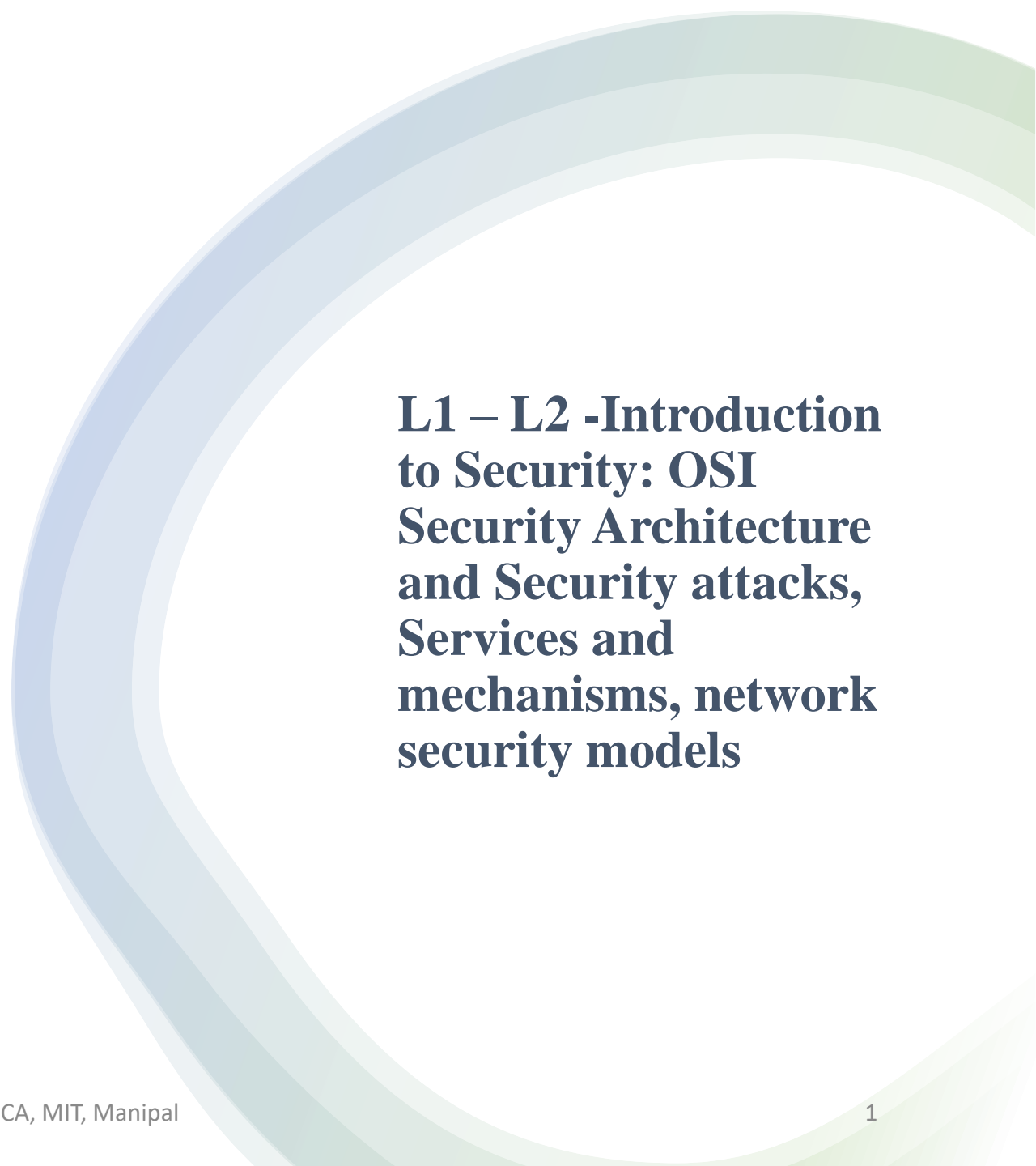




Data Security and Privacy

DSE 3258



**L1 – L2 -Introduction
to Security: OSI
Security Architecture
and Security attacks,
Services and
mechanisms, network
security models**

