

COMPUTER & NETWORK SECURITY

BEC714B

Course Objectives:

- **Preparation:** To prepare students with fundamental knowledge/ overview in the field of Network Security with knowledge of security mechanisms and services.
- **Core Competence:** To equip students with a basic foundation of Network Security by delivering the basics of Transport Level Security, Secure Socket Layer, Internet Protocol security, Intruders, Intrusion detection and Malicious Software, Firewalls, Firewall characteristics, Biasing and Configuration

Module-1 Syllabus (BEC714B)

- **Attacks on Computers and Computer Security:** Need for Security, Security Approaches, Principles of Security Types of Attacks. (Text2: Chapter1)

Security Mechanisms, Services and Attacks, A model for Network security (Text1: Chapter1: 3, 4, 5, 6)

TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 5th Edition, 2014, ISBN: 978-81-317- 6166-3 2.
2. Atul Kahate, "Cryptography and Network Security", TMH, 2003.

Course Outcomes: After studying this course, students will be able to:

- Explain network security services and mechanisms and explain security concepts
- Illustrate the concept of Transport Level Security and Secure Socket Layer.
- Explain Security concerns in Internet Protocol security
- Explain Intruders, Intrusion detection and Malicious Software
- Describe Firewalls, Firewall Characteristics, Biasing and Configuration

MODULE 1

Attacks on Computers and Computer Security

Attacks on Computers and Computer Security: Need for Security

Network security is the practice of **protecting a computer network** from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. People realized that data on computers is an extremely important aspect of modern life. Therefore, various areas in security began to gain prominence. **Two typical examples of such security mechanisms were as follows:**

- Provide a user **identification and password to every user**, and use that information to authenticate a user.
- **Encode information** stored in the databases in some fashion, so that it is **not visible** to users who do not have the right permission.

Example of information traveling from Client to server over the internet.

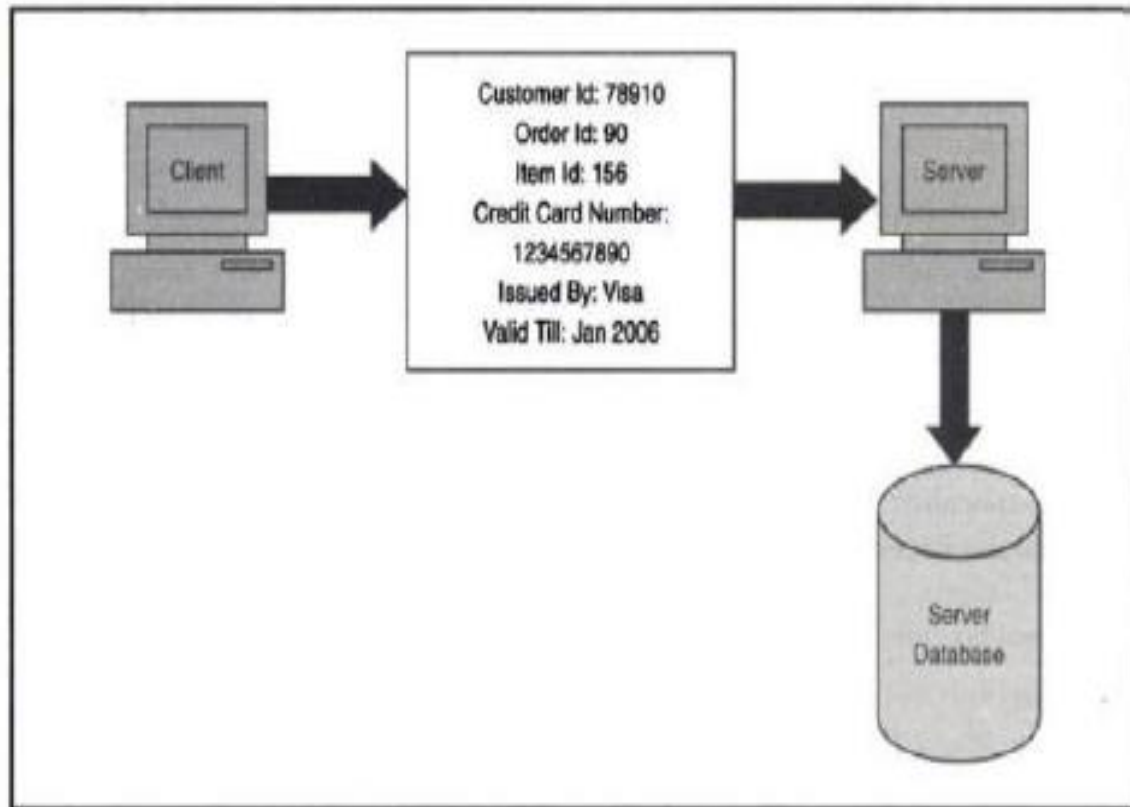


Fig 1.1 Information travelling from a client to a server over the internet

The various security holes in this are:

- An **intruder can capture** the credit card details as they travel from the client to the server.
- Once the merchant receives the credit card details and validates them so as to process the order and later obtain payments, the merchant stores the credit card details into its database. **An attacker can succeed in accessing this database and gain access to all the credit card numbers stored there.**

