INTRODUCTION TO CRYPTOGRAPHY

TOPICS:

- DEFINITION OF CRYPTOGRAPHY
- SECURITY GOALS
- SERVICES AND MECHANISMS CRYPTOGRAPHIC ATTACKS
- MODEL FOR NETWORK SECURITY
- ENCRYPTION
- ONE-TIME PAD

WHAT IS CRYPTOGRAPHY?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

ENCRYPTION AND DECRYPTION:

Encryption and decryption Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption. The following figure shows this process.

HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key

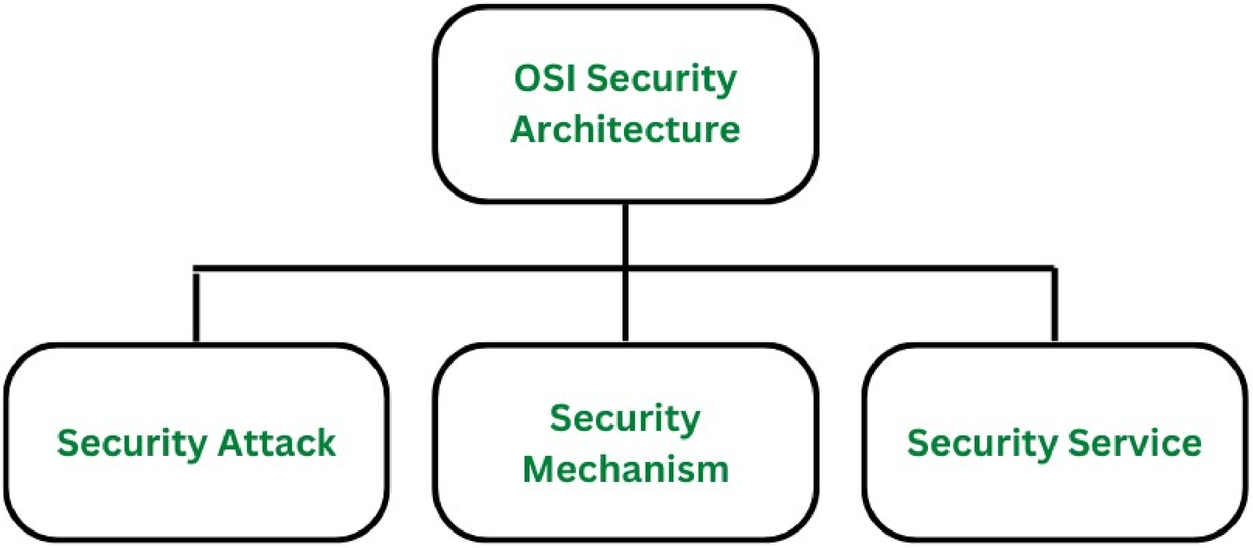
Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

1. **COMPUTER SECURITY:**
   In simple term it means the collection of tools designed to protect data and thwart hackers. Thwart is meant by prevents from accomplishing something.
2. **NETWORK SECURITY:**
   In simple terms it measures to protect data during their transmission.

3. **INTERNET SECURITY:**
   In simple terms it measures to protect data during their transmission over a collection of interconnected networks.

CLASSIFICATION OF OSI SECURITY ARCHITECTURE:



OSI SECURITY ARCHITECTURE:

The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data.