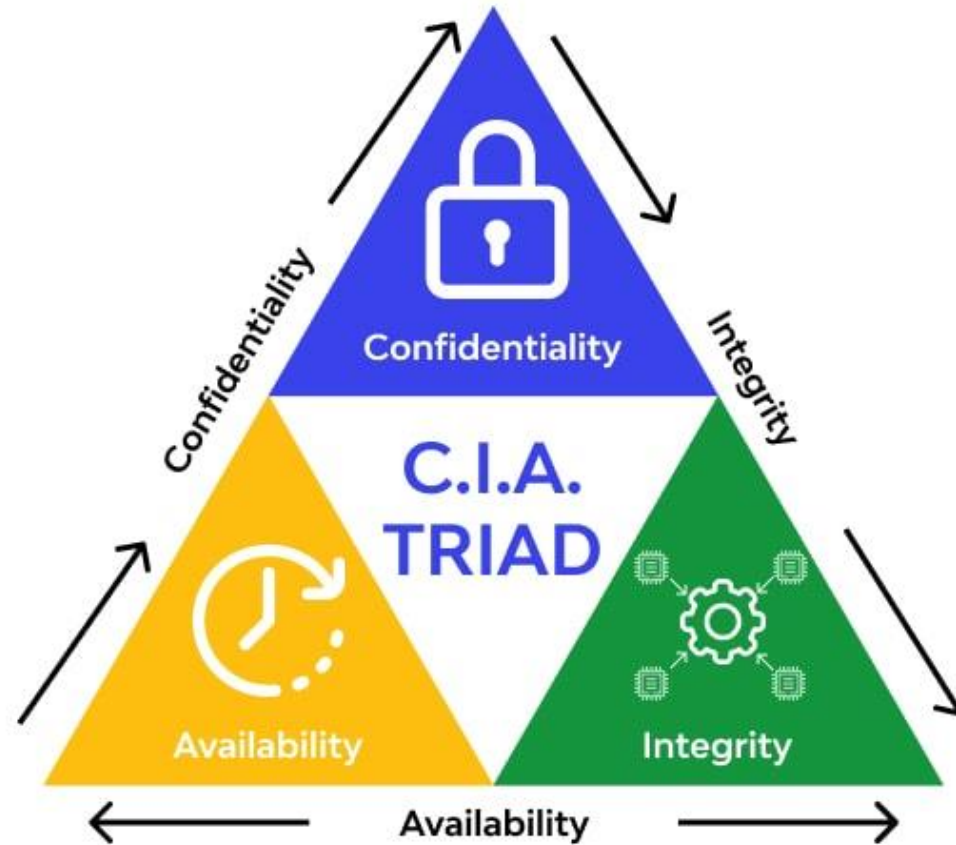
Introduction

- **What is computer security?**

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 (including hardware, software, firmware, information/data, and telecommunications).

NIST Computer Security Handbook [NIST95]

Three key objectives of Computer Security



Three key objectives of Computer Security

Confidentiality:

- ✓ **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:

- ✓ **Data integrity:** Assures that information (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.

