6...

Network Security

Objectives...

- To know the need for Network Security
- To learn about Security Services: Message-confidentiality, Integrity, Authentication, Non repudiation
- To study about types of Attack
- To get knowledge of Cryptography, PlainText, Cipher Text, Encryption, Decryption
- To learn Substitution Techniques, Caesar Cipher, and Transposition Cipher
- To get information about Firewalls, Steganography and Copyright

6.1 INTRODUCTION

- Network/Computer security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Users choose or are assigned an ID and password or other authenticating information that allows them to access the information and programs within their authority.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among business, organizations government agencies and individuals.
- Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.
- Providing network security means controlling systems to prevent any accidental and/or intentional data loss.
- The overall computer security is the protection of data and assets from unauthorized access, use, alteration or destruction.

- Mainly there are two types of security as explained below:
  1. **Physical Security:** Physical security includes protecting all hardware units of a network against any unauthorized access (here, preferably a theft minded person who want to steel the hardware units and destroy them) and against any natural disaster.
  2. **Logical Security:** The logical security deals with protecting the network data (software) from unauthorized access and of course from natural disaster.

6.2 NEED FOR SECURITY

- There are common mechanism to provide the basic security:
  1. Authenticate a user by providing a user identification and password to every user.
  2. Encode the information stored in the databases, so that it is not visible to those users who do not have right permission.
- Computer security deals with prevention and detection of unauthorized actions by users of a computer. In simple words security is defined as, "protecting information/ data from unintended/unauthorized access".

OR

- Security can be defined as, "the extent to which access the data can be restricted and hence protected against its illegal misuse and alteration."
- However, there are many examples of what could happen if there are insufficient securities built in applications developed for the Internet.
- To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).
- With the advent of computers, information storage became electronic. Instead of being stored on physical media, it was stored in computers. The three security requirements however, did not change. The files stored in computers require confidentiality, integrity and availability.
- In the companies or business organizations, the security measures are very important to protect the data/information. These security measures include authentications, encryptions, access control, confidentiality, etc.
- The money transaction using credit card requires more security. There are many attacks reported using such transactions.

6.3 SECURITY SERVICES (S-22)

- Security service is a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

6.3.1 Messages

- Network security means to protect information. It deals with the prevention and detection of unauthorized actions by users of a computer.
- Before discussing general network security threats, we need to be familiar with the principle of security itself. The four principles of security are Confidentiality, Integrity, Authentication and Non-repudiation.

6.3.1.1 Confidentiality

- Confidentiality means maintain security and secrecy. This means only authorized people can see protected data or resources. The main issue here is to decide what is confidential and who has the right to access it.
- Confidentiality is concerned with keeping data secure from those who lack the need to know it.
- The objects are not disclosed to unauthorized subjects. If user X is sending the envelope (contains check) to user Y then user X will ensure that no one else, user Y gets the envelope.
- If another user Z gets access to this message without the permission and knowledge of X and Y then this type of attack is called interception. Interception causes loss of message confidentiality.

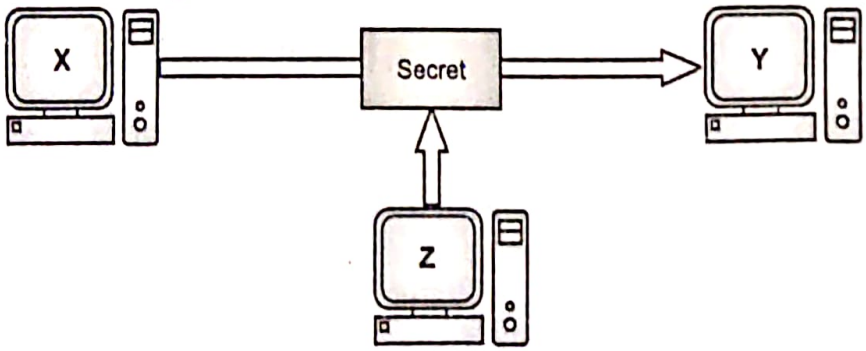


Fig. 6.1: Loss of Confidentiality

6.3.2 Integrity

- Integrity is concerned with keeping data pure and trustworthy by protecting data/information from intentional or accidental changes/modifications.
- The objects retain their veracity. The user X and user Y ensures that the contents in the envelope should not be tamper or change by other user. If content of message is change before it reaches to the intended recipient, then integrity of message is lost.
- The user X wants to send the message to user Y, The user Z change the original message contents by accessing it, and send the change message to user Y. Both X and Y are unaware of the such change. This attack is called modification. Modification causes loss of integrity.

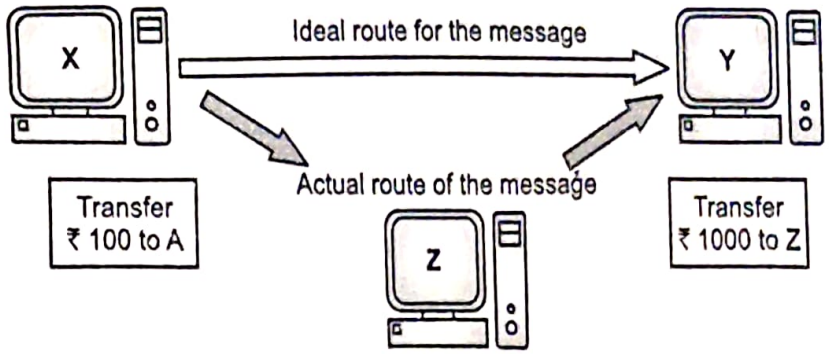


Fig 6.2: Loss of Integrity

- In short, integrity concerned with preventing unauthorized modification/alteration of data/information.

6.3.3 Authentication

- Message authentication ensures that the message has been sent by a genuine identity and not by the fraud.
- Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying authorizations.
- If authentication principle followed, guarantees the valid and genuine message received from a trusted source through a valid transmission.
- Apart from intruders, the transfer of message between two people also faces other external problems like noise, which may alter the original message constructed by the sender. To ensure this, message authentication is needed.
- The service used to provide message authentication is a Message Authentication Code (MAC).
- MAC stands for Message Authentication Code. A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.

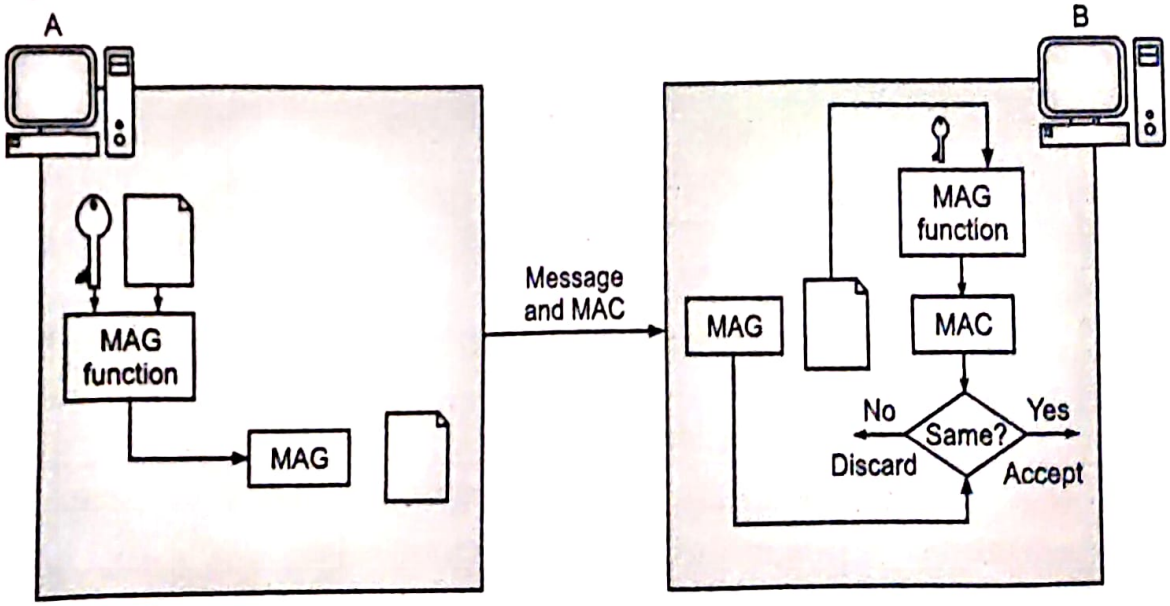


Fig. 6.3: MAC created by user A (sender) and checked by user B (Receiver)

- In MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message.

6.3.4 Non-repudiation

- Non-repudiation refers to the fact that sender refuses sometimes for the transmission of the malicious messages. Therefore, it is important to have some methodology to verify the original sender of the message.
- In this principle, the user sends the message and later refuses (repudiates) that he/she had send the message. If Y deposits a check in the account and money get transferred from X's account to Y's account, and then X refuses having sent the check. In this fund transfer process, X's signature is required. Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

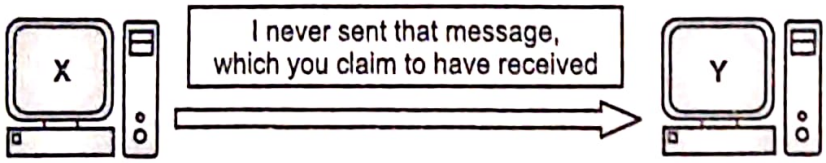


Fig. 6.4: Establishing Non-repudiation

Table 6.1: Summary of Security Principles

Sr. No.	Security Principle	Description	Compromising Attack	Security Solution
1.	Confidentiality	Only intended recipient must be able to access the message that has been sent secretly.	Interception	Symmetric key algorithms like DES, AES or IDEA and Asymmetric key algorithms like RSA.
2.	Integrity	Contents of the message must not be altered or modified by any means.	Modification	Message Digest algorithms like SHA, MD5.
3.	Authentication	The sender of the message must be properly identified.	Fabrication	Digital Signatures.
4.	Non-repudiation	One must not refuse transmission of the message.	Refusal of transmission	Digital Signatures.

