

MODULE-1**Attacks on Computers and Computer Security:**

Need for Security, Security Approaches, Principles of Security, Types of Attacks.(Text 2)

Security Mechanisms, Services and Attacks, A model for Network security (Text1)

TEXT BOOK:

1. William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325-1877-3 (Text1: Chapter1: 3, 4, 5, 6)
2. Atul Kahate, “Cryptography and Network Security”, TMH, 2003. (Text2: Chapter1)

REFERENCE BOOKS:

1. Cryptography and Network Security, Behrouz A. Forouzan, TMH, 2007.
2. Cryptography and Network Security, Atul Kahate, TMH, 2003.

1.1 INTRODUCTION

- It is essential to know what we are trying to protect.
- What are the various dangers when we use computers, computer networks, and the biggest network of them all, the Internet?
- What are the likely pitfalls?
- What can happen if we do not set up the right security policies, framework and technology implementations?.

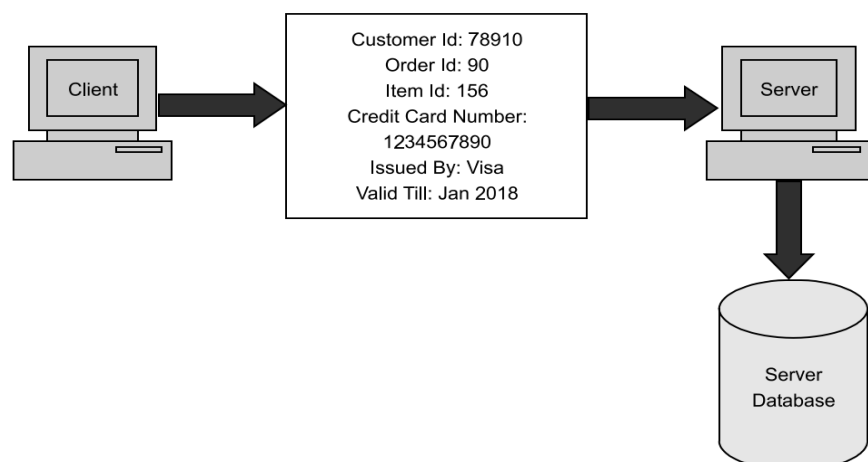
1.2 THE NEED FOR SECURITY

1.2.1 Basic Concepts

Most previous computer applications had no, or at best, very little security. This continued for a number of years until the importance of data was truly realized. Until then, computer data was considered to be useful, but not something to be protected. 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.

There were many examples of what could happen if there was insufficient security built in applications developed for the Internet. Figure 1.1 shows such an example of what can happen



when you use your credit card for making purchases over the Internet. From the user's computer, the user details such as user id, order details such as order id and item id, and payment details

such as credit-card information travel across the Internet to the server (i.e. to the merchant's computer). The merchant's server stores these details in its database.

1.2.2 Modern Nature of Attacks

1. Automating Attacks

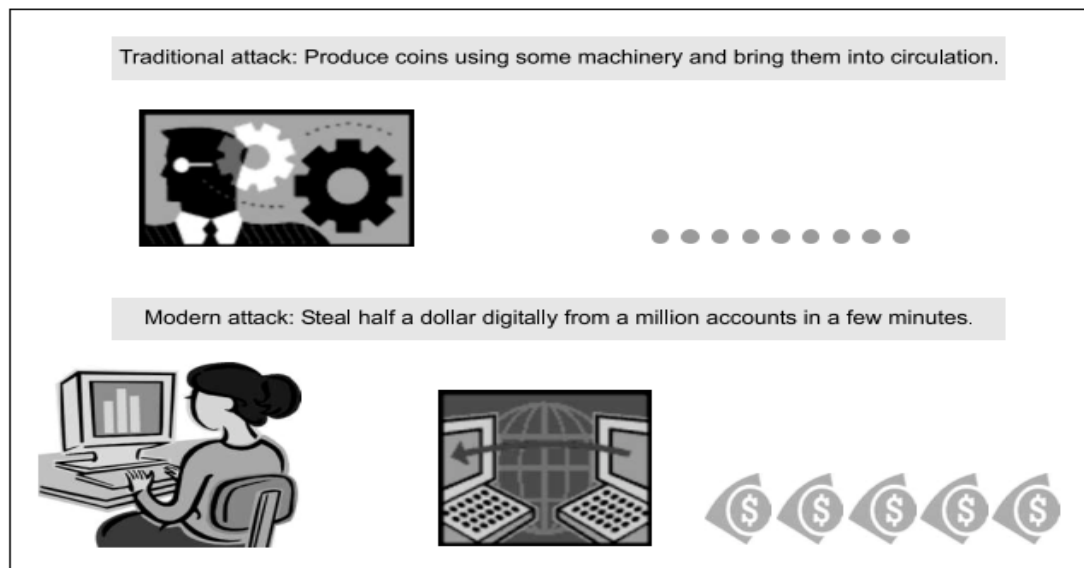


Fig. 1.2 The changing nature of attacks due to automation

The morale of the story is:

Humans dislike mundane and repetitive tasks. Automating them can cause financial destruction

or a security nuisance quite rapidly.

2. Privacy Concerns

Collecting information about people and later (mis)using it is turning out to be a huge problem these days. The so-called data mining applications gather, process, and tabulate all sorts of details about individuals. People can then illegally sell this information.

3. Distance Does not Matter

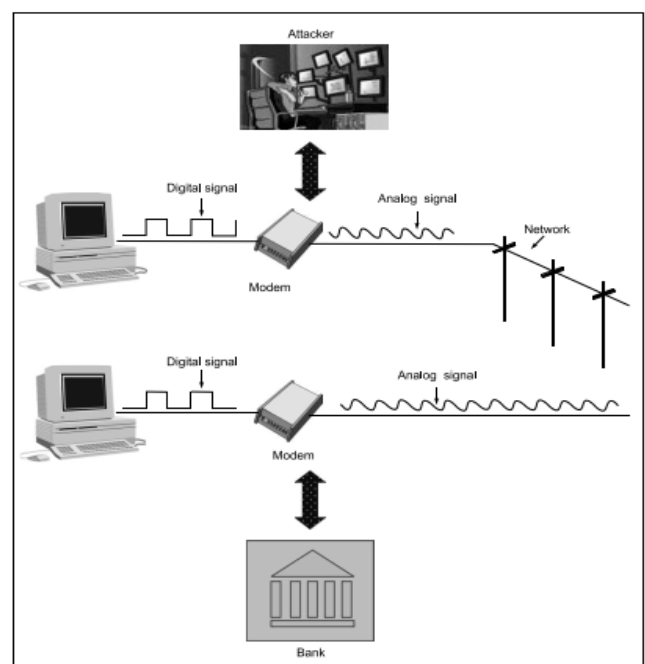


Fig. 1.3 Attacks can now be launched from a distance

1.3 SECURITY APPROACHES

1.3.1 Trusted Systems

A trusted system is a computer system that can be trusted to a specified extent to enforce a specific security policy.

