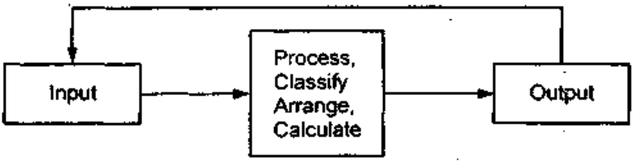
UNIT
1

History of Information Systems

Q. 1. What is an Information system? Explain the importance and basics of information systems.

Ans. An Information system is a set of interrelated components that collect, process, store or distribute information to support decision-making and control in an organization. Information system consists of data, hardware, software, procedures and people. The major functions are: input, storage, processing, control and output. Therefore, an Information system is a system, whether automated or normal, that comprises people, machines and/or methods organized to collect, process, transmit and disseminate data that represent user information.

Today, we live in 'Information Age' mainly because of advances in computer and communications technology. Most of the workforce today has jobs that are Information-intensive. Added to this is the dimension of the newly emerging 'mobile workers' who work away from their offices. So, Information systems now have become an inseparable part of business organization.



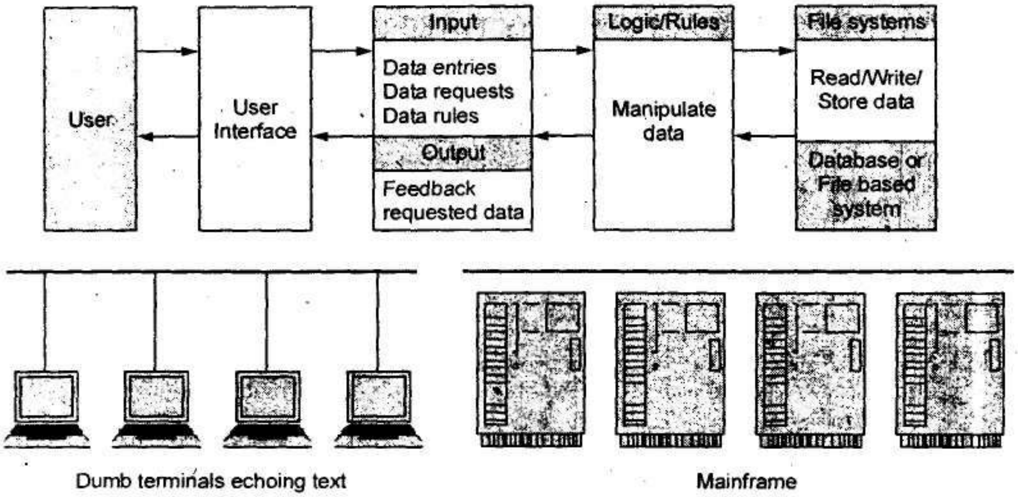
Some application of information technologies are:

1. **Multimedia Applications:** Multimedia is the term used to denote the combination of multiple mediums. Multimedia includes the combination of text, audio, video, graphics and animation. We define a multimedia system as a computer controlled environment which is used to process individual image, sound and text.
2. **Office Application and Desktop publishing:** Computers are also finding applications in day to day office problems. An electronic office uses computers for procurements of files, office communication, assisting in decision making and administrative work. There are word processing tools like MS Word, Word star, Spread sheet, Excel etc.
3. **Education and Research:** Information technology has proved to be extremely useful for education and research. A lot of time of wasted in finding the relevant information source. With the popularity of the World Wide Web and easy accessibility to the internet, it now takes few seconds to find any desired information.
4. **Banking and Financial Institutions:** Information technology has helped the banking and financial institutions to automate their business process and minimize the transactional delays with the application of computers, it has become possible to clear the recurring dues like payment for electricity, telephone bill, shopping bill etc.