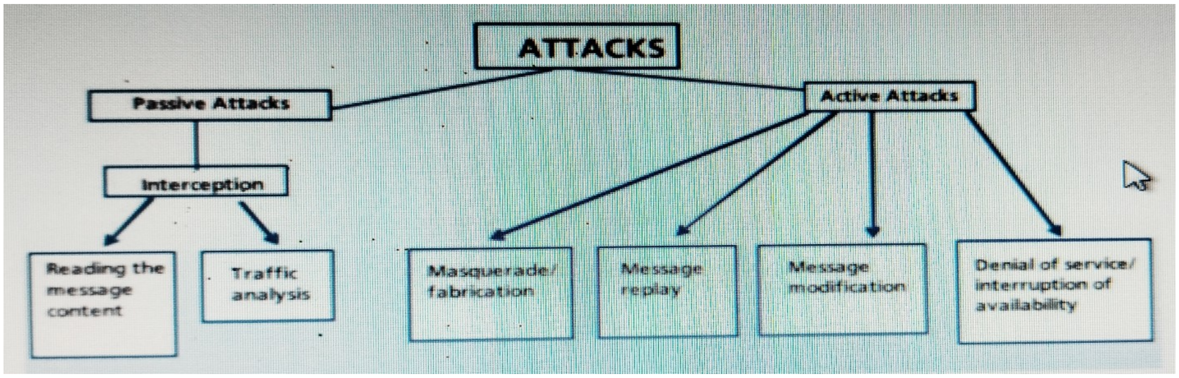
OSI Security Architecture is categorized into three broad categories namely **security attack, security mechanism, and security services.**

TYPES OF SECURITY ATTACKS:

There are two types of attacks:

1. Active attacks

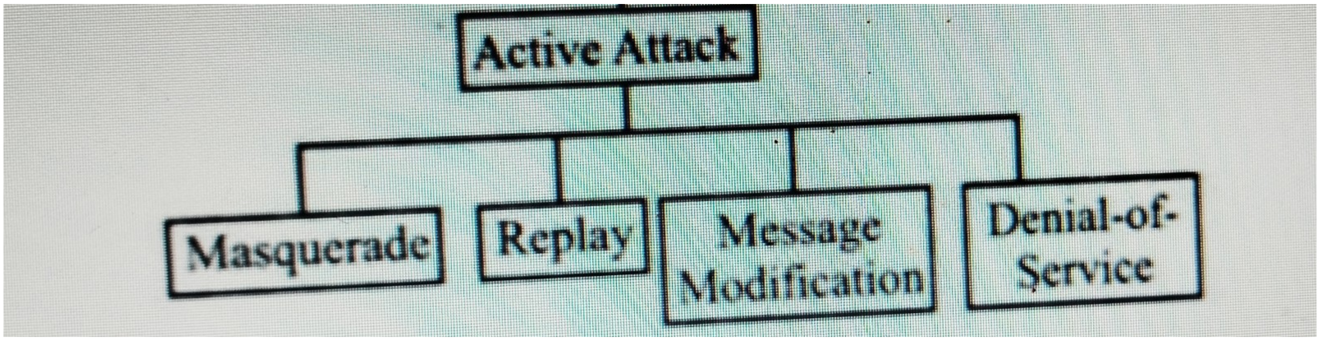
2. Passive attacks



Active attacks:

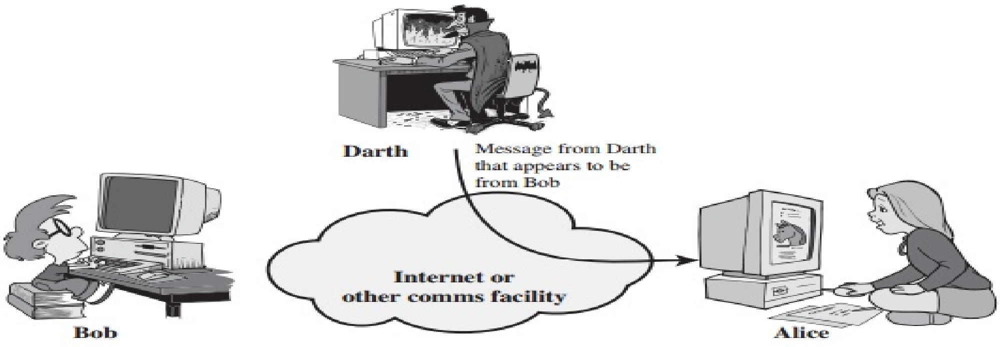
An active attack is an attempt to alter system resources or affect their operation. I.e., these attacks involve in some modification to the original message in some manner or the creation of a false stream.

