**Various identity management techniques adopted in online social networks**

**Identity and Access Management**

* It is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required.
* The services and resources you want to access can be specified in IAM. IAM doesn’t provide any replica or backup.
* IAM can be used for many purposes such as, if one want's to control access of individual and group access

**IAM Components:**

* **Roles:**These are defined sets of permissions that can be assigned to users. For example, an "Admin" role might have the ability to manage all resources, while a "Viewer" role can only view resources.
* **Groups:**These are collections of users who share similar permissions. Instead of assigning permissions individually, users are grouped, and permissions are assigned to the group. This simplifies management, especially in large organizations.
* **Policies:** These are documents that define permissions and rules. They dictate what actions users or groups can perform on which resources. Policies are used to grant roles to users or groups, specifying the level of access.

**Techniques Used:**

**1. Authentication Techniques:** These are used to verify the user’s identity before granting access to the account or system.

**a) Username and Password**

* The most common and basic form of identity authentication.
* Users create a unique username and a secret password known only to them.
* While simple to implement, this method is vulnerable to attacks like phishing, brute force attacks, and password reuse across sites.
* Weak or predictable passwords often lead to unauthorized access.

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

* Adds an extra layer of security by requiring a second piece of information in addition to the password.
* Typically, this is a One-Time Password (OTP) sent to the user's phone, or generated by an authentication app like Google Authenticator.
* Significantly reduces the risk of account hijacking, especially if the primary password is compromised.

**c) Biometric Authentication**

* Uses physical traits such as fingerprint, facial recognition, iris scan, or voice for identity verification.
* Biometrics are unique to each individual, making impersonation extremely difficult.
* Often used in mobile applications and devices, particularly for apps that manage sensitive personal data.

**d) OAuth (Open Authorization)**

* Allows users to log into third-party services using their existing account credentials from platforms like Google or Facebook.
* Reduces the number of usernames and passwords users need to remember.
* Also minimizes the risk of password leakage since credentials are not shared with the third-party service.

**e) CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)**

* Designed to differentiate between human users and automated bots.
* Requires users to solve a challenge, such as identifying objects in images or typing distorted characters.
* Helps in blocking automated account creation and login attempts.

**2. Profile Verification Mechanisms:** These methods ensure that the identity information associated with user profiles is accurate and trustworthy.

**a) Verified Badges**

* Some users, particularly public figures, influencers, and brands, receive a special "verified" badge (commonly a blue checkmark).
* This indicates that the platform has authenticated their identity through documents or background checks.
* Helps users identify genuine accounts and avoid being misled by impersonators.

**b) Phone Number and Email Verification**

* Platforms often require users to verify their mobile number or email address by entering a code sent to them.
* Ensures that the user can be contacted and that the account is tied to a valid communication channel.
* Helps in account recovery and reduces the creation of multiple fake accounts.

**c) Government ID Submission**

* Some platforms may request users to submit scanned copies of official identification documents.
* This is especially common when accounts are reported for impersonation or when applying for profile verification.
* It helps to establish real-world identity with legal proof.

**d) AI-Based Profile Analysis**

* Social networks increasingly use artificial intelligence to detect fake accounts.
* Algorithms evaluate behavior such as rapid friend requests, spam messages, or repeated posting patterns to flag suspicious accounts.

**3. Privacy Settings and Access Controls:** These tools empower users to manage and control how their personal data and identity are presented and accessed.

**a) Custom Visibility Controls**

* Users can choose the audience for each post or piece of profile information.
* For example, a user may choose to show their phone number to only friends, while making their posts visible to everyone.
* Helps in maintaining appropriate boundaries and protecting sensitive data.

**b) Blocking and Reporting Features**

* Users can block individuals who behave inappropriately or violate community standards.
* Additionally, abusive, harmful, or fake profiles can be reported for review by the platform’s moderation team.

**d) End-to-End Encryption**

* Platforms such as WhatsApp and Messenger use encryption that ensures that only the sender and receiver can read the messages.
* This prevents third-party interception, including by the platform itself.

**4. Federated Identity and Single Sign-On (SSO):** These techniques allow users to authenticate with multiple systems using a single digital identity.

**a) Single Sign-On (SSO)**

* Enables users to access multiple services after a single login session.
* For instance, signing in to a Google account also provides access to YouTube, Gmail, and Google Docs.
* Simplifies login processes and reduces the need to remember multiple passwords.

**b) Federated Identity**

* Enables identity verification across multiple platforms or organizations without re-entering credentials.
* Commonly used in enterprise networks, educational platforms, and integrated social applications.

**5. Digital Identity Monitoring and Behavior Analysis:** These techniques help identify anomalies and prevent identity fraud or impersonation.

**a) Behavioral Biometrics**

* Systems monitor the way users interact with devices—such as typing speed, scroll patterns, and click timing—to recognize anomalies.
* If the behavior suddenly changes, the system may flag the session as suspicious.

**b) Automated Bot Detection**

* Algorithms track patterns like mass messaging, rapid friend requests, or non-human interaction speeds to detect bot behavior.
* Flagged accounts may be suspended or reviewed.

**c) Unusual Activity Notifications**

* Users are alerted when there is an unusual login attempt from a new device or geographic location.
* Often followed by a prompt to verify identity or change password.

**6. Legal and Ethical Compliance Techniques:** These ensure that platforms handle identity data in compliance with global laws and ethical standards.

**a) GDPR, CCPA, and Other Laws**

* These laws require companies to be transparent about data collection, usage, and sharing.
* Users must be given options to opt in or out and to access or delete their data.

**b) Consent-Based Data Handling**

* Platforms must clearly seek user consent before collecting personal information.
* Consent must be revocable at any time.

**c) Right to Be Forgotten**

* Allows users to request permanent deletion of their data and account.
* Enforced as a legal right in the European Union and supported on platforms like Facebook and Google.

**e) Child and Minor Protection Mechanisms**

* Enforced age limits, parental controls, and restricted profiles help ensure the safe use of social media by minors.

**Conclusion**

Identity management in online social networks is essential for ensuring user safety, privacy, and trust. A combination of authentication, verification, behavioral monitoring, privacy controls, and legal compliance forms the foundation of a secure and user-centric identity system. As technology evolves, new trends like decentralized identity and AI-based monitoring will redefine how identity is managed online.