Modern Nature of attacks

The salient features of the modern nature of attacks are:

- **Automating attacks:** Humans dislike repetitive and difficult tasks. Automating them can cause destruction more rapidly. Rather than producing fake currency on a mas scale, modern thieves will excel in stealing a very low amount from million bank accounts in a matter of a few minutes.
- **Privacy concerns:** Collecting information about people and later misusing it is turning out to be a huge problem. The data mining applications gather, process and tabulate all sorts of details about individuals. People can illegally sell this information.
- **Distance does not matter:** Thieves would earlier attack banks, as banks had money. These days Money is in digital form and moves around using computer network. It is easier for modern thief to attempt an attack on the computer system of the bank, sitting at home

Security Approaches

Trusted systems

- A trusted system is a computer system that can be trusted to a specified extent to enforce a specified security policy.
- Trusted system uses the term reference monitor, an entity at the logical heart of the computer system which is responsible for all decisions across controls.
- The reference monitor should be tamperproof, always be invoked and small enough so that it can be independently tested.
- The mathematical foundation for trusted systems was provided by two independent, yet interrelated works. In 1974, a technique called as Bell-LaPadula model was devised which was a highly trustworthy computer system designed as a collection of objects (files, disks and printers) and subjects (users, processes or threads).

Security Models

An organization can take several approaches to implement its security model. The various approaches are:

- a) **No security:** This is the simplest model with no security at all.
- b) **Security through obscurity:** In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.
- c) **Host security:** In this scheme, the security for each host is enforced individually. This is a safe approach, but the complexity and diversity of modern sites/organizations makes the task harder and difficult to scale.
- d) **Network security:** Host security is tough to achieve as organization grows and becomes more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

Security Management Practices

Good security management practices always have a good security policy which takes care of 4 key aspects.

- 1) **Affordability:** How much money and efforts does this security implementation cost?
- 2) **Functionality:** What is the mechanism of providing security?
- 3) **Cultural issues:** Does the policy gel well with people's expectations, working style and beliefs?
- 4) **Legality:** Does the policy meet the legal requirements?

1.3 Principles of Security

The four chief principles of security are:

- 1) Confidentiality**
- 2) Authentication**
- 3) Integrity**
- 4) Non repudiation**

Two more principles that are linked to the overall system are:

- 5) Access control**
- 6) Availability**

1) Confidentiality

- The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.
- Confidentiality gets compromised if an unauthorized person is able to access a message. Example of compromising the confidentiality of a message is shown in Fig 1.2

Here the user of computer A sends a message to the user of computer B. Another user C gets access to this message, which is not desired, and therefore, defeats the purpose of confidentiality.

- **Example:-** A confidential email message sent by A to B, which is accessed by C without the permission or knowledge of A and B. This type of attack is called as **interception**.

“Interception causes loss of message confidentiality”

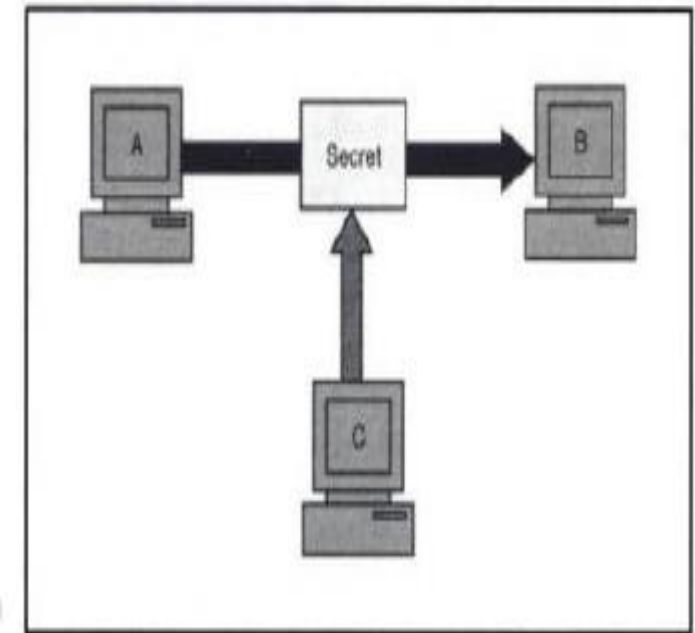


Fig 1.2 Loss of confidentiality

2) Authentication:

- Authentication establishes **proof of identities**.
- The authentication process ensures that the origin of an electronic message or document is correctly identified.
- For instance, suppose that user C sends an electronic document over the Internet to user B, posing as user A. How would user B know that the message has come from user C, who is posing as user A.

Example: User C posing as user A, sends a funds transfer request (from A's account to C's account) to bank B. The bank will transfer the funds from A's account to C's account, thinking that user A has requested for the funds transfer. This type of attack is called as **fabrication**.