Additional Objectives

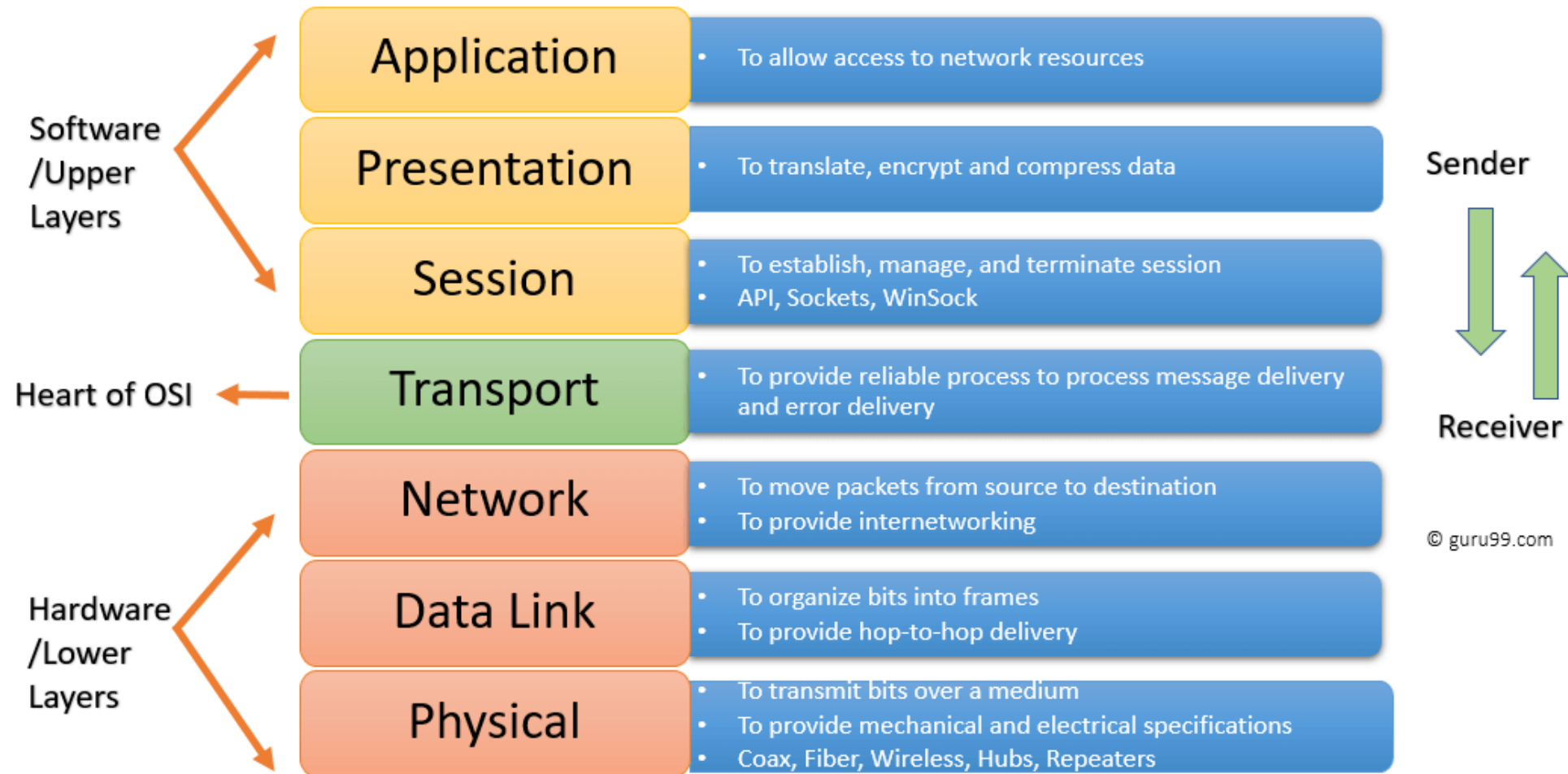
Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

An *authentication* is a process that ensures and confirms a user's identity or role that someone has.

