Unit VII

Introduction to Computer Security

Content

- Computer Security Concepts
- Security Attacks
- Security Services
- Security Mechanisms
- Techniques
- Model for Network Security.

Computer Security Concepts

- Before the widespread use of data processing equipment, the security of information valuable to an organisation was provided primarily by physical (lock and key)
- With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident
- Another major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer
- Security required to protect the data during the transmission over the network.
- Computer security
  - The generic name for the collection of tools designed to protect data and to thwart hackers
- Internet security (lower case “i” refers to any interconnected collection of network)
  - Consists of measures to deter(to stopdoing), prevent, detect, and correct
  - security violations that involve the transmission of information

- e.g hack the massage over the network and get authorized access.

Computer Security

The NIST *Computer Security Handbook* defines the term computer security as:

NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology based on existing standards.

"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)"

Computer Security Objectives

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

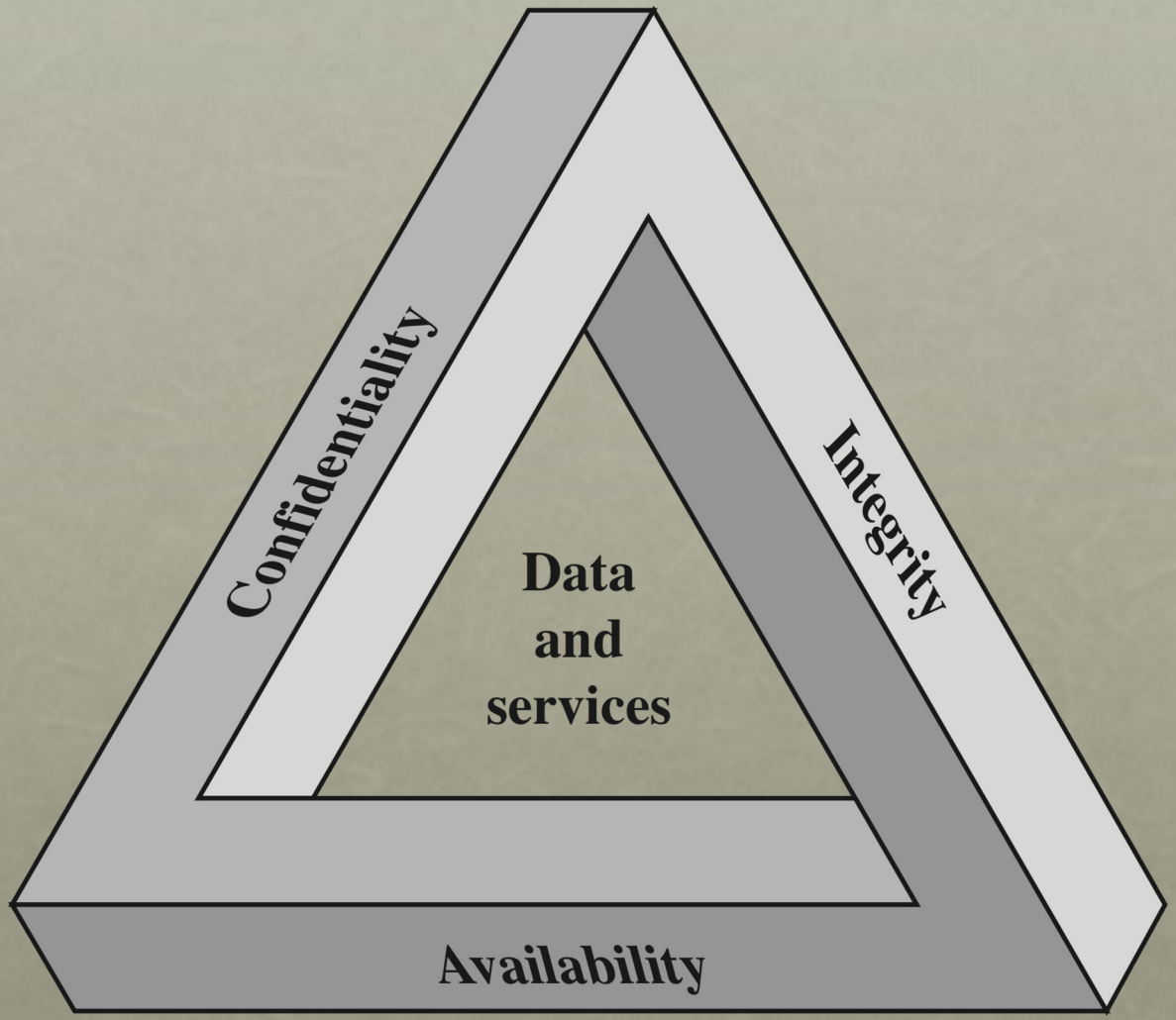
- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired (un altered) manner, free from deliberate unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

- This three The three concepts embody the fundamental security objectives for both data and for information and computing services.
-

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Possible additional concepts:

CIA triad to define security objectives is well estab_x005F_x0002_lished, some in the security field feel that additional concept are required