These attacks can be classified in to four categories:



Masquerade:

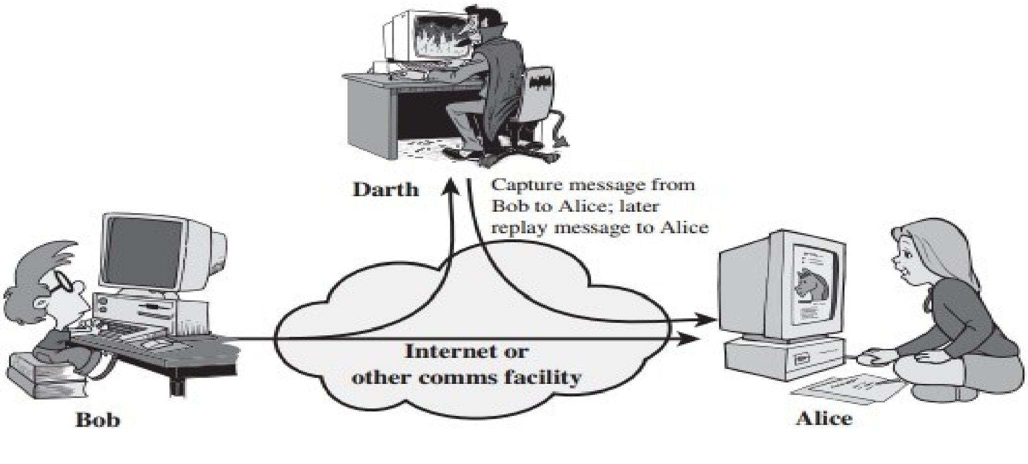
One entity pretends to be a different entity. It is generally done by using stolen IDs and passwords or through bypassing authentication mechanism.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Replay:

This attack involves capturing a copy of the message sent by the original sender and retransmitting it later to bring an unauthorized result.

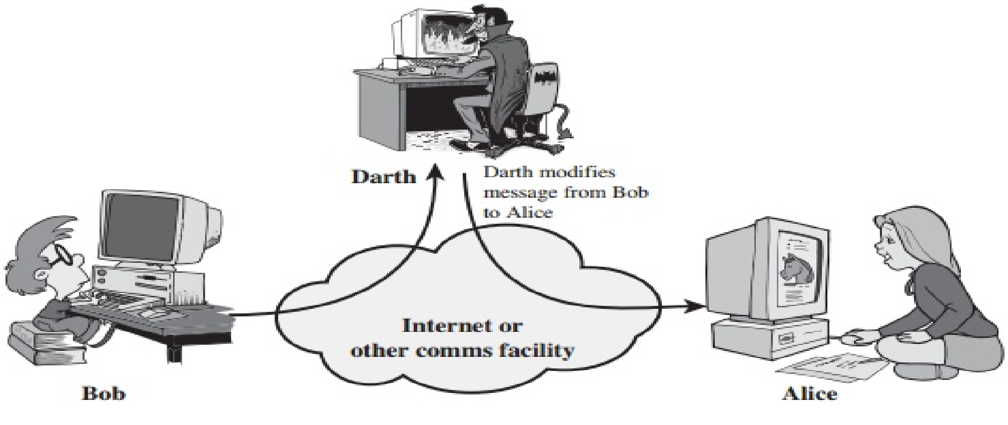

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Modification of messages:

➢ some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

➢ For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to "Allow Fred Brown to read confidential file accounts."


