authorization, authentication, and access control are fundamental concepts in cybersecurity and information security, each serving a distinct role in ensuring the confidentiality, integrity, and availability of data and systems. Here are the key differences between these three concepts:

   - **Authentication:**
     - Definition: Authentication is the process of verifying the identity of a user, system, or entity attempting to access a resource or system. It ensures that the entity is who they claim to be.
     - Purpose: The primary purpose of authentication is to establish trust in the identity of the user or entity, preventing unauthorized access.
     - Methods: Authentication methods include something you know (e.g., passwords or PINs), something you have (e.g., smart cards or security tokens), something you are (e.g., biometrics like fingerprint or facial recognition), or a combination of these factors (multi-factor authentication).
     - Example: When you enter your username and password to log in to an online banking account, the system checks whether the credentials match those stored for your account.
   - **Authorization:**
     - Definition: Authorization is the process of granting or denying specific permissions or privileges to authenticated users or entities based on their verified identity.
     - Purpose: Authorization ensures that users or entities have the appropriate level of access to resources, systems, or data once their identity has been authenticated.
     - Methods: Authorization is typically managed through access control lists (ACLs), role-based access control (RBAC), or attribute-based access control (ABAC). It defines who can access what resources and what actions they can perform.

  - Example: After successfully logging in to an email account, authorization determines whether the user has permission to read, send, or delete emails and access specific folders.

- **Access Control:**
  - Definition: Access control is a broader concept that encompasses both authentication and authorization. It involves policies, procedures, and mechanisms that restrict or allow access to resources, systems, or data based on security policies and rules.
  - Purpose: Access control is the overarching framework that governs who can access what resources, under what conditions, and what actions they can perform. It ensures that only authorized entities gain access.
  - Components: Access control includes authentication (verifying identity) and authorization (granting permissions). It also encompasses mechanisms like firewalls, encryption, intrusion detection systems, and security policies.
  - Example: An organization's network infrastructure may use access control to allow only authorized employees to access certain network segments, authenticate their identities with usernames and passwords, and authorize specific actions based on their roles.

In summary, authentication focuses on verifying the identity of users or entities, authorization determines what they are allowed to do once their identity is established, and access control is the overarching framework that combines both to manage and enforce security policies. Together, these concepts play a crucial role in safeguarding information and systems from unauthorized access and misuse.

2. **What is the difference between need-to-know and need-to-use?**

"Need-to-know" and "need-to-use" are principles related to information and data access control in the context of security and confidentiality. While they share some similarities, they have distinct meanings:

Need-to-Know:

- Definition: Need-to-know is a security principle that restricts access to sensitive information only to individuals or entities who have a legitimate and specific requirement to access that information for their job or task.
- Purpose: The primary purpose of need-to-know is to minimize the exposure of sensitive information and limit access to individuals on a "need-to-know" basis. This principle is often applied in contexts where the information is highly classified or confidential.
- Access Control: Under the need-to-know principle, individuals are granted access to specific information based on their job roles, responsibilities, and the relevance of the information to their duties. Those who do not have a legitimate need to know the information are denied access.
- Examples: In government and military settings, classified information is typically restricted to individuals with a specific security clearance and a demonstrated need-to-know for that information. Similarly, in healthcare, patient records may only be accessible to healthcare professionals directly involved in a patient's care.

Need-to-Use:

- Definition: Need-to-use is a related but broader principle that focuses on granting access to data or resources based on an individual's requirement to use that data for a specific purpose.
- Purpose: The primary purpose of need-to-use is to ensure that access to data or resources is granted based on the necessity for a particular task or function, even if that task involves the processing or manipulation of data rather than just knowledge of its existence.
- Access Control: Under the need-to-use principle, access is granted based on the specific tasks or functions that an individual or entity needs to perform. This includes not only viewing or knowing the data but also actively using it for a defined purpose.
- Examples: In a corporate setting, employees may have access to customer data based on their job roles, such as customer support representatives needing access to customer records to provide assistance. In this case, the employees have a need-to-use the data to fulfill their job responsibilities.

In summary, while both need-to-know and need-to-use principles involve controlling access to information, need-to-know is primarily concerned with restricting access to individuals who require specific knowledge, while need-to-use encompasses granting access based on the requirement to actively use data or resources for specific tasks or functions. Need-to-know is often associated with highly classified or sensitive information, while need-to-use is a broader concept applied in various organizational contexts.

