Introduction to CS

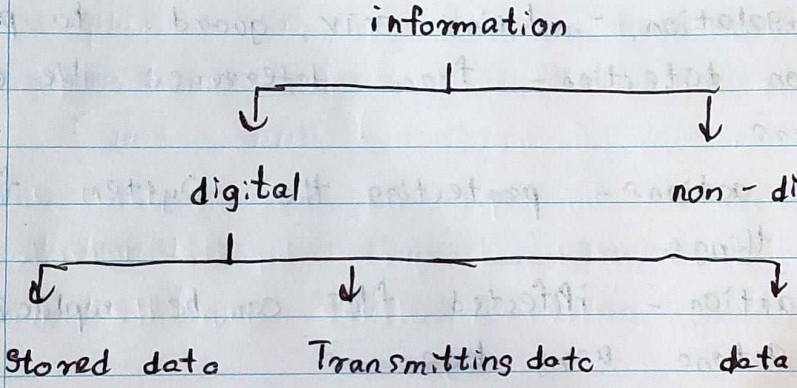
lec 1

- Computer Security.

protecting a information System with availability intergrity and confidentiality including hardwares, Softwares informations, network etc.

- Information Security.

protecting information & Systems from unauthorized access, use and modification with C, I, A.



CIA Triade

- Confidentiality - only authorized users should access the data,,
- Intregity - only authorized people should change The data.
- availability - Whe authorized user need a data it should be available to him/her at any time.

also called as Computer Security objectives.

NO.

Date:

Authenticity (Authentication - (Verifying the user by password, face unlock, biometrics)

Data origin authentication - Verifying that user A got the some massage that sent by b.

Accountability - able of trace back the action that took by users. it supports

- non repudiation - Sender cant say that he didn't send that massage.
- deterrence - Preventing unauthorized users not to harm the system.
- fault isolation, - having CCTV, guard to prevent.
- intrusion detection - from deterrence we can identify the intruders.
- prevent actions - protecting the system from happening these things.
- legal action - infected files can be replaced. or taking legal actions using logs.

key terms need to know in cs.

- System resource - assets that need to protect (Hardware, Software, Data, network)
- Vulnerabilities - Weakness of System that accured due to bad implimentation, operational or managment. (bugs, weakness).

Threat - a possibleties of something can happen. (harm)

Attack - a threat that carried out
- Passive attake - Just read the informations in system
- Active attake - Changing the informations in system.

Adversay / Attaker / intruder - entity that operate the attack.

Countermeasure - safety mesures that took to provide security.

Risk - expected loss due to an attack.

exploits - is an software that contain Commands to take advantage of a bug or Vulnerability to gain access to system (DOS, DDOS).

Vulnerability asresment - process of defining, identifying classifying and prioritizing Vulnerabilities - outcome report.

Penetration testing / pen testing / ethical hacking
= Way of finding Vulnerabilities that an attacker could exploid in a Information System, network or Web application.

- goals of penataration testing.
  - identify Weak spots.
  - Mesure Security policy.
  - Test the Staff.

Threats and Attacks.

4 - types

(01) Unauthorized disclosure.
(02) Deception.
(03) Disruption.
(04) Usurpation.

(01) Unauthorized disclosure

- allowing unauthorized people to access data.

- attake types :
  - exposure - Intruder takes all sensitive data such as credit card numbers etc.
  - Interception - Intruder gain access to transmitting data (take a copy of message)
  - Inference - by guessing size of data and pattern of network do a intelligent guess by the intruder.
  - Intrusion - after a attake gain the access to data.

(02) Deception

- receiving false data from unauthorized users and beliving it to be true (theat)

- Attak types :
  - Masquerade - unauthorized user gain access to system and act like authorized user.
  - falsification - Intruder modifies or replace or creat data.
  - Repudiation - Intruder blocks sending, receiving and processing of data.

(03) Disruption.

- An event that interrupts the operation of the System services and functions.

- Attack types.
  - Incapacitation - Intruder trying to make System unavailable by damaging System and hardware.
  - Corruption - Modifing the System services and functions or data.
  - Obstruction - Intruder tryis to overload interfering the System (Dos, DDos)

(04) Usurpation -

gaining the control of the System by intruder.

- Attack types.
  - Misappropriation - Unauthorized program over the hardware and System.
  - Misuse - Disabling Security functions.

Threats and ~~attacks~~. Assets

4 - types

(01) Threats on hardware
(02) Threats on Software
(03) Threats on data
(04) Threats on network and Communication.

NO. Date:

(01) Threats on hardware.

- damaging or stealing hardware (effect availability)

(02) Threats on Software.

- Deleting and damaging (availability) and modifying (Intergrity / Authenticity).

(03) Threats on data.

destroying, accessing and modifying data may effect availability, Confidentiality and integrity.

(04) Threats on network and communication.

messages are being deleted or leaked or modified over the network. Can be passive and active

active attack types.

- Replay - Catch the data and retransmit it.
- Masquerade - one entity pretending to be another entity. (Replay).
- Data modification - data recorded or modified by intruder
- Denial of Service - preventing from accessing services.

Categories of Security Services
6 - types

(01) Authentication. - make sure Communication is authentic
(02) Access control - limit and control access to users
(03) Data Confidentiality - protect data
(04) Data integrity - Confirm data send by authorized user
(05) Non repudiation - prevent from denying data.
(06) Availability. - data should be available.

Computer Security Strategy aspects
(03)

(01) Specification / policy - What to do
(02) Implementation - How to do
(03) Correctness - Does it work.

(01) factors of Security policy.
- The value of assets
- System's Vulnerabilities
- Threats and attacks
- Cost for security failures and recovery

(02) Security implementation. (04)

- Prevention -
- Detection
- Response
- Recovery

NO. Date: / /

(03) Correctness

- testing and analyzing system meet the all policies and specifications