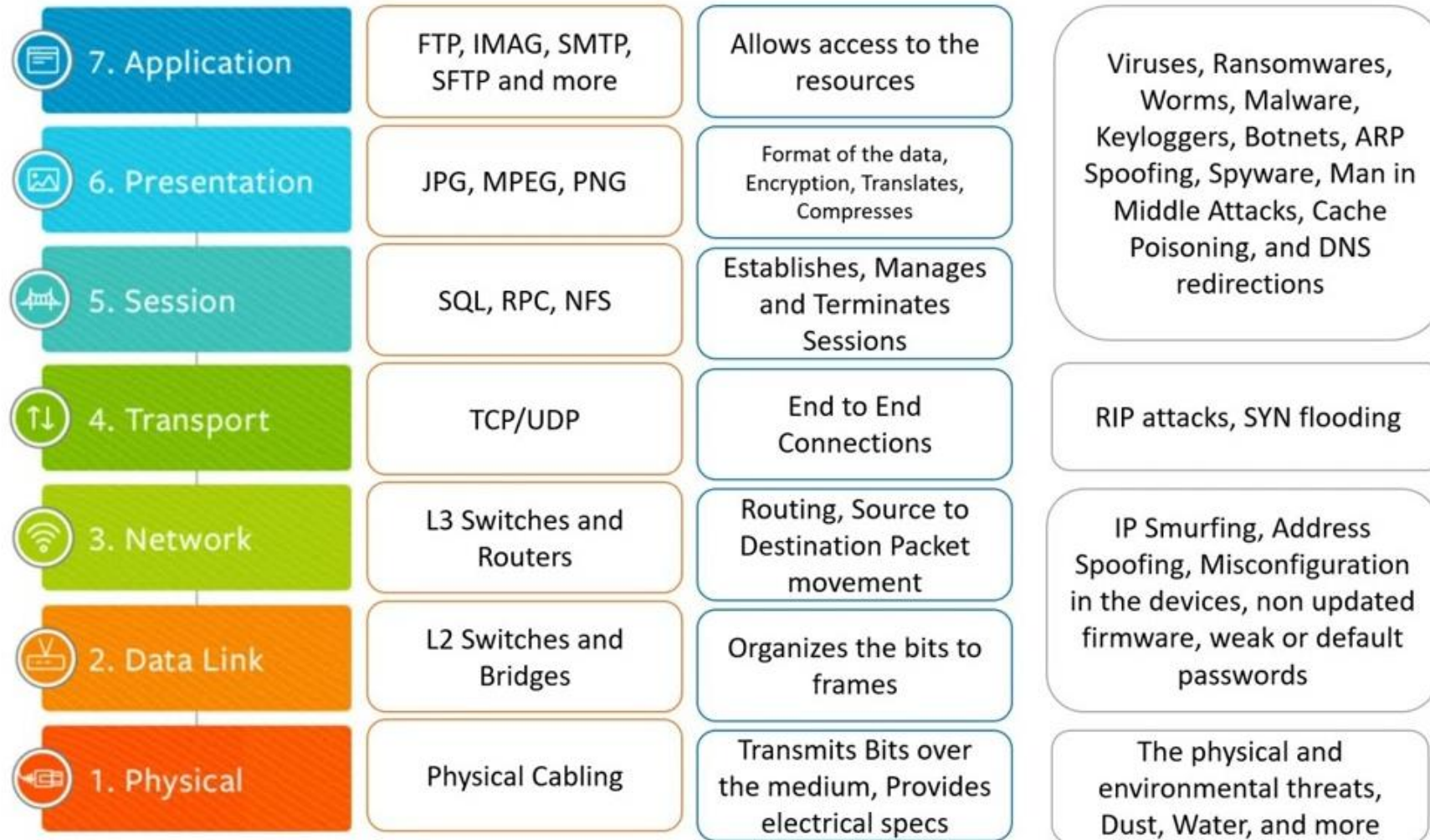
Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention etc.

It means that every individual who works with an information system should have specific responsibilities for information assurance. The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance.

The OSI Security Architecture



The OSI Security Architecture

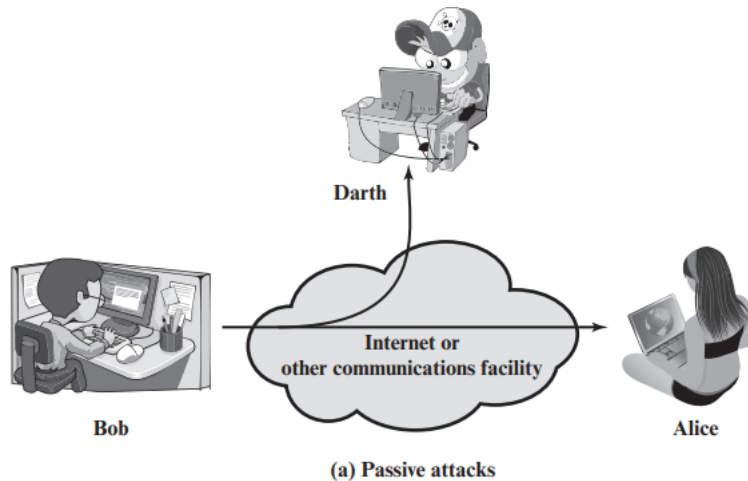


The OSI Security Architecture

- **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 attack

• Passive Attack



- ✓ Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- ✓ Two types : *Release of message contents* and *Traffic analysis*.

