Software Security Core Concepts

CONFIDENTIALITY

(MFA) Multi Factor Authentication

Confidentiality : Process

Customer Id ← Identification → Authentication → Authorization (MFA)

→ Accounting (logging)

For MFA → We should take one components from each section

- Something you have (eg: Number / email)
- Something you know (Pin / Pass)
- Something you are (eg: Biometric)

Something you have	Something you know	Something you are

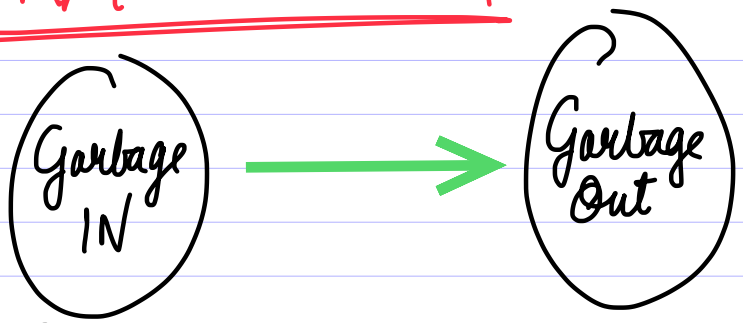
Authorization – Process of Providing Permission

How to Authorize ?

- Who has requested for access?
- Which is the object on which access is required?
- What level of access is required?

Accounting (logging) → So the user cannot deny that they have perform the activity

INTEGRITY



What is it ?

→ Data that software keeps/produce are valid and reliable

How to implement ?

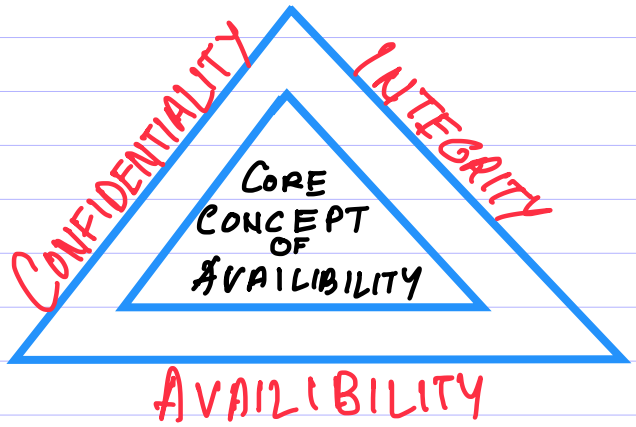
→ Allowing only authenticated user to write/insert valid data

- Hashing (MD5, SHA-256)
- Digital Signature
- Coding

AVALIBILITY

→ User should get services reasonibly fast

3 PILLARS OF SECURITY



Secure Software Design Principles

What is it?

- Key security best practices in all lifecycle of Software development
- Why?
  - → Give enough time and resource, and security can be breached
  - → 80:20 rule and **ROI**

Least Privilege

→ What is it?

Giving the least amount of rights to a human user or application for perform any task

→ Process

No Privilege → Establish need to know → Permission granted with timebound.

Seperation Of Duties

- Any critical tasks can not be completed without involving multiple parties.

Defense in Depth

→ Attackers need to get through multiple

layers of security (based on criticality, no of layers will be increased)

→ Make sure single breach doesn't create complete failure

FAIL SAFE

When software faces exceptions and errors, it should fail in safe state where security can't be compromised

ECONOMY OF MECHANISM

Keep the design of software as simple as possible. Simple systems are easier to defend troubleshoot and administer

→ Using existing trusted components
→ Using only essential services & protocols

OPEN DESIGN

What is it ?

→ Security of system is independent of desig

Psychological Acceptability

What is it?

→ User is key element of security
→ Mistake from a single user makes whole system vulnerable

How to implement?

→ User should not find huge operational headache

→ User made aware of circumventing security.

Element Single Point of Failure