CIA Triad (Information Security Fundamentals)

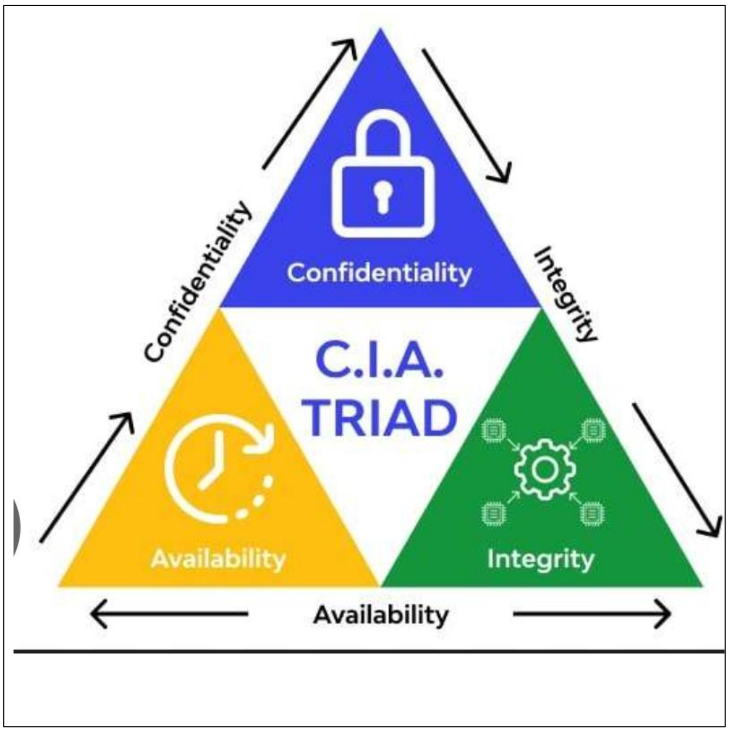

Figure 1: CIA Triad: Confidentiality, Integrity, and Availability

The **CIA Triad** is a core cybersecurity model that defines the three primary objectives of information security systems:

- Confidentiality
- Integrity
- Availability

Every security control, policy, and defense mechanism exists to protect one or more of these principles.

1. Confidentiality

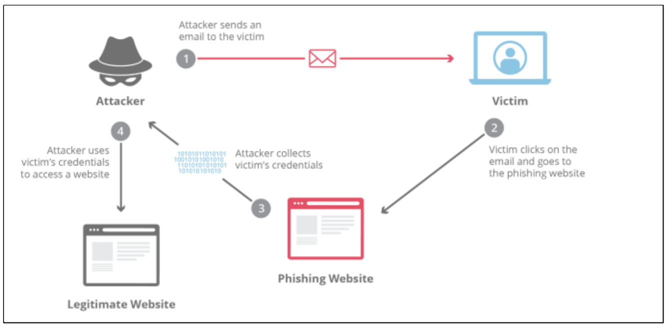
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

Figure 2: Confidentiality Example: Restricted access and encryption

Definition:
Confidentiality ensures that information is accessible only to authorized users, processes, or systems.

Best Example:
Only HR personnel can access employee salary data. Even if data is stolen, encryption ensures attackers cannot read it.

Attacks:
Phishing, credential theft, packet sniffing.

2. Integrity

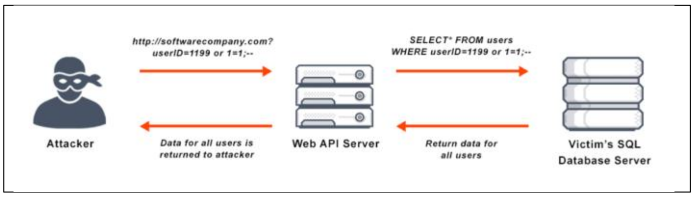

Figure 3: Integrity Example: Hash verification and tamper detection

Definition:
Integrity ensures that data remains accurate, complete, and unaltered.

Best Example:
Software downloads are verified using checksum hashes to ensure files were not modified.

Attacks:
SQL injection, malware modification, MITM attacks.

3. Availability

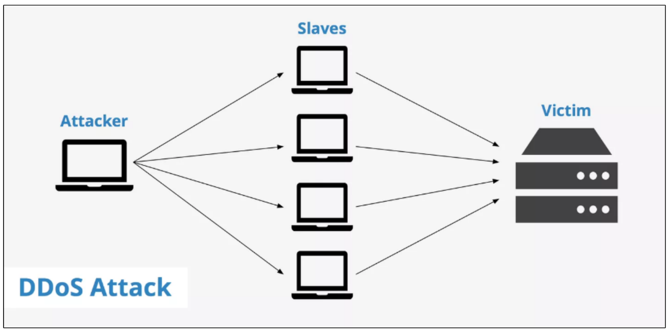

Figure 4: Availability Example: Redundancy and load balancing

Definition:
Availability ensures systems and data are accessible when needed.

Best Example:
A banking website remains online during peak traffic using backup servers and load balancers.

Attacks:
DDoS, ransomware, hardware failures.

Attack Mapping Summary

- Phishing → Confidentiality
- SQL Injection → Integrity
- DDoS → Availability

One-Line Memory Rule

- Confidentiality: Who can see the data?
- Integrity: Can the data be trusted?
- Availability: Can the data be accessed when needed?

Note: legitimate - means **authorized, valid, genuine, or allowed according to rules or policy**.
In cybersecurity, it refers to **normal, approved users or traffic**, not malicious activity.