Trusted systems were initially of primary interest to the military. However, these days, they have spanned across various areas, most prominently in the banking and financial community, but the concept never caught on. Trusted systems often use the term reference monitor. This is an entity that is at the logical heart of the computer system. It is mainly responsible for all the decisions related to access controls.

Naturally, following are the expectations from the reference monitor:

- (a) It should be tamper-proof.
- (b) It should always be invoked.
- (c) It should be small enough so that it can be tested independently.

1.3.2 Security Models

An organization can take several approaches to implement its security model. Let us summarize these approaches.

1. No Security

In this simplest case, the approach could be a decision to implement no security at all.

2. 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.

3. Host Security

In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organizations makes the task even harder.

4. Network Security

Host security is tough to achieve as organizations grow and become 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.

1.3.3 Security-Management Practices

Good security-management practices always talk of a security policy being in place. Putting a security policy in place is actually quite tough. A good security policy and its proper implementation go a long way in ensuring adequate security-management practices. A good security policy generally takes care of four key aspects, as follows.

- **Affordability** How much money and effort does this security implementation cost?
- **Functionality** What is the mechanism of providing security?
- **Cultural Issues** Does the policy complement the people's expectations, working style and beliefs?
- **Legality** Does the policy meet the legal requirements?

Once a security policy is in place, the following points should be ensured.

- (a) Explanation of the policy to all concerned.
- (b) Outline everybody's responsibilities.
- (c) Use simple language in all communications.
- (d) Accountability should be established.
- (e) Provide for exceptions and periodic reviews

1.4 PRINCIPLES OF SECURITY

Let us assume that a person A wants to send a cheque worth \$100 to another person B. Normally, what are the factors that A and B will think of, in such a case? A will write the cheque for \$100, put it inside an envelope, and send it to B.

- A will like to ensure that no one except B gets the envelope, and even if someone else gets it, he/she does not come to know about the cheque. This is the principle of confidentiality.
- A and B will further like to make sure that no one can tamper with the contents of the cheque (such as its amount, date, signature, name of the payee, etc.). This is the principle of integrity.
- B would like to be assured that the check has indeed come from A, and not from someone else posing as A (as it could be a fake check in that case). This is the principle of authentication.
- What will happen tomorrow if B deposits the check in his/her account, the money is transferred from A's account to B's account, and then A refuses having written/sent the check? The court of law will use A's signature to disallow A to refute this claim, and settle the dispute. This is the principle of non-repudiation.

These are the four chief principles of security.

1.4.1 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.

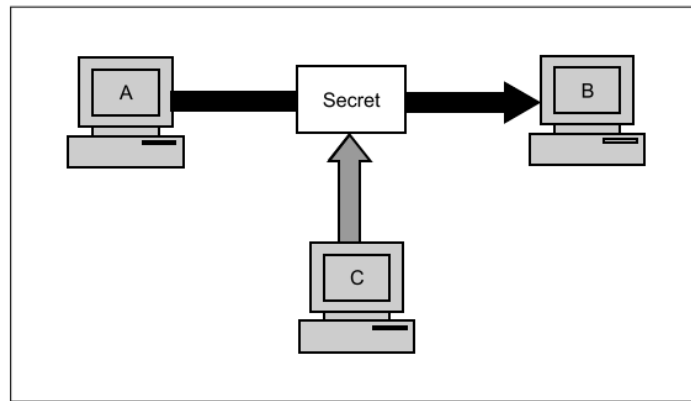


Fig. 1.4 Loss of confidentiality

Fig. 1.4. Here, the user of computer A sends a message to the user of computer B. (Actually, from here onwards, we shall use the term A to mean the user A, B to mean user B, etc., although we shall just show the computers of users A, B, etc.).

Interception causes loss of message confidentiality.

1.4.2 Authentication

Authentication mechanisms help establish proof of identities.

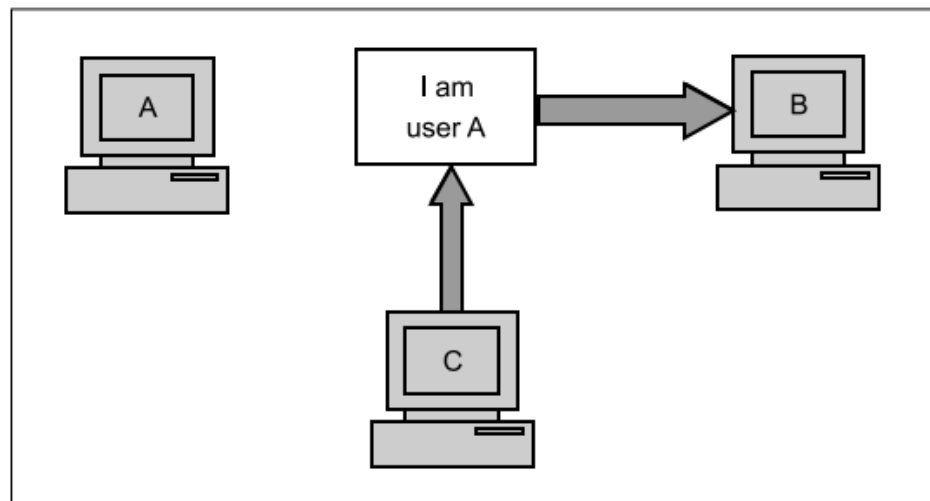


Fig. 1.5 Absence of authentication

This type of attack is called fabrication.

Fabrication is possible in absence of proper authentication mechanisms

1.4.3 Integrity

This type of attack is called Modification. Modification causes loss of message integrity.

