**Overview of Authorization**

* **Authorization** determines **what a user** is allowed to do after authentication.
* It works closely with authentication, but while authentication verifies **who** the user is, authorization decides **what actions** the user can take.

**Key Security Principles in Authorization**

1. **Principle of Least Privilege**:
   * Users are given **only the minimum access** necessary to perform their tasks.
   * Access should only last as long as needed.
2. **Separation of Duties**:
   * Users shouldn't have **conflicting roles** that could lead to abuse of system privileges.
   * Example: Someone in customer service shouldn't be able to rate their own performance.
   * This helps prevent **system misuse** and errors.

**Authorization Systems and Roles**

* Authorization typically depends on a **user’s role** or **system permissions**.
* These systems are important for **managing access to networks, databases, and processes** in organizations.

**Common Authorization Protocols**

1. **HTTP Basic Authentication**:
   * Used to verify users requesting access to a web server.
   * However, **Basic Auth** transmits **usernames and passwords openly**, which makes it **vulnerable** to attacks.
   * **HTTPS** (secure version of HTTP) is now more common, as it encrypts data, preventing exposure of sensitive credentials.
2. **OAuth**:
   * An **open-standard protocol** that shares access permissions between applications without transmitting sensitive information like usernames and passwords.
   * Instead, it uses **API tokens**, which are small, encrypted blocks containing user identity and site permissions.
   * OAuth allows secure third-party access (e.g., using your Google account to sign up for another service), without sharing credentials.

**Security Benefits of OAuth**

* OAuth helps **minimize risks** by using encrypted tokens instead of sensitive data like passwords.
* Even if one platform is compromised, **API tokens** help prevent exposure of passwords, especially when **multi-factor authentication (MFA)** is in place.

**Next Steps in Access Control**

* In addition to **authorization**, monitoring **user access** is crucial for securing systems.
* The final part of the **authentication, authorization, and accounting (AAA)** framework, **accounting**, will focus on how we track and audit access.

**Accounting in Access Control Systems**

**What is Accounting?**

* **Accounting** is the practice of **monitoring access logs** to track who accesses systems, when they access them, and what resources they use.
* Access logs are essential for **security analysts**, helping identify trends (e.g., failed logins) and uncover **security incidents**, such as **data breaches**.

**Importance of Access Logs**

* Access logs capture detailed information about each **user session**.
* They are critical in **investigating security events** and identifying suspicious activities like unauthorized access attempts or breaches.

**How Access Logs Work**

* **Session Tracking**:
  + A **session** starts when a user accesses a system, usually involving network requests and responses (e.g., when visiting a website).
  + Two key actions take place:
    1. **Session ID Creation**: A unique **token** that identifies the user and their device.
    2. **Session Cookies**: Tokens exchanged between the server and the user’s device to validate the session and manage its duration.

**Role of Session Cookies**

* **Session Cookies** ensure that sensitive data (e.g., passwords) is not transmitted repeatedly.
* They make web sessions more efficient by linking the user’s session with the correct data without exposing personal credentials.

**Risks Associated with Session Cookies**

* **Session Hijacking**: If an attacker steals a session cookie, they can **impersonate** the legitimate user and carry out malicious activities like stealing money or private data.
  + This is especially dangerous in cases where a **single sign-on (SSO)** credential is compromised, allowing access to multiple systems.

**Why Accounting is Important**

* **Monitoring session logs** helps detect unusual activities that might indicate **unauthorized access** or **stolen data**.
* **Accounting** provides valuable insights to keep systems secure by identifying potential threats early.

Would you like to know more about any specific aspect of accounting or how session hijacking is prevented?