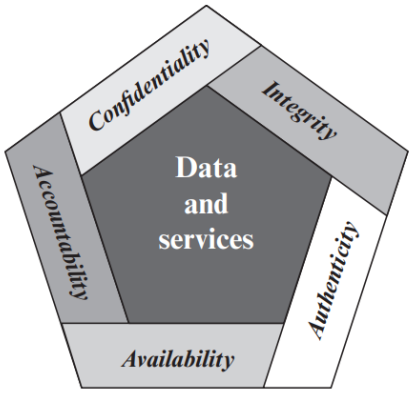
Arab Academy of Science, Technology and Maritime Transport
College Of Engineering & Technology
Course: Data Security
Course Code: ECE4304
Lecturer: Dr. Mahmoud Yehia

Basic concepts in Data Security

Data Security: The practice of protecting digital information from unauthorized access, corruption, or modification.



Confidentiality: It refers to our ability to protect our data from those who are not authorized to view it and accessible only to authorized individuals.

Threats to confidentiality:

- **Hackers:** Individuals who use technical skills to break into systems, exploit vulnerabilities, or steal data.
  - **Example:** A hacker uses a brute-force attack to guess a weak password and gain access to a system.
- **Masqueraders:** Individuals who pretend to be someone else (an authorized user) to gain access to systems or data.
  - **Example:** Receiving a fake email that looks like it's from your bank, asking for your password.
- **Unauthorized Users:** Individuals or entities who try to access systems, data, or resources without proper permission or authorization.
  - **Example:** A **student** tries to gain access to the **academic portal** as an **instructor** to change their grades.
- **Unprotected Downloads:** Downloading files or software from the internet without proper security measures, such as encryption, verification, or scanning for malware.
  - **Example:** Downloading a free game or software from an untrusted website without checking if it's safe.
- **Malware:** short for malicious software and is like any software, but intentionally designed to harm, exploit, or compromise systems, networks, or data.
  - **Example:** A fake game app that steals your contacts and messages. (**Trojans**)

Integrity: It refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner during storage or transmission.

- **Example:** Using hash functions to verify that a file has not been altered during transfer.

Availability: Ensuring that data and resources are accessible to authorized users when needed.

- **Example:** A company regularly backs up its customer database to an offsite server. If the primary server fails, the backup ensures the data is still accessible.

Threats to Availability:

- **Human Factors (Intentional):** Deliberate actions by individuals to disrupt systems, data, or resources, making them unavailable.

- **Example:** A hacker sends millions of fake requests to an online store, causing the website to crash so legitimate customers can't shop. (**Denial-of-Service (DoS) Attack**)

- **Human Factors (Unintentional):** Accidental actions by individuals that lead to systems, data, or resources becoming unavailable.

- **Example:** An employee accidentally spills coffee on a server, causing it to short-circuit and crash.

- **Non-Human Factors:** Events or issues not caused by humans that disrupt systems, data, or resources, making them unavailable.

- **Example:** A natural disaster like a flood or earthquake damages a data center, taking down multiple websites and services.

Authentication: The process of verifying the identity of a user, system, or device to ensure they are who they claim to be. Purpose is to prevent unauthorized access to system, data, or resources.

- **Example:** Logging into your email account with a username and password.

Common Authentication Techniques:

- **Password-Based Authentication:** Users provide a username and password to prove their identity.

- **Example:** Logging into your Facebook account with your email and password.

- **Two-Factor Authentication (2FA):** Requires two forms of verification which are **something you know** (password) and **something you have** (a code sent to your phone).

- **Example:** Logging into your bank account with a password and a one-time code sent to your phone.

- **Biometric Authentication:** Uses unique physical characteristics to verify identity, such as fingerprints, facial recognition, or voice patterns.

- **Example:** Unlocking your smartphone with your fingerprint or face.

- **Certificate-Based Authentication:** an encrypted piece of data which contains information about its owner, issuer of certificate, and some other data.

- **Example:** Logging into a secure government website using a digital certificate stored on your computer.

Authorization: Granting or denying access to specific resources based on a user's identity and permissions.

- **Example:** On the academic portal, only instructors have the credentials and permissions to delete, add, or update files like lectures and sheets, while students can only view and download them. This ensures proper access control and security.

Accountability: means making sure that people are responsible for their actions and can be identified if something goes wrong. It's about tracking who did what, so actions are traceable and answerable.

---

threat vs. Attack:

Threat: A threat is a potential danger that could exploit a vulnerability in a system. It's like someone thinking about breaking into your house but hasn't done it yet.

- **Example:** A hacker planning to steal data from a company's database is a threat.

Attack: An attack is the actual attempt to harm or exploit a system. It's when the threat is carried out.

- **Example:** The hacker actually breaking into the company's database and stealing data is an attack.

- Difference: A threat is the **possibility of harm**, while an attack is **the action of causing harm**.

Security Attacks:

Passive Attack: the attacker observes or monitors the system but does not alter or disrupt it. The goal is usually to gather information without being detected.

- **Examples:**
  - **Packet Sniffing:** A hacker captures data packets being sent over a network (like passwords or emails) but doesn't interfere with the communication.
  - **Traffic Analysis:** Traffic analysis involves studying the **patterns** of network traffic (e.g., who is communicating, when, how often, and how much data is being sent) without necessarily looking at the content of the packets.
- **Key Point:** Passive attacks are hard to detect because they don't change the system.

Active Attack: the attacker **interacts with or modifies** the system. The goal is to disrupt, alter, or damage the system or data.

- **Examples:**
  - **Denial of Service (DoS):** A hacker floods a website with traffic to crash it, making it unavailable to users.
  - **Man-in-the-Middle (MITM):** A hacker intercepts and alters communication between two parties without their knowledge.
- **Key Point:** Active attacks are easier to detect because they cause noticeable changes or disruptions.

Important terminologies:

- **Plaintext**: The original, readable message or data before it is encrypted.

- **Ciphertext:** The scrambled, unreadable version of the plaintext after encryption.

- **key:** A piece of information (like a code) used to encrypt or decrypt data.

- **Cipher:** A method or algorithm used to encrypt plaintext into ciphertext or decrypt ciphertext back into plaintext.

- **Encryption**: The process of converting plaintext into ciphertext to protect its confidentiality.

- **Decryption:** The process of converting ciphertext back into plaintext so it can be read.

- **Symmetric Encryption:** A type of encryption where the same key is used to encrypt and decrypt data.
  - **Example:** The AES (Advanced Encryption Standard) cipher
- **Asymmetric Encryption:** A type of encryption that uses two different keys: a public key to encrypt and a private key to decrypt.
  - **Example:** The RSA (Rivest-Shamir-Adleman) cipher

- **Public Key:** A key that is shared publicly and used to encrypt data.
  - **Example**: If Alice wants to send Bob a secure message, she uses Bob's public key to encrypt it.

- **Private Key:** A secret key that is kept private and used to decrypt
  - **Example**: Only Bob has his private key, which he uses to decrypt the message Alice sent him.