6.3.5 Entity (User) - Authentication

- User authentication is performed in almost all human-to-computer interactions other than guest and automatically logged in accounts.
- One of the key aspects of cryptography and network/Internet security is authentication. Authentication helps establish trust by identifying the particular user/system. Authentication ensures that the applicant is really who he/she claims to be.
- Authentication is process of establishing the legitimacy of a node or user before allowing access to requested information.
- In most computer security contexts, user authentication is the fundamental building block and the primary line of defense. User authentication is the basis for most types of access control and for user accountability.
- RFC 2828 defines user authentication as, "the process of verifying an identity claimed by or for a system entity".
- User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User A only has access to relevant information and cannot see the sensitive information of User B.
- There are many methods to authenticate a user. Traditionally, user ids and passwords have been used. But there are many security concerns in this mechanism. Passwords can travel in clear text or can be stored in clear text on the server, both of which are dangerous propositions. Modern password-based authentication techniques use alternatives as encrypting passwords, or using something derived from the passwords in order to protect them.
- Authentication tokens add randomness to the password-based mechanism, and make it far more secure. This mechanism requires the user to possess the tokens. Authentication tokens are quite popular in applications that demand high security.
- Certificate-based authentication has emerged as a modern authentication mechanism, thanks to the emergence of the PKI technology. This is also quite strong, if implanted correctly. Smart cards can also be used in conjunction with this technology. Smart cards facilitate cryptographic operations inside the card, making the whole process a lot more secure and reliable.
- Biometrics is also getting a lot of attention these days, and is based on human biological characteristics. However, it has still not matured completely.
- In next sections, the above approaches of user authentication are explained in detail.

Types of Authentication:

- The main types of authentication available are Password based authentication, Token based authentication, Biometric based authentication and Image based authentication.

6.3.5.1 Password Based Authentication

- A password is a string of alphabets, numbers and special characters, which is supposed to be known only to the entity (usually person) that is being authenticated.
- Clear Text Password is the simplest Password based authentication mechanism. It works as follows as shown in Fig. 6. 5.
  - It prompts for user ID and Password.
  - User enters user ID and Password.
  - Validation User ID and Password.
  - Authentication Results.
  - User is informed accepted or rejected accordingly.

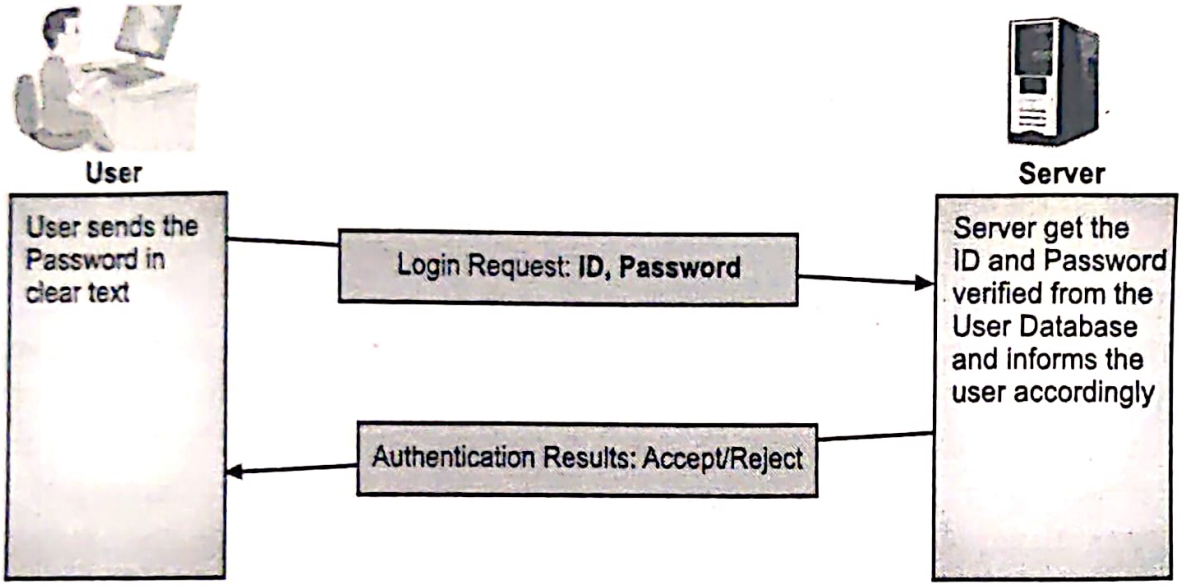


Fig. 6.5: User Authentication using Clear Text Password

- Problems with clear text passwords are as follows:
  1. Database contains passwords in clear text which is not secure. It is advised that password should not be stored in clear text in databases. Instead the passwords should be stored in encrypted form in database.
  2. Password travel in clear text from user's computer to the server. If the attacker breaks into the communication link, he can easily obtain the clear text password.

Improvements Over Basic Password Based Authentication:

- The variations from the basic password-based authentication are not to use password itself, but to use something that is derived from passwords.

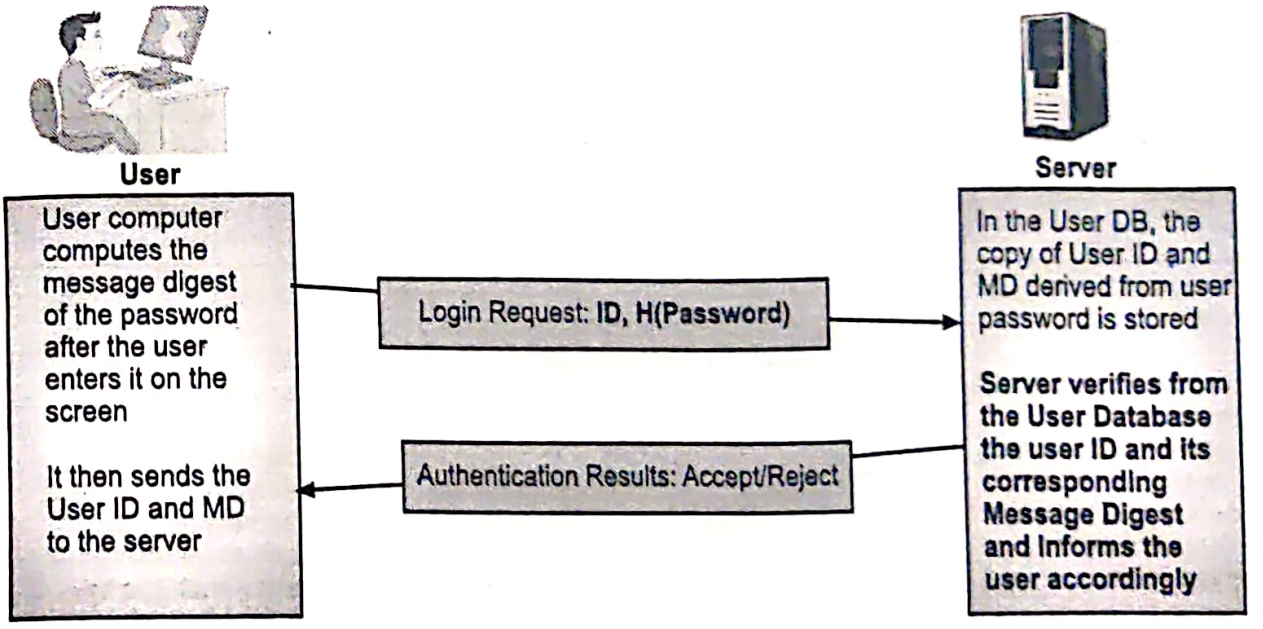
1. Storing Password in Encrypted or Derived Format:

- In this method, instead of storing password in clear text, it is stored in encrypted format. This method works as follows:
  - The user ID and password travels to the server in clear text.

- The server encrypts the password using password-encryption program and store it in database.
- When user wants to be authenticated the user enters the password, user's computer performs the same algorithm locally, and sends the derived password to server for verification.
- The server's user-authentication program now check the user-id and encrypted password against the database and inform user accepted or rejected accordingly.

2. Message Digest (MD) of Passwords:

- To solve the above problem of storing password in clear text in database, message digests as derived passwords stored in the user database. It works as follows shown in Fig. 6.16.
  - When a user needs to be authenticated, the user enters the ID and Password.
  - User's computer computes the message digest of the password
  - User's computer sends the user ID and computed Message Digest to the server for authentication.
  - Server verifies from the user databases the user ID and its corresponding Message Digest and inform user accepted or rejected accordingly.



* H(Password) = Message Digest (MD) derived from the User Password

Fig. 6.6: User Authentication using Message Digest of password

Problems with the Message Digests of the Passwords:

- An Attacker cannot compute the original password back from the message digest of the password, but he can simply copy the User ID and the corresponding Message Digest of the password, and submit them after some time to the same server as a part of the new login request.

- The server has no way of knowing that this login attempt is not from a legitimate user, but actually an attacker. This is called as REPLAY ATTACK, because the attacker simply replays the sequence of the actions of a normal user.

3. **Adding Randomness:**

- To improve the security and to detect a replay attack we need to add a bit of unpredictability or randomness to the earlier schemes. This will ensure that the replay attack is foiled:

  (i) **Storing Message Digests as derived passwords in the user database:** User Ids and corresponding MDs are stored in user Database with the server.