Authenticity

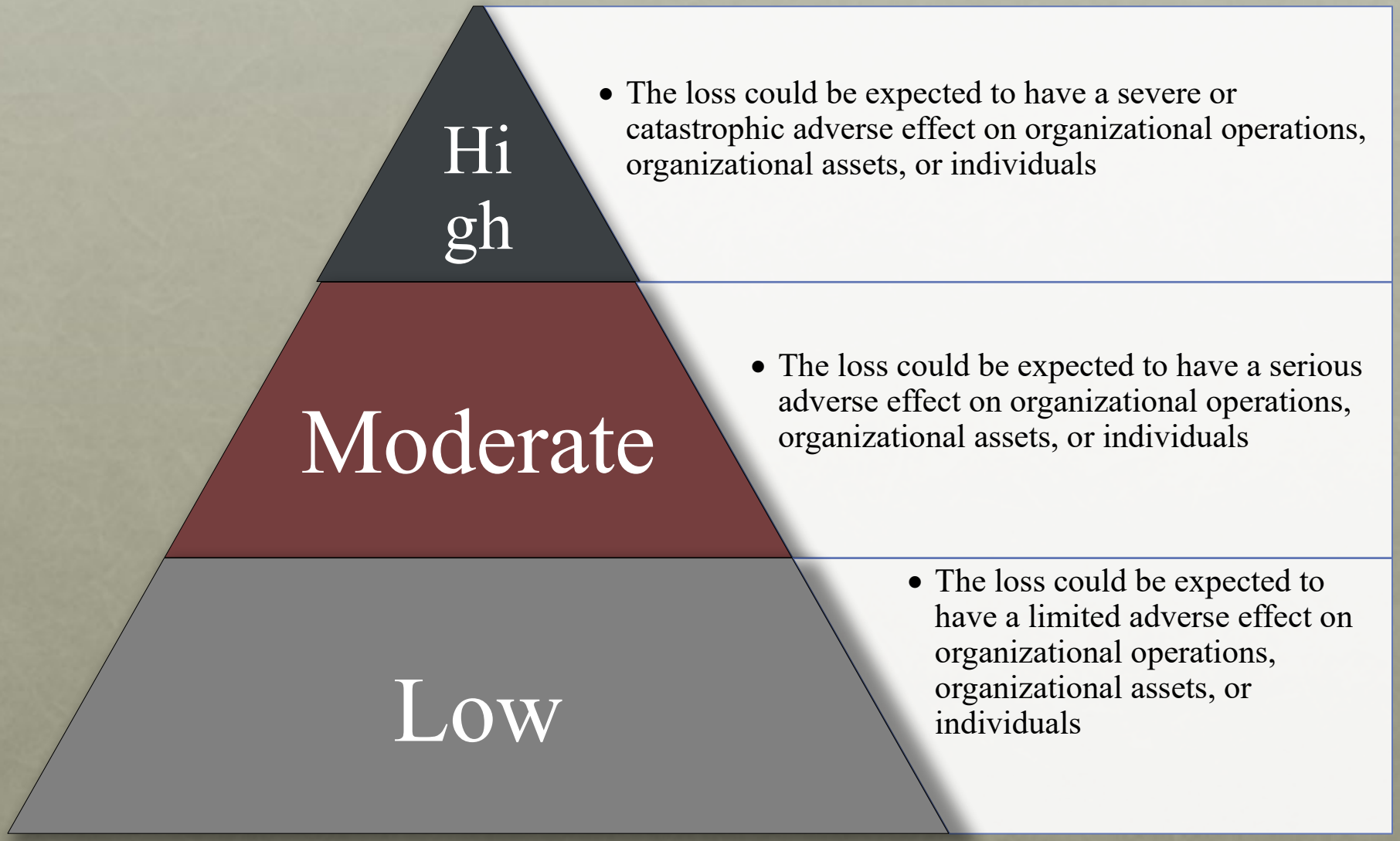
- Verifying that users are who they say they are or not and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

- Accountability:
  - the traceability of actions performed by a user, process or device. For example, the use of unique user identification and authentication supports accountability, whereas the use of shared user IDs and passwords destroys accountability.
  - Systems must keep record for their activities for further tracing if required.
- E.g Three leveles of impact on organization in term of security.

Breach of Security Levels of Impact



Low : Result in minor finanicial loss or result in minor harm to individuals or result in minior damange to oranizational assests

Modarate : Result in significant damage in finanicial loss or individuals or oranizational assests.

High : loss could be severe.
Cause a severe degradation may organization not able to perform one or more ot its primary functions. Major finanical loss , result in finanical loss or assest loss. Or individual major injuries.

Examples of Security Requirements

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

Regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous online poll

Availability

The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

An online telephone directory lookup application would be classified as a low-availability requirement

- Confidentiality

Grade information should only be available to students,and employee that required the information. (so it assign modarate confidentiality).
Student enrollment information (view) can be at modarate level
List of students faculty or department list is assign low confidentiality.

- Integrity : E.g hospital system.

Patient decease information can be update by the respective doctor. . if it is changed by the nurse (who is allowed to modified) then data may harm to the hospital or individual patient. So it must be traceable to track the modification done by whom.
Here patient decease information is required high integrity . Inaccurate information could result in serious harm to patient.

- Availability
- System which provide the authentication service for applications. Interruption of service result in inability for customers to access computing resource.

Computer Security Challenges

- Security is not simple . Mechanisms to meet the requirements can be complex
- Potential attacks on the security features need to be considered while developing the security algorithms
- Procedures used to provide particular services are often counter-intuitive(not obvious from statement of requirement) e.g login requirement then security of password.
- It is necessary to decide where to use the various security mechanisms. At what point security mechanism required (e.g online money transfer) at what layer of network what security mechanisms required.
- Security mechanisms typically involve more than a particular algorithm or protocol

- Security is essentially a battle of wits between a perpetrator and the designer. any weak design of system (in term of security) become advantage of hacker.
- Security required regular, constant monitiorng .
- Strong security is often viewed as an impediment(obstruction) to efficient and less user-friendly operation

OSI Security Architecture

- OSI security architecture was developed in the context of OSI protocol architecture.
- The OSI security architecture focuses on security attacks, mechanisms, and services.
- In the literature, the terms threat and attack are commonly used to mean more or less the same thing.
-
- Threat
  - A Threat is a possible security risk that might exploit the vulnerability of a system or asset.
- Attack
  - An attack, on the other hand, is the actual act of exploiting the information security system's weaknesses and harm the system.
- OSI security archi. Focuses on security attacks,mechanisms and services

Table 1.1
Threats and Attacks (RFC 4949)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

OSI Security Architecture

- Security attack
  - Any action that compromises(harm/damage) 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
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Security Attacks

- A means of classifying security attacks, 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

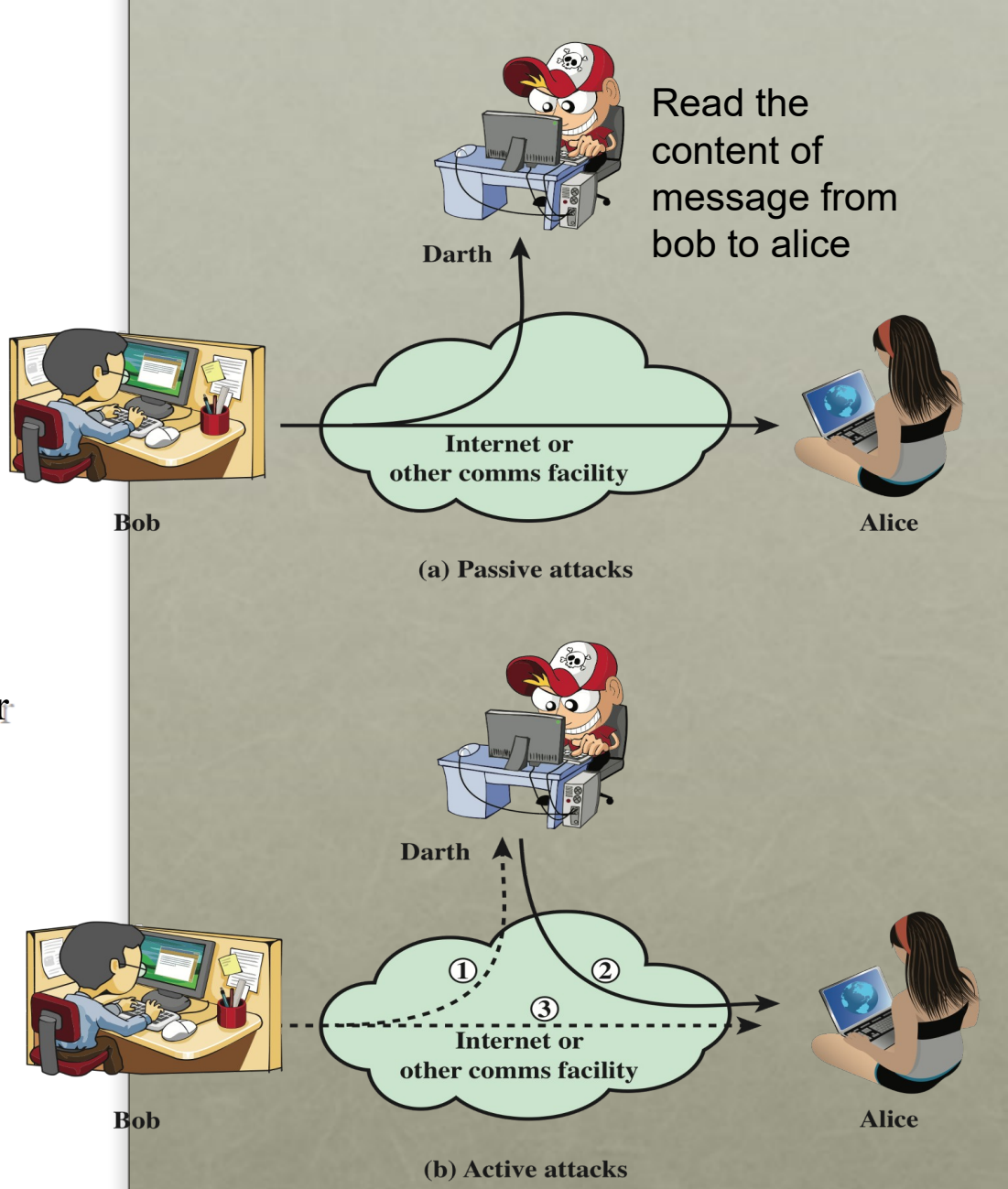
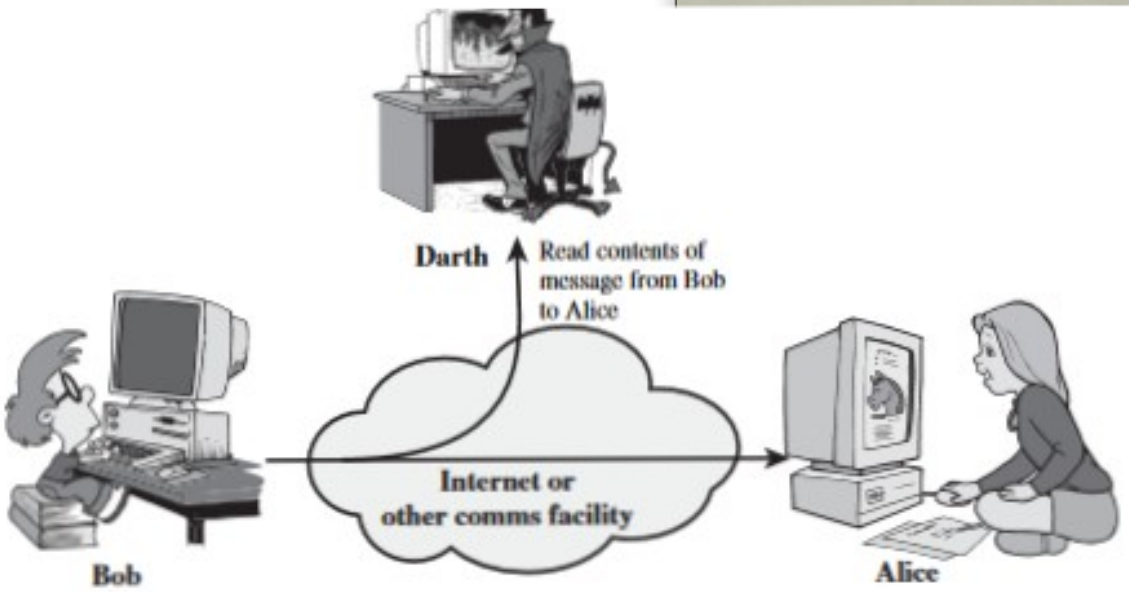