- "Fabrication is possible in the absence of proper authentication mechanisms"

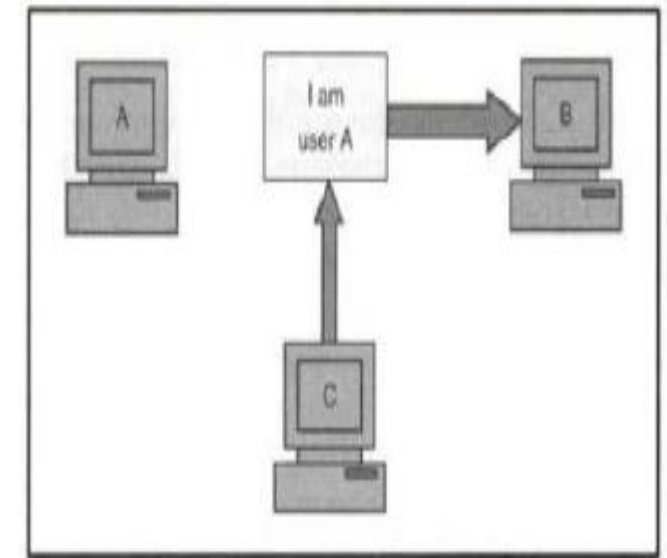


Fig 1.3 Absence of authentication

3) Integrity:

➤ When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, the integrity of the message is lost.

➤ **Example:** Suppose you write a cheque for \$100 to pay for the goods bought from the store, but in the account statement it is observed that the cheque resulted in a payment of \$1000! This is the case of loss of message integrity.

➤ Fig 1.4 demonstrates loss of integrity. User C tampers (modifies) a message originally sent by user A, which is actually destined for user B.

➤ User C somehow manages to access the message, change its contents and send the changed message to user B. Neither A nor B knows that the contents of the message were changed after user A had sent it. This type of attack is called as **modification**.

➤ “Modification causes loss of message integrity”

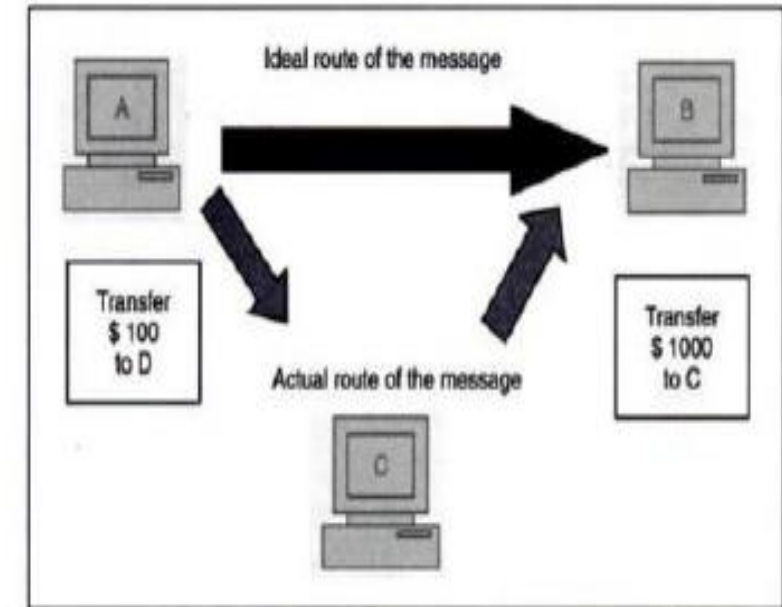


Fig 1.4 Loss of integrity

4) Non repudiation:

- There are situations where a user sends a message and later refuses that the message was sent. This is repudiation (refuse to accept).
- **Example:** User A could send a fund transfer request to bank B over the internet. After the bank performs the funds transfer as per A's request, A could claim that he never sent the fund transfer request to the bank.
- Thus, A repudiates, or denies the fund transfer instruction. The principle of non-repudiation defeats such possibilities of denying something, having done it. "Non repudiation does not allow the sender of a message to refuse the claim of not sending that message".

5) Access control:

- The principle of access control determines who should be able to access what. For instance, we should be able to specify that user A can view the records in a database, but cannot update them. However, another user B might be allowed to make updates as well. An access control mechanism can be set up to ensure this.
- Access control is broadly related to two areas: role management and rule management.
- **Role management** concentrates on the user side (which user can do what) **Rule management** focuses on the resources side (which resource is accessible, and under what circumstances).
- Based on the decisions taken here, an access control matrix is prepared, which lists the users against a list of items they can access (it can say that user A can write to file X, but can only update files Y and Z). An **access control list (ACL)** is a subset of an access control matrix. Access control specifies and controls who can access what."