  (ii) **User sends a login request:** It contains only user ID.

  (iii) **Server creates a random Challenge:** Server first verifies the validity of user ID. Then it sends a random challenge (a random number) to the user. Random challenge travels as plaintext from server to user computer.

  (iv) **User Signs the Random Challenge with the Message Digest of the Password:** User Computer's computes the Message Digest (MD) of its password. User Computer's encrypts the Random Challenge by using MD of the Password. (symmetric key encryption). User Computer's sends the random challenge, which is encrypted with the message digest of the password to the server.

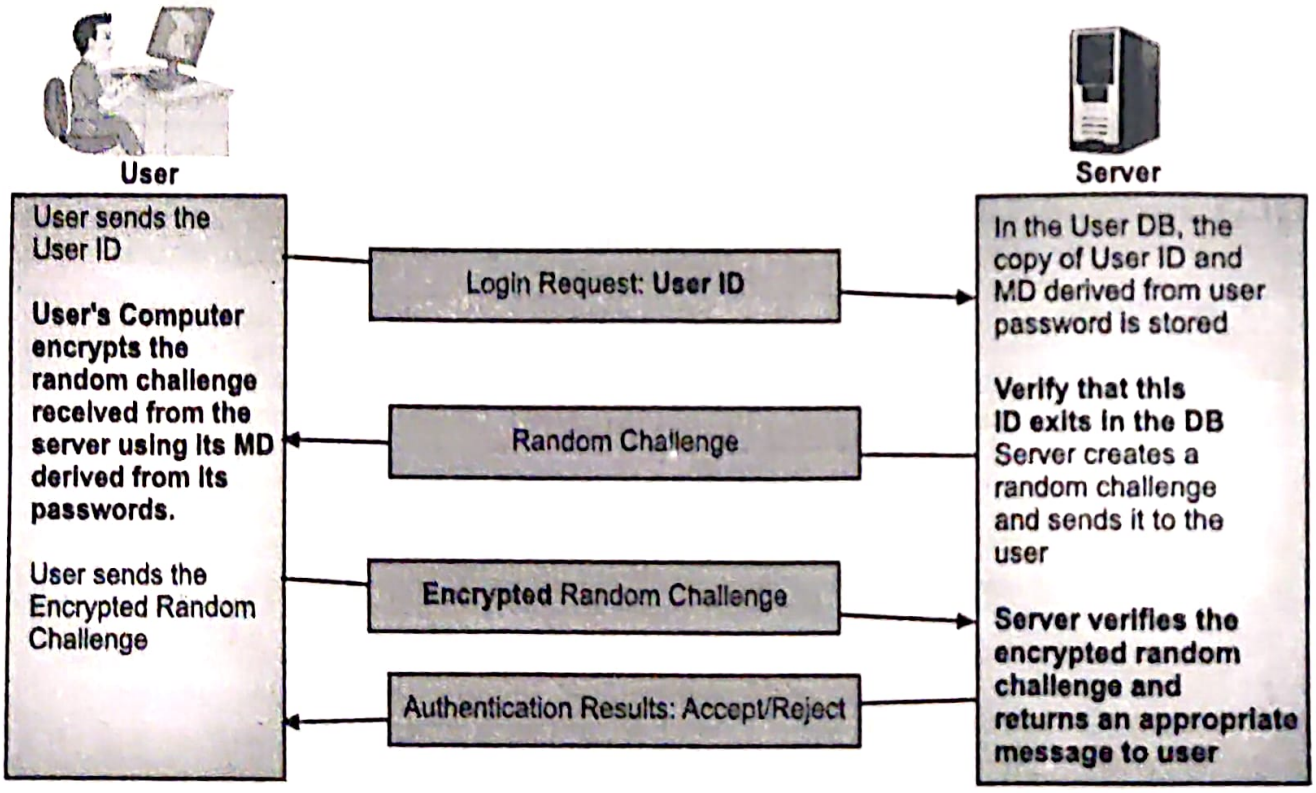


Fig. 6.7: Password Authentication using Randomness

(v) **Server Verifies the Encrypted Random Challenge from the user:** Server can do the verification in two ways either decrypting the Random Challenge or comparing the challenge values or it can encrypt the Random Challenge by the MD of the password and compare the two encrypted entities.

(vi) **Server returns an appropriate message back to the user Note:** The Random Challenge value is different every time. Therefore the random challenge encrypted with the MD of password would also be different. Therefore replay attacks can easy to detect.

Problems with the Passwords:

- Typically an organization has a number of applications, networks, shared resources and intranets. These applications may have varying needs of security measures; each resource may demand its own username and password. In that case end users/network administrators have to keep a large number of user ids and passwords to be used with different applications.
- Password maintenance is a very big concern for system administrations.
- Organizations specify password policies, which mandate the structure of passwords. For instance, an organization policy could have some of the following policies governing the passwords of its users:
  1. The password length must be at least 8 characters.
  2. It must not contain any blanks.
  3. There must be at least one lower case alphabet, one upper case alphabet, one digit and one special character in the password.
  4. The password must begin with an alphabet.
- There exit other authentication mechanisms as well besides password based authentication.

6.3.5.2 Authentication Tokens

- It is an extremely useful alternative to a password. An authentication token is a small device that generates a new random value every time it is used. This random value becomes the basis for authentication. These small devices are usually of the size of a small key chain, calculators or smart cards.
- In short, authentication token is a portable device for user authentication. Authentication tokens operate by challenge and response, time-based code sequences, or other techniques that may include paper-based lists of one-time passwords.
- Usually an authentication token has the features like processor, LCD for displaying outputs, battery, optionally a small keypad for entering information and optionally a real-time clock.

- Each authentication token is pre-programmed with a unique number called as a Random Seed or just Seed. The seed value forms the basis for ensuring the uniqueness of the output produced by the token.

Steps Involved in Authentication Token:

Step 1: Creation of a Token: It is created by the authentication servers that are designed to use with authentication tokens. A unique value i.e. a seed is automatically placed or pre-programmed inside each token by the server. Server also keeps a copy of the seed against the user ID in the user database. Seed can be conceptually considered as a user password. Difference is that the user password is known to the user, seed value remains unknown to the user.

Step 2: Use of the Token: An authentication token automatically generates pseudorandom numbers called one-time passwords. One Time Password (OTP) is generated randomly by authentication tokens using seed value.

Step 3: Validating Token: When a user wants to be authenticated by any server, the user will get a screen to enter user ID and the latest One time password. The users enter its ID and gets is latest one-time password from the authentication token. The user ID and password travels to the server as a part of the login request. Server verifies the ID, and one-time password using the stored seed value from user DB. Then Server sends an appropriate message back to the user.

6.3.5.3 Types of Authentication Tokens

- There are main two types of authentication tokens namely, Synchronous dynamic token or time-based tokens and Asynchronous dynamic token or challenge or response tokens.
- A synchronous token generates a unique password at fixed time intervals with the authentication server. An asynchronous token generates the password based on a challenge/response technique with the authentication server, with the token device providing the correct answer to the authentication server's challenge.

1. **Synchronous Dynamic Token:**

- Synchronous dynamic token use time or counters to synchronize a displayed token code with the code expected by the Authentication Server (AS).
- Time-based synchronous dynamic token display dynamic token codes that change frequently, such as every 60 seconds. The dynamic code is only good during that window.
- The AS knows the serial number of each authorized token, as well as the user with whom it is associated and the time. It can predict the dynamic code of each token using these three pieces of information.

- Counter based synchronous dynamic tokens use a simple counter, the AS expects token code 1, and the user's token displays the same code 1. Once used, the token displays the second code, and the server also expects token code 2.

2. **Asynchronous Dynamic Token:**

- Asynchronous dynamic tokens are not synchronized with a central server. The most common variety is challenge-response tokens.
- Challenge-response token authentication systems produce a challenge or input the token device.
- The user manually enters the information into the device along with their PIN, and the device produces an output, which is then sent to the system.
- The advantage of a token device is, it usually only implemented in very secure environments because of the cost of deploying the token device.
- The disadvantages of tokens are their small size and their price. If the token breaks or becomes lost, a replacement will be needed to gain access.

6.3.5.4 Multifactor Authentication

- One method for ensuring proper authentication security is the use of multifactor authentication. Multifactor authentication gets its name from the use of multiple authentication factors.
- We can think of a factor as a category of authentication. There are three authentication factors that can be used namely **'something you know'**, (would be a password, a PIN etc.), **'something you have'** (would be a token or a smart card etc.) and **'something you are'** (would be biometric identity, like a fingerprints, retina etc.).
- In order for something be considered multifactor authentication, it must make use of at least two of the three factors mentioned. For example, when a user attempts to authenticate, he or she may have to enter both their password and a one-time use token code.
- If the authentication token device gets stolen, PIN numbers are used to generate one-time passwords with the authentication token devices.
  1. **Password is a 1-factor authentication:** It is something you know.
  2. **Authentication Token are 2-factor authentication:** We must have something that is authentication token itself and PIN to protect it.

6.3.5.5 Biometric Authentication

- Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems.
- The biometric technologies involved are based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures.

- Biometric authentication is the application of that proof of identity as part of a process validating a user for access to a system.
- Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking; even just logging in to a computer or smart phone.
- Biometric verification is considered a subset of biometric authentication. Di Nardo defines biometrics as, "the automated use of physiological or behavioral characteristics to determine or verify identity".