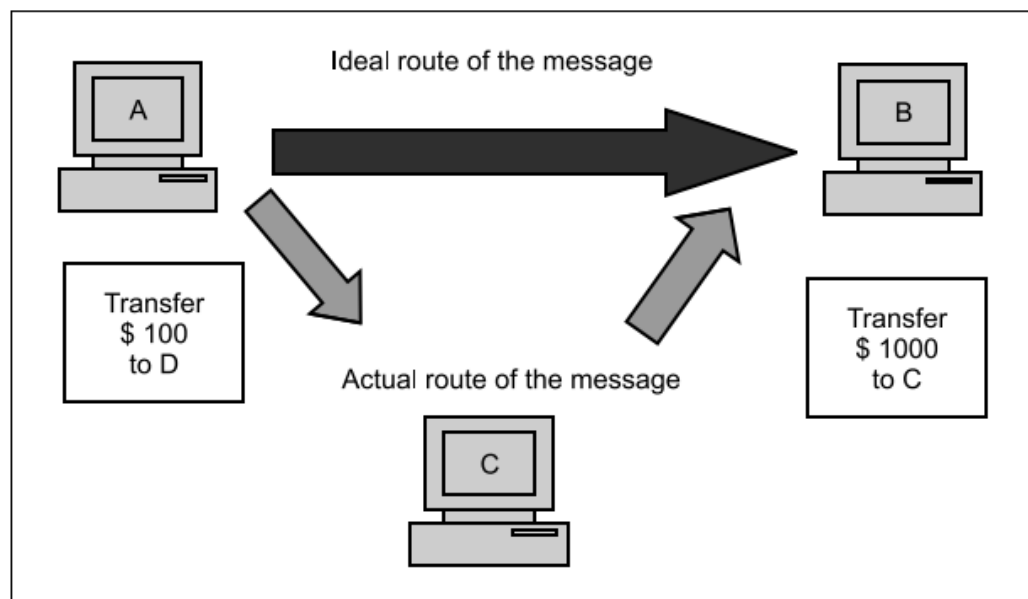


Fig. 1.6 Loss of integrity

1.4.4 Non-repudiation

non-repudiation

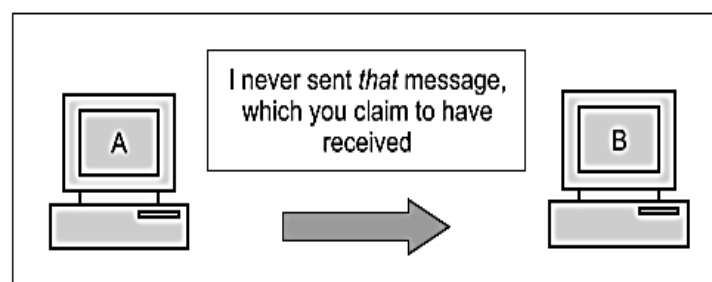


Fig. 1.7 Establishing non-repudiation

Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

1.4.5 Access Control

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), whereas rule management focuses on the resources side (which resource is accessible, and under what circumstances). An Access Control List (ACL) is a subset of an access-control matrix. Access control specifies and controls who can access what.

1.4.6 Availability

An attack is called interruption. Interruption puts the availability of resources in danger.

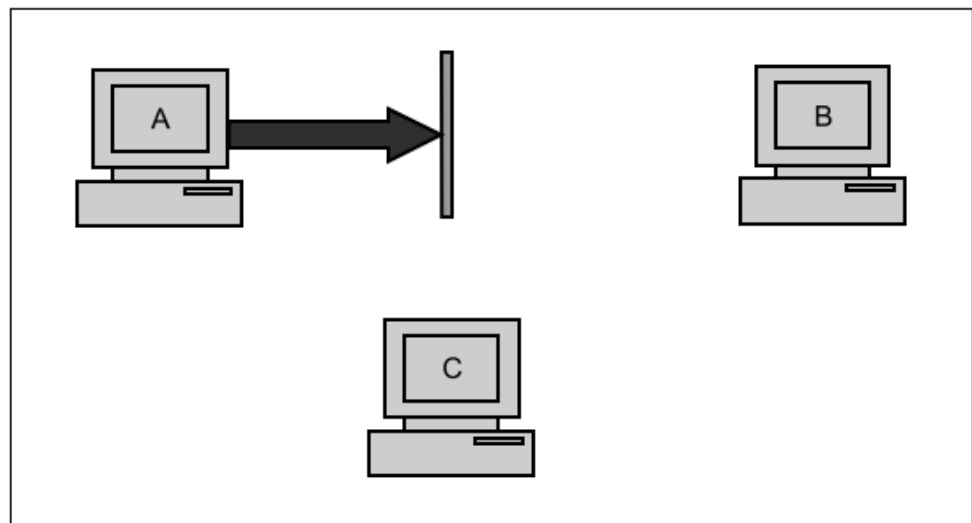


Fig. 1.8 Attack on availability

A very less known standard on similar lines is the OSI standard for Security Model (titled OSI Security Model 7498-2). This also defines seven layers of security in the form of

- Authentication
- Access control
- Non-repudiation
- Data integrity
- Confidentiality
- Assurance or availability
- Notarization or signature

1.4.7 Ethical and Legal Issues

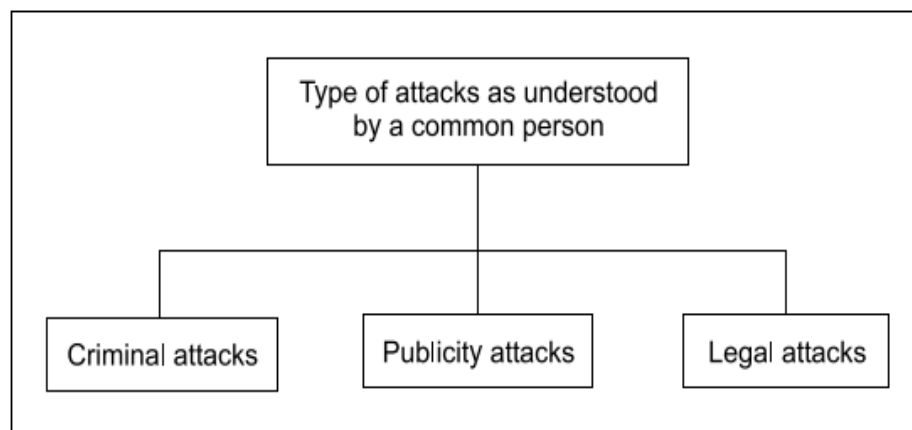
Classically, the ethical issues in security systems are classified into the following four categories:

- Privacy -This deals with the right of an individual to control personal information.
- Accuracy - talks about the responsibility for the authenticity, fidelity, and accuracy of information.
- Property- Here, we find out the owner of the information. We also talk about who controls access.
- Accessibility -This deals with the issue of what information does an organization have the right to

collect? And in that situation, it also expects to know what the measures are, which will safeguard against any unforeseen eventualities.

1.5 TYPES OF ATTACKS

Attacks: A General View



1.5.2 Attacks: A Technical View

From a technical point of view, we can classify the types of attacks on computers and network systems into two categories for better understanding:

- (a) Theoretical concepts behind these attacks, and
- (b) Practical approaches used by the attackers.

Theoretical Concepts

- Interception
- Fabrication
- Modification
- Interruption

These attacks are further grouped into two types: passive attacks and active attacks, as shown in Fig. 1.10.

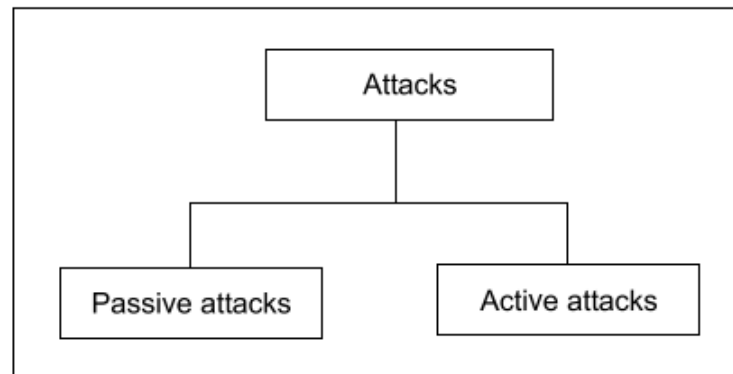


Fig. 1.10 Types of attacks

Passive attacks do not involve any modifications to the contents of an original message.