6) Availability:

- The principle of availability states that resources (information) should be available to authorized parties at all times.
- **Example:** Due to the intentional actions of another unauthorized user C, an authorized user A may not be able to contact a server computer B as shown in fig 1.5.
- This would defeat the principle of availability. Such an attack is called as **interruption**.
- “Interruption puts the availability of resources in danger”

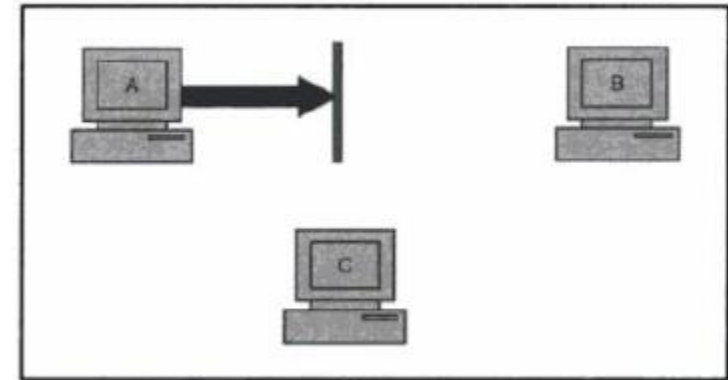


Fig 1.5 Attack on availability

7) Ethical and Legal issues:

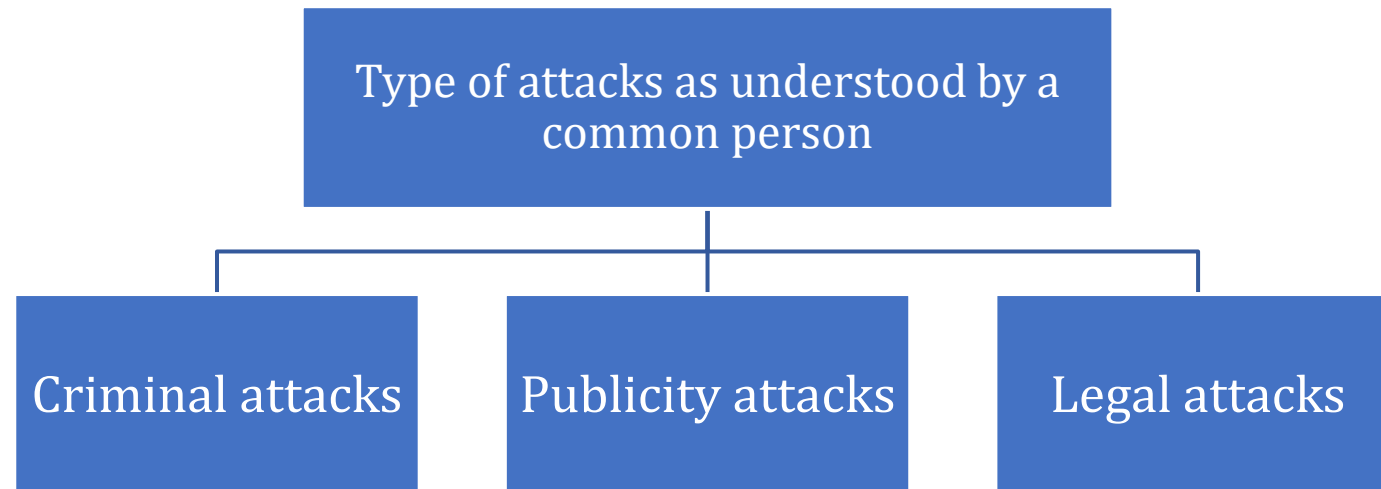
- The ethical issues in security systems are classified into four categories:
 - Privacy – deals with the right of an individual to control personal information.
 - Accuracy – deals about the responsibility for the authenticity, fidelity and accuracy of information.
 - Property – talks about the owner of the information and about who controls access.
 - Accessibility – deals with the issue of type of information an organization has the right to collect.

- While dealing with legal issues, there is a hierarchy of regulatory bodies that govern the legality of information security which can be classified as follows:
 - International -e.g International Cybercrime Treaty
 - Federal – e.g. FERPA, Patriot Act
 - State – e.g. UCITA
 - Organization – e.g. Computer use policy

TYPES OF ATTACKS

Attacks: A general view

Attacks can be classified into two views : **A common man's view** and **technological view**.



Criminal Attack	Description
Fraud	Modern fraud attacks concentrate on manipulating some aspects of electronic currency, credit cards, electronic stock certificates,cheques, letters of credit, purchase order, ATMs etc.
Scams	Some forms of scams are sales of services, auctions, multi- level marketing schemes, general merchandise and business opportunities etc. People are tempted to send money in return of great profits, but end up losing their money.
Destruction	The main motive behind these attacks is some sort of grudge. Example: Some unhappy employees attack their own organization; terrorists strike at bigger levels
Identity theft	An attacker does not steal anything from a legitimate user,instead he becomes that legitimate user! Example, it is much easier to manage to get the password of someone else's bank account or to actually be able to get a credit card on someone else's name. That privilege can be misused until it gets detected.
Intellectual property theft	Intellectual property theft ranges from stealing companies' trade secrets, databases, digital music and videos, electronic documents and books, Identity theft, Intellectual property theft software and etc.

➤ **Publicity Attacks**

- Occurs because **the attackers want to see their names appear on television, news channels and newspapers** for publicity. These types of attackers are usually not hardcore criminals.
- They are people such as students in universities or employees in large organizations, who seek publicity by adopting a novel approach of attacking computer systems.

