**Discuss different authentication and authorization mechanism in online social network.**

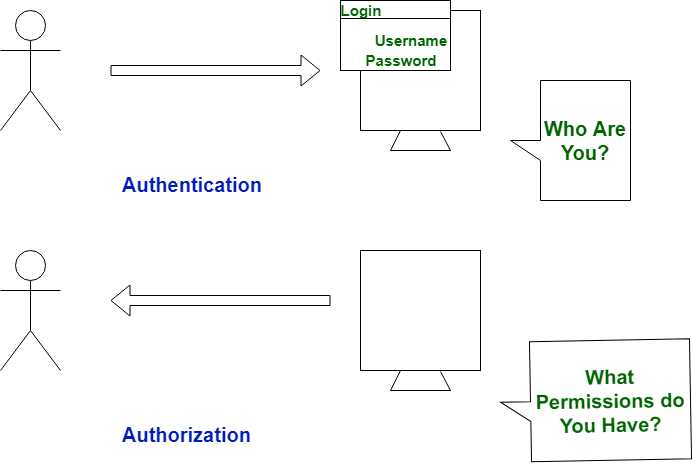
**What is Authentication?**

* Authentication is the method of verifying the identity of a consumer or system to ensure they’re who they claim to be.
* It involves checking credentials which include usernames, passwords, or biometric information like fingerprints or facial recognition.
* This step is vital for securing access to systems, programs, and sensitive records.
* By confirming identities, authentication saves you from unauthorized entry and protects you against safety breaches.

**What is Authorization?**

* Authorization is the process of deciding what a verified user or system is allowed to do.
* It happens after authentication and makes sure they have the right permissions to access certain data or perform specific actions.
* This helps keep the system secure by preventing unauthorized access.

**Diagram:**



Online Social Networks (OSNs) like Facebook, Instagram, LinkedIn, and Twitter are platforms where people connect, share, and interact. These platforms deal with sensitive personal data like photos, videos, messages, and location.

To protect user accounts and privacy, two core security mechanisms are used:

* Authentication: Confirms the identity of a user (e.g., is this really Alice logging in?).
* Authorization: Decides what that user can access (e.g., can Alice view Bob’s profile or post in a group?).

These two work together to maintain data confidentiality, integrity, and availability.

**1. Authentication Mechanisms**

Authentication ensures that only **authorized individuals** can access their accounts. It prevents identity theft, hacking, and unauthorized logins.

**a) Password-based Authentication**

This is the most common and basic form of authentication.

* Every user creates a **unique combination** of a **username (or email)** and **password** when signing up.
* The password is usually stored in the system in an **encrypted or hashed format** (using algorithms like bcrypt or SHA-256).
* When the user logs in, the system checks the entered password by comparing it with the stored hash.

🔹 **Example**:  
When a user logs in to Facebook with their email and password, the backend checks the credentials against the stored database.

🔹 **Challenges**:

* Weak passwords like "password123" are easily cracked.
* People often **reuse passwords** across multiple sites.
* Passwords can be stolen via **phishing**, **keylogging**, or **brute-force attacks**.

🔹 **Solution**:

* Enforce **strong password rules** (e.g., mix of letters, numbers, symbols).
* Use **password managers** and **multi-factor authentication**.

**b) Two-Factor Authentication (2FA)**

2FA provides an **extra layer of security** by requiring two forms of identification:

1. Something you **know** (your password)
2. Something you **have** (your phone, OTP app, email)

After entering the password, the system asks for an **OTP** (One-Time Password) or a **push notification confirmation**.

🔹 **Example**:  
Instagram or Gmail may send an OTP to your mobile after logging in. You must enter it to proceed.

🔹 **Benefits**:

* Even if your password is stolen, hackers can’t access your account without the second factor.
* Highly effective against **unauthorized access**.

**c) OAuth (Open Authorization)**

OAuth allows users to **log in through other trusted providers** (like Google, Facebook, Apple) without creating a new password for each app.

🔹 **How it works**:

* When you click **“Log in with Google”**, the system redirects you to Google.
* You log in to Google, which confirms your identity.
* Google sends a **token** to the app (like Pinterest), allowing you to access it.

🔹 **Example**:  
LinkedIn allows users to log in using their Microsoft or Google accounts.