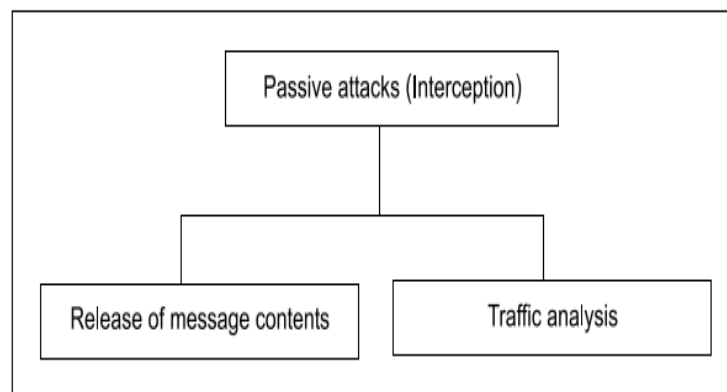


Fig. 1.11 Passive attacks

Figure 1.11 shows further classification of passive attacks into two sub-categories. These categories are, namely release of message contents and traffic analysis.

Release of message contents is quite simple to understand. When you send a confidential email message to your friend, you desire that only he/she be able to access it.

Traffic-analysis attack.

Active Attacks

In active attacks, the contents of the original message are modified in some way.

- Trying to pose as another entity involves masquerade attacks.
- Modification attacks can be classified further into replay attacks and alteration of messages.
- Fabrication causes Denial Of Service (DOS) attacks.

This classification is shown in Fig. 1.12.

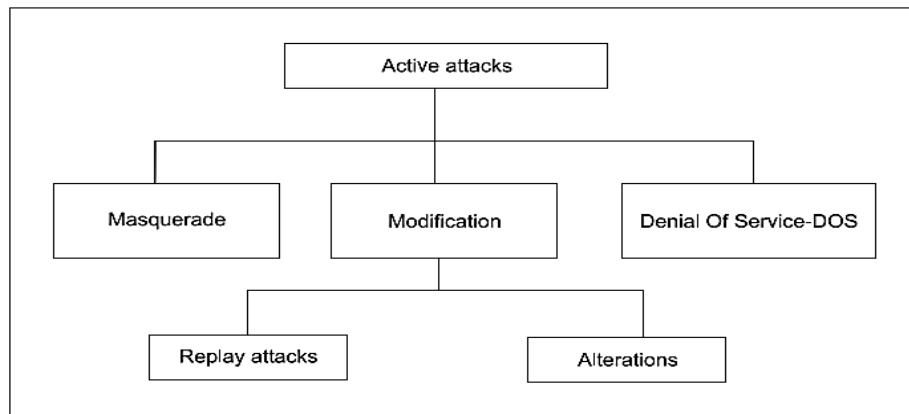


Fig. 1.12 Active attacks

1.5.3 The Practical Side of Attacks

The attacks discussed earlier can come in a number of forms in real life. They can be classified into two broad categories: application-level attacks and network-level attacks, as shown in Fig. 1.13.

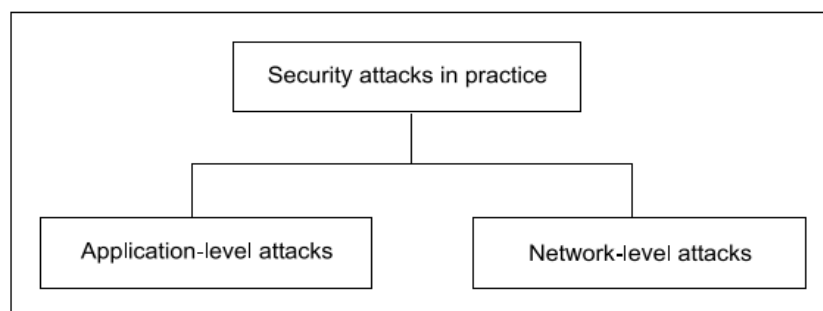


Fig. 1.13 Practical side of attacks

1.5.4 Programs that Attack

1. Virus

One can launch an application-level attack or a network level attack using a virus. In simple terms, a virus is a piece of program code that attaches itself to legitimate program code, and runs when the legitimate program runs.

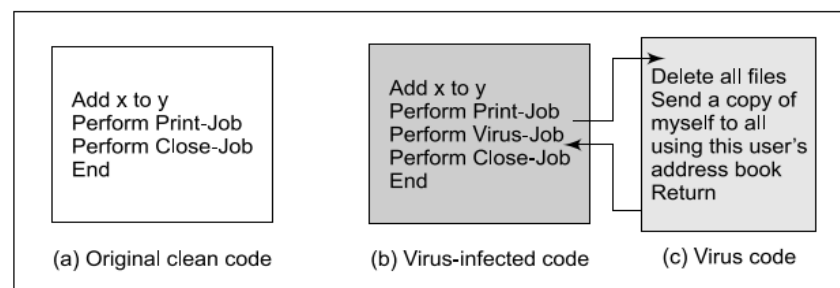


Fig. 1.14 Virus

A virus is a computer program that attaches itself to another legitimate program, and causes damage to the computer system or to the network.

During its lifetime, a virus goes through four phases:

- (a) Dormant Phase
- (b) Propagation Phase
- (c) Triggering Phase
- (d) Execution Phase

Viruses can be classified into the following categories:

- (a) **Parasitic Virus** This is the most common form of virus. Such a virus attaches itself to executable files and keeps replicating. Whenever the infected file is executed, the virus looks for other executable files to attach itself and spread.
- (b) **Memory-resident Virus** This type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.
- (c) **Boot sector Virus** This type of virus infects the master boot record of the disk and spreads on the disk when the operating system starts booting the computer.
- (d) **Stealth Virus** This virus has intelligence built in, which prevents anti-virus software programs from detecting it.
- (e) **Polymorphic Virus** A virus that keeps changing its signature (i.e. identity) on every execution, making it very difficult to detect.
- (f) **Metamorphic Virus** In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

2. Worm

A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.