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

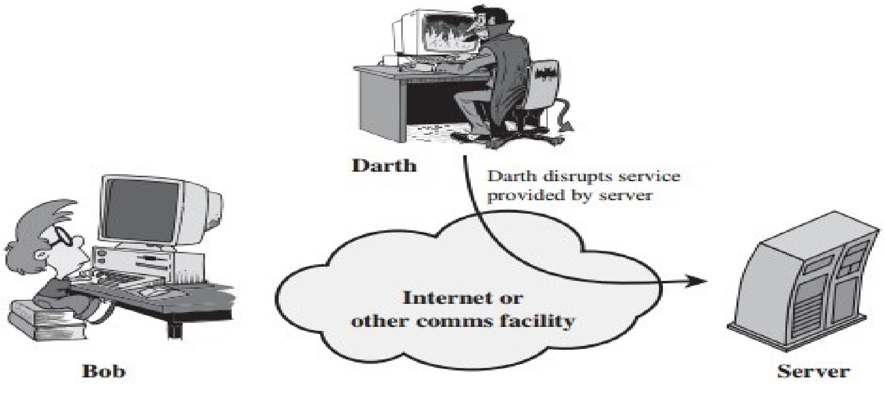
Denial of service:

➢ A denial-of-service (DOS) is a form of cyber attack that prevent legitimate users from accessing a computer or network.

➢ In a DOS attack, rapid and continuous online requests are sent to a target server in order to overload the server's bandwidth.

➢ Prevent the normal use or management of communication facilities.

➢ Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

Passive Attacks:

➢ Passive attacks are those where the attacker indulges in eavesdropping or monitoring of data transmission.

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

There are two types of passive attacks:

1. Release of message contents

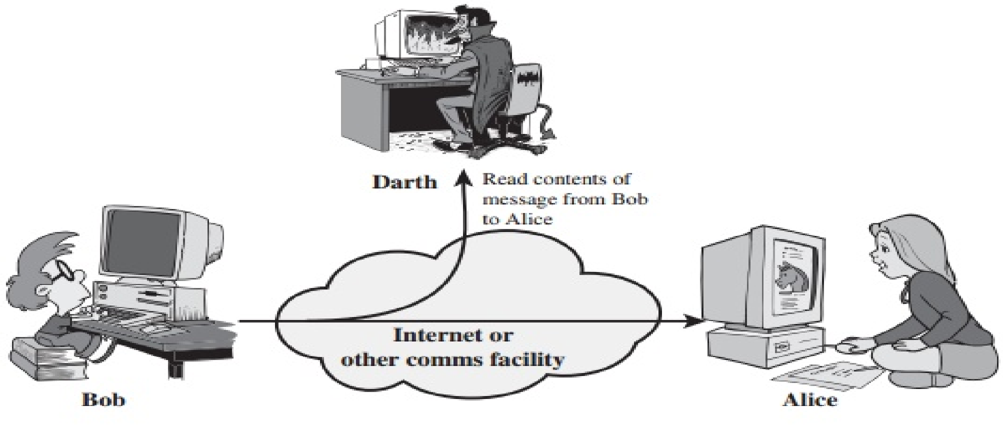
2. Traffic analysis

Release of message contents:

➢ The release of message contents is a type of attack that analyzes and read the message delivered between senders to receiver.

➢ A telephone conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information.

➢ We would like to prevent an opponent from getting the contents of these transmissions.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

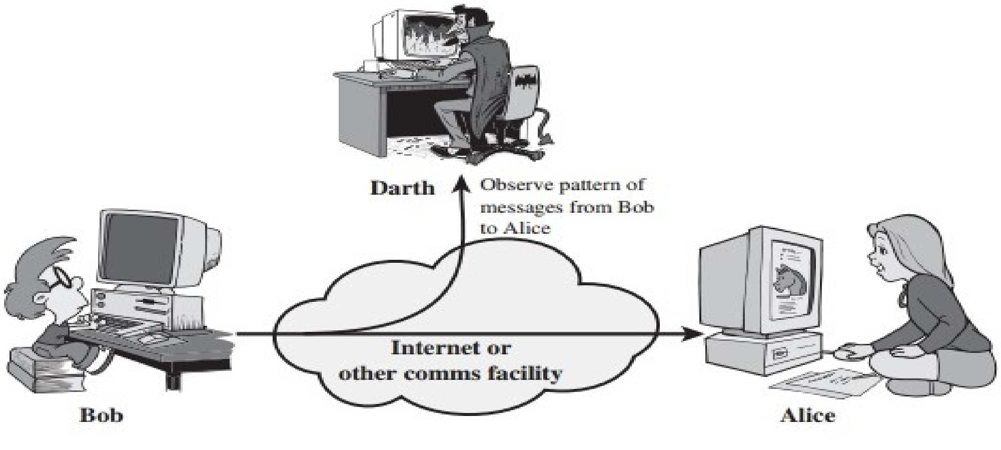
(a) Release of message contents

Traffic analysis:

➢ The attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behaviour patterns.

