Armaan Shamsaasef

Authentification, Authorization, and Accounting (AAA)

Notes: AAA - Authentication, Authorization, and Accounting (SY0-701 - 1.2)

Core Concept: AAA (Triple-A) is a security framework for controlling access to computer resources, enforcing policies, and auditing usage. It defines the process from user identification to tracking their actions.

The Three Components of AAA

1. Authentication

- Definition: The process of verifying the identity of a user or system.
- Key Question: "Who are you?" / "Are you who you say you are?"
- Process: The user provides their identity (e.g., a username) and then proves that identity with one or more credentials.
- Common Methods:
    - Something you know: Password, PIN, Passphrase.
    - Something you have: Smart card, Security key, Mobile device (for an app code).
    - Something you are: Biometrics (Fingerprint, Retinal scan, Facial recognition).
    - Using multiple methods is Multi-Factor Authentication (MFA).

---

2. Authorization

- Definition: The process of determining what permissions, rights, or level of access an authenticated user has.
- Key Question: "What are you allowed to do?"

- Process: After authentication, the system checks what resources, data, or actions the user is permitted to access.
- Common Implementations:
    - Permissions: Read, Write, Modify, Execute.
    - Role-Based Access Control (RBAC): Rights are assigned based on a user's role (e.g., Admin, User, Guest).
    - Location or Time-based rules: Restricting access to certain hours or from specific networks.

---

3. Accounting

- Definition: The process of tracking and logging user activities and resource access.
- Key Question: "What did you do?"
- Process: Recording user actions, logon times, data transferred, and commands executed. These logs are used for auditing and analysis.
- Primary Uses:
    - Auditing: For compliance with laws and regulations.
    - Forensics: To investigate security incidents.
    - Billing: For chargeback accounting (e.g., in cloud services).
    - Trend Analysis: Understanding usage patterns.

The AAA Process in Order

1. **Authentication**: A user provides a username and password. The system verifies their identity.
2. **Authorization**: The system checks and applies the user's permissions, allowing them to access only the files they are authorized for.
3. **Accounting**: The system logs the user's login time, the files they accessed, and their logout time.

Key Takeaway

The AAA framework creates a comprehensive access control model:

- **Authentication** verifies identity.
- **Authorization** defines the scope of access.
- **Accounting** tracks actions for accountability and security analysis.