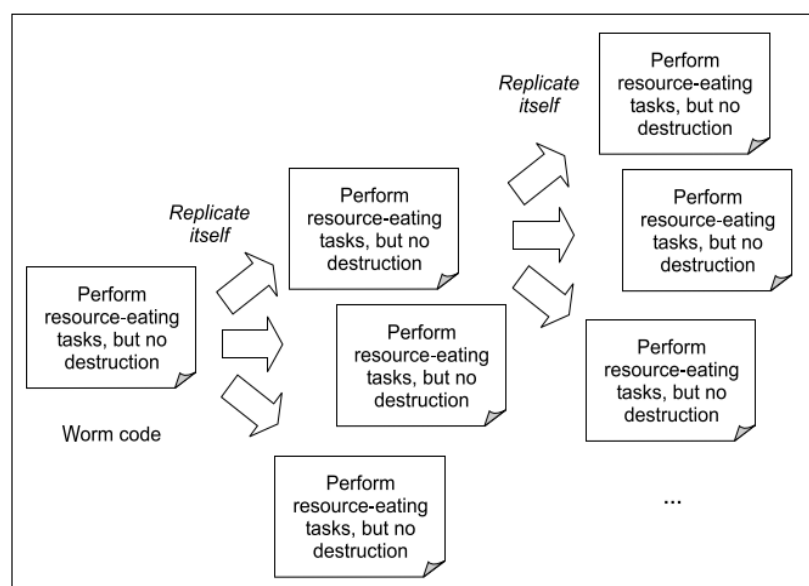


Fig. 1.15 Worm

3. Trojan Horse

A Trojan horse allows an attacker to obtain some confidential information about a computer or a network.

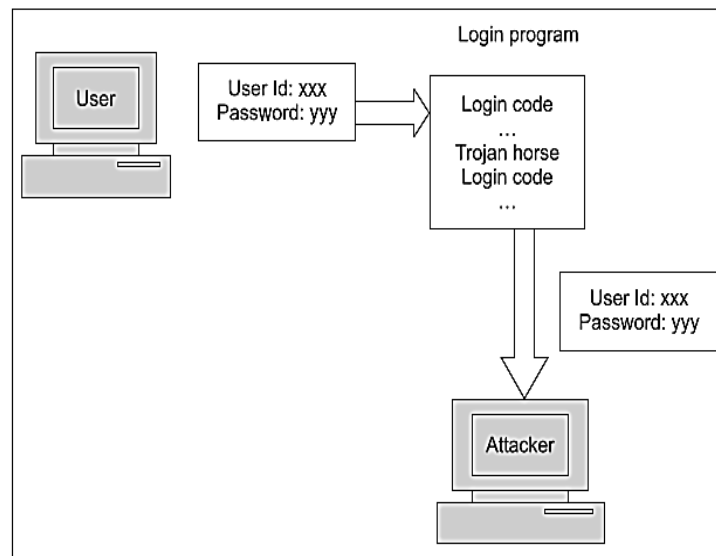


Fig. 1.16 Trojan horse

1.5.5 Dealing with Viruses

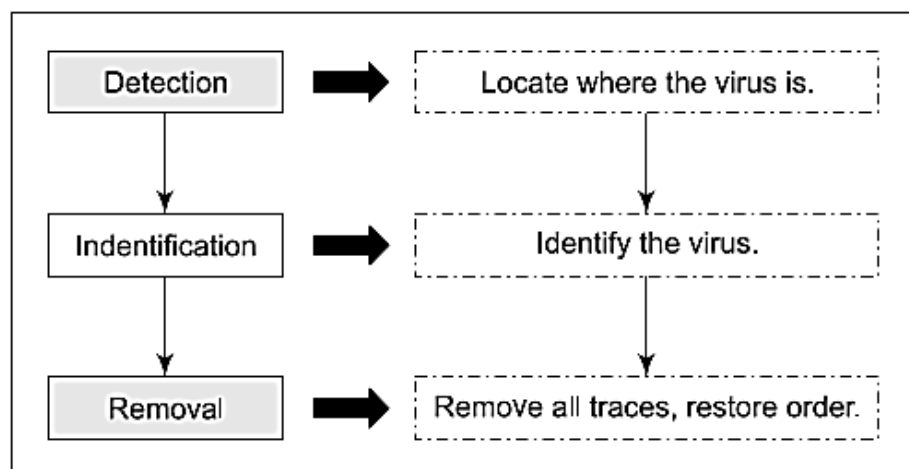


Fig. 1.17 Virus-elimination steps

There is a category of software called behavior-blocking software, which integrates with the operating system of the computer and keeps a watch on virus-like behavior in real time. Whenever such an action is detected, this software blocks it, preventing damages. The actions under watch can be

- Opening, viewing, modifying, deleting files
- Network communications
- Modification of settings such as start-up scripts

- Attempts to format disks
- Modification of executable files
- Scripting of email and instant messaging to send executable content to others

1. First Generation

These anti-virus software programs were called simple scanners. They needed a virus signature to identify a virus. A variation of such programs kept a watch on the length of programs and looked for changes so as to possibly identify a virus attack.

2. Second Generation

These anti-virus software programs did not rely on simple virus signatures. Rather, they used heuristic rules to look for possible virus attacks. The idea was to look for code blocks that were commonly associated with viruses. For example, such a program could look for an encryption key used by a virus, find it, decrypt and remove the virus, and clean the code. Another variation of these anti-virus programs used to store some identification about the file (e. g. a message digest, which we shall study later) are also notorious for detecting changes in the contents of the file.

3. Third Generation

These anti-virus software programs were memory resident. They watched for viruses based on actions, rather than their structure. Thus, it is not necessary to maintain a large database of virus signatures. Instead, the focus is to keep watch on a small number of suspect actions.

4. Fourth Generation

These anti-virus software programs package many anti-virus techniques together (e.g. scanners, activity monitoring). They also contain access control features, thus thwarting the attempts of viruses to infect files.

1.5.6 Specific Attacks

1. Sniffing and Spoofing

On the Internet, computers exchange messages with each other in the form of small groups of data, called packets. A packet, like a postal envelope contains the actual data to be sent, and the

addressing information. Attackers target these packets, as they travel from the source computer to the destination computer over the Internet. These attacks take two main forms: (a) Packet sniffing (also called snooping), and (b) Packet spoofing. Since the protocol used in this communication is called Internet Protocol (IP), other names for these two attacks are (a) IP sniffing, and (b) IP spoofing. The meaning remains the same.