➢ In this type of attack, an intruder observes the frequency and length of msg. being exchanged between communicating nodes.

➢ Attacker can then use this information for guessing the nature of communication that was taking place.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

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

PRINCIPLES OF SECURITY/ SECURITY SERVICES:

The classification of security services are as follows:

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.

➢ Unauthorized party could be a person, a program or a computer.

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

➢ Interception causes loss of message confidentiality.

Authentication:

➢ Authentication mechanism helps to establish proof of identities.

➢ The authentication process ensures that the origin of a electronic message or document is correctly identified. This concept is shown in figure.

➢ Fabrication is possible in absence of proper authentication mechanisms.

Data Integrity:

➢ when the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

➢ For example, consider that user A sends message to user B. User C tampers with a message originally sent by user A, which is actually meant for user B. User C change its contents and send the changed message to user B. User B has no way of knowing that the contents of the message changed after user A had sent it. User A also does not know about this change. This type of attack is called modification.

➢ Modification causes of loss of message integrity

Non repudiation:

Non repudiation 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.

Access control:

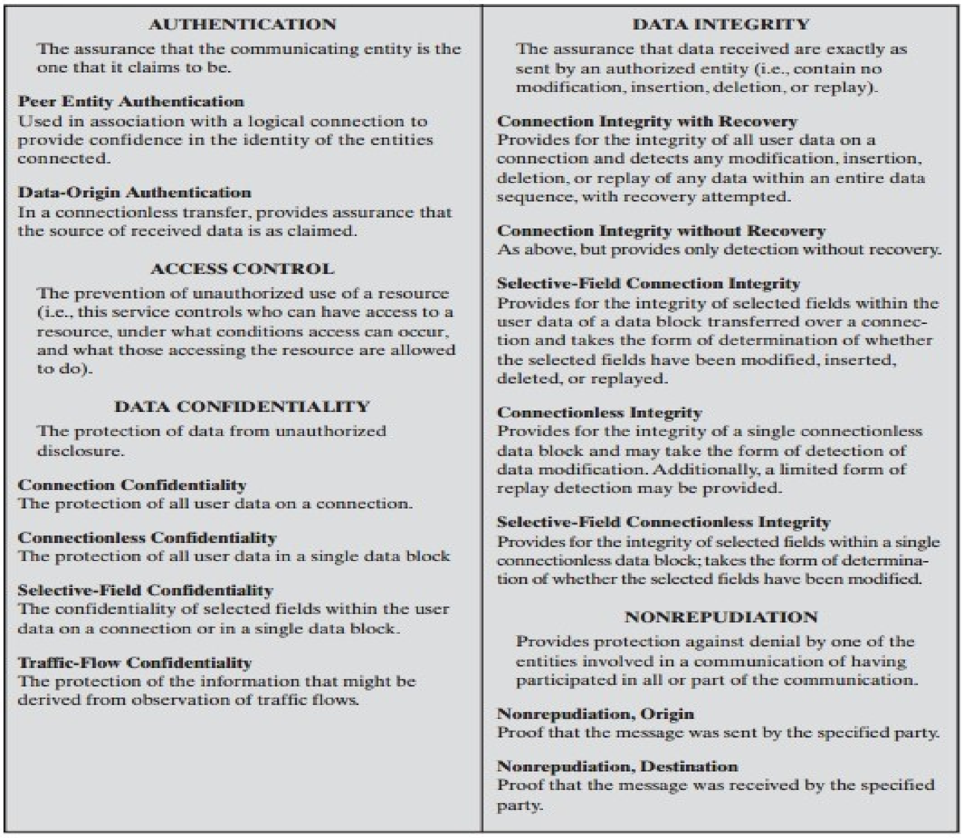
Access control determines and controls who can access what. It regulates which user has access to the resource, under what circumstances.

