Chapter 4
User Authentication

Table of Contents

What is User Authentication?

User authentication is the process of verifying the identity of a user attempting to access a system, application, or network.

The primary goal is to ensure that only authorized individuals can access sensitive information or perform specific actions.

Authentication acts as the first line of defense in information security, establishing trust between the user and the system.

Key Objectives of User Authentication

1. **Identity Verification**:
    - Confirm that the user is who they claim to be.
2. **Access Control**:
    - Restrict system access to authorized users only.

3. **Protection Against Unauthorized Access**:
    - Prevent unauthorized users from accessing, modifying, or damaging resources.

Authentication Factors

User authentication methods are often categorized based on the type of information used to verify identity:

1. **Knowledge Factors** (Something the user knows):
    - **Passwords**: Secret words or phrases.
    - **PINs**: Personal Identification Numbers.
    - **Security Questions**: Answers to predefined questions.
2. **Possession Factors** (Something the user has):
    - **Smartphones**: Devices that can receive OTPs (One-Time Passwords).

- **Security Tokens**: Physical devices that generate authentication codes.
- **Smart Cards**: Cards with embedded chips that store authentication data.

3. **Inherence Factors** (Something the user is):
   - **Biometrics**: Fingerprints, facial recognition, iris scans, voice recognition.
4. **Location Factors** (Somewhere the user is):
   - **Geolocation**: Physical location verification using GPS or IP address.

Types of User Authentication

1. **Password-based Authentication**:
   - Users provide a username and password. Security can be enhanced with techniques like salting, hashing, and implementing strict password

policies.

2. **Biometric Authentication**:
    - Uses unique biological characteristics such as fingerprints, facial recognition, or iris scans. Offers high security but may raise privacy concerns and accuracy issues.
3. **Two-Factor Authentication (2FA)**:
    - Combines two different factors, typically something the user knows (password) and something the user has (smartphone or token), to enhance security.
4. **Multi-Factor Authentication (MFA)**:
    - Extends 2FA by requiring two or more factors from different categories, further enhancing security.

5. **Single Sign-On (SSO)**:
    - Allows users to authenticate once and gain access to multiple related systems without needing to log in again for each one, providing convenience but centralizing risk.
6. **Token-based Authentication**:
    - Users are issued a unique token, which can be a physical device (like a USB token) or a software-based token, used to verify identity. Tokens are often used in combination with other authentication factors.

Benefits of Effective User Authentication

- **Security**: Protects sensitive data from unauthorized access.
- **User Trust**: Builds confidence in the system's ability

to safeguard personal information.

- **Compliance**: Meets regulatory requirements for data protection and privacy.
- **Efficiency**: Streamlines access management, reducing the risk of security breaches.

Challenges in User Authentication

- **Usability vs. Security**: Balancing strong security measures with user convenience.
- **Password Management**: Users often create weak passwords or reuse them across multiple sites.
- **Biometric Data**: Privacy concerns and potential for false positives/negatives.

User Authentication Principles

1. Confidentiality

- Ensure that user credentials (like passwords) are kept secret and protected from unauthorized access. This often involves encryption and secure storage mechanisms.

2. Integrity

- Verify that the data and credentials provided by the user have not been tampered with. Techniques like hashing and digital signatures help maintain data integrity.

3. Availability

- Ensure that the authentication system is reliable and available when users need to access resources. This involves designing systems with redundancy and failover mechanisms.

4. Authentication Factors

Authentication typically involves one or more of the following factors:

- **Something You Know**: Knowledge-based authentication, such as passwords or PINs.
- **Something You Have**: Possession-based authentication, such as security tokens, smart cards, or mobile devices.
- **Something You Are**: Inherent-based authentication, such as biometric verification (fingerprints, facial recognition, iris scans).

5. Multi-Factor Authentication (MFA)

- MFA combines two or more authentication factors to increase security. For example, using a password (something you know) and a fingerprint (something you are).

6. Single Sign-On (SSO)

- SSO allows users to authenticate once and gain access to multiple related systems without having to log in again. This improves user experience and reduces password fatigue.

Password-Based Authentication

Password-based authentication is the most common and traditional method of verifying a user's identity. It involves users providing a secret code, known as a password, along with their username to gain access to a system, application, or network.

How Password-Based Authentication Works

1. **User Creation**:
    - When a user account is created, the user chooses

a password which is then stored in a secured manner (hashed and possibly salted) in the system's database.

2. **Login Process**:
    - The user enters their username and password.
    - The system retrieves the stored password hash for the given username and compares it with the hash of the entered password.
    - If the hashes match, the user is authenticated and granted access.