3. **Describe the process for authorizing users.**

The process for authorizing users, often referred to as user access authorization or access control, involves defining, managing, and granting permissions and privileges to individuals or entities based on their roles, responsibilities, and the principle of least privilege. Below is a general overview of the user authorization process:

- Identification and Authentication: Before authorization can occur, users must first be identified and authenticated. Identification involves establishing the user's identity (e.g., username or employee ID), while authentication verifies that the user is who they claim to be using methods like passwords, biometrics, or multi-factor authentication.
- Role-Based Access Control (RBAC): Many organizations implement role-based access control (RBAC), which involves categorizing users into roles based on their job functions. Roles are associated with specific permissions and access rights.
- Authorization Policies and Rules: Organizations define authorization policies and rules that specify what actions or resources users in various roles are allowed to access. These policies are often documented in access control lists (ACLs) or access control matrices.
- Access Control Lists (ACLs): ACLs are lists of permissions associated with specific resources (e.g., files, folders, databases). They specify which users or groups have read, write, execute, or other permissions for each resource.
- Authorization Levels: Users are granted authorization levels or privileges based on their roles, responsibilities, and the specific permissions required to perform their tasks. These levels may include read-only access, read-write access, administrative privileges, and more.

- Request for Access: When a user requires access to a resource or system, they submit a request for access. This request typically includes details about the resource, the reason for access, and the user's role.
- Access Request Review: Authorization requests are reviewed and evaluated by designated personnel or automated systems responsible for access control. The review assesses whether the requested access aligns with the user's role and job responsibilities.
- Approval Workflow: In many organizations, access requests follow an approval workflow. The request may need to be approved by a supervisor, manager, or administrator before access is granted.
- Access Granting: After approval, the necessary permissions and privileges are granted to the user's account or identity. This may involve modifying ACLs, updating role assignments, or configuring access settings in the relevant systems.
- Monitoring and Audit: Access activities are continuously monitored, and access logs are maintained to track user interactions with resources and systems. Regular audits help ensure that access remains aligned with policies and roles.
- Periodic Review and Recertification: Authorization levels and access rights should be periodically reviewed to ensure they remain appropriate. This process, known as recertification, helps identify and revoke unnecessary or outdated access.
- Revocation of Access: When a user's role changes, they no longer require certain access, or there are security concerns, access may need to be revoked or modified promptly to prevent unauthorized access.
- Documentation and Reporting: Detailed records of user authorizations, access requests, approvals, and changes are maintained for compliance, auditing, and reporting purposes.

The user authorization process is essential for ensuring that individuals or entities have appropriate access to resources and data while adhering to security and compliance requirements. It plays a critical role in safeguarding information and systems against unauthorized access and misuse.

4. In the context of user authentication, what is the distinction between identification and verification?

Identification is the initial step in the authentication process, during which a user confirms that they are who they claim to be by entering data like a username, email address, or account number. While it cannot speak for them, this identifier aids the system to identify the persona of the possible user. In basic terms, identification offers an answer to the query, "Whoever do you claim to be?" It mimics presenting a photo ID to get into a secure building without extra verification.

Verification: On the other hand, verification is the subsequent process which evaluates the accuracy of the user's claim made during identification. Presenting credentials or evidence to support the claimed identity typically involves the user using something they know (such as a password), someone they have (e.g. as an electronic card or smart device), or something they are (e.g. as biometric data like their fingerprints or facial recognition technologies). By checking whether the credentials the user gave match the records connected to the stated identity, verification validates the user's identification.

5. Describe the functions of the various components in Figure 5.2.

Multi Factor authentication refers to the use of more than one of the authentication means in the preceding list (see Figure 5.2). Typically, this strategy involves the use of authentication technologies from two of the classes of factors described in the preceding section, such as a PIN plus a hardware token (knowledge factor plus possession factor) or a PIN and a biometric factor (knowledge factor plus inherence factor). Multifactor authentication is generally more secure than single-factor authentication because the failure modes for different factors are largely independent.

So, for example, a hardware token might be lost or stolen, but the PIN required for use with the token would not be lost or stolen at the same time. This assumption is not always true, however. For example, a PIN attached to a hardware token is compromised at the same time that the token is lost or stolen. Nevertheless, multi-factor authentication is an important means of reducing vulnerability.

An example of two-factor authentication is commonly used for web-based services, including online banking, PayPal, and Facebook. Typically, the user provides a password. Then a six-digit code is sent as a text message to the user's cellphone, and the user must enter the code to complete the login.

