Unit-1: Introduction

Computer Security Concepts:

The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as:
The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security.

■■ **Confidentiality:** This term covers two related concepts:

Data Confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals 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:** This term covers two related concepts:

Data Integrity: Assures that data (both stored and in transmitted packets) 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.

■■ **Availability:** Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the **CIA triad**.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture below. Two of the most commonly mentioned are:

■■ **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

■■ **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

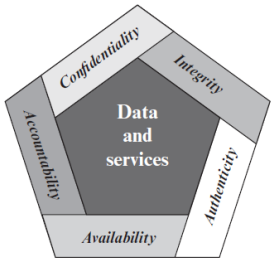


Figure: Essential Network and Computer Security Requirements

The OSI Security Architecture:

The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations-sponsored agency that develops standards, called Recommendations, relating to telecommunications and to Open Systems Interconnection (OSI).

The ITU-T Recommendation X.800, i.e., Security Architecture for OSI, defines a systematic approach to assess effectively the security needs of an organization and to evaluate and choose various security products and policies. This architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.
The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as:

■■ **Security Attack:** Any action that compromises the security of information owned by an organization.

■■ **Security Mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

■■ **Security Service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

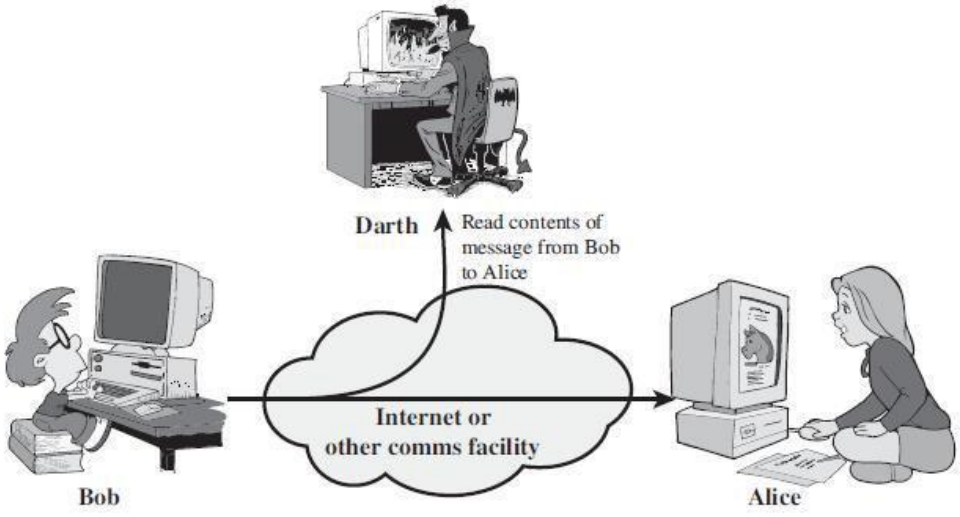
Security Attacks:

A useful means of classifying security attacks is in terms of passive attacks and active attacks. A *passive attack* attempts to learn or make use of information from the system but does not affect system resources. An *active attack* attempts to alter system resources or affect their operation.

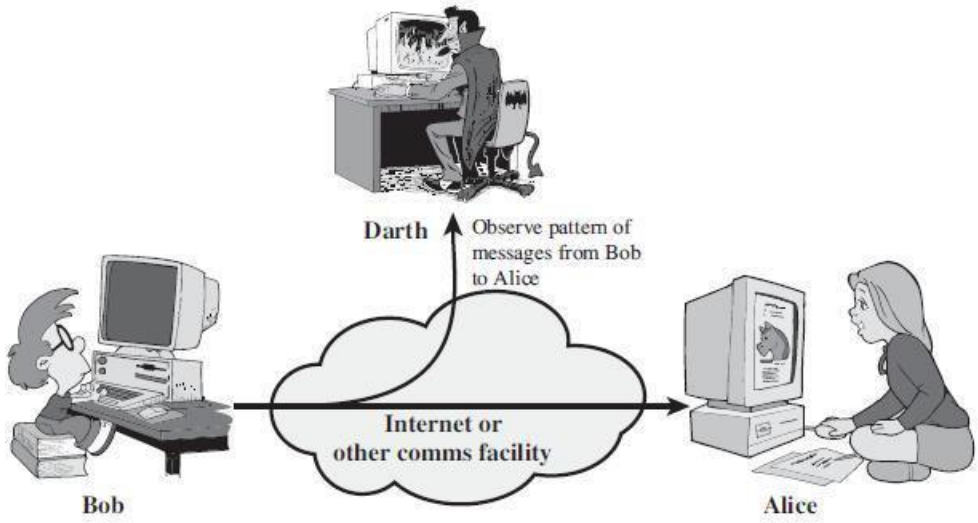
Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are:

i) Release of Message Contents: A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



ii) Traffic Analysis: Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

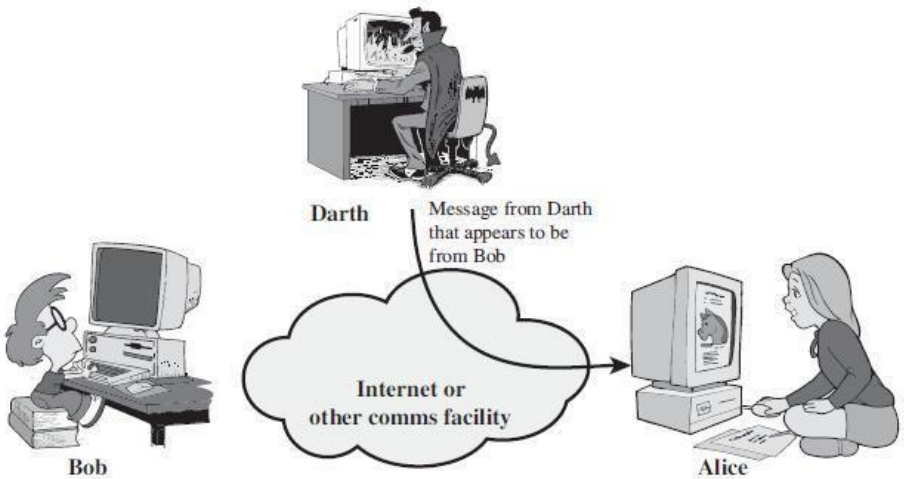


Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption.

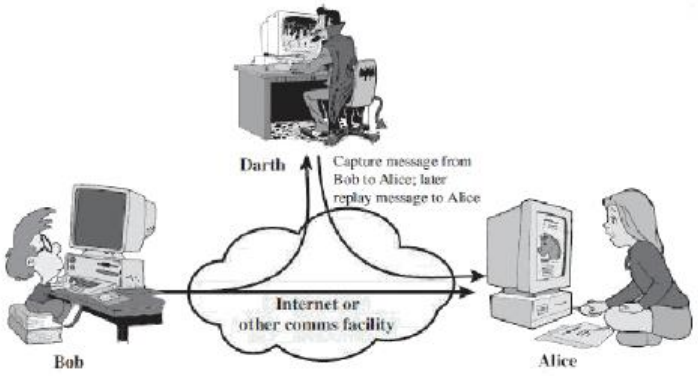
Active Attacks:

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

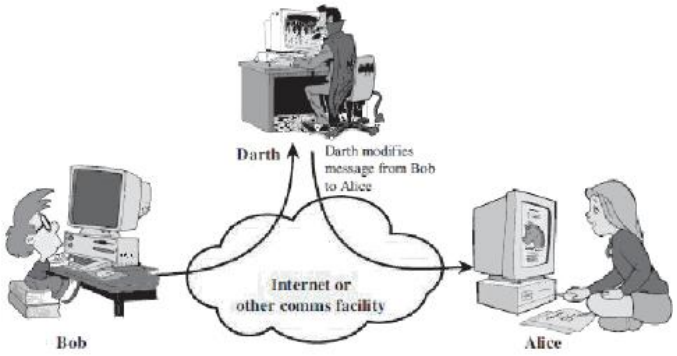
i) Masquerade: It takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



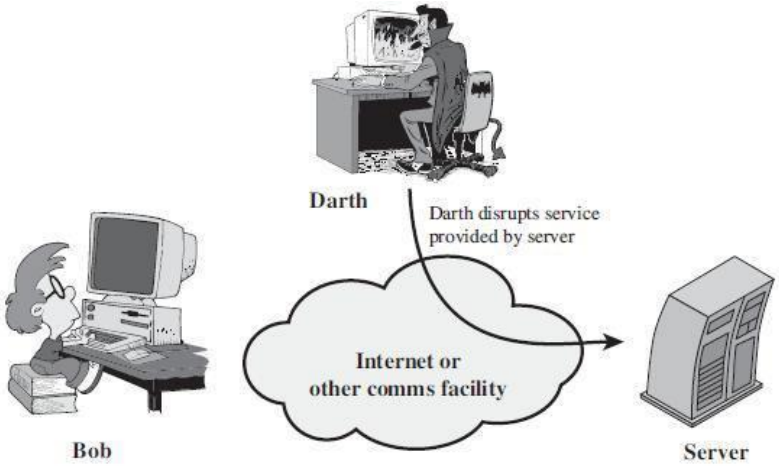
ii) Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.



iii) Modification of messages: It simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



iv) Denial of Service: It prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.



Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

Security Services:

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 4949, which provides the following definition: A processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block. **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

Security Services (X.800)

I) Authentication:

The authentication service is concerned with assuring that a communication is authentic.

Two specific authentication services are defined in X.800:

i) Peer entity authentication:

Two entities are considered peers if they implement the same protocol in different systems (e.g., two TCP modules in two communicating systems).

Peer entity authentication is provided for use at the establishment of or during the data transfer phase of a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

ii) Data origin authentication:

This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

II) Access Control:

It is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

III) Data Confidentiality:

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time.

For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message.

The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

IV) Data Integrity:

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection.

A connection-oriented integrity service deals with a stream of messages and assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service.

On the other hand, a connectionless integrity service deals with individual messages without regard to any larger context and generally provides protection against message modification only.

V) Non-Repudiation:

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Availability Service:

Both X.800 and RFC 4949 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them). A variety of attacks can result in the loss of or reduction in availability. This service addresses the security concerns raised by denial-of-service attacks.

Security Services:

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Security Mechanisms (X.800)

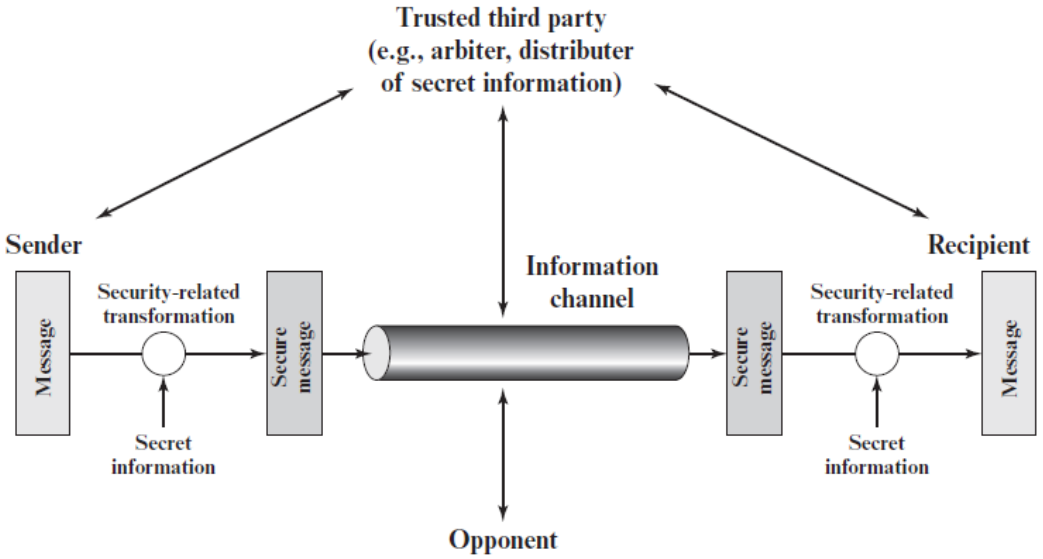
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Mechanism

Relationship between Security Services and Mechanisms

A Model for Network Security:

A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.



Model for Network Security

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All of the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.

Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

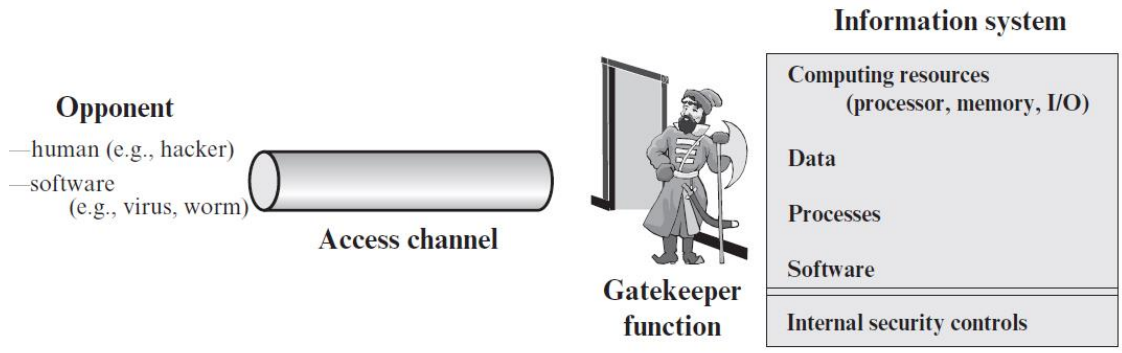
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

1. Information access threats: Intercept or modify data on behalf of users who should not have access to that data.

2. Service threats: Exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They also can be inserted into a system across a network; this latter mechanism is of more concern in network security. The security mechanisms needed to cope with unwanted access fall into two broad categories.



Network Access Security Model

The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Standards:

Standards have been developed to cover management practices and the overall architecture of security mechanisms and services. Various organizations have been involved in the development or promotion of these standards.

The most important of these organizations are as follows:

■■ **National Institute of Standards and Technology:** NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation.

Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

■■ **Internet Society:** ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the **Internet Engineering Task Force (IETF)** and the **Internet Architecture Board (IAB)**. These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

ACADEMIC SESSION: EVEN SEMESTER (2023-24)

Assignment No. 1 (Unit-1)

Name of Subject: Network & System Security (TCS 619) **Course: B.Tech.**

Branch: CSE (All Sections) **Semester: VI**

Date of Issue: 12-02-2024 **Date of Submission: 20-02-2024**

Instructions:

1. **Use A-4 sized blank pages.**
2. **Submit the stapled hard-copy on the Date of Submission.**
3. **Attempt all questions. Each question carries equal marks.**

Questions: **Max. Marks: 20**

1. What is the OSI Security Architecture?
2. Why are passive attacks difficult to detect and active attacks difficult to prevent?
3. Identify the different security attacks prevented by the security mechanisms defined in X.800.
4. List and briefly define the fundamental security design principles.
5. Explain the Masquerade attack with an example.

Layered Architecture :

Understand that the entire process of communication is divided/

I) broken into smaller seven pieces. Each seven modules will be taking care of a simpler task & they are specifically assigned for it. So, whenever there is an issue, we can simply identify that which layer is not working & thus can easily troubleshoot it.

II) Each layer is specifically trained, tuned & enhanced over the period of time, so that the functionality of a particular task gets more efficient & thus the combination of these seven layers gives more reliability & performance on the network.

III) Each layer operates on the incoming data in a pre-defined way & passes on the data to the next level.