Availability:

➢ The principle of availability is that resources should be available to authorized parties at all times.

➢ For example, due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server B. This would defeat the principle of availability. Such an attack is called interruption.

➢ Interruption causes loss of availability.



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

SECURITY MECHANISMS:

Specific security mechanisms:-

Decipherment:

This refers to the transformation of the message or data with the help of mathematical algorithms. The main aim of this mechanism is to provide confidentiality. The two techniques that are used for decipherment are cryptography and steganography.

Data integrity:

This refers to the method of ensuring the integrity of data. For this, the sender computes a check value by applying some process over the data being sent, and then appends this value to the data. On receiving the data, the receiver again computes the check value by applying the same process over the received data. If the newly computed check value is same as the received one, then it means that the integrity of data is preserved.

Digital signature:

This refers to the method of electronic signing of data by the sender and electronic verification of the signature by the receiver. It provides information about the author, date and time of the signature, so that the receiver can prove the sender's identity.

Authentication exchange:

This refers to the exchange of some information between two communicating parties to prove their identity to each other.

Traffic padding:

This refers to the insertion of extra bits into the stream of data traffic to prevent traffic analysis attempts by attackers.

Routing control:

This refers to the selection of a physically secured route for data transfer. It also allows changing of route if there is any possibility of eavesdropping on a certain route.

Notarization:

This refers to the selection of a trusted third party for ensuring secure communication between two communicating parties.

Access control:

It refers to the methods used to ensure that a user has the right to access the data or resource.

Pervasive security mechanisms:-

Trusted functionality:

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

Security label:

The marking bound to a resource that names or designates the security attributes of that resource.

Event detection:

Detection of security-relevant events:

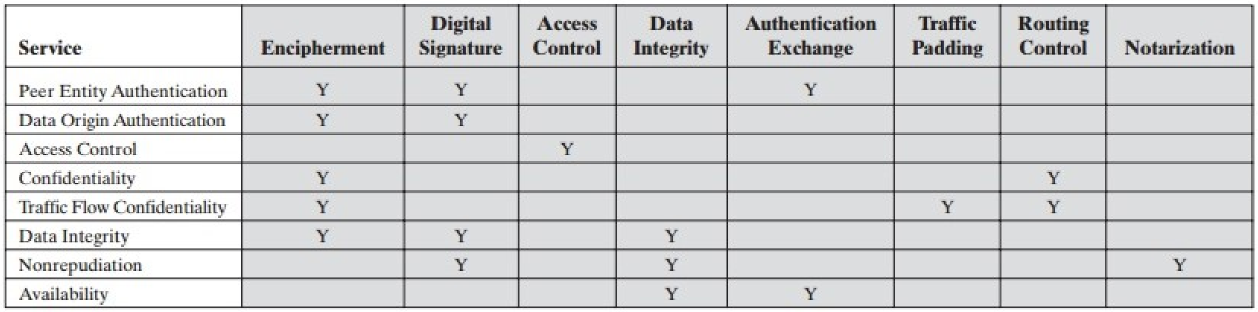
Security audit trail:

Data collect 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.

Relation between security service and mechanisms:



Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

A MODEL FOR NETWORK SECURITY

- 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.