Working of Biometric Authentication System:

- The user database contains a sample of user's biometric characteristics.
- During the authentication, the user is required to provide another sample of the users' biometric characteristic.
- This is matched with the one in the database, and if the two samples are same, the user is considered to be a valid one.
- The samples produced during every authentication process can vary slightly (e.g. cuts on the finger). So an approximate match can be acceptable.
- This is also the reason why, during the user registration process, multiple samples of the user biometric data are created. They are combined and their average stored in the user database, so that the different possibilities of the user's samples during the actual authentication can roughly map to this average sample.
- The biometric authentication process consists of several stages such as measurement, signal processing, pattern matching, and decision making.
- Measurement involves sensing biometric characteristics and is necessary both for the creation of the reference model and for each authentication trial. For example, when voice verification is utilized, this stage involves recording one's voice through a microphone.
- Then the digital data are mathematically modeled. When the user wants to be authenticated, the device compares the received data to the user model and makes a decision mostly based on a pre-calculated threshold.
- Any Biometric Authentication System defines following two configurable parameters:
  1. **False Accept Ratio (FAR):** FAR is a measurement of the chance that a user who should be rejected is actually accepted by a system as good enough.
  2. **False Reject Ratio (FRR):** It is a measurement of the chance that a user who should be accepted as valid is actually rejected by a system as not good enough.
- Thus FAR and FRR are exactly opposite to each other and in general can be controlled by a confidence threshold. To increase the security of the system, the threshold can be increased, which decreases FA errors and increases FR errors.

Types of Biometric Authentication Techniques:

- Biometric techniques are generally classified into two sub-categories namely, Physiological techniques and Behavioral techniques.

1. Physiological Techniques:

- Physiological biometrics is related to human body shape and features. With the change of this body geometry, these biometrics need to be updated to avoid failure of authentication. In general, the accuracy of physiological biometrics is higher than behavioral biometrics.
- Several techniques mentioned below:
  - **(i) Retina Scans,** produce an image of the blood vessel pattern in the light-sensitive surface lining the individual's inner eye.
  - **(ii) Iris Recognition,** is used to identify individuals based on unique patterns within the ring shaped region surrounding the pupil of the eye.
  - **(iii) Finger Scanning,** the digital version of the ink-and-paper fingerprinting process, and works with details in the pattern of raised areas and branches in a human finger image.
  - **(iv) Finger Vein ID,** is based on the unique vascular pattern in an individual's finger.
  - **(v) Facial Recognition Systems,** work with numeric codes called face prints, which identify 80 nodal points on a human face.
  - **(vi) Voice Identification Systems,** rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

2. Behavioral Techniques:

- Behavioral biometrics is related to certain kind of behavior of an individual. Hence, this authentication system can prevent a person from accessing a cyber-system, if his current behavior pattern is different from the stored behavioral pattern.
- Examples of this type of biometrics are keystroke analysis, mouse dynamics, signature, gesture, etc.

(i) Keystroke Analysis:

- Keystroke recognition is a behavioral biometric trait which captures the unique way a person types in order to correctly verifies the identity of the individual.
- Typing patterns are generally extracted from computer keyboards, phone's virtual keyboard, etc. In order to extract features for keystroke recognition, it is needed to consider the time taken to move between two keys, how hard the buttons are pressed, and how long a key is pressed before it is released.

(ii) Signature Authentication:

- Handwritten signature authentication is based on systems for signature verification and signature identification. The given signature belongs to a particular person or is

not decided through a signature identification system, whereas the signature verification system decides if a given signature belongs to a claimed person or not.

- Signature-based authentication can be either static or dynamic. In the static mode (referred to as off-line), only the digital image of the signature is available.
- In the dynamic mode, also called "on-line", signatures are acquired by means of a graphic tablet or a pen-sensitive computer display.

Advantages and Limitations of Biometric Systems:

Advantages:

1. Improved security.
2. Improved customer experience.
3. Cannot be forgotten or lost.
4. Reduced operational costs.

Limitations:

1. Biometrics can be complicated and costly to deploy. All biometric deployments require installation of their own hardware and application servers.
2. The market is still fractured. Should you buy a fingerprint reader, a voice recognition system or an iris scanner? Since each product differs greatly in its approach and installation, it is difficult to compare them during a typical company bid process.
3. Biometric data is like any other data. It sits on servers, which are bait for hackers if not properly hardened and secured. Therefore, when reviewing any biometric product, make sure it transmits data securely, meaning encrypted, from the biometric reader back to the authenticating server. And, make sure the authenticating server has been hardened, patched and protected.
4. Biometric readers are prone to errors. Fingerprints can smudge, faces and voices can be changed and all of them can be misread, blocking a legitimate user, or permitting access to an unauthorized or malicious user.
5. Difficulties with user acceptance. Properly trained employees may be willing to use biometrics devices, but customers, like those logging on to the Web site, may be more reluctant to use – or worse, forced to purchase – a device that's difficult to use or makes doing business, such as banking, on the site, a hassle instead of a convenience. And both the employees and customers may be squeamish about exposing their eyes to devices like iris scanners, even if they appear harmless.

6.3.5.6 Image-based Authentication

- Common user authentication based on passwords has the main drawback of the human difficulty in recalling them. An authentication system based on character strings as password is very vulnerable.

- An attacker can guess the user password when people use words that are easy to remember or he can use the well-known dictionary attacks methods for discovering the password.
- Images are easier to remember than passwords. An authentication method based on images can improve the security of the user authentication compared to that of textual password.
- An image based authentication system has following advantages:
  1. The user can remember images more easily than passwords ;
  2. The system will be less vulnerable to hacker attack techniques. For this reason, the use of personal/personalized images can be a means of user authentication more effective than string based (password) authentication.
  3. Moreover, modern compression and transmission techniques make image exchange between different devices (e.g. mobile phones, personal digital assistants, laptops, and workstations) in heterogeneous networks practically feasible.
- An authentication system can collect user images to be used by a challenge and response protocol for authenticating the user. Functionalities such as scalability, progressive image transmission, client/server interactivity are undoubtedly necessary in order to make the image exchange and user authentication process feasible.
- The image-based authentication identifies users by utilizing the clicked information that is inputted from the user on specific images that are displayed on the monitor as the password.
- When the clicked information is equal to the clicked information that is registered on the authentication server, the user is identified correctly. This method is mainly utilized for high-priority services such as e-commerce and Internet-baking services.

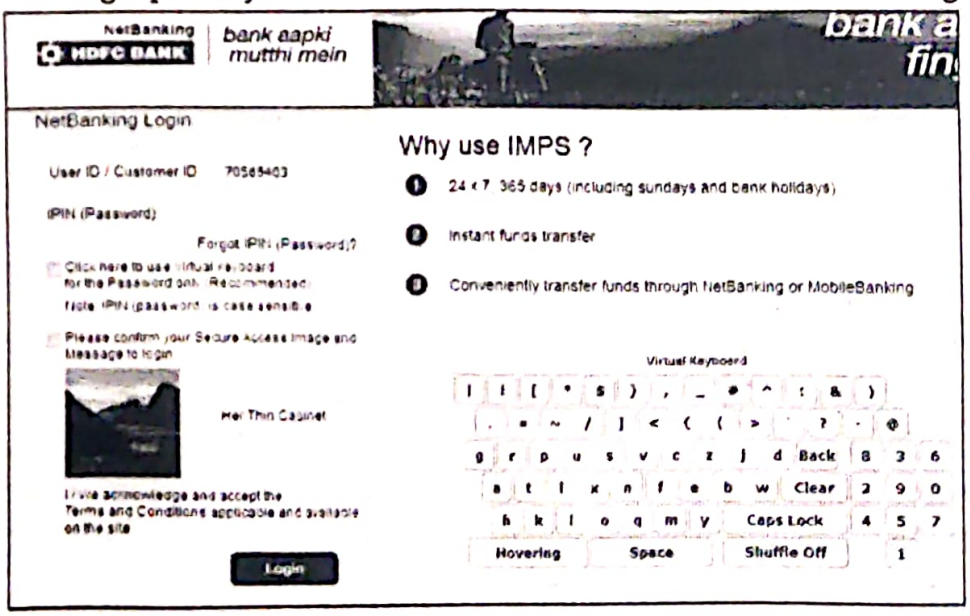


Fig. 6.8: An Example of the Image-based Authentication applied on the Internet Banking Service

6.4 TYPE OF ATTACKS

- An attack is a threat that is carried out (threat action) and if successful, leads to an undesirable violation of security. The person who carrying out the attack is referred to as attacker.
- In the next section, we will study various types of attacks.

6.4.1 Attacks (A General View)

- A network security attack refers to, an act of breaching the security provisions of a network.
- Attacks are classified into three categories as shown in Fig. 6.9.

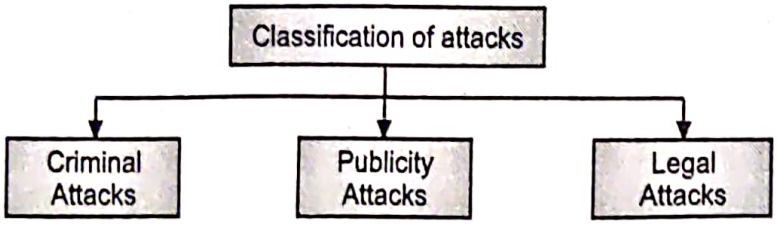


Fig. 6.9: Classification of Attacks

- These attacks have explained below:
  1. **Criminal Attacks:** The aim of the attacker is to maximize financial gain by attacking computer system. Fraud (credit cards, ATM, checks etc.), Scams (sale of services, auctions, business opportunities), Destructions, identity theft, intellectual property theft, Brand theft are some form of criminal attacks.
  2. **Publicity Attacks:** These types of attacks are usually not hardcore criminals. The people or students of university, or employees, uses a novel approach of attacking computer systems for publicity. For example, damage of web pages of a site by attacking it.
  3. **Legal Attacks:** The attacker attacks the computer system and the attacked party manages to take the attacker to the court. In such case, the attackers try to convince the judge that there is a weakness in the computer system and easily escape.