Figure 1.1 Security Attacks

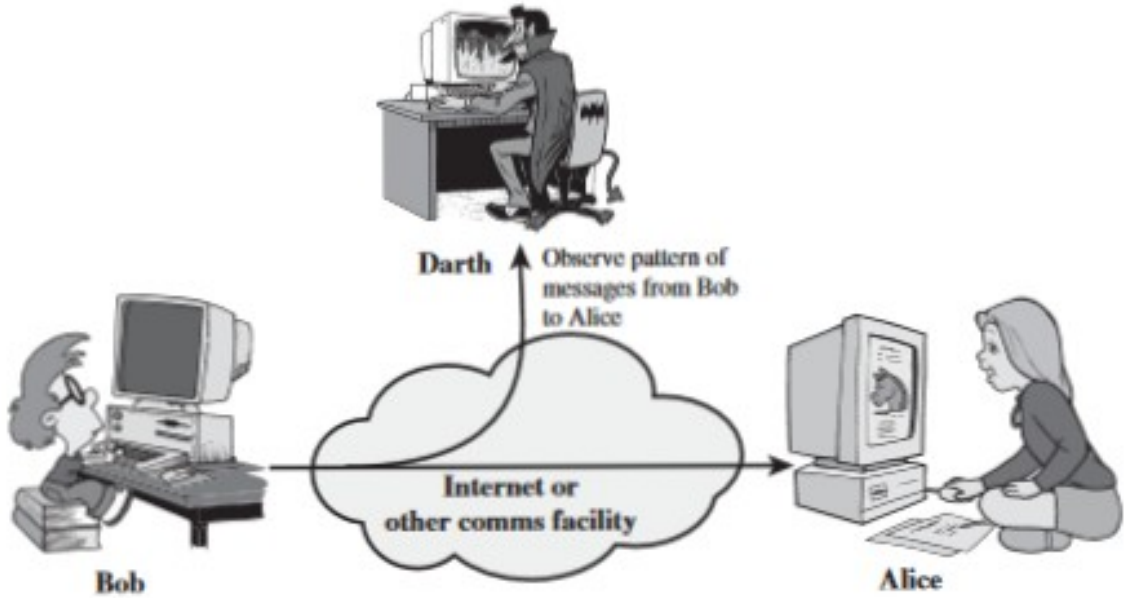
Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of transmissions.
- Goal of the opponent/attacker is to obtain information that is being transmitted

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis



(a) Release of message contents



Release of message content :

A tele-phone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information which may be read by attacker

traffic analysis

- involves analyzing network traffic as it moves to and from the target systems. These types of attacks use statistical methods to analyze and interpret the patterns
- 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 communica-
- tion that was taking place

Passive Attach Nature

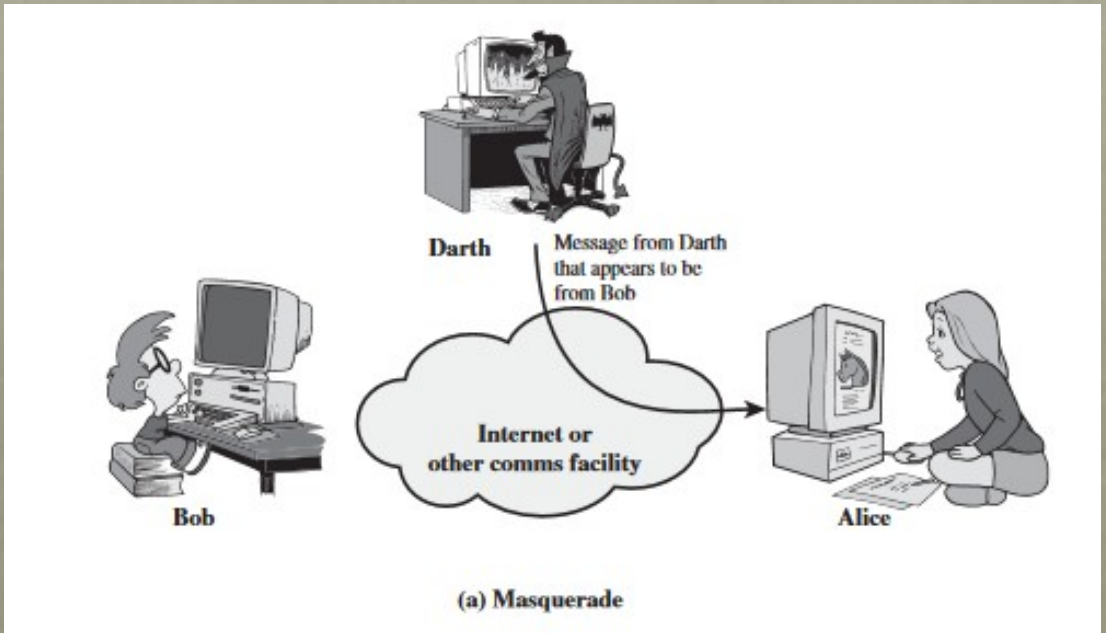
- Passive attacks are very difficult to detect,
- because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic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

