Password

- **Identification**
  - Presentation of a user identity for the system
  - Typically by a username
- **Authentication**
  - Establishing confidence in the validity of a claimed identity
  - Typically using a password
  - Secret series of characters known only to owner
- **Design goals of passwords**
  - Simple enough for average users
  - Secure enough for most applications

Password Management

- **Definition:** A secret string used for user authentication
- **Password Types:** PIN (short, numeric) and Passphrase (longer, word-based)
- **Goals:** Ensure confidentiality, integrity, and availability of passwords
- **Main Threats:** Capturing, guessing, cracking, replacing, and using compromised passwords
- **Recommendations:** Use strong passwords, limit login attempts, manage password expiration carefully, educate users

Access Control Lists (ACLs)

- **Definition:** A list of permissions attached to system resources
- **Syntax:** Subject + Object + Allowed Operation
- **Common Uses:** File permissions, network firewall rules
- **Advantages:** Simple to implement, foundational for many controls
- **Limitations:** Poor scalability, difficult to manage with role changes
- There are **two types** of ACLs
  - **File ACLs:** manage user or group rights for files and executables.
  - **Network ACLs:** act as firewalls by determining which IP addresses or port numbers are allowed to access the network.

Role-Based Access Control (RBAC)

- **Separation of Duties (SoD):** RBAC supports SoD by ensuring no single role has excessive privileges
- **Role Hierarchy:** Roles can be structured in a hierarchy (e.g., Manager > Employee)
- **Dynamic Assignment:** Roles can be temporarily assigned based on context (e.g., project-based access)
- **Auditability:** Easier to audit because permissions are tied to roles, not individuals

Information Assurance and Security: Hardware and Software Controls

Firewalls

- **Definition:** Hardware/software that controls traffic between networks
- **Functions:** Restrict inbound/outbound traffic, block unauthorized access, protect internal networks
- **Types:** Packet filtering, deep packet inspection, perimeter firewalls, interior firewalls
- **Limitations:** Cannot protect against internal threats, encrypted traffic, or misconfiguration

Intrusion Detection/Prevention Systems (IDS/IPS)

- **IDS:** Monitors systems for malicious activity or policy violations (Network-based and Host-based)
- **IPS:** Attempts to block detected threats
- **Detection Methods:** Signature-based, anomaly-based, protocol state-based
- **Limitations:** False positives/false negatives, potential evasion by attackers

Intrusion Detection/Prevention Systems (IDS/IPS) (Cont'd)

- **Network-based IDS (NIDS):** Monitors network traffic for suspicious patterns.
- **Host-based IDS (HIDS):** Monitors activities on individual hosts (files, system calls, logs).
- **Detection Methods**
  - **Signature-based:** Detects known attacks using predefined patterns.
  - **Anomaly-based:** Detects abnormal behavior compared to normal activity.
  - **Protocol-state-based:** Detects misuse or deviations in protocol operations.

Patching Operating Systems and Applications

- **Patch:** Software update fixing security or functional issues
- **Patch Management:** Process of identifying, testing, deploying, and verifying patches
- **Challenges:** Testing conflicts, user non-compliance, diverse environments, resource overload
- **Best Practices:** Prioritize patches, stagger deployments, verify installation

End Point Protection

- **Definition:** Security implemented on end-user devices (desktops, laptops, mobiles)
- **Functions:** Anti-virus, anti-malware, intrusion detection, system update monitoring
- **Detection Mechanisms:** Signature-based and reputation-based scoring
- **Role:** Last line of defense, protects against internal threats and compromised devices
- **Example:** When an employee accidentally downloads malware, endpoint protection like CrowdStrike or Microsoft Defender blocks the threat before it can spread or encrypt files.