6.4.2 Attacks (A Technical View)

- The attacks are generally classified into four categories in terms of principle of security as follows:

1. **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Availability is concerned with keeping data and resources available for authorized use when they are needed.

   Examples:

   (i) Destroying some hardware (disk or cable).

(ii) Disabling file system.

(iii) Swamping a computer with jobs or communication link with packets.

2. **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality.

   Examples:

   (i) Wiretapping to capture data in a network.

   (ii) Illicitly copying data or programs.

3. **Modification:** An unauthorized party gains access and tampers an asset. This is an attack on integrity.

   Examples:

   (i) Changing data files.

   (ii) Altering a program.

   (iii) Altering the contents of a message.

4. **Fabrication:** An unauthorized party inserts a counterfeit object into the system. This is an attack on authenticity.

   Examples:

   (i) Insertion of records in data files.

   (ii) Insertion of spurious messages in a network (message replay).

- These attacks are further grouped into active attacks and passive attacks as shown in the Fig. 6.10.

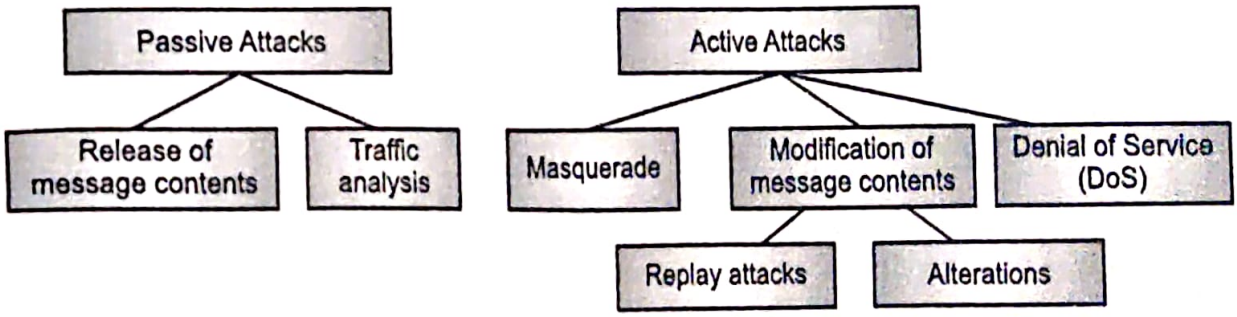


Fig. 6.10: Active and Passive Attacks

6.4.2.1 Active Attacks

- In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses.
- Active attacks include attempts to avoid or break protection features, to introduce malicious code, and to steal or modify information.
- These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

- Active attacks result in the disclosure or dissemination of data files or modification of data.
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into three categories: masquerade, modification of messages, and Denial of Service (DoS).
- Modification attacks can be classified further into replay attacks and alteration of messages.
- Fabrication causes Denial of Service (DOS) attacks.

1. **Masquerade Attacks:** These attacks takes place when one entity pretends to be a different entity. The user Z might pose as user X and send the message to user Y. 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.

   Example: An entity captures an authentication sequence and replays it later to impersonate the original entity.

2. **Modification of Messages:** A portion of a legitimate message has been altered to produce an undesirable effect. In other words, some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver, even if we do not require confidentiality for all communications, we do not want any of our messages to be modified in transit.

   Example: If we are exchanging purchase requisitions, we do not want the items, amounts or billing information to be modified.

3. **Replay Attacks:** An attack in which a service already authorized and completed is forged by another duplicate request in an attempt to repeat authorized commands. Replay involves capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

   Example: The user X wants to send some amount to the user Z's bank account. Both X and Y have account with bank Y. User X sends an electronic message to bank Y for fund transfer. User Z could capture this message and send second copy of the same to bank Y. Bank Y would have no idea that this is an unauthorized message and treats the second message as different message. So user Z would get the benefits of the fund transfer twice.

4. **Denial of Service (DoS):** Prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.

Examples: An entity may suppress all messages directed to a particular destination (For example, 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.

5. **Alteration:** Alteration of message involves some changes/modifications in the original message.

6.4.2.2 Passive Attacks

- A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.
- Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.
- Passive interception of network operations enables adversaries to see upcoming actions.
- Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.
- Passive network security attacks are in the nature of eavesdropping of transmissions of many types.
- The goal of passive attack or the hacker is to gain information being transmitted in the message to gain an edge on the other party.
- There are two main types of passive attacks as explained below:

1. **Release of a Message Contents:** In this contents of a message are read and a message may be carrying sensitive or confidential data. Release of message content - is easy to grasp just from its name and what it does it easily figured out also. In this type of passive attack a mail message, phone call any transferred message pretty much of sensitive information that would be intercepted or listened to.

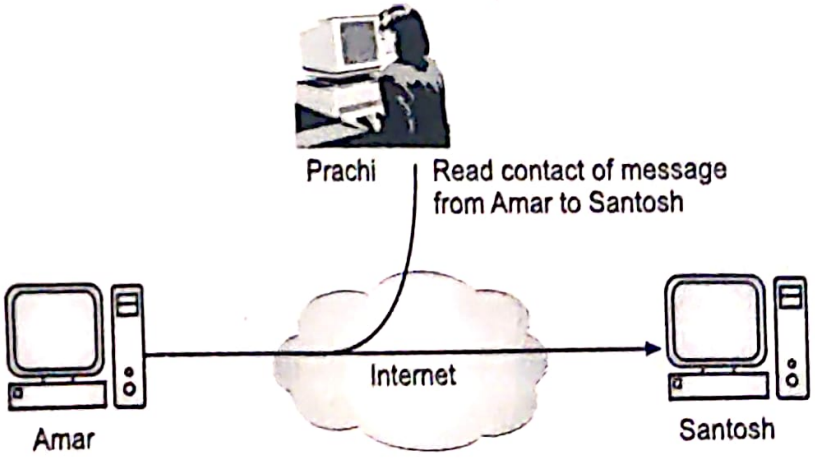


Fig. 6.11: Release of Message Contents

2. **Traffic Analysis:** In traffic analysis the intruder makes inferences by observing message patterns and can be done even if messages are encrypted. Traffic Analysis is a little more complicated. It is very subtle and hard to detect. It would be like this if we had a way to hide the information in the message and the hacker has still viewed the information this would be a traffic analysis attack.

- Passive attacks are very hard to detect because they do not damage or change the information so we cannot tell they have been attacked.
- There are many different programs out there which can help monitor against this type of network attack and against many other attacks. Again these are made for spying and for the attacker not to be noticed.

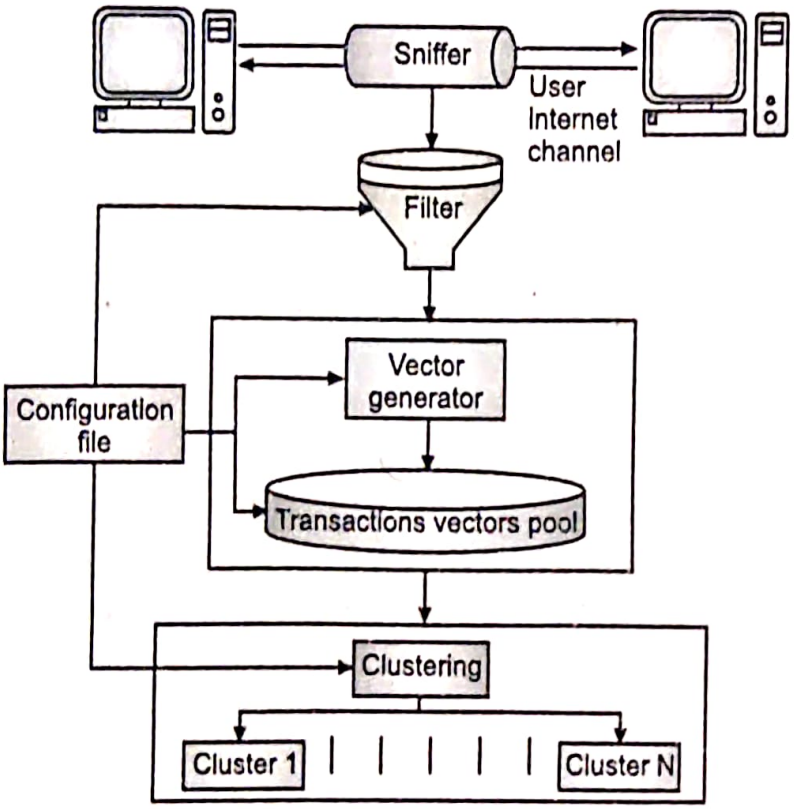


Fig. 6.12: Traffic Analysis

6.4.3 Programs that Attack

- In this section we study various programs which cause attacks:

1. **Virus:**

- A virus is a computer program that attacks itself to another legitimate program, and causes damage to the computer system or to the network.
- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity such as some may cause only mildly annoying effects while others can damage the hardware, software or files.

- Almost all viruses are attached to an executable file, which means the virus may exist on the computer but it actually cannot infect the computer unless we run or open the malicious program.

2. Worm:

- A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.
- A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- The biggest danger with a worm is its capability to replicate itself on the system, so rather than the computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

3. Trojan Horse:

- A Trojan Horse allows an attacker to obtain some confidential information about a computer or a network.
- The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on the computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor they do self-replicate.