2. Phishing

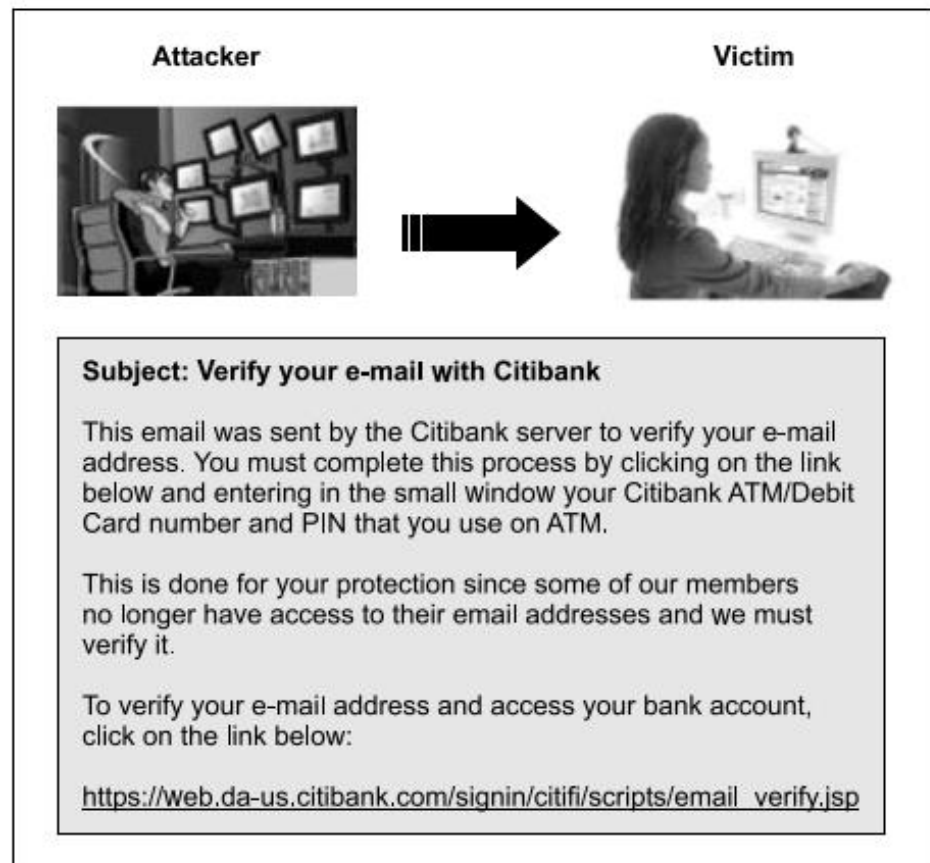


Fig. 1.19 Attacker sends a forged email to the innocent victim (customer)

Figure 1.20 shows a fake email sent by an attacker to an authorized PayPal user.

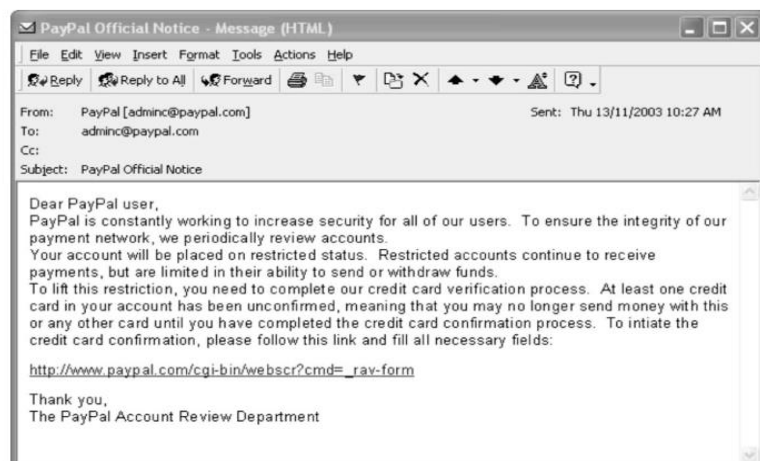


Fig. 1.20 Fake email from the attacker to a PayPal user

3. Pharming (DNS Spoofing)

Another attack, known earlier as DNS spoofing or DNS poisoning, is now called pharming attack. As we know, using the Domain Name System (DNS), people can identify Web sites with human-readable names (such as `www.yahoo.com`), and computers can continue to treat them as IP addresses (such as `120.10.81.67`). For this, a special server computer called a DNS server maintains the mappings between domain names and the corresponding IP addresses. The DNS server could be located anywhere. Usually, it is with the Internet Service Provider (ISP) of the users.

DNS Name	IP Address	DNS Name	IP Address
<code>www.amazon.com</code>	<code>161.20.10.16</code>	<code>www.amazon.com</code>	<code>161.20.10.16</code>
<code>www.yahoo.com</code>	<code>121.41.67.89</code>	<code>www.yahoo.com</code>	<code>121.41.67.89</code>
<code>www.bob.com</code>	<code>100.10.10.20</code>	<code>www.bob.com</code>	<code>100.20.20.20</code>
...	...	...	...
Before the attack		After the attack	

Fig. 1.22 Effect of the DNS attack

1.5 Security Mechanisms

A **security mechanism** is a technique or process used to **detect, prevent, or recover from security attacks**. Security mechanisms are implemented to provide various security services such as confidentiality, integrity, authentication, access control, and non-repudiation.

According to the **X.800 Security Architecture**, security mechanisms are classified into **Specific Security Mechanisms** and **Pervasive Security Mechanisms**.

Specific Security Mechanisms	Description
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 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.
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.

Pervasive Security Mechanisms	Description
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 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	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			

1.6 Security Services

AUTHENTICATION	DATA INTEGRITY
Definition: The assurance that the communicating entity is the one that it claims to be.	Definition: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.	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.
Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.	Connection Integrity without Recovery Same as above, but provides only detection without recovery.
ACCESS CONTROL	Selective-Field Connection Integrity Provides for the integrity of selected fields within the user data of a data block transferred over a connection and determines whether the selected fields have been modified, inserted, deleted, or replayed.
Definition: 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).	Connectionless Integrity Provides for the integrity of a single connectionless data block and may detect data modification. Additionally, a limited form of replay detection may be provided.
DATA CONFIDENTIALITY	Selective-Field Connectionless Integrity Provides for the integrity of selected fields within a single connectionless data block and determines whether the selected fields have been modified.
Definition: The protection of data from unauthorized disclosure.	NONREPUDIATION

Connection Confidentiality The protection of all user data on a connection.	Definition: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Connectionless Confidentiality The protection of all user data in a single data block.	Nonrepudiation, Origin Proof that the message was sent by the specified party.
Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.	Nonrepudiation, Destination Proof that the message was received by the specified party.
Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.	

Security Attacks

A useful means of classifying security attacks, used both in X.800 and RFC 2828, 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

Definition

A **Passive Attack** is a type of security attack in which an unauthorized person **monitors, listens to, or observes** the communication between two parties without modifying the data. The primary objective is **to obtain confidential information** while remaining undetected.

Characteristics of Passive Attacks

- Does **not alter** the original data.
- Difficult to detect because communication appears normal.
- Aims to **collect information** rather than damage systems.
- Prevention is more practical than detection.
- Encryption is the primary defense mechanism.