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

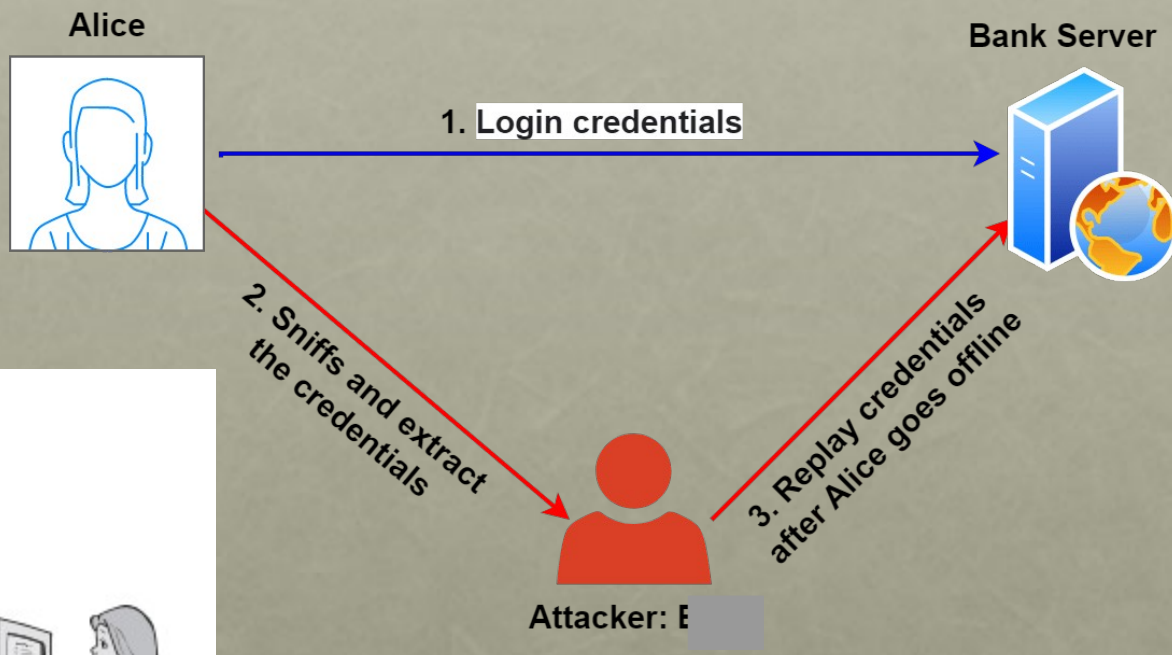
Masquerade	• Takes place when one entity pretends to be a different entity • Usually includes one of the other forms of active attack
Replay	• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Modification of messages	• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	• Prevents or inhibits (prevent) • the normal use or management of communications facilities

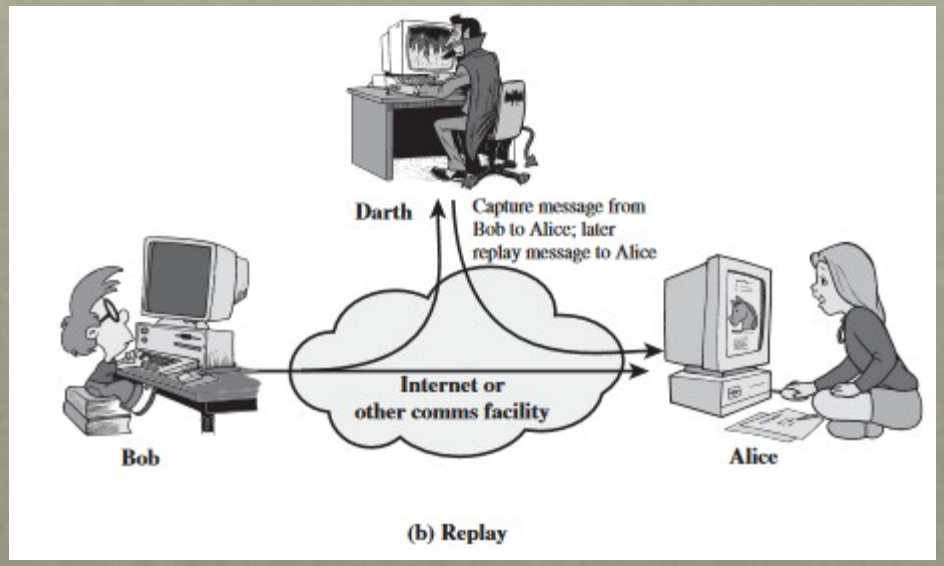
- A masquerade attack is any cyber attack that involves the use of a manipulated, spoofed or stolen user identifier – device, digital signature, network address to gain the access of the system.
- Gaining unauthorized access and stealing data
-
-