6. **Describe the three principal authentication factors.**

When a user or system tries to access a resource or system, authentication is the process used to confirm that person or system's identity. We establish this identity using authentication factors. The key authentication factors are as follows:

- The Use of Knowledge-Based Authentication is dependent on data that the user is aware of and able to offer that includes a password, Personal Identification Number, passphrase, or the responses to security questions and the most common way used is through passwords where users are asked to submit their special password but if not handled properly it may be open to numerous threats like credential theft, phishing, and password guessing.
- When a user uses possession-based authentication, they must have something tangible in their possession, like a hardware token, smart card, smartphone, or security token which includes one-time passwords or cryptographic keys generated by hardware tokens and smart cards must be presented that is by sending one-time codes via SMS or mobile apps, mobile devices can be utilized for possession-based authentication which in return provides an extra layer of security because, even if the attacker knew the user's password, they would still require physical access to the possession in order to gain entry.
- Biometric authentication relies on distinctive physical or behavioral characteristics of the user, such as fingerprints, retina scans, voice recognition, facial recognition, and even typing or mouse movement patterns this is because each person's biometrics are distinctive, when properly used, they may be extremely secure as it provides a practical and user-friendly method to confirm identification, biometric authentication is becoming more and more used in mobile devices and access control systems. However, because it cannot be altered if compromised, biometric data should be managed and preserved securely.

7. **What is multifactor authentication?**

With multi-factor authentication (MFA), a user must give two or more verification factors in order to access a resource, such as an application, an online account, or a VPN. A solid identity and access management (IAM) policy must include MFA. MFA requests one or more extra verification criteria in addition to a username and password, which lessens the chance that a cyberattack will be successful. The main advantage of MFA is that it will increase the security of your company by forcing users to provide identification other than a login and password.

Although crucial, usernames and passwords can be stolen by other parties and are subject to brute force assaults. When you require the usage of an MFA element, such as a physical hardware key or thumbprint, you may be more confident that your company will be protected from cybercriminals. MFA functions by requesting extra verification data (factors).

One-time passwords (OTPs) are among the MFA factors that consumers come across most frequently. OTPs are the four to eight-digit codes that you frequently get via email, SMS, or a mobile app. OTPs create a fresh code every so often or each time an authentication request is made. The seed value, which is given to the user when they initially register, and another factor—which could just be an increasing counter or a time value—are used to construct the code.

8. **Describe four common access control policies.**

Organizations can impose access regulations and provide user permissions using access control models. There are four different types of access control techniques: mandatory access control (MAC), role-based access control (RBAC), discretionary access control (DAC), and rule-based access control (RBAC or RB-RBAC). The level of access required by each user, the security requirements, the infrastructure, etc. are taken into consideration while selecting a method.

- Discretionary Access Control (DAC): The ability to choose which users can access which resources is granted by the discretionary access control (DAC) method of control, which is used by the business owner or designated IT professional. Any files or data that relate to that authorization can be accessed if you have the necessary credentials. This approach relies on active management and supervision from either an individual or a department. Due to the fact that any credential can receive any authorisation, it is versatile. The person in charge, however, must put up a lot of effort to keep track of each user and provide them authorization.

- Mandatory Access Control (MAC): One of the harshest types of access control is mandatory access control (MAC), which is commonly accepted. The only way a user can gain access to MAC is with the authorization of a system administrator, most often the Chief Security Officer or someone with a similar designation. MAC does not grant access to users based on their attributes or credentials. Government entities employ this method most commonly because it generates a strong sense of security around important and sensitive data. Although MAC is a useful approach for access control, it is extremely constrictive and solely depends on one person to grant and revoke permissions. It significantly increases the demand on the CSO to create a solid permissions structure and manage its operation.
- Role-Based Access Control (RBAC): Role-based access control (RBAC) is another access control approach that is best suited to businesses that must adhere to stringent compliance or security standards.Using this architecture, users can access particular resources according to their roles. This makes it possible to guarantee that nobody will be able to see or utilize information that is unrelated to their job duties. Since it guarantees workers have access to only what they require to perform their duties and nothing more, this model is secure while still being user-friendly.
- Rule-Based Access Control (RBAC): RBAC is a dynamic access control mechanism that bases access choices on a set of rules.RBAC compares requests for access to a set of predetermined rules or policies. These laws may depend on a number of variables, such as user characteristics, the time of day, a particular region, and more.

9. **What is the difference between an access control list and a capability ticket?**

There are two alternative ways for regulating access to resources in a computer system: the Access Control List (ACL) and the Capability Ticket. They have different access control strategies but similar purposes:

ACL: ACL is a list of permissions connected to a resource or object. It details which users or groups may read, write, or execute a resource. ACLs, which specify who has access to a resource and what actions they may take on it, are typically administered by the system or resource owner. When managing ACLs in big systems with lots of users and resources, complexity can arise.