Receive Data → Process Data → Send the data

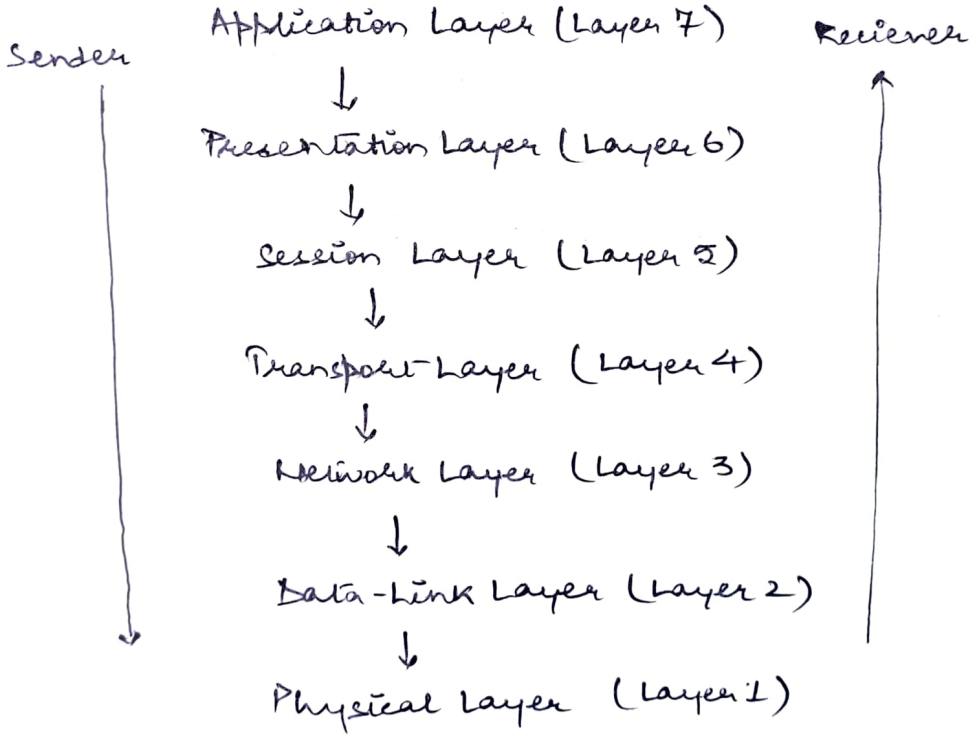
⇒ In a layered architecture, the data sequentially moves from one layer to the other.

* An internet user works on which layer ?

ISO-OSI Reference Model :

* ISO - International Organization for Standardization.
  It is an independent, non-governmental, international standard development organization composed of representatives from the national standards organizations of member countries.

* OSI - Open Systems Interconnection.
  It is a set of internationally recognised, non-proprietary standards for networking and for operating system involved in networking purposes.



The OSI-Reference Model

All People Seem To Need Data Processing } Phrase

ISO-OSI Model supports various Protocols at different layers. They are:

Layers	Protocols/Standards or formats
I) Application Layer	1) Hyper Text Transfer Protocol (HTTP) 2) File Transfer Protocol (FTP) 3) Trivial file transfer Protocol (TFTP) 4) Domain Name service (DNS) 5) Simple Mail Transfer Protocol (SMTP) 6) Secure file Transfer Protocol (SFTP) 7) Simple Network Management Protocol (SNMP) 8) Remote Login (Rlogin) 9) Multipurpose Internet Mail Extension (MIME)
II) Presentation Layer	1) Motion Picture Experts Group (MPEG) 2) Joint Photographic Experts Group (JPEG) 3) Tagged Image file format (TIFF)
III) Session Layer	1) Structured Query Language (SQL) 2) X-Window System 3) AppleTalk session Protocol (ASP) 4) Digital Network Architecture session control Protocol (DNA SCP) 5) Network file system (NFS) 6) Remote Procedure call (RPC)
IV) Transport Layer	1) Transmission Control Protocol (TCP) 2) User Datagram Protocol (UDP) 3) Sequenced Packet Exchange (SPX)
V) Network Layer	1) Internet Protocol (IP) 2) Open Shortest Path First (OSPF) 3) Internet control message Protocol (ICMP) 4) Routing Information Protocol (RIP)

Layers	Protocols / Standards or Formats
VI) Data-Link Layer	1) Address Resolution Protocol (ARP) 2) Reverse Address Resolution Protocol (RARP) 3) Serial Line Internet Protocol (SLIP) 4) Point-to-Point Protocol (PPP)
VII) Physical Layer	Family of IEEE 802 LAN/WAN standards.