Release of message contents :

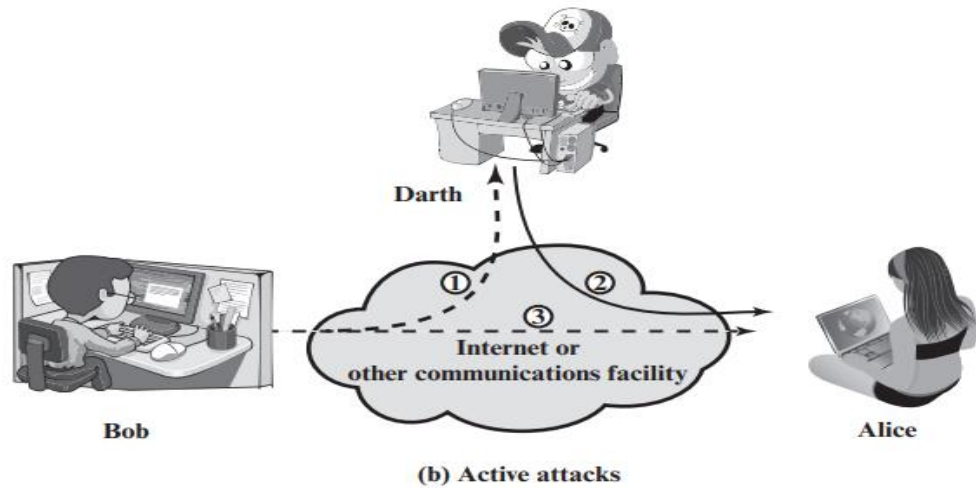
- Happens when confidential user data are released publicly over the network.
- Attacker is monitoring unprotected communication mediums and intercepting them. such as unencrypted data, emails, telephone calls, etc., which results in lost data confidentiality.

Traffic analysis:

- Is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- We need a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.
- If we had encryption protection in place, an opponent might still 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

Security attack

- **Active Attack**

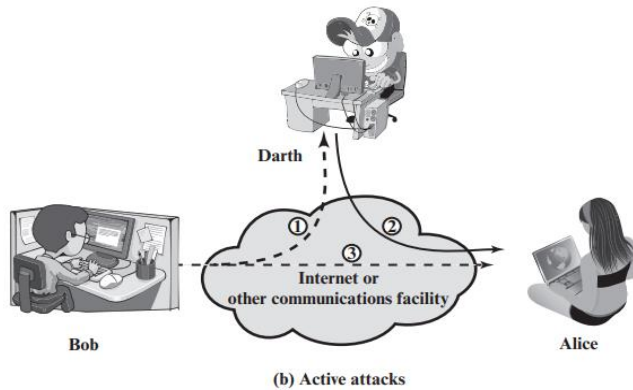


- ✓ An active attack attempts to alter system resources or affect their operation.
- ✓ Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: **masquerade, replay, modification of messages, and denial of service.**

Masquerade

- Takes place when one entity pretends to be a different entity (path 2 of Figure is active).
- A masquerade attack usually includes one of the other forms of active attack. 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.

Security attack



Replay:

Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (paths 1, 2, and 3 active).

Modification of messages

Means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (paths 1 and 2 active).

Denial of service

Prevents or inhibits the normal use or management of communications facilities (path 3 active). 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.

Active attack	Passive attack
In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
In active attacks, the victim gets notified about the attack.	Unlike active attacks, in passive attacks, victims do not get informed about the attack.
The damage done with active attacks can be harmful to the system and its resources.	The passive attacks do not harm the system.
In active attacks, the system resources can be changed.	In passive attacks, the system resources remain unchanged.
They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.