1. Release of Message Contents

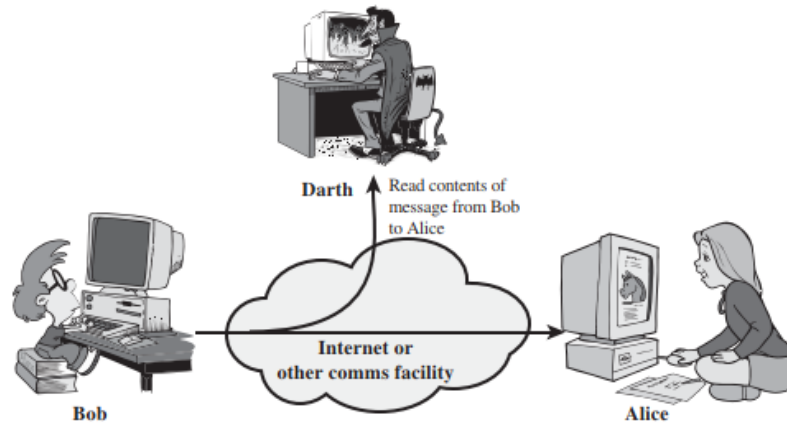
In this attack, the attacker **captures and reads confidential information** transmitted over a communication channel.

Examples include:

- Telephone conversations

- Email messages
- File transfers
- Online banking transactions

The goal is to obtain sensitive information such as passwords, financial data, or personal details.



(a) Release of message contents

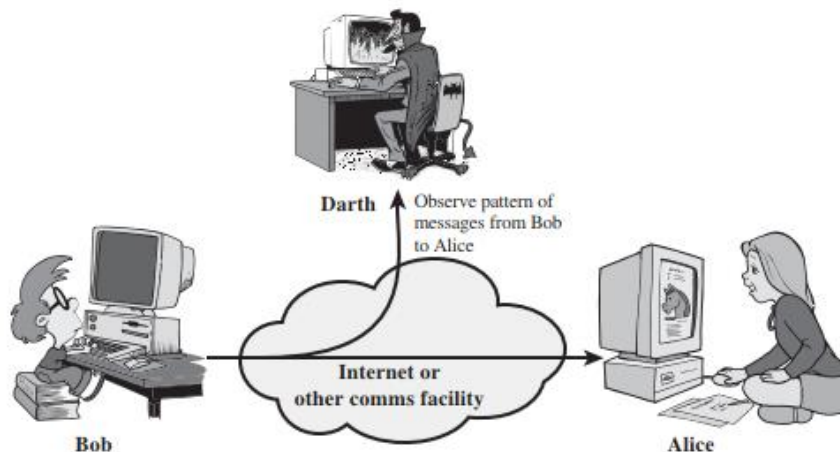
2. Traffic Analysis

When encryption protects message contents, attackers may still gather valuable information by analyzing communication patterns.

The attacker observes:

- Source and destination addresses
- Frequency of communication
- Message length
- Time of transmission

Although the message contents remain hidden, these patterns may reveal important information about the nature of the communication.



(b) Traffic analysis

Active Attacks

Definition

An **Active Attack** is a type of security attack in which an attacker **modifies, inserts, deletes, or disrupts** the data being transmitted. Unlike passive attacks, active attacks affect the **integrity, authenticity, or availability** of information and system resources.

Characteristics of Active Attacks

- **Modify or alter** data during transmission.
- Can create **false or fake data streams**.
- Easier to detect than passive attacks.
- More difficult to prevent completely.
- Detection and recovery are the primary security objectives.

1. Masquerade Attack

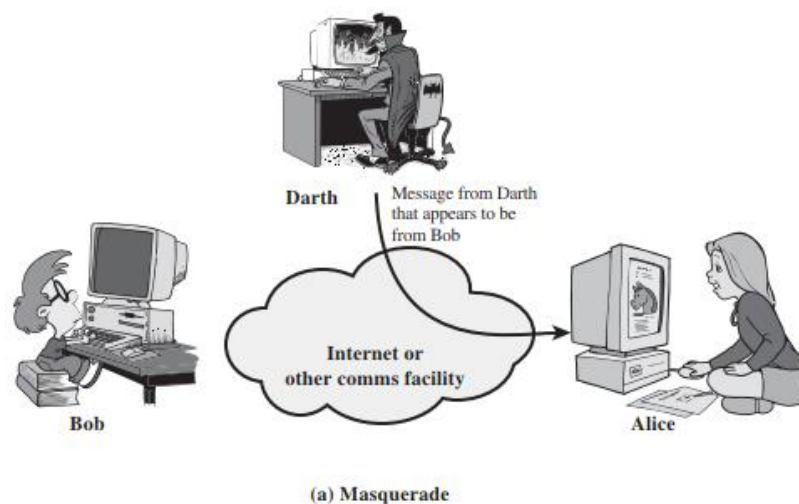
A **Masquerade Attack** occurs when an attacker **impersonates a legitimate user** to gain unauthorized access to a system or network.

Features

- Uses stolen usernames, passwords, or authentication tokens.
- Often combined with replay attacks.
- Violates authentication and access control.

Example

An attacker steals an administrator's login credentials and accesses confidential company data.



2. Replay Attack

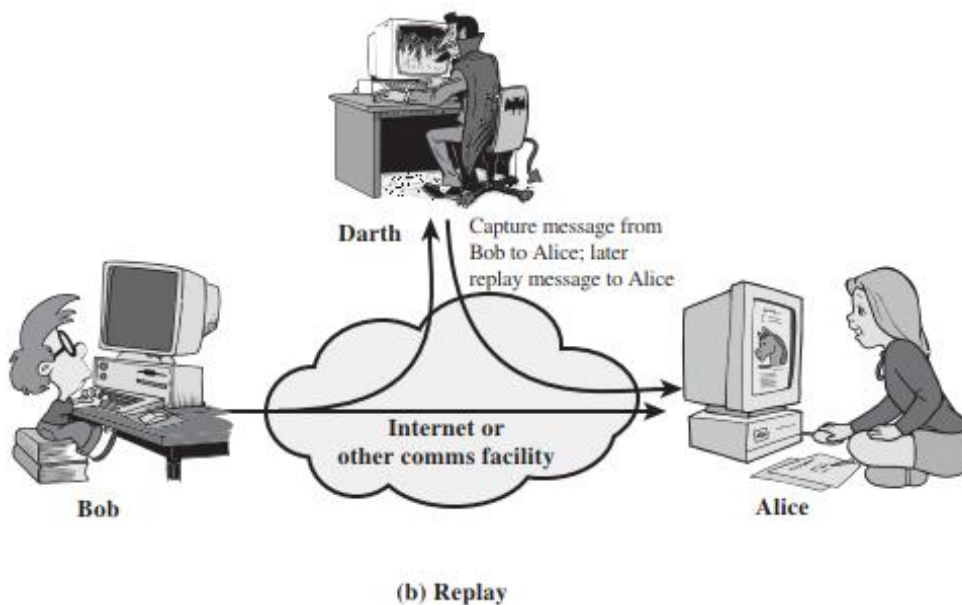
A **Replay Attack** occurs when an attacker **captures valid data** during transmission and **retransmits it later** to deceive the receiver.

Features

- No modification of captured data is necessary.
- Previously valid messages are reused.
- Common in authentication systems.