Types of Password-Based Authentication

Password-based authentication methods vary in terms of how passwords are stored and processed. Here are three primary types:

a. Store Password in Plain Text

Description:

- Passwords are stored in the database as plain text, exactly as the user entered them.

Process:

1. User creates an account and provides a password.
2. The system stores the password in its original form (plain text) in the database.
3. During login, the user provides the password.
4. The system compares the entered password with the stored plain text password.
5. If they match, the user is authenticated.

Advantages:

- Simplicity: Easy to implement with minimal processing.

Disadvantages:

- High Security Risk: If the database is compromised, all user passwords are exposed in plain text, making it extremely vulnerable to breaches.

b. Derived from Password (Encrypted Passwords)

Description:

- Passwords are encrypted before being stored in the database. During authentication, the system encrypts the entered password and compares it to the stored encrypted version.

Process:

1. User creates an account and provides a password.
2. The system encrypts the password using an encryption algorithm.
3. The encrypted password is stored in the database.
4. During login, the user provides the password.
5. The system encrypts the entered password using the same encryption algorithm.

6. The encrypted entered password is compared with the stored encrypted password.
7. If they match, the user is authenticated.

Advantages:

- Improved Security: Encrypted passwords are more secure than plain text, making it harder for attackers to retrieve the original passwords.

Disadvantages:

- Encryption Key Management: The security of the system depends on how well the encryption keys are managed. If keys are compromised, security is breached.

c. Message Digest Password (Hashed Passwords)

Description:

- Passwords are hashed using a cryptographic hash function before being stored in the database. During

authentication, the system hashes the entered password and compares it to the stored hash.

Process:

1. User creates an account and provides a password.
2. The system applies a cryptographic hash function to the password.
3. The hashed password (digest) is stored in the database.
4. During login, the user provides the password.
5. The system applies the same cryptographic hash function to the entered password.
6. The hashed entered password is compared with the stored hashed password.
7. If they match, the user is authenticated.

Advantages:

- High Security: Hashing is a one-way function, meaning it's practically infeasible to reverse the hash

to obtain the original password.

Disadvantages:

- Processing Overhead: Cryptographic hash functions require computational resources.

Token-Based Authentication

Token-based authentication is a security protocol that allows users to verify their identity and gain access to systems, applications, or networks by using a token. A token is a piece of data that serves as a credential to access resources. This method is popular for its ability to provide secure, scalable, and stateless authentication.