Q. 2. Explain the changing nature of Information Systems.

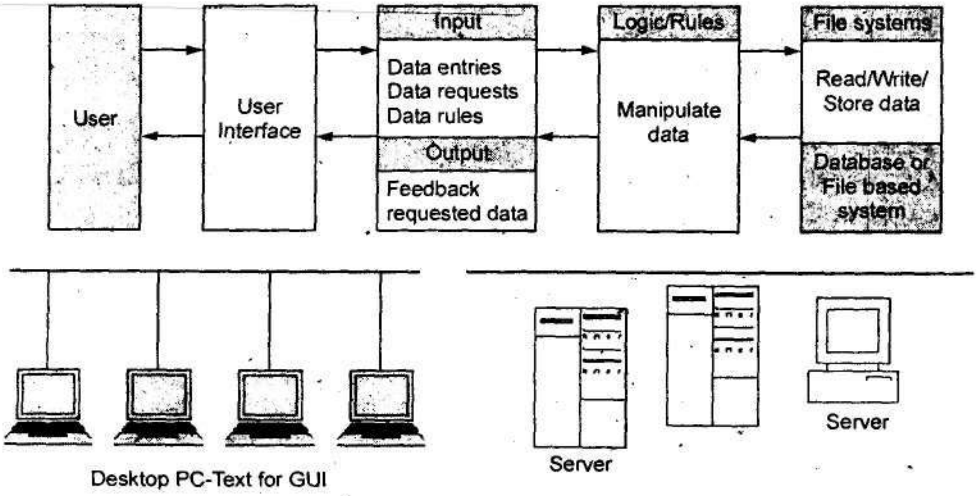
Ans. In the past decade, the nature of Information system has undergone a dramatic change, from mainframe based information system to client/server computing to today's web based information system, with the internet having made the revolution.

In mainframe based information system, all intelligence is within the central host computer. Users interact with the host through a terminal that captures keystrokes and sends that information to the host . However, it does not support graphical user interface (GUI).



Mainframe-based Information systems

The client-server software architecture is a versatile, message based and modular infrastructure that is intended to improve usability, flexibility, interoperability and scalability as compared to centralized, mainframe, time sharing computing



Slient/Server based Information system

Q. 3. What is the need of distributed information systems in the globalization of businesses?

Ans. Businesses today have no geographical boundaries as globalization has become the mantra of success in the digital economy led by the rise of e-business.

- We are in the realm of not only terabytes of data but also multimedia, multi-geo order of information system.
- Today's firms are characterized by electronic commerce to operate in the "digital markets" where an Information system links buyers and sellers to exchange information, products, services and payments.
- Thus, today, the era is of the "extended enterprise" and to serve the needs of such networked enterprises; the Information system, too, are no more confined to a single location, single computer. So, there is great need of Distributed information systems.

Q. 4. What is the role of Internet and Web services?

Ans. The internet has revolutionized communication and thereby its contribution to information sharing. With access to a computer and an appropriate connection, anyone can interact with others worldwide. Web services play a complementary and dominant role in building global information system for today's dynamic business world.

"Web services are self-contained modular, applications that can be described, published, located and invoked over a network, generally the World Wide Web (WWW)."

Web services have been proven to give a strong return on investment (ROI) and make computer based information system more adaptable. They also bring productivity, flexibility and low maintenance cost in the development of information system by integrating components from various third-party vendors.

Q. 5. What are Information system threats and attacks?

Ans. A threat is a possible event that can harm an information system.

Security threats have four principal sources:-

1. **Human error:** for example, inadvertent disclosure of confidential information.
2. **Computer abuse or crime:** A generic example is when a person intends to be malicious and starts to steal information from sites, or cause damage to, a computer or a computer network.
3. **Natural and political disasters:** This can happen in the form of natural calamities and wars, riots etc.
4. **Failure of hardware or software:** for example, server malfunctioning, software errors etc.

Security threats related to computer crime or abuse include:

1. Impersonation
2. Trojan horse method
3. Logic bomb
4. Computer viruses
5. DoS
6. Dial diddling
7. Salami technique

8. Spoofing
9. Super-Zapping
10. Scavenging
11. Data leakage
12. Wire tapping
13. Theft of mobile devices.

1. **Impersonation:** the impersonation enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.
2. **Trojan horse method:** Concealing within an authorized program as a set of instructions that will cause unauthorized act.
3. **Logic bomb:** Unauthorized instructions which stay dormant until a specific event occurs, at which they bring into effect unauthorized act.
4. **Computer Viruses:** Segments of code that are able to perform malicious acts and insert copies of themselves into other programs in the system. Cause of this replication, a virus will progressively infect healthy program and systems.
5. **Worms:** independent programs that make and transmit. Copies of themselves through telecommunication (TC) networks.
6. **DoS:** Rendering the system unusable by legitimate users.
7. **Dial Diddling:** Changing data before or during input, often to change the contents of a database.
8. **Salami technique:** Diverting small amount of money from large no. of accounts maintained by the system. This small amount will not be noticed.
9. **Spoofing:** Configuring s computer system to masquerade as another system over the network in order to get unauthorized access to the resources of the system being mimicked is entitled to.
10. **Super-Zapping:** Using a system's program that can bypass regular system controls to perform unauthorized acts.
11. **Scavenging:** Unauthorized access to information by searching through the residue after a job has been run on a computer. Technique range from searching waste baskets or dumpsters for print-outs to scanning the contents of a computer's memory.
12. **Data leakage:** There are a variety of methods for obtaining the data stored in a system. The data may be encoded into an innocuous report in sophisticated ways, for example, as the number of characters per line.
13. **Wire tapping:** Tapping computer lines to obtain information.
14. **Theft of mobile devices:** this is a new dimension that is coming up given the increase in mobile work force.

Q. 6. Give the classification of threats and assessing damages.

or

How will you classify threats and assessing damages?

Ans. Threats consist of the following properties:

1. **Asset:** Asset is something of value to the organization (information in electronic or physical form, Information system, a group of people with unique expertise, etc.)
2. **Actor:** Who or what may violate the security requirements- Confidentiality, integrity and availability (CIA) – of an asset. Actors can be from inside or outside the organization.
3. **Motive:** indication of whether the actor's intentions are deliberate or accidental.
4. **Access:** how the asset will be accessed by the actor (network access or physical access.)
5. **Outcome:** The immediate result of violating the security requirements of an asset (disclosure, modification, destruction, loss, interruption, etc.)

The major categories of damages resulting from threats to the information system are:

(a) Destruction of information and/or other resources.

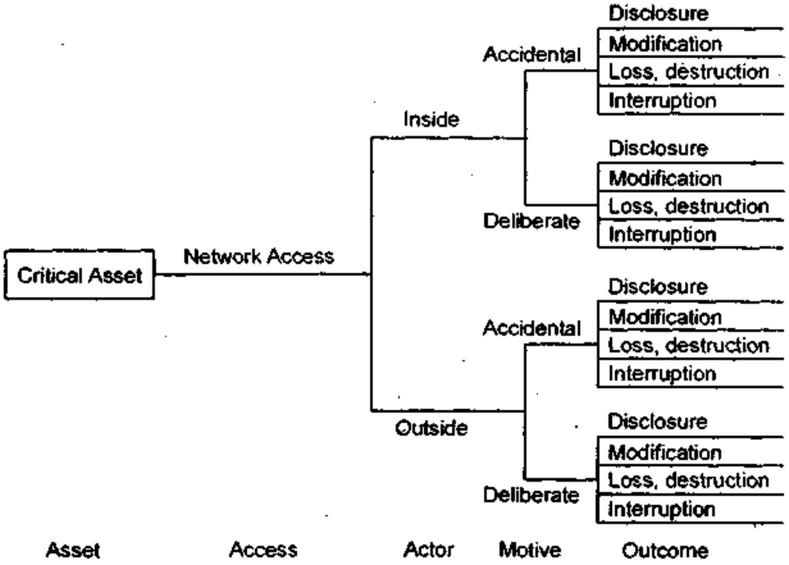
(b) Corruption or modification of information

(c) Theft, removal of loss of information

(d) Disclosure of information (Confidential data)

(e) Modification of important and/or sensitive information

(f) Interruption of access to important information, software, applications or services.



Generic Threat Profile

There are five categories of logical and physical assets:

1. **Information:** Documented (paper or electronic) data or intellectual property used to meet the mission of an organization.
2. **Software:** Software applications and services that process, store or transmit information.
3. **Hardware:** IT physical devices considering their replacement costs.
4. **People:** People in an organization who possess skills, competencies, knowledge and experience that are difficult to replace.

