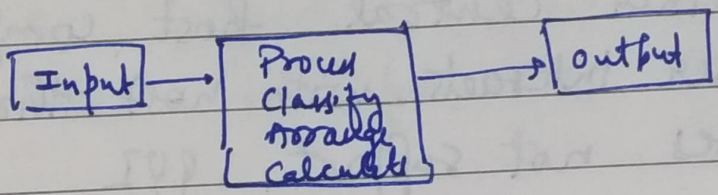
Unit-1

Page No.
Date

Information Systems

- It is a set of interrelated components that collects, process, store or distributes information, to support decision making & control in an organisation.

- It consists of data, hardware, software, procedures and people.



Applications

(1) Multimedia Applications : includes the combination of text, audio, video, graphics & animation.

(2) Office Applications : Ex MS word, Excel, etc.

(3) Education & Research : With WWW / Internet we can easily find any desired information

(4) Banking & financial Institution
- automate their business process &
- minimize transactional delays, handling ~~accounts~~ bills

Page No.
Date

Changing Nature of Information System

- Information system has undergone a dramatic change from
  ① mainframe based information system to
  ② client/Server Computing to
  web based information System (Internet)

- In mainframe, all information is within central host computer.
  User interacts with host through terminal.
  Does not support GUI.

- In Client-Server, improves usability, flexibility & scalability. GUI.

Need of Distributed information

- to serve the needs of networked enterprise.
- no single point failure

Page No.
Date

Role of Internet & Web Services

① revolutionised comm. & information sharing. anyone can interact with anyone
② inc productivity, flexibility, low cost.

Information System Threats & Attacks

A Threat is possible event that can harm an information system.

Four (4) principle sources :-

① Human Error
② Computer Abuse or crime / hacking
③ Natural / Political Disaster
④ Failure of hardware / software

Page No.
Date

Security Threats related to hacking

1. Impersonization
2. Trojan horse
3. Logic Bomb - Unauthorized instruction that stays dormant until a specific event occ
4. Viruses - malicious act, replication, affect health progra
5. worms - independent programs that make & transmit
6. DOS
7. Dial Diddling - changing data before or during input to change contents of database.
8. Salami Technique - diverting small amount of money from large no. of account. → not noticed
9. Spoofing - make a system masquerade as another system to get unauthorized access.
10. Super-Zapping - program than can bypass regular system controls
11. Scavenging
12. Data leakage
13. Theft of Mobile Device
14. Wire Tapping - Tapping Computer lines to get information

Page No
Date

Classification of Threats

1. Asset
2. Actor - who violates security requirement. CIA (confidientiality, integrity, availability) of asset, can be from outside or inside of org.
3. Motive - deliberate / ~~intentional~~ accidental
4. Outcome - steal/ damage

Categories of damage Outcomes

1. Destruction of information & other resources
2. Corruption / Modification of information
3. Theft of information.
4. Disclosure of confidential data.
5. Interruption of access to info information/ services

Categories of assets < Physical / logical

1. Data
2. Software
3. Hardware
4. People
5. Systems.

Page No.
Date

Security Challenges faced by Mobile

1. Managing registry settings & configuration
2. Authentication service Security
3. Cryptography Security
4. LDAP Security (light weight directory Access Protocol)
5. RAS Security (Remote Access Server)
6. Media player Control Security
7. Networking API security

There are 2 components of security in mobile computing -

- Security of device
- Security of network

Page No.
Date

① Cryptographic Security

- The CGA (cryptographic generated address) can be used to protect IP layer signaling protocol including neighbour discovery & motility protocols.

- These are deployed on palms, common device used in mobile computing.

② LDAP - is a software protocol enabling anyone to locate org., individuals and other resources such as files & devices in network.

③ RAS - for protecting business sensitive data that may reside on employees mobile device. A personal firewall is used to protect data for user connecting through direct internet or RAS connection.

④ Media Player Control Security
- corrupt files posing as normal music / video file would allow attacker to gain access of user's device.

⑤ Network API Security - online payments, web services

Page No.
Date

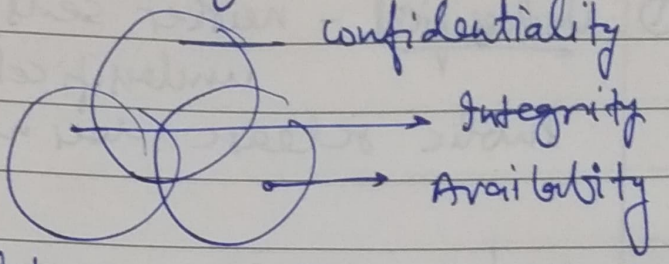
Security of Laptops - Measures

Physical security

1. Cables and hardwired locks
2. Laptop Safes - made of poly-carbonate
3. Motion Sensor & Alarm
4. Warning labels & stamps - contains tracking info., to deter theives
5. Other
   - ↳ firewall
   - ↳ encryption software
   - ↳ updating antivirus regularly
   - ↳ Disabling IR & wireless chord when not in use
   - ↳ Password protection
   - ↳ Backing up data regularly

Principle of Information Security / (CIA)

- following 3 are considered to be pillars of Information Security



Confidentiality - attempt to prevent intentional or unintentional disclosure of unauthorized access

Integrity : It ensures that -
1) modification of data is not done by unauthorized personnel
2) data is consistent.

Availability - Ensures reliable & timely access to data by appropriate personnel

Imp Terms:

① Privacy : level of confidentiality
② Authorization : rights & permission granted to an individual.
③ Authentication : It establish user ID and ensures user is who they are.
④ Accountability : Audit trails & logs. account actions of users.

How Information is classified

→ On the basis of level of sensitivity of information

① Unclassified - neither sensitive nor unclassified.
Public release does not violate confidentiality

② SBU (Sensitive But Unclassified)
③ Confidential
④ Secret
⑤ Top Secret - national security

→ classification on a 'need to know' basics in a company
① Private ② Public ③ Sensitive

Roles	Responsibilities
① Owner	delegate responsibilities & authorization levels
② Custodian	routine backups, testing, administration, data restoration
③ User	