6.4.4 Specific Attacks

- There are at least seven types of network attacks which explained below:

1. Packet Spoofing (Identity Spoofing or IP Address Spoofing):

- Any internet connected device necessarily sends IP datagrams into the network. Such internet data packets carry the sender's IP address as well as application layer data.
- If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocol to place an arbitrary IP address into the data packet's source address field.
- This is known as IP spoofing, which makes any payload appear to come from any source. With a spoofed source IP address on a datagram, it is difficult to find the host that actually sent the datagram.
- The countermeasure for spoofing is ingress filtering. Routers usually perform this. Routers that perform ingress filtering check the IP address of incoming datagrams and determine whether the source addresses that are known to be reachable via that interface.
- If the source address is not in the valid range, then such packets will be discarded.

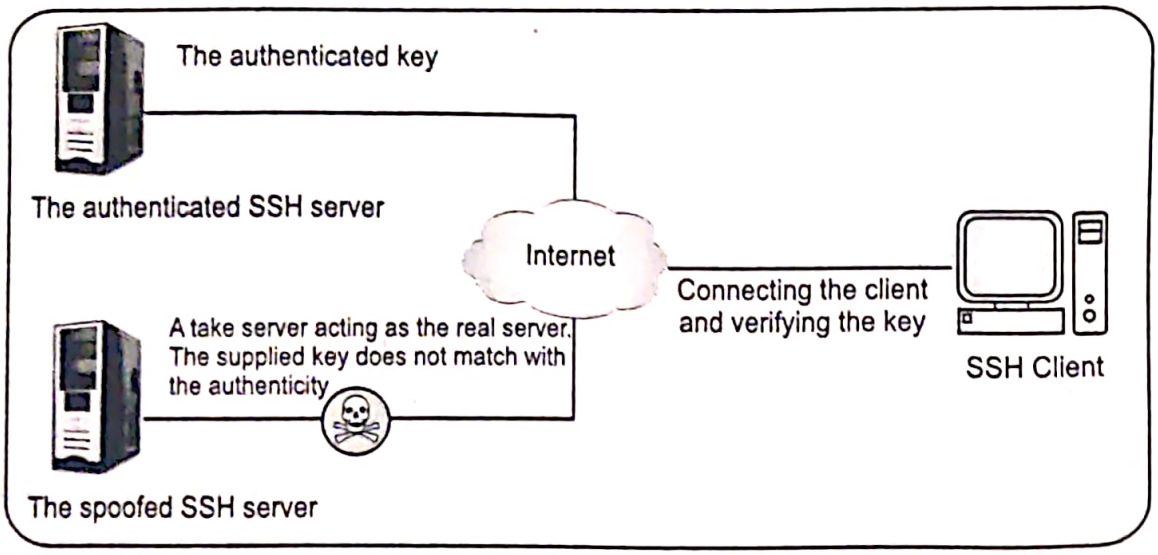


Fig. 6.13: Packet Spoofing Attack

2. Packet Sniffing:

- Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the Ethernet layer in combination with Network Interface Cards (NIC) to capture all traffic traveling to and from internet host site.

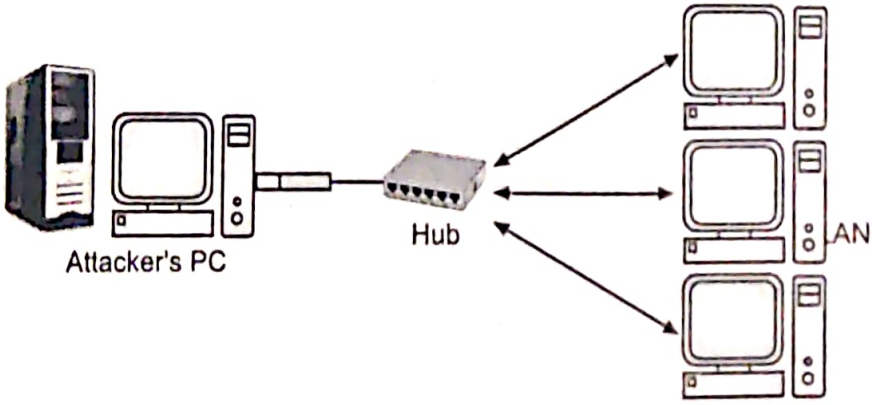


Fig. 6.14: Packet Sniffing Concept

- Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site.
- A sniffer placed on any backbone device, inter network link or network aggregation point therefore it will be able to monitor a whole lot of traffic.
- Most of packet sniffers are passive and they listen all data link layer frames passing by the device's network interface. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion.
- The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways:

  (i) Host-based: Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.

(ii) Network-based: Solutions tend to check for the presence of running processes and log files, which consume a lot of sniffer programs. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files.

- The best countermeasure against sniffing is end-to-end or user-to-user encryption.

3. Mapping (Eavesdropping):

- Before attacking a network, attackers would like to know the IP address of machines on the network, the operating systems they use, and the services that they offer.
- With this information, their attacks can be more focused and are less likely to cause alarm. The process of gathering this information is known as mapping.

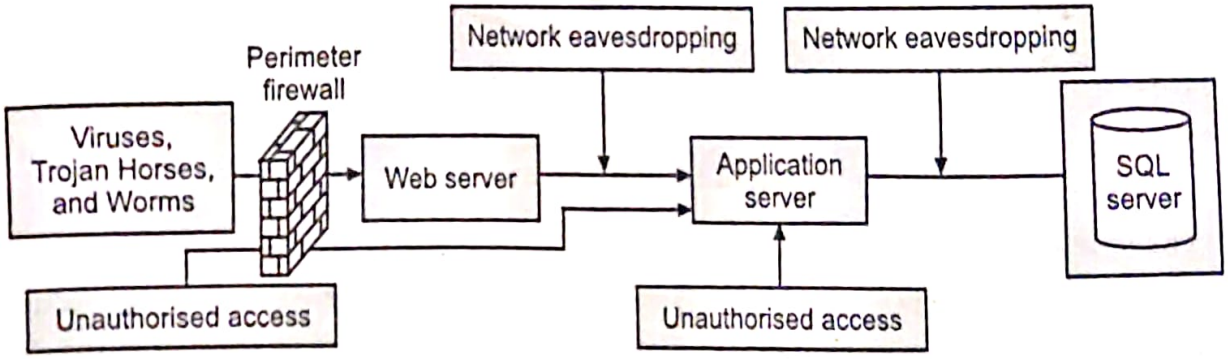


Fig. 6.15: Process of Mapping (Eavesdropping)

- In general, the majority of network communications occur in an unsecured or clear text format, which allows an attacker who has gained access to data paths in your network to listen in or interpret the traffic.
- When an attacker is eavesdropping on your communications, it is referred to as *sniffing* or *snooping*. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise.
- Counter measures are strong encryption services that are based on cryptography only. Otherwise, the data can be read by others as it traverses the network.

4. Phishing:

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims.

- Phishing emails may contain links to websites that are infected with malware.

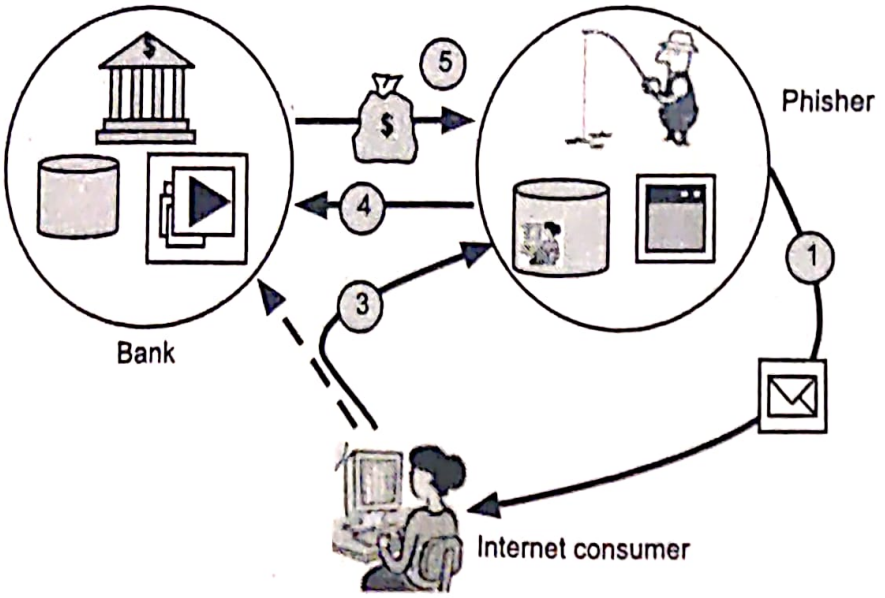


Fig. 6.16: Phishing Attack

5. Pharming (DNS Spoofing):

- DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

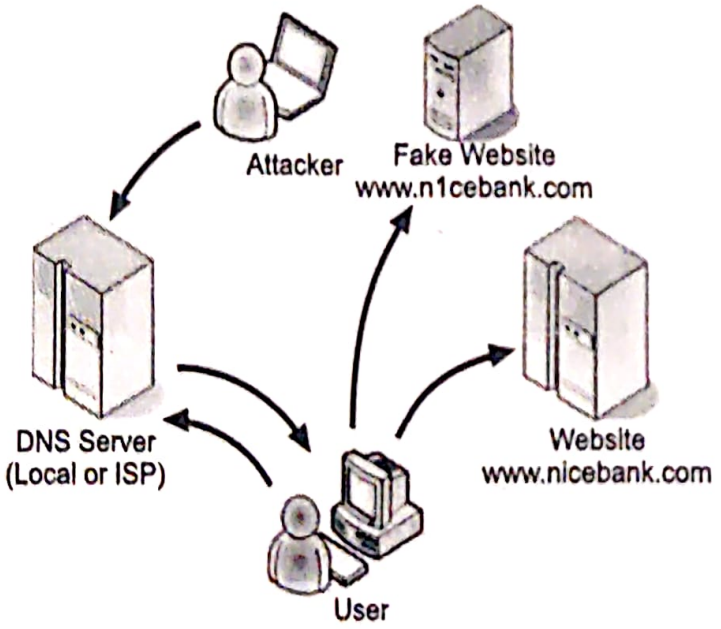


Fig. 6.17: DNS Spoofing Attack

- A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask

another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time. This means if it receives another request for the same translation, it can reply without needing to ask any other servers, until that cache expires.

