~~Chapter~~

# Software Security

↳ Softwoare security is simply a collection of ~~methods~~ used to protect computer programs and the sensitive information handled by them against malicious attacks. It covers a wide range of functions to safeguard softwoare and its correlated data privacy, accuracy and accessibility respectively.

↳ [Reln betn Security & Dependability ]

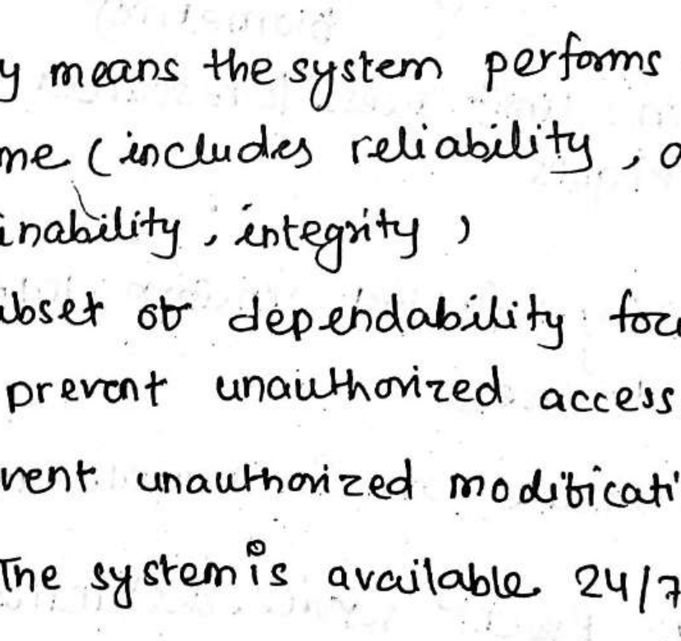
Relationship betn security and ~~availability~~ Dependability

→ Dependability means the system performs correctly and reliably overtime (includes reliability, availability, safety, maintainability, integrity )

Security is a subset of dependability focusing on confidentiality : prevent unauthorized access.

Integrity : prevent unauthorized modification.

Availability: The system is available 24/7 for intended users.



A system can not be full dependable without Security

Example: If a banking system is reliable but not secure (hackers can steal money, it can't be considered reliable.

Security Requirements for Dependable Systems

Security Requirement ensures that dependable systems stay functional under attack. The security requirement for dependable systems are:

i) Authentication: Verify users identity (e.g. password, biometrics)

ii) Authorization: Limit access to resources based on users rights

iii) confediantility: Protect sensitive data From unauthorized access.

iv) Integrity: Ensure data is accurate and unaltered.

v) ~~A~~Availability: Prevent service desbuction (e.g. DDOS Attack)

vi) Non repudiation: Ensures action can't be denied, Later (e.g. digital signature)

## Secure systems Design Principles

Design principle help build secure systems from the start.

| Principle | Description |
|---|---|
| least of privilige | Give minimum access necessary |
| fail state Defaults | Default should be deny access unless explicitly allowed |
| Economy of mechanism | keep design of simple ~~tiict~~ to avoid hidden flaws |
| complete mediatiation | check every acess request |
| Open design | Security should rely on secrecy of design. |
| seperation of Duties | Divide critical tasks among different peoples or components |
| Defence in Depth | multiple layers of security control |
| Psychological Acceptability | Security measure should not hinder usability. |

Security Testing and Accurance Techniques

↳ Testing and accurance ensures that system is actually secure:

- Penetration Testing Ethical Hacking
  → simulated attack to find vulnerabities.

- Static Analysis
  → Analyze the source code for ~~to~~ vulnerabities (without running the program)

- Dynamic Analysis
  → Analyze the program while it's running to find the issues

- formal verification
  → Use mathematical methods to prove correctness and Security.

- Security Audit
  ↳ Manual revielos of security policies, system design and implementation.

- Fuzzy Testing
  ↳ ~~fe~~ Input random data to depect crashes or unexpected behavior.

## Common Vulnerabities ~~and attack vectors~~

i) Buffer ~~overflow~~ overflow

→ writing more data ~~Dh~~ then a buffer can ~~o~~ hold

ii) SQL injection

→ Inserting ~~sql~~ malicious SQL queries

iii) Cross - site ~~expecting~~ Scripting (XSS)

→ Injecting malicious scripts into the web pages.

iv) Cross- site request Forgery (CSRF)

→ Forcing user to execute unwanted actions

v) Insecure Authentication

→ ~~use p~~ ~~with~~ weak password policies or login mechanism

vi) ~~mix con~~ mis configuration

→ pure security settings(e.g. default password)

## common attacks

i) ~~Phising~~ Phishing

→ Trick users to give credentials

ii) Malware

→ Software that damages or steals data

iii) Social Engineering

→ manipulating people to gain access.

Intersecting Communication

iv) Denial of Service (DOS)

→ overloading system to make service unavailable.