Security Service

- 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.
- Security services implement security policies and are implemented by security mechanisms.
 - **Authentication**
 - **Access Control**
 - **Data Confidentiality**
 - **Nonrepudiation**
 - **Data Integrity**
 - **Availability Service**

Security Service

Authentication

- The authentication service is concerned with assuring that a communication is authentic.
- In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
- In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, **at the time of connection initiation**, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be.
- Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Security Service

Authentication

Two specific authentication services are defined in X.800:

- **Peer Entity Authentication**

Two entities are considered peers if they implement the same protocol in different systems; for example two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times 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

- **Data-Origin Authentication**

It does not provide protection against the duplication or modification of data units.

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.

Security Service

Access Control

In the context of network security, access control 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.

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).

Security Service

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

Security Service

Data Confidentiality

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.

Security Service

Data Integrity

- It can apply to a stream of messages, a single message, or selected fields within a message.
- A connection-oriented integrity service, one that deals with a stream of messages, 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, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.
- We can make a distinction between service with and without recovery.
- If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data.

Security Service

Data Integrity

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.

Security Service

Nonrepudiation

- 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.

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 Service

Availability Service

- X.800 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)
- X.800 treats availability as a property to be associated with various security services.
- An availability service is one that protects a system to ensure its availability.
- This service addresses the security concerns raised by denial-of-service attacks.
- It depends on proper management and control of system resources and thus depends on access control service and other security services.

Security Mechanism

- The mechanisms are divided into those that are implemented in a specific protocol layer, and those that are not specific to any particular protocol layer or security service.

Specific Security Mechanisms

- **Encipherment**
- **Digital Signature**
- **Access Control**
- **Data Integrity**
- **Authentication Exchange**
- **Traffic Padding**
- **Routing Control**
- **Notarization**

Pervasive Security Mechanisms

Trusted Functionality
Security Label
Event Detection
Security Audit Trail
Security Recovery

Security Mechanism

Specific Security Mechanisms: May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

- **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.

- **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).

- **Access Control**

- A variety of mechanisms that enforce access rights to resources. A variety of mechanisms used to assure the integrity of a data unit or stream of data units

Security Mechanism

Specific Security Mechanisms:

- **Authentication Exchange**

A mechanism intended to ensure the identity of an entity by means of information exchange.

- **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 Mechanism

Pervasive Security Mechanisms: Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

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.

Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions

Table 1.4, based on one in X.800, indicates the relationship between security services and security mechanisms.

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE	MECHANISM							
	Encipherment	Digital signature	Access control	Data integrity	Authentication	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			

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.
- 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 the techniques for providing security have two components:
 - **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.
 - **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

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.
- 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 the techniques for providing security have two components:
 - **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.
 - **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

Model for Network Security

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 away 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 makes use of the security algorithm and the secret information to achieve a particular security service.