- When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (often an attacker's).

6.5 CRYPTOGRAPHY (W-22)

- Cryptography is the study of secret (crypto) writing (graphy).
- Cryptography is the art of achieving security by encoding messages to make them non-readable.
- It concerned with developing algorithms which may be used to:
  1. Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  2. Verify the correctness of a message to the recipient (authentication). Cryptography forms the basis of many technological solutions to computer and communications security problems.
- Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques.
- Cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to non-readable format.
- Cryptology is a combination of Cryptography and Cryptanalysis, (See Fig. 6.18).

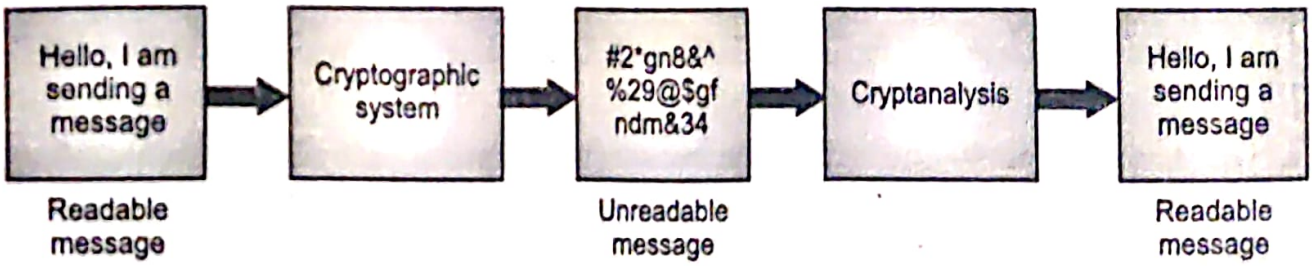


Fig. 6.18: Cryptographic and Cryptanalysis System

Purpose of Cryptography:

- Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.

- In computer field cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.
- Within the context of any application-to-application communication, there are some specific security requirements, including:
  1. **Authentication:** The process of proving one's identity, (the primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak).
  2. **Privacy/Confidentiality:** Ensuring that no one can read the message except the intended receiver.
  3. **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
  4. **Non-repudiation:** A mechanism to prove that the sender really sent this message.
- Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.
- There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.
- In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext.

Objectives of Cryptography:

- Modern cryptography concerns itself with the following four objectives or goals:
  1. **Confidentiality:** The information cannot be understood by anyone for whom it was unintended.
  2. **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
  3. **Non-repudiation:** The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
  4. **Authentication:** The sender and receiver can confirm each other's identity and the origin/ destination of the information.

6.5.1 Plaintext and Ciphertext

- The plaintext or clear text message can be understood by anybody, (sender, recipients) else who gets access total message.
- When a plaintext message is codified using any suitable scheme (encryption), the resulting message is called ciphertext.
- Fig. 6.19 shows an example for plaintext and ciphertext messages.

Plaintext: YOUAREACOMPUTEREXPERT

Ciphertext: BRXDUHDFRPSXWUHASHUW

Fig. 6.19: Plaintext and Ciphertext

- In short, plaintext refers to the original unencrypted message that the sender wishes to send while ciphertext refers to the encrypted message that is received by the receiver.
- Fig. 6.20 shows basic model for encryption.

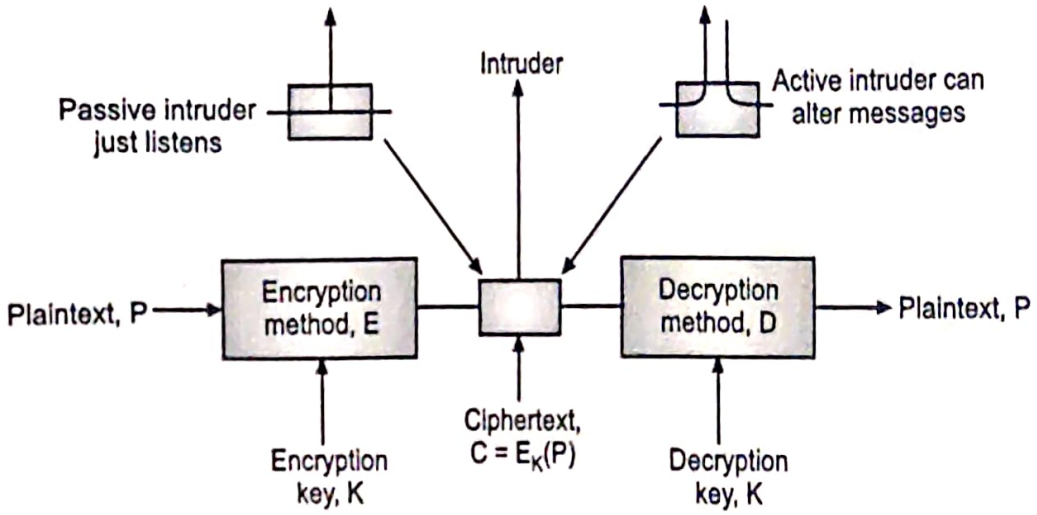


Fig. 6.20: The Basic Encryption Model

- The messages to be encrypted, known as the 'plaintext', are transformed by a function that is parameterized by a 'key'.
- The output of the encryption process, known as the 'ciphertext', is then transmitted, often by messenger or radio.
- We assume that the enemy, or 'intruder', hears and accurately copies down the complete ciphertext.
- However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily.
- Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify messages before they get to the receiver (active intruder).
- The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.
- Encryption methods have historically been divided into two categories namely, substitution ciphers and transposition ciphers.

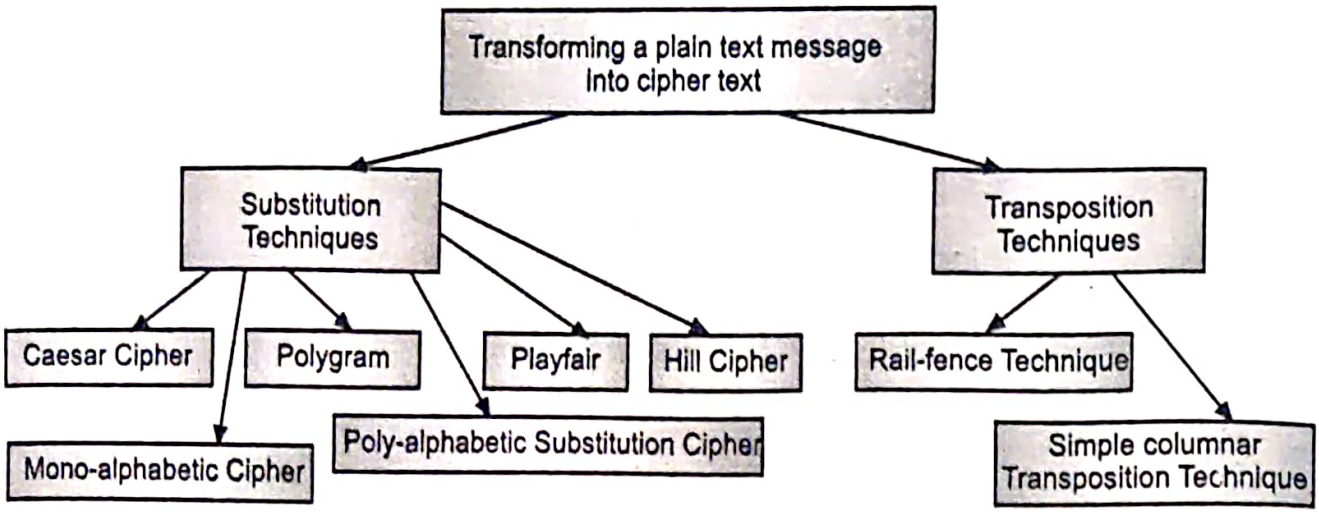


Fig. 6.21: Techniques of Transforming a Plaintext into Ciphertext

6.5.2 Encryption and Decryption

- Encryption is the process of converting the original information which is in meaningful and readable form (in cryptography we called it as plaintext) into unreadable form (in cryptography we called it is ciphertext) and requires a key for this conversion.
- The process of converting the ciphertext into plaintext is called decryption. Decryption is the reverse process of encryption and also uses a key for conversion.
- There are a number of algorithms available for encryption. Depending upon the number of key/keys used encryption is divided into two types namely, symmetric encryption and asymmetric encryption.
- A model used for encryption and decryption process is called a cryptosystem. The area of study in which one can study various techniques of encryption is known as cryptography.
- There are various techniques available to derive the plaintext or decrypt the ciphertext without much knowledge about the key and plaintext and this process is called cryptanalysis. The area of cryptography and cryptanalysis together are called cryptology.
- Fig. 6.22 (a) shows encryption and decryption process.