➤ **Legal attacks**

- This form of attack is quite novel and unique. **The attacker tries to make the judge or jury doubtful about the security of a computer system.**
- The attacker attacks the computer system and the attacked party (Bank or organization) manages to take the attacker to the court. **The attacker tries to convince the judge that there is inherent weakness in the computer security system and exploits the weakness of the judge.**

Attacks: A Technical view

The types of attacks on computers and network systems can be classified into two categories:

- Theoretical concepts behind these attacks
- Practical approaches used by the attackers.

a) Theoretical Concepts

The principles of security face threat from various attacks. These attacks are classified into four categories, as mentioned namely:

➤ **Interception -**

- This attack results from violating confidentiality.
- It means that an **unauthorized party has gained access to a resource**. The party can be a person, program or computer-based system.
- Example: Copying of data or programs and listening to network traffic.

➤ **Fabrication**

- This attack results from violating authentication.
- This **involves creation of illegal objects on a computer system.**
- Example: The attacker may add fake records to a database.

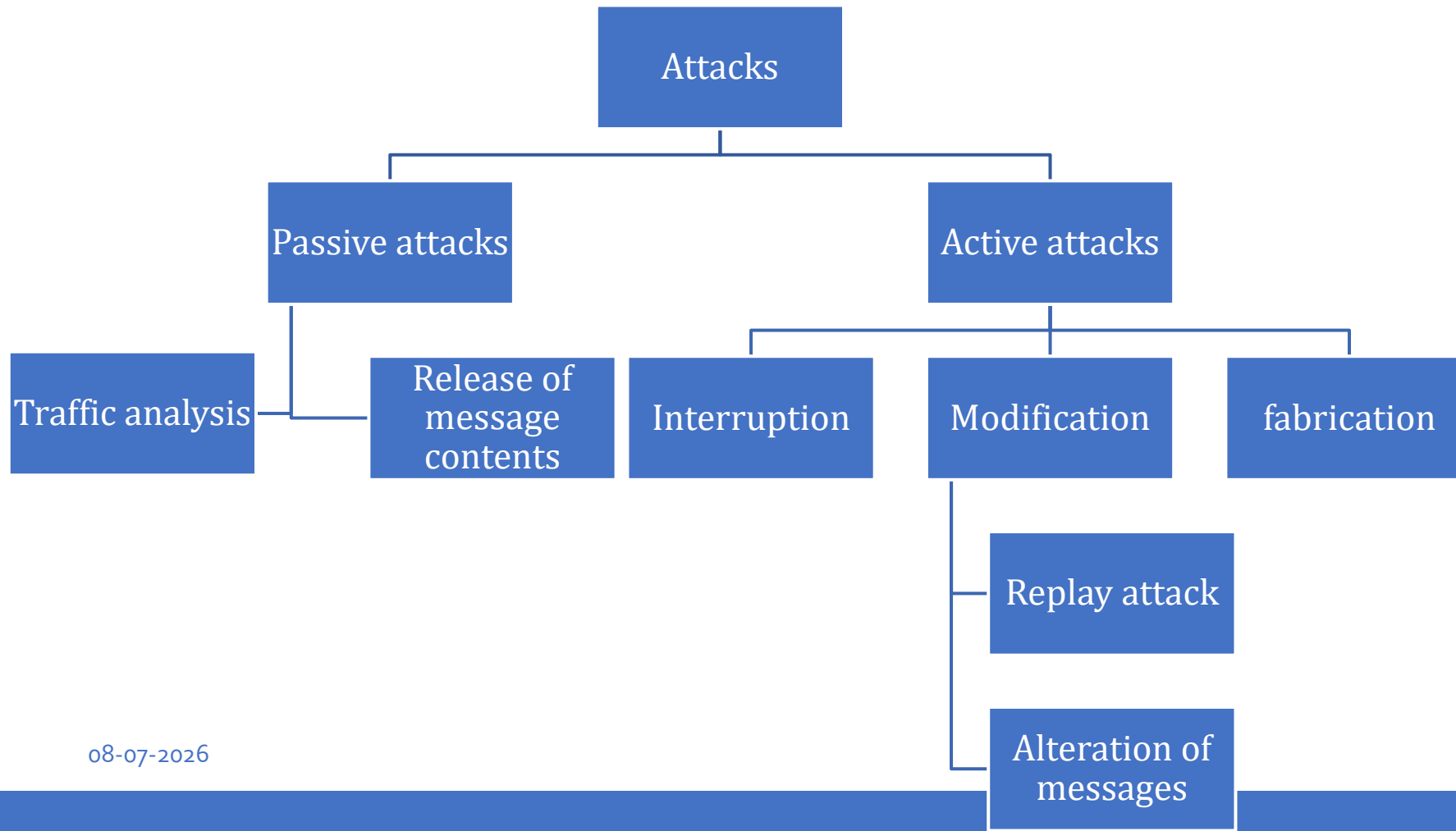
➤ **Modification**

- This attack results from violating Integrity. The attacker may **modify the values in a database.**

➤ **Interruption**

- This attack results from violating availability.
- The resource **becomes unavailable, lost or unusable.**
- Example: Causing problems to a hardware device, erasing program, data or operating system components.

