**Protection Models**

* These control **who can access what** in a system.
* **Main goal:** Manage permissions and prevent unauthorized access.
* **Types:**
  + **DAC (Discretionary Access Control):** Owner decides access.
  + **MAC (Mandatory Access Control):** System controls access based on data classification.
  + **RBAC (Role-Based Access Control):** Access depends on user's role (e.g., Admin, Guest).

**Bell-LaPadula Model (for Confidentiality)**

* Designed for **military use**.
* Rules:
  + **No Read Up**: Can’t read higher-level classified data.
  + **No Write Down**: Can’t write to lower-level data.
* Goal: Prevent data leakage.

**🧩 Biba Model (for Integrity)**

* Focuses on **data accuracy and trustworthiness**.
* Rules:
  + **No Read Down**: Can’t read less trustworthy data.
  + **No Write Up**: Can’t corrupt higher-level data.
* Goal: Protect data from unauthorized modification.

**🧩 Clark-Wilson Model**

* Focuses on **commercial systems** and **data integrity**.
* Uses well-formed transactions and separation of duties.
*  **nly TPs can modify CDIs**  
  → Users can’t directly change important data; they must use trusted functions.
*  **TPs are well-formed transactions**  
  → Each TP follows business rules and avoids errors.
*  **Separation of duties**  
  → One person can’t do everything.  
  Example: One user creates a transaction, another approves it.
*  **Audit trails are maintained**  
  → Every action is recorded so it can be reviewed later.

**What is a Digital Signature?**

* A **digital signature** is like an **electronic fingerprint**.
* It is used to **verify the identity** of the sender and **protect the data** from being changed.
* It ensures the **message or document** is **authentic and unaltered**.

**🔧 How Does a Digital Signature Work?**

1. **Sender creates a message** (e.g., a file or email).
2. A **hash value** (a fixed-size string) is generated from the message.
3. This hash is **encrypted using the sender’s private key** → This becomes the digital signature.
4. The message + digital signature are sent to the receiver.
5. The **receiver decrypts the signature using the sender’s public key** to get the original hash.
6. The receiver also hashes the message on their end.
7. If both hashes match, the message is **valid and untampered**.

**🔐 Important Concepts**

* **Private Key:** Used by sender to create the signature (kept secret).
* **Public Key:** Used by receiver to verify the signature (shared with all).
* **Hash Function:** Converts the message into a short, unique code.

**🎯 Main Goals of Digital Signatures**

1. **Authentication** – Confirms that the sender is genuine.
2. **Integrity** – Confirms that the data has not been changed.
3. **Non-repudiation** – The sender **cannot deny** sending the message.

Hashing is a process that **converts any data** (like a password, message, or file) into a **fixed-size code**, called a **hash value** or **hash code**.

**🎯 Purpose of Hashing:**

1. **Secure the data**
2. **Detect any changes** in the data
3. **Store passwords safely**

**🔑 What Does a Hash Function Do?**

* A hash function:
  + Takes input of **any size**
  + Converts it into a **small, fixed-size string**
* Each input gives a **unique hash value** (same input always gives the same output)

**🧠 Simple Example:**

If your password is: MyPassword123

* After hashing, it becomes something like:  
  ab43d8f7653a98f0c8b... (just an example)

When you log in:

* The system hashes your entered password
* Compares it to the stored hash
* If both match, you get access

**Host-based security issues** are security problems that occur on **individual computer systems** (hosts).  
When we talk about host-based security, we are referring to the security of **devices or computers** that are **directly connected to a network**.

**🎯 Examples of Host-Based Security Issues:**

1. **Malware (Malicious Software):**
   * **Viruses**, **Trojans**, **Worms**, **Ransomware**, and other **malicious software** can infect a system and corrupt or steal data.
   * These programs can **control the computer without permission**.
2. **Unauthorized Access:**
   * If a computer doesn't have **strong passwords** or **authentication mechanisms**, **unauthorized users** can easily access the system.
   * **Hacking** or **brute-force attacks** allow attackers to gain entry into the system.
3. **Lack of Antivirus or Outdated Software:**
   * If **antivirus software** is not installed or is outdated, the system is not protected from viruses and malware.
   * **Not regularly updating software** also makes the system vulnerable.
4. **Insecure Configuration:**
   * If the system’s settings are not **properly configured**, attackers can easily exploit the system.
   * Leaving **default settings** unchanged or leaving unnecessary services open makes the system **vulnerable**.
5. **Data Theft or Loss:**
   * If the system doesn’t have **proper encryption**, sensitive data can be stolen.
   * Without **backup systems**, if the system crashes, data loss can occur.

**⚠️ Solutions to Host-Based Security Issues:**

1. **Install Antivirus Software:**  
   Installing **antivirus software** protects the system from viruses and malware.
2. **Use Strong Passwords & Authentication:**  
   **Strong passwords** and **multi-factor authentication (MFA)** can prevent unauthorized access.
3. **Regular Software Updates:**  
   **Updating the operating system** and **software** regularly helps patch security vulnerabilities.
4. **Configure the System Properly:**  
   **Firewalls** and **security settings** should be properly configured to secure the system.
5. **Backup & Encryption:**  
   Encrypting data and taking **regular backups** protects data from theft or loss.

**📝 Summary Table:**

| **Security Issue** | **Explanation** | **Solution** |
| --- | --- | --- |
| Malware | Viruses, Trojans, etc. | Install antivirus software |
| Unauthorized Access | Hackers accessing the system | Use strong passwords and MFA |
| Outdated Software | Weak protection | Regularly update software |

Network base:

|  |  |  |
| --- | --- | --- |
| Man-in-the-Middle (MITM) | Attacker intercepts communication | Use encryption (SSL/TLS) |
| Denial of Service (DoS) | Attack causes system to crash | Use rate limiting and load balancing |
| Packet Sniffing | Attacker captures sensitive data | Use encrypted connections (VPN, HTTPS) |
| Network Intrusion | Unauthorized access to network | Use firewalls and IDS |
| Phishing/Social Engineering | Users tricked into revealing info | Conduct awareness training |
| Unpatched Vulnerabilities | Network devices or software not updated | Regularly update software and firmware |

**Summary Table of Classification Levels:**

| **Classification Level** | **Description** | **Example** |
| --- | --- | --- |
| Public (Unclassified) | No sensitive information, freely accessible | Public website info, marketing materials |
| Internal Use Only | For internal organization use, not meant for external sharing | Internal memos, employee handbook |
| Confidential | Sensitive data, access restricted | Employee personal info, financial reports |
| Restricted / Secret | Highly sensitive, controlled access | Business strategies, classified government data |
| Top Secret | Most sensitive data, severe consequences if exposed | National security documents, military plans |