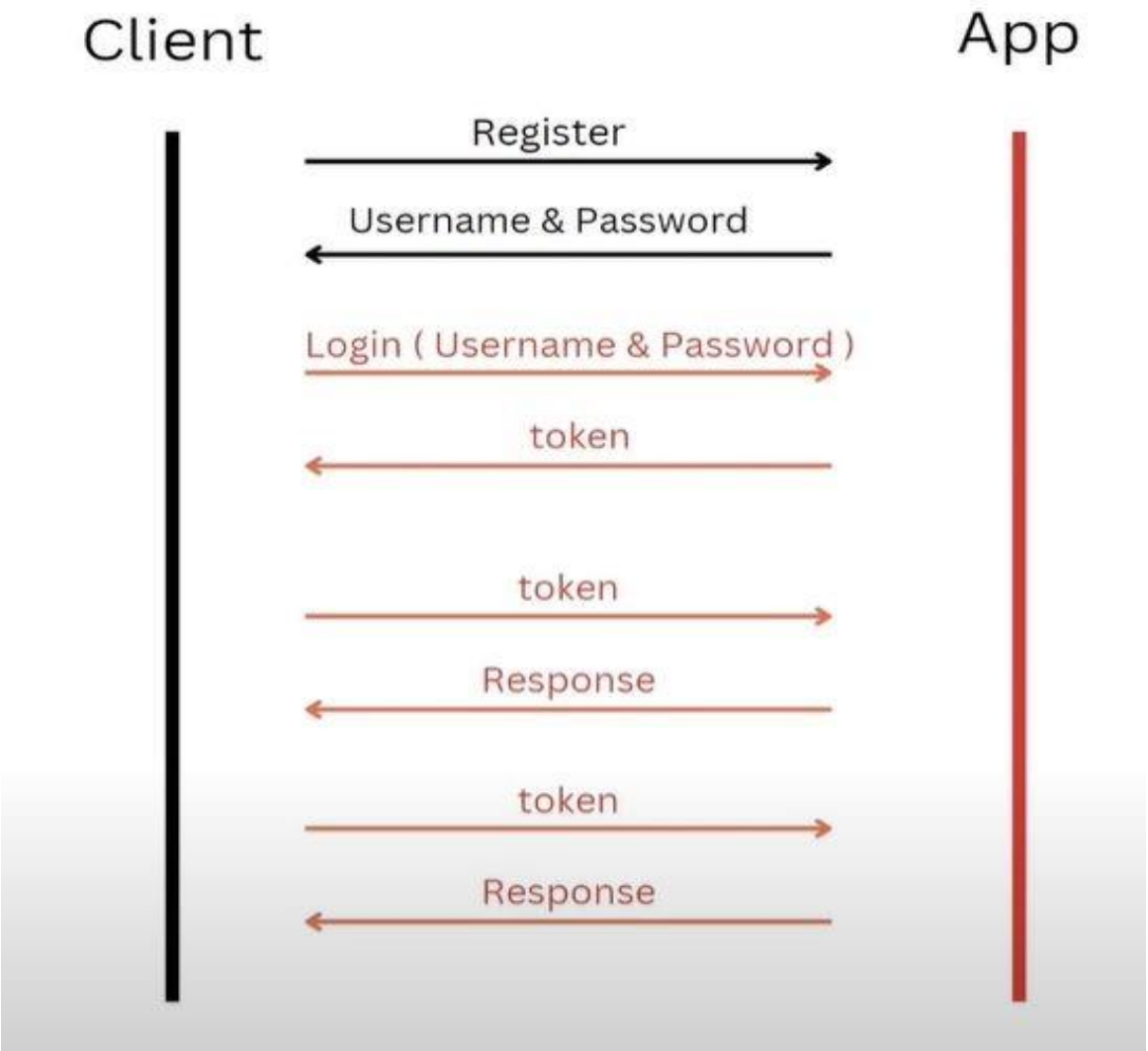
How Token-Based Authentication Works

1. **User Requests Access**:
    - The user sends a login request to the authentication server with their credentials (e.g., username and password).

2. **Authentication**:
    - The server verifies the credentials. If valid, the server generates a token for the user.
    - This token is typically a JSON Web Token (JWT) or another type of secure token.
3. **Token Issuance**:
    - The server sends the token back to the user.
    - The token contains encoded information, such as user identity and expiration time, and is signed to ensure its integrity.
4. **Token Storage**:
    - The user stores the token on their client device, often in local storage or a cookie.
5. **Accessing Resources**:
    - For subsequent requests, the user includes the token in the HTTP headers (e.g., Authorization header) when accessing protected resources.

6. **Token Verification**:

- The server verifies the token's signature and checks its validity (e.g., expiration, issuer).
- If the token is valid, the user is granted access to the requested resource.



Biometric Authentication

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify their identity.

This method uses biological data—such as fingerprints, facial recognition, iris scans, and voice recognition—to authenticate users.

Because biometric data is unique to each individual and difficult to replicate, it is considered a highly secure form of authentication.

How Biometric Authentication Works

1. **Enrollment**
    - **Capture**: The user's biometric data is captured using a biometric scanner (e.g., fingerprint reader, camera).
    - **Storage**: The captured data is processed and stored in a database or a secure module as a

biometric template.

2. **Authentication**
    - **Capture**: The user provides their biometric data for authentication (e.g., places a finger on a fingerprint scanner).
    - **Comparison**: The system captures the biometric data and compares it to the stored template.
    - **Decision**: If the captured data matches the stored template within a certain threshold, the user is authenticated.

Types of Biometric Authentication:

- Physical biometrics:
    - Fingerprints
    - Facial recognitions
    - Iris and retinas
    - Voice recognitions
    - DNA
- Behavioral biometrics:
    - Signatures
    - Behavioral characteristics of persons like walking, speaking styles, postures etc

Remote user authentications

Remote user authentications is the process of verifying the user remotely to grant access to the organization's system or network.

How does Remote user Authentication work?

1. Identification: The user needs to perform certain identity verification activities like face authentication, password authentications, fingerprint scan etc using some of the tools and software's

2. Verifications: In this step, the information generated is matched with records to confirm identity presented at step 1

The means of authentications are

1. User knowledge: passwords, answers to specific questions, PIN or OTP
2. Organization-issued assets: Smart card, cryptographic keys, physical keys
3. Biometric features: face, retina, fingerprints etc.
4. Biometric characters: Voice recognitions, typing rhythms, handwritings etc.

Two factor authentication

Two factor authentication (2FA) is a security system that requires two distinct forms of identifications in order to access something

The first factor is password and second commonly includes a text with a code sent to your phone, or biometrics using fingerprints, retinas, face etc.

Types of 2FA

- Tokens
- Magnetic cards
- SMS OTP
- USB
- Mobile signatures