🔹 **Advantages**:

* Avoids the need to remember multiple passwords.
* Safe: You don’t share your password with third-party sites.
* Easy login for users.

**d) Biometric Authentication**

This method uses a **user’s unique physical characteristics** to log in.

Common biometric identifiers:

* **Fingerprint**
* **Facial recognition**
* **Voice recognition**
* **Iris scan**

🔹 **Example**:

* WhatsApp or Facebook app can be locked/unlocked using your fingerprint or Face ID on smartphones.

🔹 **Advantages**:

* High security – difficult to replicate biometrics.
* Fast and convenient.
* No need to remember passwords.

🔹 **Limitation**:

* Requires biometric hardware on the device (fingerprint scanner, camera, etc.)

**e) Token-based Authentication**

In this method, after a user logs in successfully, the server generates a **token** (like a digital key), which is sent to the client (browser/app). The user uses this token to access protected routes or services.

The most popular token format is **JWT – JSON Web Token**.

🔹 **Example**:  
When a user opens the Twitter app, a JWT token is stored on the device. The app sends this token with every API request (like posting, commenting) to prove the user is authenticated.

🔹 **Benefits**:

* Eliminates repeated login for every action.
* More secure than using session IDs alone.
* Works well in mobile and distributed systems.

**2. Authorization Mechanisms**

Once a user is authenticated, the system needs to decide **what they are allowed to do or see**. This is where authorization mechanisms come in.

**a) Role-Based Access Control (RBAC)**

RBAC assigns **permissions based on roles** assigned to users.

* Each user is assigned a role (e.g., Admin, Moderator, User).
* Each role has specific rights (like view, edit, delete).

🔹 **Example**:  
In Facebook Groups:

* **Admin** can manage members and settings.
* **Moderator** can approve posts or remove content.
* **Member** can only post and comment.

🔹 **Benefits**:

* Simple to manage.
* Helps organize users in large systems.

**b) Attribute-Based Access Control (ABAC)**

ABAC gives access based on a combination of **attributes**:

* User attributes (age, gender, location)
* Resource attributes (content type)
* Environment conditions (time, device, location)

🔹 **Example**:  
On TikTok, only users above 18 and with over 1,000 followers can start a live stream.

🔹 **Advantages**:

* Fine-grained and dynamic.
* Adjusts permissions based on user behavior or context.

**c) Access Control Lists (ACLs)**

In ACLs, each **resource has a list of users and permissions**.

🔹 **Example**:  
You post a photo on Facebook and choose to share it only with 5 close friends. Only these people (in the ACL) can view it.

🔹 **Benefits**:

* Direct control over **who can access specific content**.
* Ideal for protecting personal content.

**d) Privacy Settings (User-Controlled Authorization)**

Most social networks allow users to control **who can see or interact** with their content.

🔹 **Settings include**:

* Public
* Friends only
* Friends of friends
* Custom (specific users)
* Only me

🔹 **Example**:  
On Instagram, setting your profile to **Private** means only your followers (who you approve) can view your posts and stories.

🔹 **Benefit**:

* Gives users control over their personal data.
* Helps maintain **online privacy** and **digital boundaries**.

**3. Supporting Security Features**

To support authentication and authorization, OSNs implement extra features:

**🔸 CAPTCHA**

* Ensures the user is **not a bot**.
* Often used during login, sign-up, or suspicious activity.

🔹 **Example**:  
Twitter asks you to click on "I’m not a robot" and select traffic lights.

**🔸 Session Timeout**

* Automatically logs out users after inactivity.
* Protects against misuse on public/shared devices.

**🔸 Account Lockouts**

* Temporarily locks accounts after **multiple wrong attempts**.
* Prevents brute-force attacks.

**🔸 HTTPS & Encryption**

* All communication is encrypted via **SSL/TLS** to prevent data theft.

🔹 **Example**:  
URL starts with https:// on Facebook, ensuring secure login.

**Conclusion**

Authentication and Authorization are **fundamental to securing online social networks**.

* **Authentication** confirms who you are.
* **Authorization** controls what you can do.

Using advanced techniques like **OAuth**, **2FA**, **RBAC**, **Privacy Settings**, and **Token-based Access**, social networks provide a **safe, controlled, and private user experience**.