Capability Ticket: Alternative strategy is capability-based access control, in which permission to access a resource is demonstrated by the possession of a token or "capability”. Capability tickets are special tokens that are given by the owner of the resource rather than a list of users who have access to it. A user has to show a valid capability ticket in order to access a resource. Because capability tickets reflect a single right to access a resource rather than a list of permissions, they can be more precisely granular than permissions lists.

10. What is the difference between role-based access control and attribute-based access control?

There are two main approaches used in access control for computer systems: Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). In a simpler method known as RBAC, access rights are connected to predetermined roles within an organization. Users are given certain roles depending on their duties or job functions, and these roles govern their access. RBAC is simple to create and operate, but it might not be able to handle more complicated situations where the needs for access control depend on a number of different circumstances.

ABAC is a more adaptable and flexible solution to access control, on the other hand. It takes a variety of factors into account, such as user factors (like department or clearance level), resource factors (like sensitivity or location), and environmental factors (like time of day or network location). ABAC enables dynamic access management and fine-grained control by comparing these qualities to a set of rules or policies before making access decisions.

Because it is more flexible than RBAC and can be used to a wider variety of circumstances, ABAC is particularly helpful in cases where access control requirements are complex and diverse.

11. What is identity and access management?

Identity and Access Management (IAM) is a core framework used by organizations to secure digital assets and control access to sensitive data. IAM encompasses functions like user authentication, authorization, and user lifecycle management. Authentication verifies users' identities, ensuring they are who they claim to be, while authorization sets permissions based on predefined policies, often using role-based access control (RBAC).

IAM manages the complete lifecycle of user identities, from onboarding to offboarding, and offers features like Single Sign-On (SSO) for user convenience and Multi-Factor Authentication (MFA) for enhanced security. IAM also provides audit and reporting capabilities crucial for regulatory compliance and security monitoring. In essence, IAM ensures appropriate resource access while mitigating unauthorized access and security risks.[5]

12. Describe three deployment approaches for identity and access management.

- **On-Premises Deployment:**

  In on-premises IAM, organizations maintain their entire IAM system within physical data centers. This offers full control and suits regulated industries. Yet, it demands substantial upfront investments, ongoing maintenance, and comprehensive security management, with scalability limitations.

- **Cloud-Based Deployment (IDaaS)**:

  Cloud-based IAM, known as IDaaS, involves hosting IAM solutions with an external cloud provider. It's scalable, cost-effective, and reduces infrastructure management. However, it necessitates trust in the cloud provider for data security and compliance.

- **Hybrid Deployment:** Hybrid IAM blends on-premises and cloud-based IAM components, providing flexibility. It's suitable for gradual transitions or balancing control with scalability but can introduce complexities in managing and integrating IAM elements. Careful planning is vital for success.

13. What is federated identity management?

Federated identity management is similar to SSO scaled across multiple enterprises who have established a trust relationship enabling their users to access services across the various enterprises using the same credentials.

The organizations in agreement form a trust domain, each with the responsibility of maintaining their own identity management. They link through a third party that keeps records of each user's (from any enterprise) credentials and broken access to other services in the trust domain based on assigned permissions.

14. What is meant by single sign-on?

According to Cloudfare (2023), single sign-on (SSO) is the practice of using one set of NTLM credentials to gain access to multiple sites within an intranet. It works by creating an authentication token for a verified user. Any app in which the user is authenticated to access, will be passed the same SSO token instead of a username and password to grant the user access.

An identity management service issues tokens and manages their validity. The common standard for authentication token is called the Security Assertion Markup Language (SAML).

References

[1] Cloudfare (2023), *What is single sign-on (SSO)?*, date accessed 9/15/2023, https://www.cloudflare.com/learning/access-management/what-is-sso/

[2] Awati, R, & Rosencrance, L, (2021), *Identity and access management,* date accessed 9/15/2023, https://www.techtarget.com/searchsecurity/definition/federated-identity-management

[3] OneLogin (2023), *What is Multi-Factor Authentication (MFA)?*, date accessed 9/15/2023, https://www.onelogin.com/learn/what-is-mfa

[4] ThreatBlockr (2023), *What are the 4 Types of Access Control?,* date accessed 9/15/2023, https://www.threatblockr.com/blog/4-types-of-access-control/

[5] *Definition of Identity and Access Management (IAM) - Gartner Information Technology Glossary*. (n.d.). Gartner.

https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam