Date _____ Day _____

CHAPTER # 01

- **Computer Security:** Measures and controls that ensure confidentiality, integrity and availability of information system assets including hardware, software, firmware and information being processed, stored and communicated.
  - ↳ Confidentiality
    - ↳ Data Confidentiality: Assures that private or confidential info is not made available or disclosed to unauthorized individuals
    - ↳ Privacy: Assures that individual control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
  - ↳ Integrity
    - ↳ Data Integrity: Assures that information and programs are changed only in a specified and authorized manner
    - ↳ System Integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Date _____ Day _____

- These three concepts forms CIA Triad
  - Confidentiality – Loss of confidentiality is the unauthorized disclosure of information
  - Integrity – Loss of integrity is unauthorized modification or destruction of info.
  - Availability – A Loss of availability is the desruption of access to or of info or an information system

- Authenticity — The property of being genuine and being able to be verified and trusted
  ↳ This means verifying that users are who they say that they are and that each input arriving at the system came from a trusted source.

- Accountability — The security goal that generates the requirements for actions of an entity to be traced uniquly to that entity.
  ↳ We must be able to trace a security breach to a responsible party.
  ↳ System must keep records of their activities to permit later forensic analysis to trace security breaches.

Date _____ Day _____

- Three levels of impact on organization
  ① Low ② Moderate ③ High

Real World Examples :

① Confidentiality
- High — Student's grade info
- Moderate — Student's enrollement info
- Low — List of teachers

② Integrity
- High — Not one should be able to update a patients info
- Moderate — Fake reviews can mislead customers
- Low — Anonymous online Poll.

③ Availability —
- High — Authentication server down
- Moderate — A public web for a university that provide info of students
- Low — An online telephone directory

- Non repudiation : It is the assurance that someone cannot deny (repudiate) the validity of their actions in a communication or a transaction.
  "Non denial possible "

Date _____ Day _____

- System resources or Asset
  - ↳ Hardware - Data processing, Data storage and Data communications device
  - ↳ Software - OS, system utilities & apps
  - ↳ Data - Files, Databases
  - ↳ Communication facilities & Networks - LAN, WAN, Routers

- In the context of security, our concern is with the vulnerabilities of system resources
  - ↳ the system can be corrupted
    - ↳ Stored date may differ than what it actualy should be
  - ↳ the system can become leaky
    - ↳ someone who should not have the acess of some info, has that access
  - ↳ They system can become unavailable or slow
    - ↳ using the system bcm impossible, like our very own FLEX