These attacks are further grouped into two types:



Passive attacks

- Passive attacks are those, **wherein the attacker indulges in eavesdropping or monitoring of data transmission.**
- The attacker aims to obtain information that is in transit.
- The term passive indicates that the attacker **does not attempt to perform any modifications to the data.**
- Passive attacks are harder to detect.
- The general approach to deal with passive attacks is to think about prevention, rather than detection or corrective actions.
- **Passive attacks can be further classified into two sub-categories. These categories are:**
 - **Release of message contents**
 - **Traffic analysis.**

Release of message contents:

- When a confidential email message is sent, **it is desired that only the recipient is able to access it**. Otherwise, the contents of the message are released against our wishes to someone else.
- **Using certain security mechanisms**, we can prevent release of message contents. For example, we can encode messages using a code language, so that only the desired parties understand the contents of a message, because only they know the code language.
- However, if many such messages are passing through, a passive attacker could try to figure out similarities between them to come up with some sort of pattern that provides the attacker some clues regarding the communication that is taking place.
- Such attempts of analysing (encoded) messages to come up with likely patterns are the work of the **traffic analysis attack**.

Active attacks

- **The active attacks are based on modification of the original message** in some manner or the creation of a false message. These attacks cannot be prevented easily.
- They can be detected with some effort and attempts can be made to recover from them. These attacks can be in the form of **interruption, modification and fabrication**.
- In active attacks, the contents of the original message are modified in some way.
- Trying to pose as another entity involves **masquerade (interruption)** attacks.
- Modification attacks can be classified further into **replay attacks** and **alteration of messages**.
- Fabrication causes **Denial Of Service (DOS)** attacks.

Masquerade is caused when an unauthorized entity pretends to be another entity.

- Example: **User C might pose as user A and send a message to user B.** User B might be led to believe that the message indeed came from user A. In masquerade attacks, an entity poses as another entity.
- Example, the attack may involve capturing the user's authentication sequence (e.g. user ID and password). Later those details can be used to gain illegal access to the computer system.

Replay attack is caused when a user captures a sequence of events or some data units and re-sends them.

- For instance, suppose user **A wants to transfer some amount to user C's bank account.**
- Both users A and C have accounts with bank B. User A might send an electronic message to bank B, requesting for the funds transfer.
- User C could capture this message and send a second copy of the same to bank B. Bank B would have no idea that this is an unauthorized message and would treat this as a second and different, funds transfer request from user A. Therefore, user C would get the benefit of the funds transfer twice: once authorized, once through a replay attack.

Alteration of messages involves some change to the original message.

- For instance, suppose user A sends an electronic message Transfer \$100 to D's account to bank B. User C might capture this and change it to Transfer \$1000 to C's account.
- Both the beneficiary and the amount have been changed - instead, only one of these could have also caused alteration of the message.

Denial Of Service (DOS) attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

- For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, **so as to flood the network and deny other legitimate users from using the network facilities.**

Chapter 2

Security Mechanisms, Services and Attacks, A model for Network security

(Text1: Chapter1: 3, 4, 5, 6).

Security Mechanisms Table lists the **security mechanisms defined in X.800**. The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

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.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

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.

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

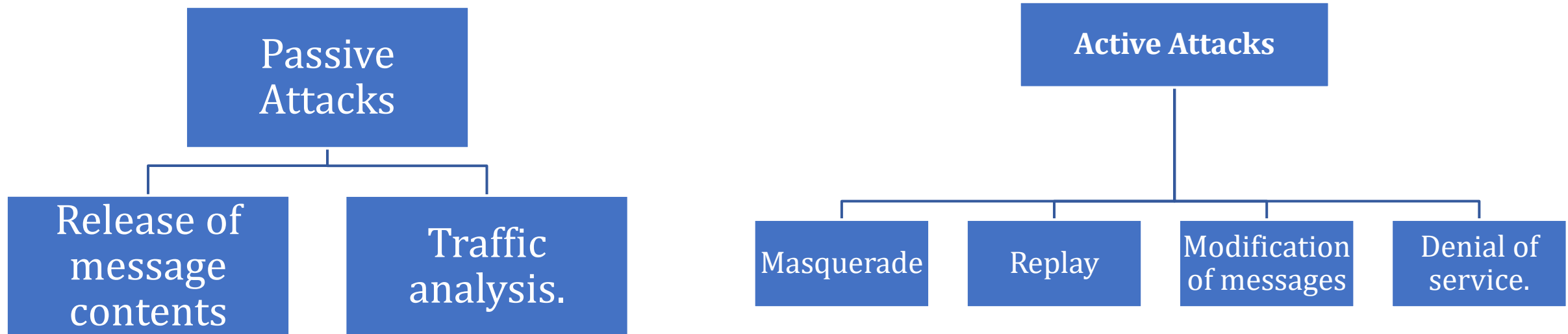
The use of a trusted third party to assure certain properties of a data exchange.

Table is 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			

Security Attacks



The 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.**

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 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.