5. **Systems:** Information system that process and store information (a system is a combination of information, software and hardware assets.)

Another way of grouping threats is based on some common themes as follows:

1. **Human actors using network access:** The threats in this category are network-based threats to an organization's critical assets.
2. **Human actors using physical access:** The threats in this category are physical threats to an organization's critical assets.
3. **System problems:** The threats in this category are problem with an organization's IT systems. Examples include hardware defects, software defects, viruses and other system related problems.
4. **Other problems:** The threats in this category are problems or situations that are outside the control of an organization. Examples include natural disasters, power outages etc.

Q. 7. What are the security challenges faced by the mobile devices?

Ans. Mobility brings two main challenges to the information systems security: On the handheld devices, information is being taken outside of the physically controlled environment, and remote access back to the protected environment is being granted. Perceptions of the organizations to these security challenges are important in devising appropriate security operating procedure.

Some of the well known technical challenges in mobile security are:

(a) Managing the registry settings and configurations.

(b) Authentication service security.

(c) Cryptography security

(d) Light weight directory access protocol (LDAP) security.

(e) Remote access server (RAS) security.

(f) Media player control security

(g) Networking application program interface (API) security, etc.

Q. 8. What is Authentication service security? Explain in detail.

Ans. There are two components of security in mobile computing: - security of devices and security in networks. A secure network ensures that only authenticated devices can be connected to the network for obtaining the requested services.

1. **Cryptographic security for Mobile Devices:** The CGA (Cryptographically generated addresses) based authentication can be used to protect IP- layer signaling protocols including neighbor discovery and mobility protocols. Cryptographic security controls are deployed on palms, one of the common handheld devices used in mobile computing.

   The CPM (Cryptographic Provider Manager) provides encryption services to any application, allowing the encryption of only selected data or of all data and resources on the device.
2. **LDAP security for Handheld Mobile Computing Devices:** LDAP (light weight directory access protocol) is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the Public Internet or on a Corporate Intranet.
3. **RAS security for Mobile Devices:** RAS (Remote access server) is an important consideration for protecting the business- sensitive data that may reside on the employees

mobile devices. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. A personal firewall on a pocket PC or smart phone device can be an effective protective screen against threat from port scanning and other attacks, for the users connecting through a direct internet or RAS connection.

4. **Media Player Control Security**: Security attacks on mobile devices can also be through the "music gateways". Corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer.
5. **Networking API security for Mobile Computing Applications:** With the advent of electronic commerce and its further off-shoot into m-commerce, online payments are becoming popular with the payment gateways accessed remotely and possibly wirelessly. Further, with the advent of web services and their use in mobile computing applications, the API becomes an important consideration.

Q. 9. Explain Security of Laptops

or

Give the physical security countermeasures for laptops.

Ans. Laptops are common in use now days. Wireless capability in these devices has also raised security concerns owing to the information being transmitted over either, which makes it hard to detect theft of laptops has always been a major issue of concern.

Physical security Countermeasures

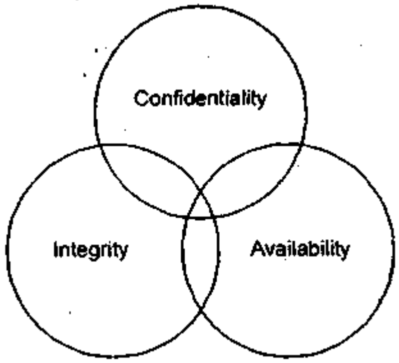
1. **Cables and hardwired locks:** Securing with cables and locks, specially designed for laptops, is the most cost efficient and ideal solution to safeguard any mobile device.
2. **Laptop safes:** Safes made of polycarbonate- the same material that is used in bulletproof windows, police riots shield and bank security screens- can be used to carry and safeguard the laptops. Unlike the security cables, it protects the entire laptop with its devices.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops and tracking missing laptops.
4. **Warming labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter thieves. These labels can be removed easily and are a low-cost solution to laptop theft.
5. **Other measures for protecting laptops:**
   - Installing encryption software to protect information to protect information stored on the laptop.
   - Using personal firewall software to block unwanted access and intrusion.
   - Updating the antivirus software regularly.
   - Disabling infrared (IR) ports and wireless cords when not in use.
   - Password protection through the use of strong passwords.
   - Backing up data on a regular basis.