Date _____ Day _____

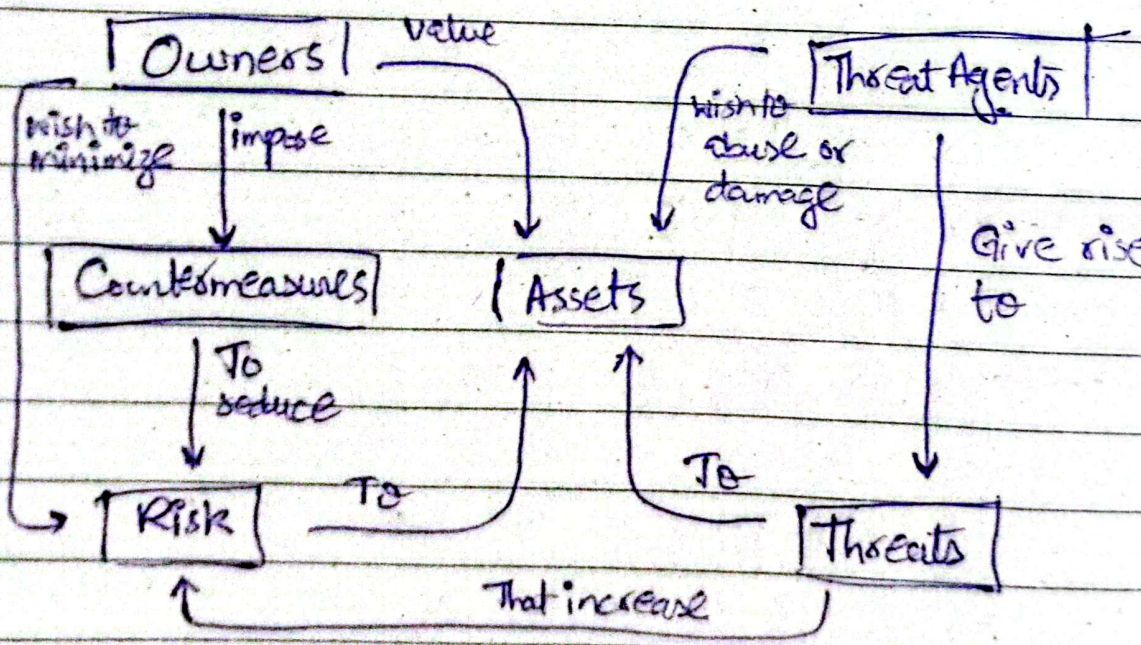
• Computer Security Terminologies

- **Adversary (threat agent)**
  Individual, group, organization or gov that conducts or has the intent to conduct detrimental activities
- **Attack**
  Any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself. (A threat that is carried out)
- **Countermeasure**
  Any thing use to protect against threats or attack
  ↳ Antivirus Software, Firewall, Encryption, CCTV camera
- **Risk**
  A measure of the extent to which an entity is threatened by a potential circumstance or event
- **Security Policy**
  A set of criteria for the provision of security services
- **Threat**
  Any event with potential to adversely impact organizational operations. (A potential security harm to asset)
- **Vulnerability**
  Weakness in an information system that could be exploited or triggered by a threat source.

Date _____ Day _____

- There are two types of attacks → DDOS
  ① Active Attacks - An attempt to alter system resource or affect their operation
  ② Passive Attack - An attempt to learn or make use of info from the system that doesnot affect system resources. (Sniffing)

- Classifying attack based on origin
  ① Inside Attack - Initiated by an entity inside the security perimeter. (Attack by authorized person)
  ② Outside Attack - An attack by unauthorized or illegitimate user.



Date _____ Day _____

→ Following are some threat consequences and the attacks which lead them.

threat to
(1) Unauthorized Disclosure [Confidentiality]
When sensitive info is exposed to peoples who should not see it.

↳ Exposure – info leaked intentionally or by accident.
- A university accidentally posts student's personal data

↳ Interception – Hacker / Listner captures data in transit
- Sniffing emails or messages over WiFi

↳ Inference – Attacker guesses sensitive info from patterns
- Traffic anlysis shows which PC's are communicating a lot.

↳ Intrusion – Attacker breakes access control to read secret data
- Attacker bypass login to read hospital records.

threat to
(2) Deception [Integrity][System & Data Integrity]
When false info or ~~user~~ identity tricks person or user

Date _____ Day _____

↳ Masquerade – Pretending to be someone else
- Hacker logs in with stolen credentials

↳ Falsification – Altering or creating fake data
- Student changing grades

↳ Repudiation – Denying an action that actually happened
- A user denies that they sent an email

(3) Disruption (threat to) [Availability] [System Integrity]
When system stop working properly.

↳ Incapacitation – Disabling a sys completely
- Virus crashes in a server.

↳ Corruption – Making system behave correctly

↳ Obstruction – Blocking / Slowing down operations.
- DDOS attack

(4) Usurpation (threat to) [Integrity] [System Integrity]
When attacker takes resource control

↳ Misappropriation – Unauth. use of resource
- Botnet using your PC for DDOS

↳ Misuse – Hacker / malicious software disables security func
- Trojan disable antivirus to hide itself

Date _____ Day _____

Communication Lines & Networks

↳ Network security attacks can be classified as passive & active attacks

↳ **Passive Attack** — The goal of attacker is to obtain information that is being transmitted. It doesn affect system resources

↳ **Active Attack** — Attacker attempts to alter the system resource. [Modification of data stream or the creation of false stream]

Two types of passive attacks

↳ Release of Message contents

↳ Preventing opponents from reading email, files & any other sensitive info.

↳ Traffic analysis

↳ Guessing the message by analyzing the encryption patterns.

- Passive attacks are difficult to detect bcz they donot involve any alteration of data

Four categories of Active attacks

↳ Replay

↳ Involves passive capture of data unit and its subsequent retransmission to produce an unauthorized effect

Date _____ Day _____

↳ Masquerade
  ↳ When one entity pretends to be a different entity.
↳ Modification of Messages
  ↳ Some portion of legitimate message is altered, delayed or reordered.
↳ Denial of Service
  ↳ Prevents the normal use of communication facility.
  ↳ Another form of service denial is the disruption of an entire network by disabling or overloading it with messages to degrade performance.

▶ FUDAMENTAL SECURITY DESIGN PRINCIPLES

① Economy of Mechanism
↳ Keep security mechanism as simple and straightforward as possible. More complex the system, the more it is exploitable.
Example: A firewall with only necessary rules, not hundreds of unused ones

② Fail-safe Default
↳ By default no one should have access, only those that have permission should have access.

Date _____ Day _____

Example: If login fails, deny acess until credentials are verified

③ Complete Mediation

↳ Ensure that every access to a resource is checked for authorization. Every time user reads a file system must excebise access control

Example: Each time file is open check user's permission

④ Open design

↳ Design of the security mechanism should be open rather than secret.

Example: AES encryption algo is public, only the key is secret

⑤ Seperation of Privilidges

↳ Multiple privilidge attributes are req to achieve access to a restricted resource

Example: Multifactor Authentication

⑥ Least Privilege

↳ Grant users and processes only the minimum permissions necessary to perform their tasks

Example; RBAC - A cashier in bank system can view transaction but not approve loans

Date _____ Day _____

⑦ Least Common Mechanism

↳ Sharing of resources among diff users or processes should be minimum possible

Example :

⑧ Psychological Acceptability

↳ Security measures should be designed in a way that it introduces a min hurdles to the use of the system

Example :

⑨ Isolation

↳ The system that has critical data, process or resources must be isolated such that it restrict public access.

Example : Virtual Machine

⑩ Encapsulation

↳ Specific form of isolation based on OOP.

Example :

⑪ Modularity

This refers to the development of security functions as separate, protected modules and the use of modular architecture for mechanism design and implementation

Date Day

(12) Layering
↳ Refers to use of multiple, overlapping protection layers
Example : Multiple bassier for the attacker

(13) Least Astonishment
↳ The UI of system must not amaze the user while accessing the secure system.

▶ COMPUTER SECURITY STRATEGY

- Security Policy
↳ Formal Statement of rules and practices that specify or regulate how a system or org. provides security services to protect sensitive and critical sys resources
↳ In developing security policy, following needs to be considered
i - The value of the assets being protected
ii - The vulnerabilities of the system
iii - Potential threats and the likelihood of attacks
↳ Trade offs to be considered
(1) Ease of use vs security
(2) Cost of security Vs cost of failure & recovery

Date _____ Day _____

- Security Implementation
  1. Prevention – Like using a secure encryption algo to preven unauth access
  2. Detetion – Detection of DDOS attack
  3. Response – They system must be able to respond to halt the attack to prevent further damage
  4. Recovery – Use of backup system, so that uncorrupted state of system can be reloaded.

- Assurance

  It is an attribute of an info syst that provides grounds for having confidence that system operates such that system's security policy is enforced

- Evaluation

  Process of examining a computer system with respect to certain criteria. Involves testing and formal analytic or mathematical techniques

▶ STANDARDS

1. NIST – National Institute of Standards & Technolo
2. ISOC – Internet Society
3. ITU-T – The integrati... Telecomunication Union
4. ISO – The International Org. for Standardiza...