1.2 Authentication vs. Authorization

1.2.1 Authentication:

Common Methods:

Usernames and Passwords:

Multi-Factor Authentication (MFA):

Biometric Authentication:

Digital Certificates:

Smart Cards:

1.2.2 Importance:

1.2.3 Authorization:

1.2 Authentication vs. Authorization

1.2.1 Authentication: The process of verifying the identity of a subject. It answers the question, "Who are you?"

Detailed Explanation:

Authentication is the process of confirming that a subject is who they claim to be.

It's about verifying credentials and establishing trust.

Authentication precedes authorization; you must know who someone is before you can decide what they can do.

Common Methods:

Usernames and Passwords: The most common method, but also the most vulnerable.

Detailed Explanation:

Users provide a username (or email address) and a secret password to verify their identity.

This method is widely used but susceptible to various attacks.

Vulnerabilities:

Password guessing and brute-force attacks: Attackers try to guess passwords by trying various combinations.

Phishing: Attackers trick users into revealing their passwords through deceptive emails or websites.

Keylogging: Attackers use malicious software to record users' keystrokes, including passwords.

Social engineering: Attackers manipulate users into revealing their passwords.

Dictionary attacks: Attackers use lists of common words and phrases to try to guess passwords.

Multi-Factor Authentication (MFA): Requires users to provide multiple forms of verification, such as a password and a one-time code from a mobile app.

Detailed Explanation:

MFA enhances security by requiring users to provide more than one type of authentication factor.

This makes it much harder for attackers to gain unauthorized access, even if one factor is compromised.

Authentication Factors:

Something you know: (e.g., password, PIN, security questions).

Something you have: (e.g., one-time code from an authenticator app, a hardware token, a smart card).

Something you are: (e.g., biometric authentication such as fingerprint or facial recognition).

Biometric Authentication: Uses unique biological characteristics, such as fingerprints, facial recognition, or voice recognition.

Detailed Explanation:

Biometric authentication uses biological traits for identification.

It offers a convenient and often secure way to authenticate users.

Types:

Fingerprint scanning: Uses fingerprints for identification.

Facial recognition: Uses facial features for identification.

Iris scanning: Uses iris patterns for identification.

Voice recognition: Uses voice characteristics for identification.

Concerns:

Privacy concerns: Collection and storage of biometric data raise privacy issues.

Potential for data breaches: Biometric data can be compromised if stored insecurely.

Difficulty in changing biometrics: Unlike passwords, biometrics cannot be easily changed if compromised.

Accuracy and reliability: Biometric systems are not always perfectly accurate and can be fooled.

Digital Certificates: Electronic documents that verify the identity of a user, website, or device.

Detailed Explanation:

Digital certificates use public-key cryptography to verify identity.

They are issued by trusted authorities and provide a high level of assurance.

Use Cases:

HTTPS: Securing web communication.

Code signing: Verifying the authenticity and integrity of software.

Secure email: Encrypting and digitally signing email messages.

Client authentication: Verifying the identity of users or devices.

Smart Cards: Physical cards with embedded chips that store user credentials.

Detailed Explanation:

Smart cards contain integrated circuits that can store and process data.

They provide a secure way to store user credentials and other sensitive information.

Use Cases:

Government IDs: National identity cards.

Banking cards: Credit cards and debit cards.

Physical access control: Access cards for buildings or restricted areas.

1.2.2 Importance:

Authentication is a prerequisite for authorization. You must know who a user is before you can determine what they are allowed to do.

Without proper authentication, authorization is meaningless.

1.2.3 Authorization: The process of determining what actions an authenticated subject is allowed to perform on a specific object. It answers the question, "What are you allowed to do?"

Detailed Explanation:

Authorization determines the level of access granted to a user after they have been authenticated.

It defines the specific permissions and restrictions placed on their actions.

Authorization is about granting or denying access to specific resources or functionalities based on the user's identity, role, or other attributes.

Examples:

Allowing a user to read a file but not modify it.

Granting an administrator the ability to delete user accounts.

Restricting access to a web page based on user role or group membership.