Example

A hacker records an online payment authentication message and replays it later to repeat the transaction.



3. Modification of Messages

In this attack, the attacker **changes the contents** of a legitimate message or **delays, deletes, or reorders** messages.

Features

- Affects data integrity.
- Alters information before it reaches the receiver.
- May change transaction details or permissions.

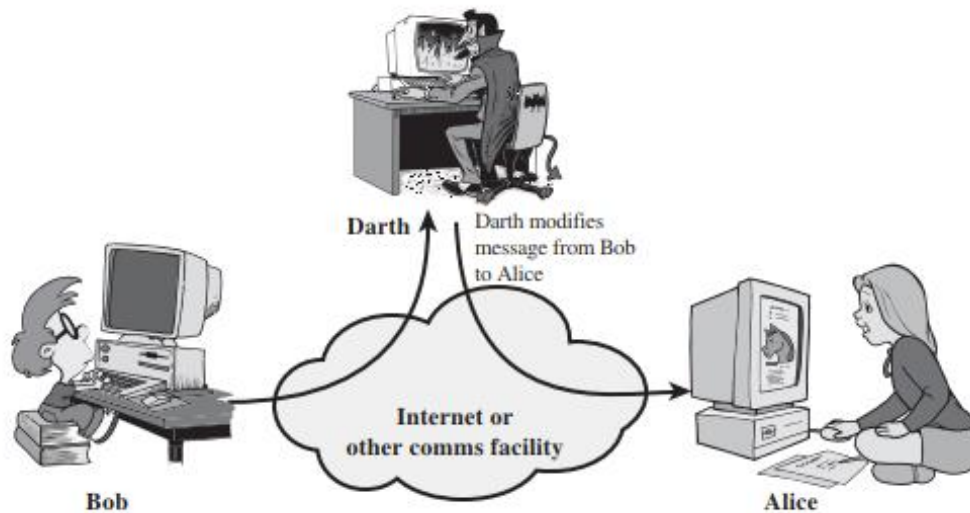
Example

Original Message:

Allow **John Smith** to read confidential files.

Modified Message:

Allow **Fred Brown** to read confidential files.



(c) Modification of messages

4. Denial of Service (DoS)

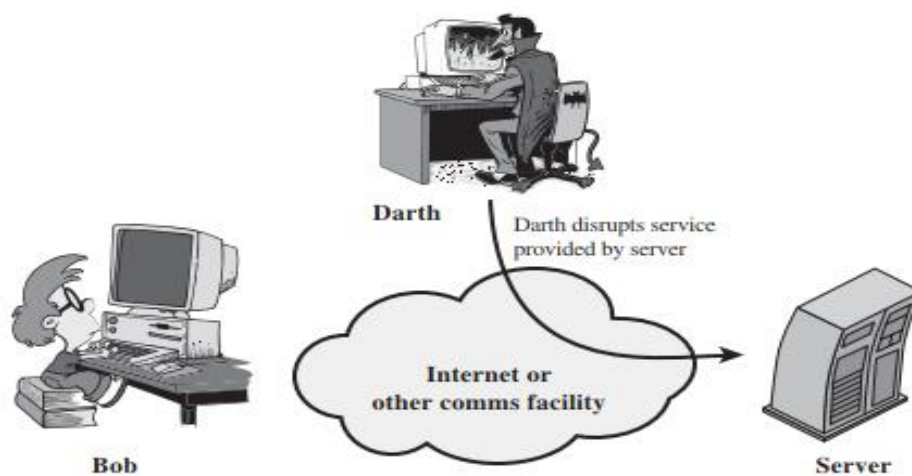
A **Denial of Service (DoS)** attack attempts to make a system or network **unavailable** to legitimate users.

Methods

- Flooding the network with excessive traffic.
- Crashing servers.
- Blocking communication channels.
- Consuming system resources.

Example

Thousands of fake requests are sent to a web server, preventing genuine users from accessing the website.



(d) Denial of service

1.7 Model for Network Security

The **Model for Network Security** explains how secure communication is established between two communicating parties over an insecure network (such as the Internet). It ensures that information remains **confidential, authentic, and secure** from attackers during transmission.

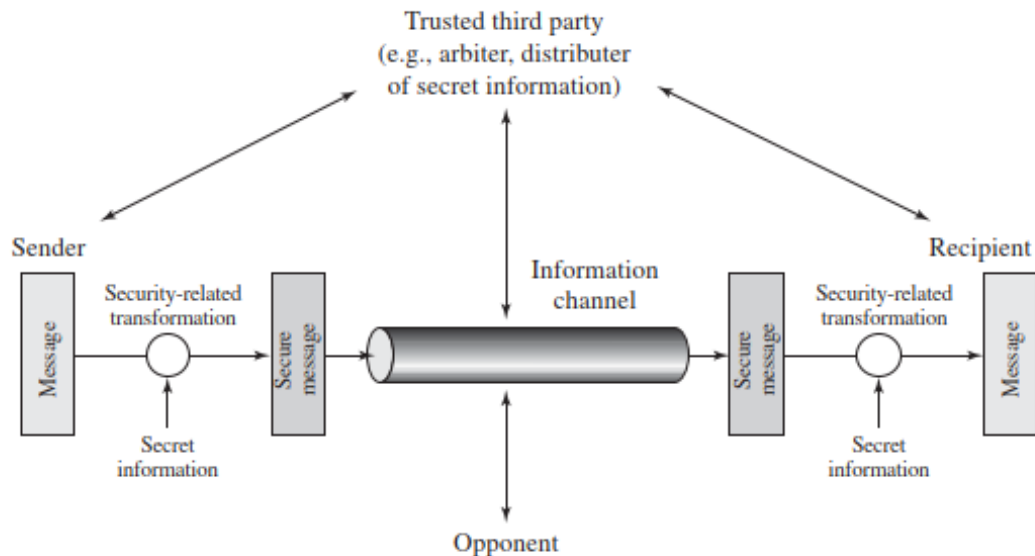


Figure 1.4 Model for Network Security

Working of the Network Security Model

1. The **sender** prepares the original message.
2. A **security transformation** (such as encryption) is applied to convert the message into an unreadable form.
3. The transformation uses a **secret key** shared between the sender and receiver.
4. The encrypted message is transmitted over the **Internet**.
5. An **attacker** may attempt to intercept or modify the message.
6. The **receiver** uses the same (or a corresponding) secret key to recover the original message.
7. If required, a **trusted third party** distributes keys or resolves authentication disputes.

Secret Information

Secret information is shared only between the communicating parties.

Examples include:

- Encryption keys
- Decryption keys
- Authentication keys
- Session keys

The security of the entire communication depends on keeping these keys confidential.

Advantages

- Protects sensitive information over insecure networks.
- Prevents unauthorized access.
- Ensures secure authentication.
- Supports secure electronic transactions.
- Enables trusted communication over the Internet.