Model for Network Security

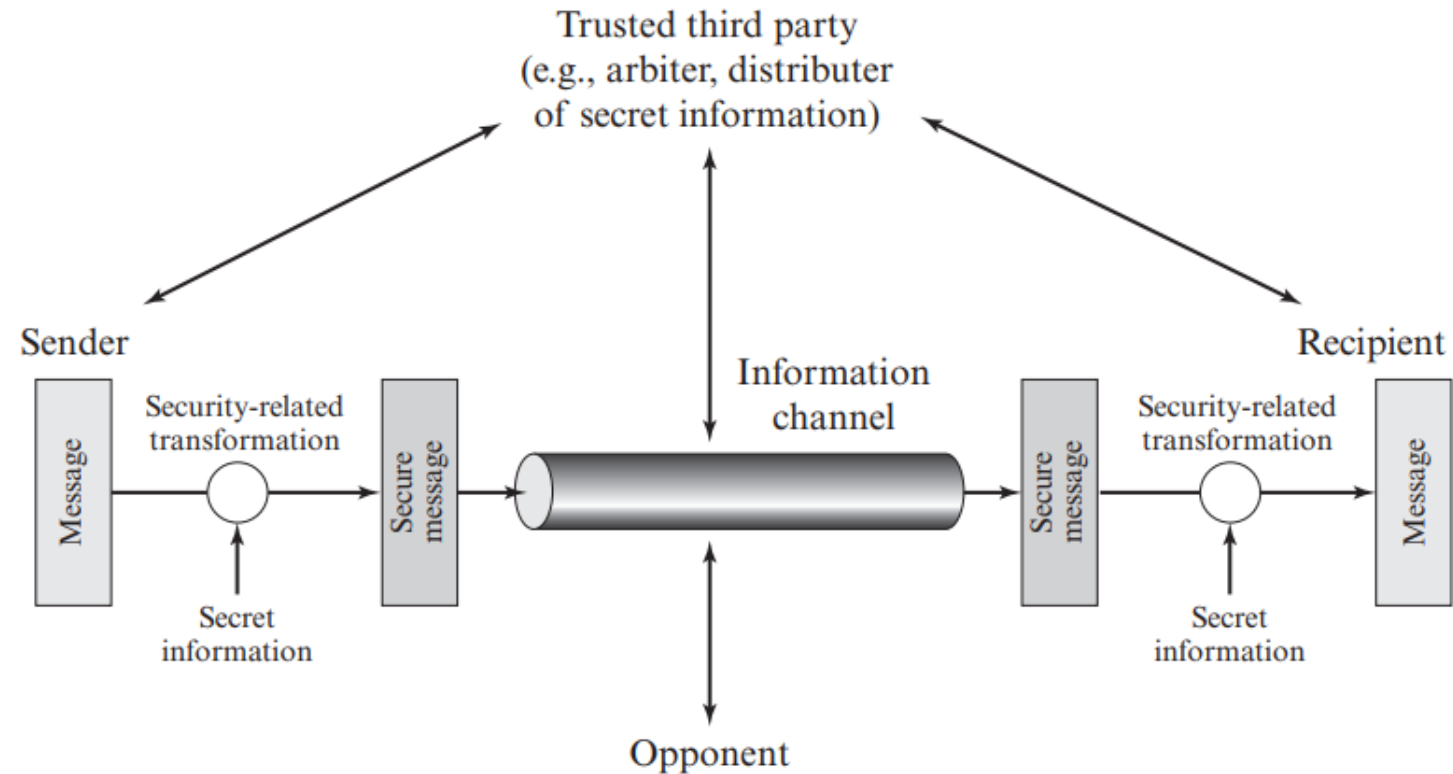


Figure 1.5 Model for Network Security

Model for Network Security

Other possible situations:

- ✓ Hackers attempt to penetrate systems that can be accessed over a network.
- ✓ The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- ✓ The intruder can be a dissatisfied employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial.
- ✓ 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:

- **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

Model for Network Security

The security mechanisms needed to cope with unwanted access fall into two broad categories .

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.

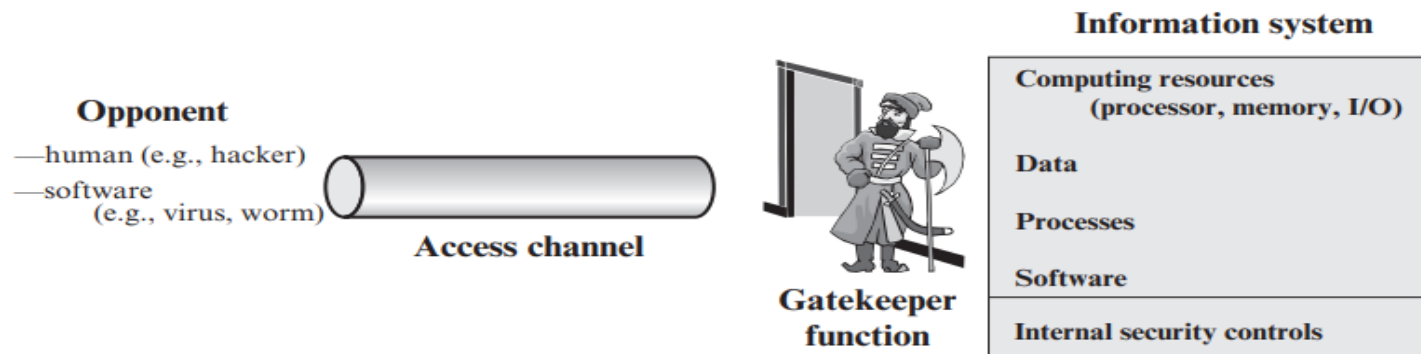


Figure 1.6 Network Access Security Model