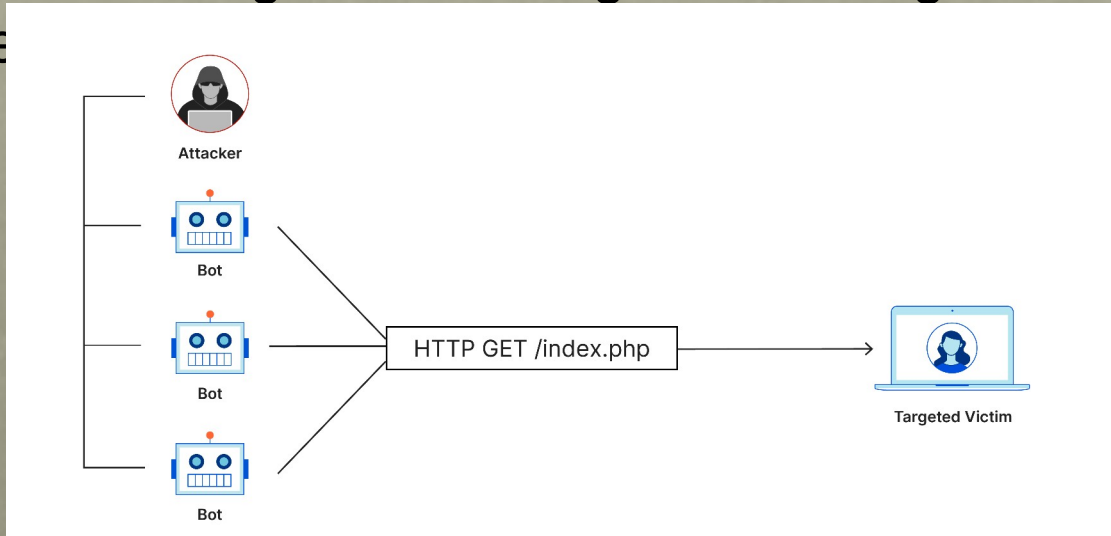
(a) Masquerade

Replay attacks are about sending the same code or link to someone in order to produce the same effect and get the same job done.





- Modification of message:
- For eg message “Allow smith to read file accounts” is modified as “Allow Fred to read file accounts”.
- Denial of Service
- Attack may have specific target . Entity may suppress all messages directed to particular desination. e.g disabling the network or overloading with messages so to degrade performance



Active Attack	Passive Attack
In an active attack, Modification in information takes place	While in a passive attack, Modification in the information does not take place.
Active Attack is a danger to Integrity as well as availability	Passive Attack is a danger to Confidentiality.
Easy to detect	Not easy to detect

Security Services

- Defined by X.800 as:
- X.800 is a security architecture for open, interconnected systems.
  - A service provided by a protocol layer of communicating open systems and that ensures adequate(enough) security of the systems or of data transfers.

- Defined by RFC 4949 as:
- A processing or communication service provided by a secuirty system to give a specific kind of protection to system resources.

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

Security Services (X.800)

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.

Authentication

- Concerned with assuring that a communication is authentic
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- **Peer entity authentication : identity of the entities connected**
- **Data origin authentication : In a connectionless transfer, provides assurance that the source of received data is as claimed.**

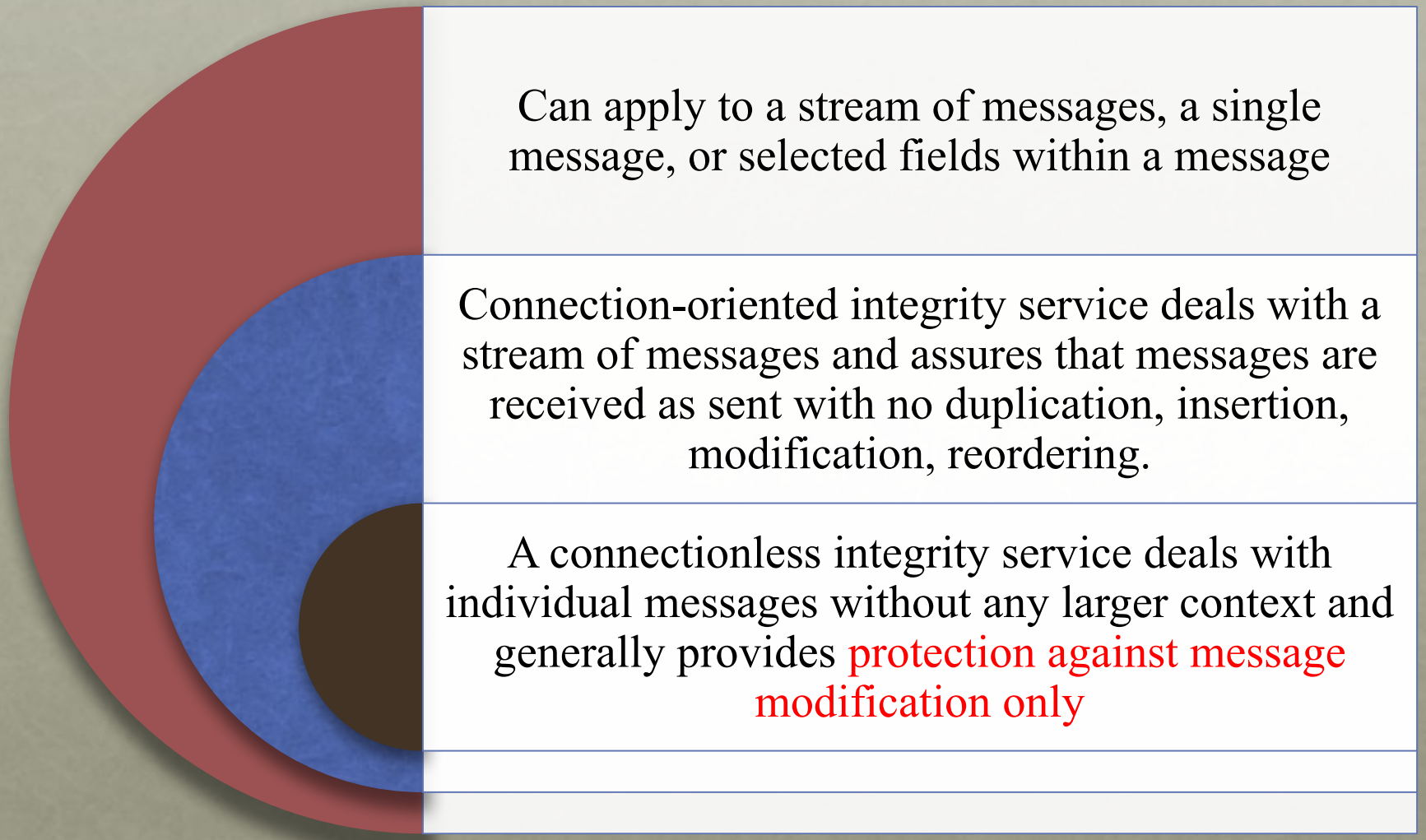
Access Control

- The 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 indentified, or authenticated, so that access rights can be tailored to the individual

Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time.
  - Narrower forms of service include the protection of a single message or even specific fields within a message
- 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

Data Integrity



- Integrity service relates to active attacks, we are concerned with detection
- 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,

Nonrepudiation

- the assurance that someone cannot deny the validity of something.
- Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged(unproven) sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Availability service

- Availability
  - 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

Model for Network Security

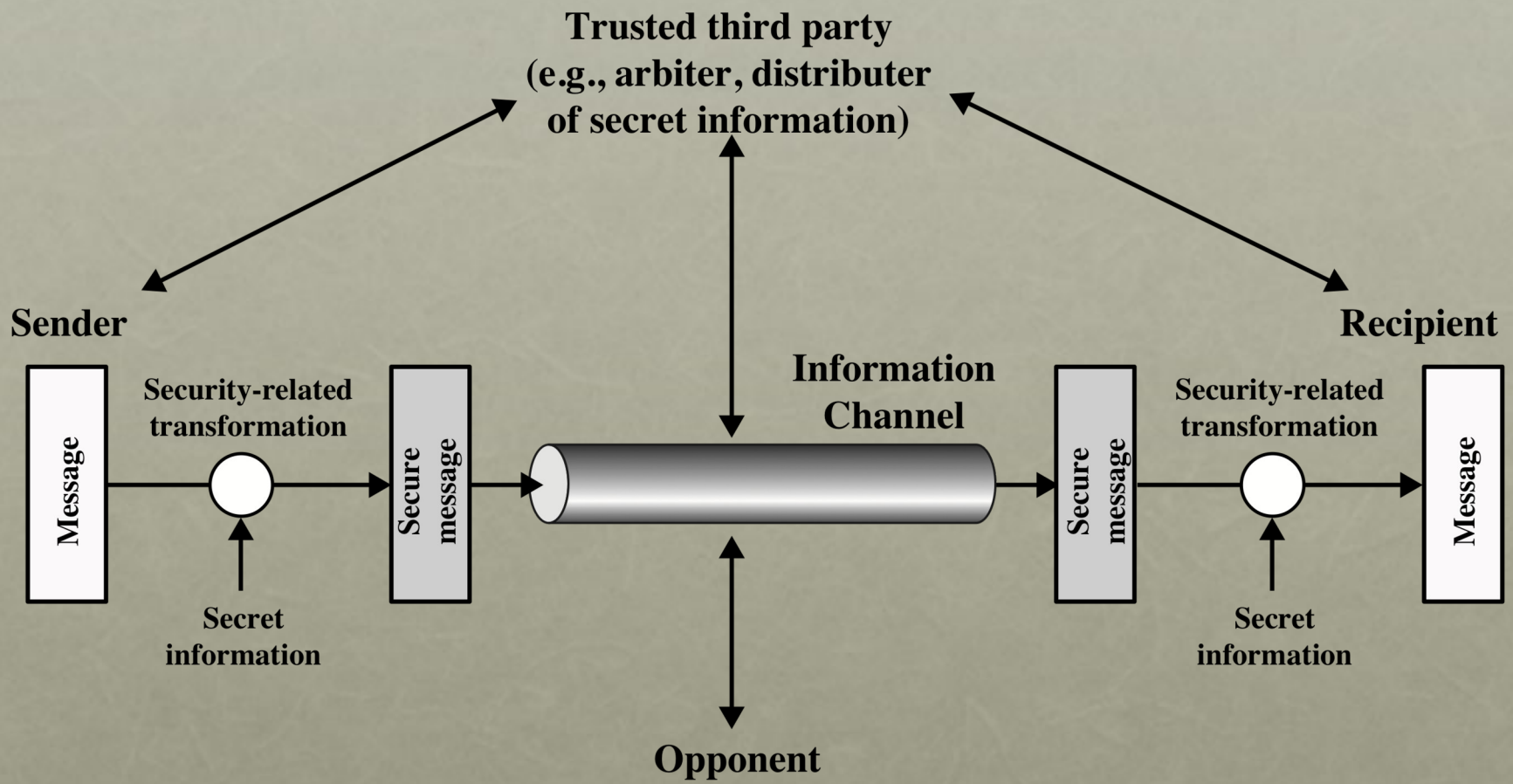


Figure 1.2 Model for Network Security

- A message is to be transferred from source to destination across some sort of Internet service.
- 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 .
- 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 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

- 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

Network Access Security Model

It is for cope with unwanted access .