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

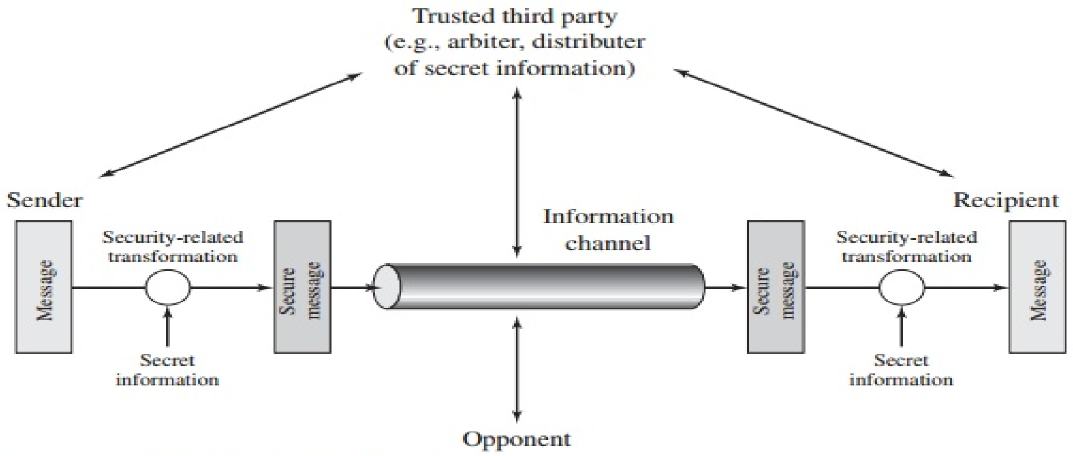


Figure 1.4 Model for Network Security

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

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- 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.

Parts one through five of this book concentrate on the types of security mechanisms and services that fit into the model shown in Figure 1.4: However, there are other security-related situations of interest that do not neatly fit this model but are considered in this book. A general model of these other situations is illustrated by Figure 1.5, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who 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 disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain.

(e.g., obtaining credit card numbers or performing illegal money transfers)

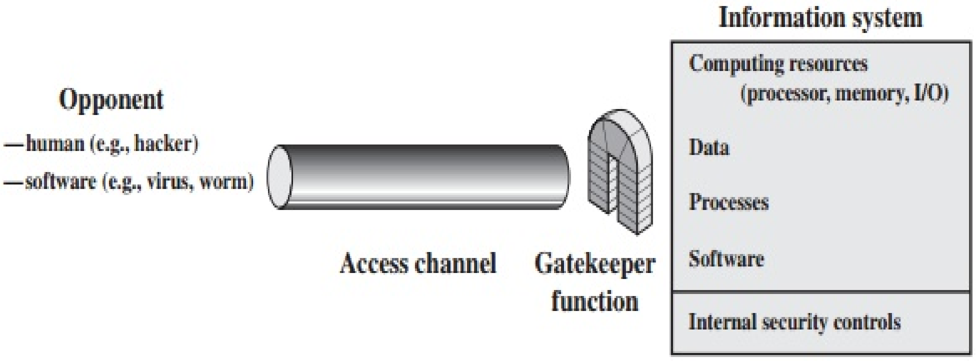


Figure 1.5 Network Access Security Model

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 pro-grams as well as utility programs, such as editors and compilers. Programs can pre-send 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.

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

The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.5). The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defence consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders. These issues are explored in Part Six.

ONE-TIME PAD:

An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Verna cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new mess-sage. Such a scheme, known as a **one-time pad**, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

An example should illustrate our point. Suppose that we are using a Viennese scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message. Consider the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: *pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
plaintext: mr mustard with the candlestick in the hall
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: *mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt*

plaintext: miss scarlet with the knife in the library

Suppose that a cryptanalyst had managed to find these two keys. Two plausible plaintexts are produced. How is the cryptanalyst to decide which is the correct decryption (i.e., which is the correct key)? If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of these two keys is more likely than the other. Thus, there is no way to decide which key is correct and there-fore which plaintext is correct.

In fact, given any plaintext of equal length to the ciphertext, there is a key that produces that plaintext. Therefore, if you did an exhaustive search of all possible keys, you would end up with many legible plaintexts, with no way of knowing which was the intended plaintext. Therefore, the code is unbreakable.

The security of the one-time pad is entirely due to the randomness of the key. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

In theory, we need look no further for a cipher. The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.

2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

******