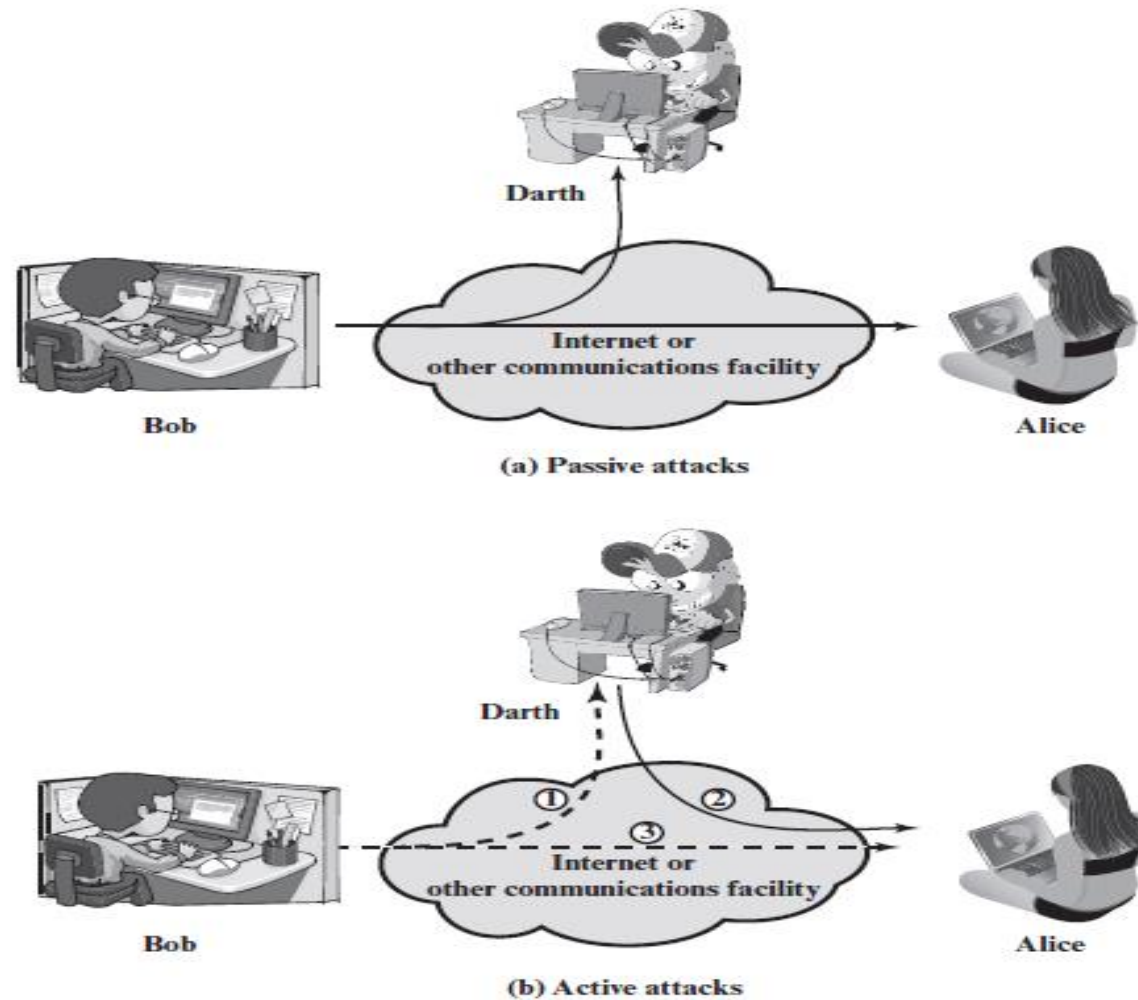


Figure 1.2 Security Attacks

A **masquerade** takes place when **one entity pretends to be a different entity** (path 2 of Figure 1.2b 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**.

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 simply 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). 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*.”

The **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**.

Security Services

Table 1.2 Security Services (X.800)

AUTHENTICATION	DATA INTEGRITY
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.	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.
ACCESS CONTROL	NONREPUDIATION
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).	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.
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.	

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.**

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.