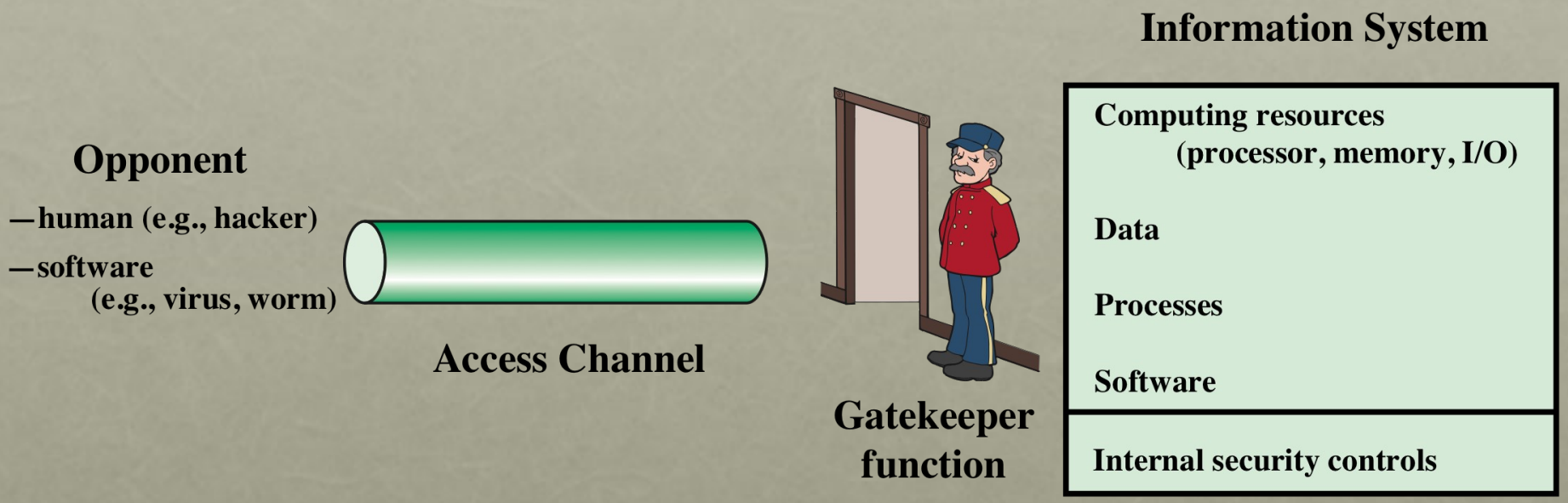
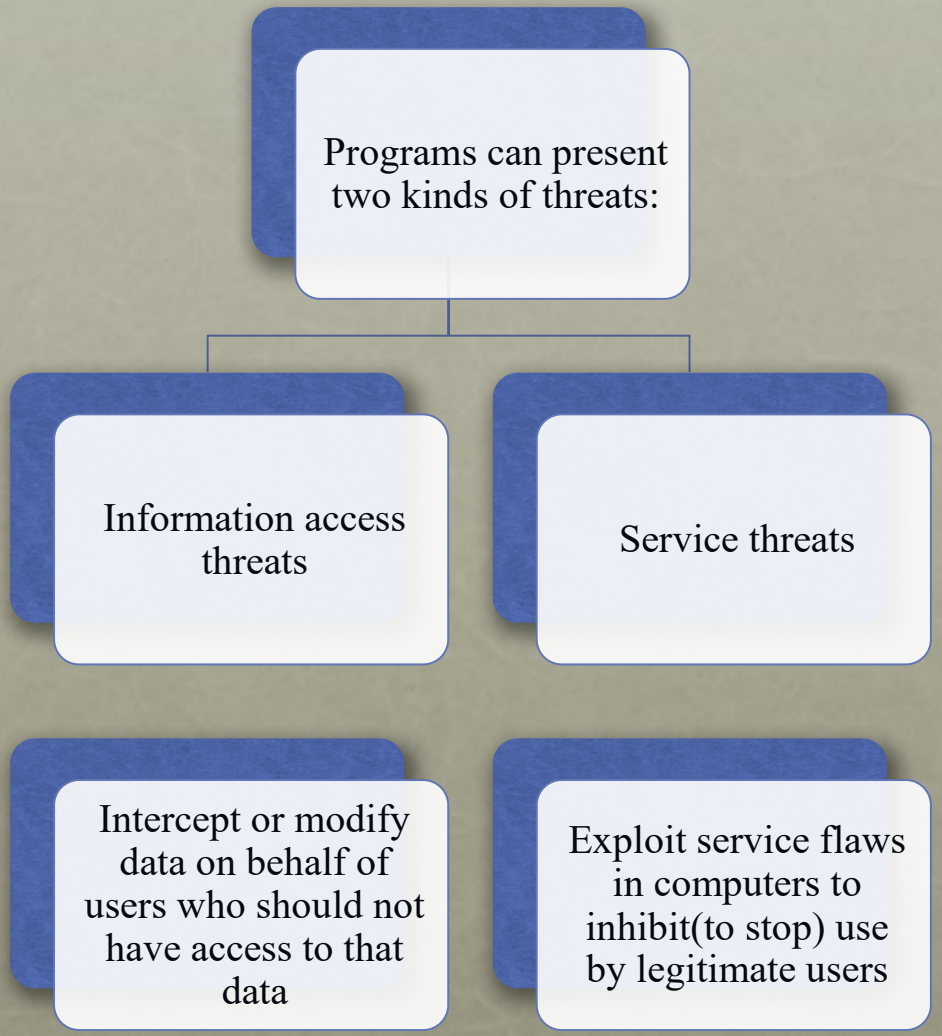


Figure 1.3 Network Access Security Model

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities(loop false) in the system and that can affect application programs as well as utility programs



- Viruses and worms are two examples of software attacks
- the security mechanisms needed to cope with unwanted access fall into two broad categories in Figure
- The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access except authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- Second layer if unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal security controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Summary

- Computer security concepts
  - Definition
  - Examples
  - Challenges
- The OSI security architecture
- Security attacks
  - Passive attacks
  - Active attacks
- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Security mechanisms
- Model for network security