Q. 10. What are the basic principles of information security? Also explain other terms in information security.

or

Explain Confidentiality, Integrity, Availability and other terms in Information Security.

Ans. The following three concepts are considered the pillars of information security: Confidentiality, Integrity and Availability (CIA). These concepts represent fundamental principles of information security. All the information security controls and safeguards, and all the threats, vulnerabilities and security processes are subject to this CIA yardstick.



Confidentiality: The concept of confidentiality implies an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity: The concept of integrity ensures that:

1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data are internally and externally consistent, i.e. the internal information is consistent among all sub entities and the internal information is consistent with the real world, external situation.

Availability: The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. Availability guarantees that the systems are up and running when they are needed and the security service needed by security practitioner are in working order.

Other Important Terms in Information Security:

1. **Identification:** It indicates the means by which users claim their identities to the system.
2. **Authentication:** This is the testing or reconciliation of evidence of a user's ID. It establishes the user's ID and ensures that the users are who they say they are. Authentication is a security measure used for verifying an individual's eligibility to receive specific categories of information.
3. **Accountability:** A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual. Audit trails and logs support accountability.

4. **Authorization:** The rights and permissions granted to an individual (or process), which enable access to a computer resource. Once a user's Id and authentication are established, authorization levels determine the extent of system rights that an operator can hold.
5. **Privacy:** This means that level of confidentiality and a privacy protection that a user is given in a system. It is an important component of security controls.

Q. 11. Explain how Information is classified. Also define the various rules.

Ans. Information classification based on the level of sensitivity of information:

1. **Unclassified:** Information that is neither sensitive nor classified. Public release of this information does not violate confidentiality.
2. **Sensitive but Unclassified (SBU):** Information that has been designated a minor secret, but may not create serious damage if disclosed. Example: Healthcare information of a hospital.
3. **Confidential:** Information that has been designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security.
4. **Secret:** Information that is designated to be of a secret nature. The unauthorized disclosure of this information could cause ***serious*** damage to country's national security.
5. **Top Secret:** This is the highest level of information classification (e.g. information in defense organizations). Any unauthorized disclosure of top secret information will cause exceptionally grave (great) damage to the country's national security.

Classification of information on a 'need-to-know' basic in a company:

1. **Public:** Public Information is that information that is similar to unclassified information. If it is disclosed, it is not expected to seriously or adversely impact the company.
2. **Sensitive:** Information that requires a higher level of classification than normal data is known as sensitive information. This information is protected from a loss of confidentiality, as well as from a loss of integrity owing to an unauthorized alteration.
3. **Private:** This information is considered of personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees. Example: - Salary levels and medical information of employees.

From the security perspective, the roles and responsibilities of all participants in the information classification program must be clearly defined.

Roles	Responsibilities
Owner An executive or manager of an organization who has final corporate responsibility of data protection and may be liable for negligence because of the failure to protect these data.	1. Making the original decision as to what level of classification the information requires based on the business needs for the protection of the data. 2. Reviewing the classification assignments periodically and making alterations as the business needs change. 3. Delegating the responsibilities of data protection duties to the custodian.

Custodian An information custodian is the delegated personnel who protect data on a day-to-day basis.	1. Running regular backups and routinely testing the validity of the backup data. 2. Performing data restoration from the backups when necessary and maintaining those retained records in accordance with legal requirements established based on information classification policy. 3. Administering the classification scheme.
User They can be considered consumers of the data, who need daily access to the information to execute their tasks. Managers and executives are also users along with the supervisory staff in an organization.	1. It is mandatory for users to follow the operating procedures that are defined in an organization's security policy, and they must adhere to the published guidelines for their use. 2. Users must take 'due care' to preserve the information's security during their work (as outlined in the corporate information use policies). 3. They must prevent 'open view' from occurring. 4. Users must use the company's computing resources only for company purposes and not for personal use.