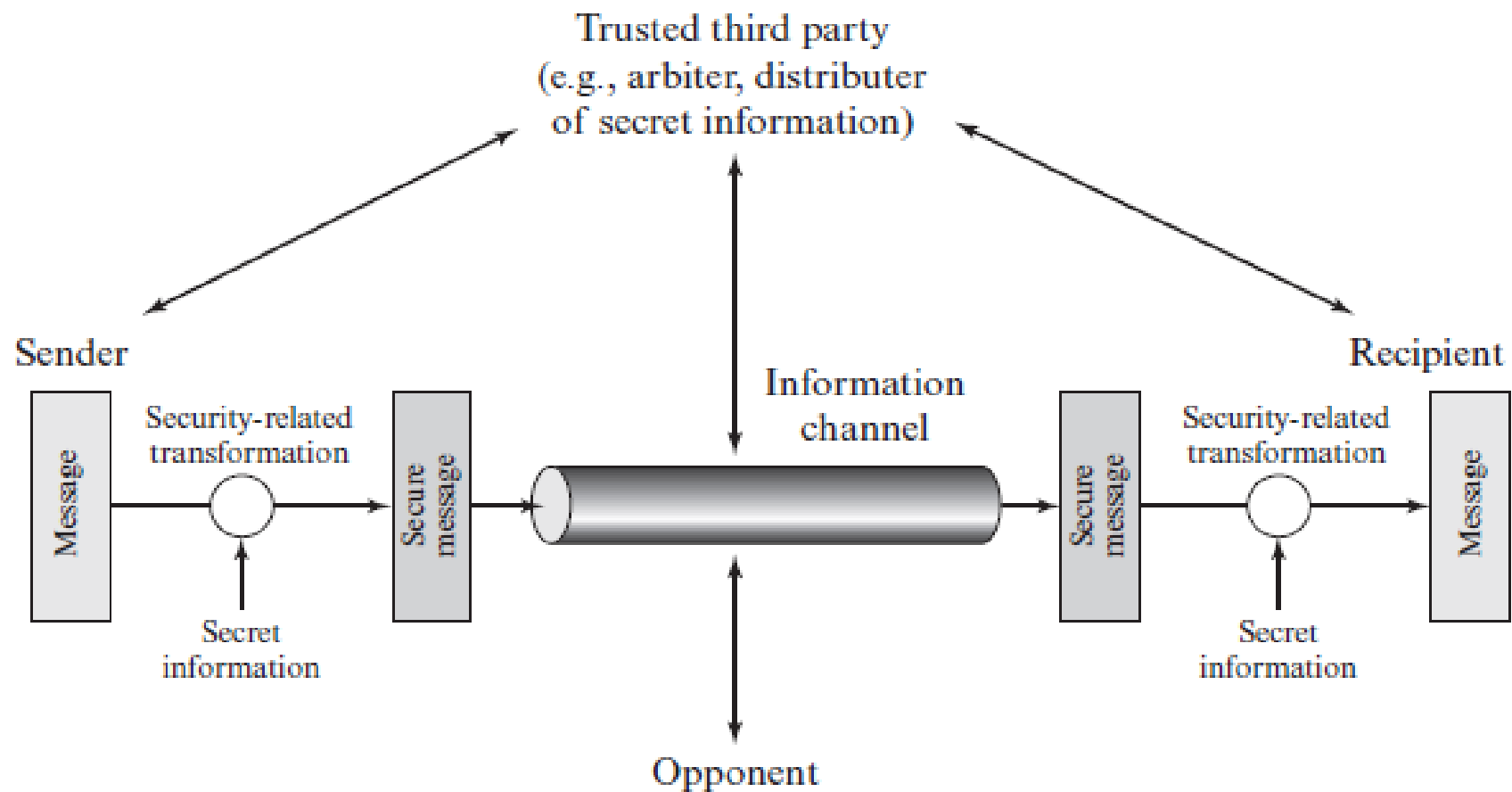


Figure 1.5 Model for Network Security

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.

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..

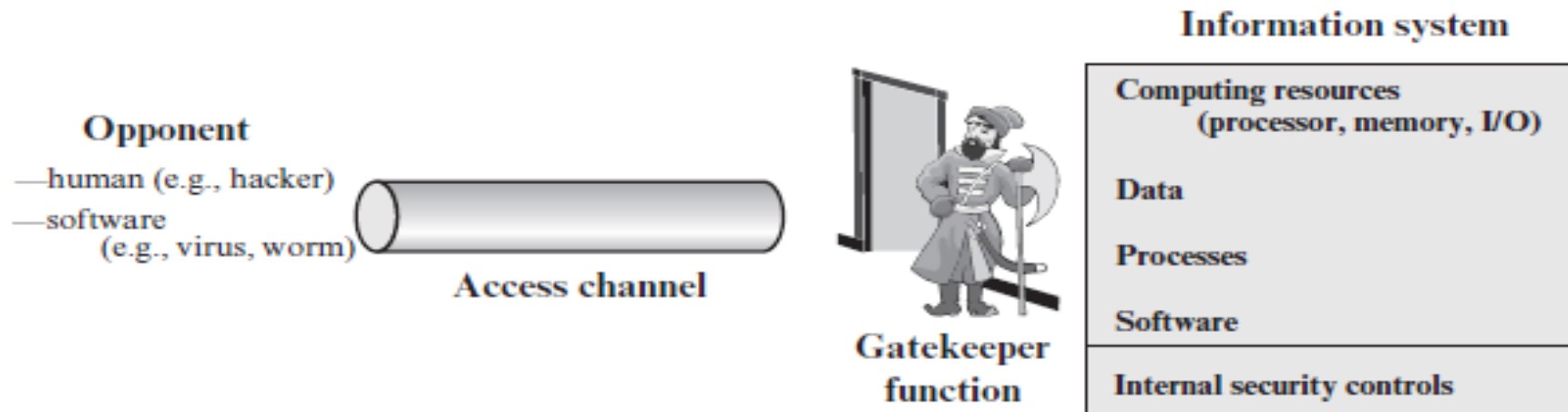


Figure 1.6 Network Access Security Model