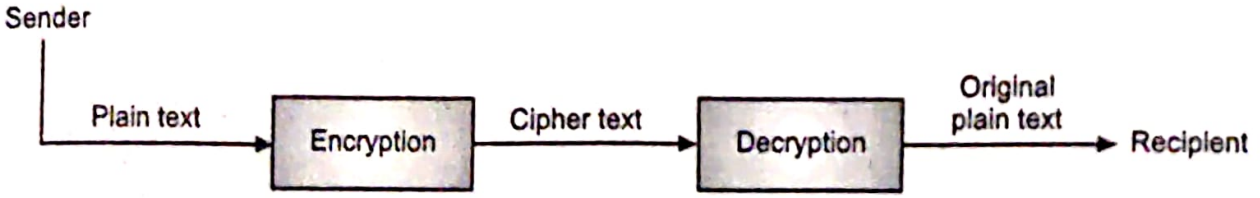


Fig. 6.22 (a): Encryption and Decryption Process

- Fig. 6.22 (b) shows an example of encryption and decryption. The process of encoding the plaintext into the ciphertext is called encryption. Decryption transforms a ciphertext message back into plaintext.

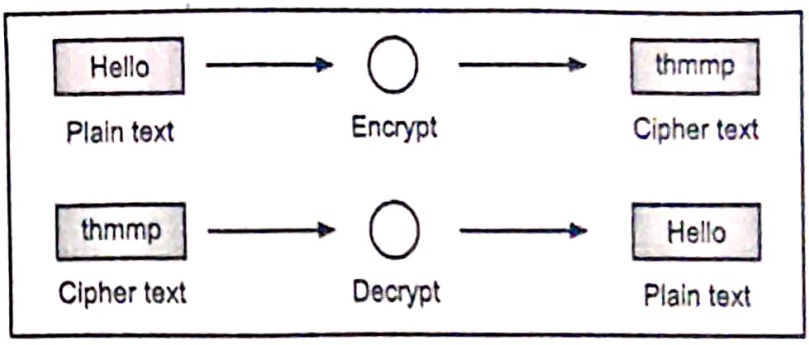


Fig. 6.22 (b): Encryption and Decryption

- Every encryption and decryption process has the algorithm and the key. The algorithm is known, but the key used for the encryption and decryption is cryptography secure.
- To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.
- There are two cryptographic mechanisms namely, Symmetric key cryptography and Asymmetric key cryptography.
- Symmetric key cryptography involves the usage of the same key for encryption and decryption. Asymmetric key cryptography involves the usage of the one key for encryption and different key for decryption.
- The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext to ciphertext; a decryption algorithm transforms the ciphertext back to plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.
- We can divide all the cryptography algorithms in the world into two groups: symmetric-key (sometimes called secret-key) cryptography algorithms and asymmetric-key (often called public-key) cryptography algorithms.

6.5.3 Symmetric Key Cryptography

- Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way.
- This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.
- Symmetric key encryption is also known as shared-key, single-key, secret-key, private-key or one-key encryption.

- In this type of message encryption, both sender and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key.
- Examples include AES (Advanced Encryption Standard) and TripleDES (Data Encryption Standard).
- In symmetric cryptography (or symmetric-key encryption), the same key is used for both encryption and decryption as shown in Fig. 6.23.

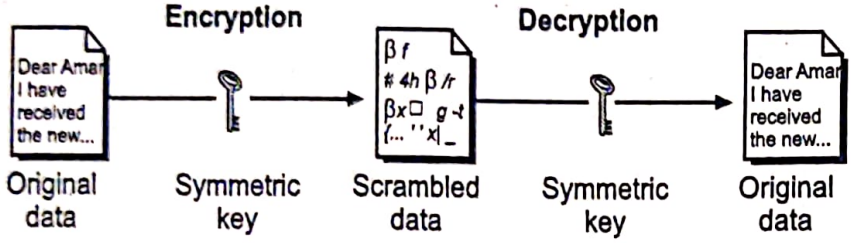


Fig. 6.23: Symmetric Key Encryption

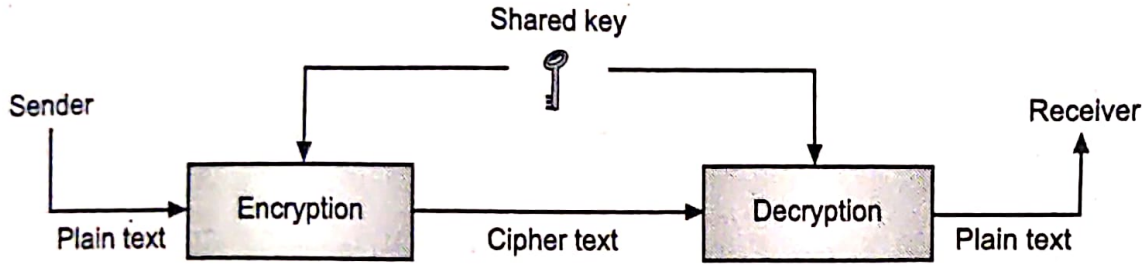


Fig. 6.24: Message Exchange Using Secret Key

- Symmetric key ciphers are valuable because:
  1. It is relatively inexpensive to produce a strong key for these ciphers.
  2. The keys tend to be much smaller for the level of protection they afford.
  3. The algorithms are relatively inexpensive to process.
- Therefore, implementing symmetric cryptography (particularly with hardware) can be highly effective because we do not experience any significant time delay as a result of the encryption and decryption.
- Symmetric cryptography also provides a degree of authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key.
- Therefore, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.
- Typically, with a symmetric key, we can exchange the key with another trusted participant; usually we produce a unique key for each pair of participants. We can be

assured that any messages that we exchange, which are encrypted in a specific key, between the participants can only be deciphered by the other participant that has that key. In this way, the key must be kept secret to each participant.

- When user A wanted to communicate with B, then we need one lock-and-key pair (A-B). When user A wanted to communicate with B and C, then we need two lock-and-key pair (A-B, and A-C), and B wants to communicate with C then pair is (B-C). When user A, B, C and D wanted to communicate with each other, then we need lock-and-key pairs (A-B, A-C, A-D, B-C, B-D, C-D). In general, for n users, the number of lock-and-key pairs is

$$n \times (n-1)/2$$

- Consequently, these keys are also referred to as secret-key ciphers. If anyone else finds the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Advantages:

1. **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
2. **Fast:** Symmetric key encryption is much faster than asymmetric key encryption.
3. **Less Computer Resources:** Single-key encryption does not require a lot of computer resources when compared to public key encryption.
4. **Prevents Widespread Message Security Compromise:** A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

Disadvantages:

1. **Need for Secure Channel for Secret Key Exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
2. **Too Many Keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
3. **Origin and Authenticity of Message cannot be Guaranteed:** Since, both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

6.5.4 Asymmetric Key Cryptography

- The concept of modern Asymmetric Cryptography or Public Key Cryptography ("PKC") was published in a Mathematics paper titled, "New directions in

cryptography" by a Stanford University professor Martin Hellman and a graduate student Whitfield Diffie in 1976. Diffie and Hellman can be regarded as the fathers of the asymmetric key cryptography.

- Asymmetric key cryptography is known as public key cryptography. It uses two separate keys namely one private and one public.
- The encryption process where different keys are used for encrypting and decrypting the information is known as asymmetric key encryption.
- Encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.
- A public-key encryption scheme has six parts:
  1. **Plaintext:** This is the readable message or data that is fed into the algorithm as input.
  2. **Encryption Algorithm:** The encryption algorithm performs various transformations on the plaintext.
  3. & 4. **Public and Private Keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
  5. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
  6. **Decryption Algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Steps in Asymmetric Key Cryptography:

- The essential steps followed in Asymmetric Key Cryptography are as follows:

  Step 1: Each user generates a pair of keys to be used for the encryption and decryption of messages.

  Step 2: Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private.

  Step 3: If Sender Rajesh wishes to send a confidential message to Amar, Rajesh encrypts the message using Amar's public key.

  Step 4: When Amar receives the message, he decrypts it using his private key. No other recipient can decrypt the message because only Amar knows Amar's private key.

- With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user's private key remains protected and secret, incoming communication is secure.

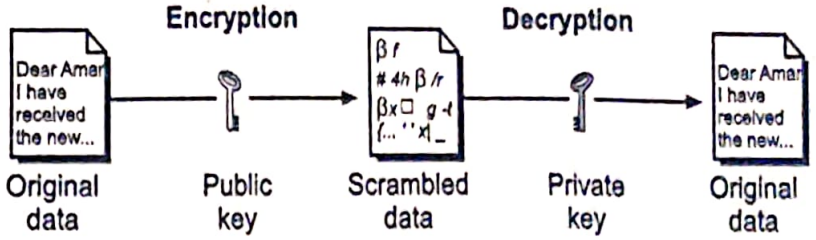


Fig. 6.25: Steps in Asymmetric Key Cryptography

- **Trapdoor Functions:** A trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are widely used in cryptography.

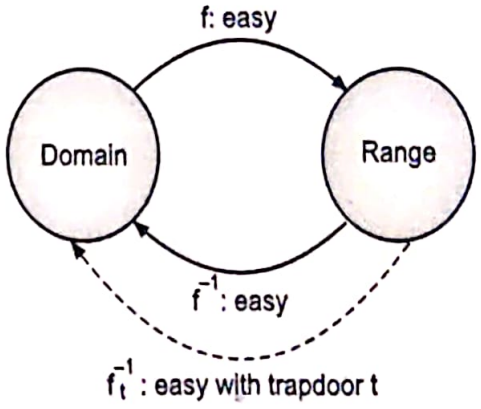


Fig. 6.26: Steps in Asymmetric Key Cryptography

Advantages:

1. **Convenience:** It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.
2. **Provides for Message Authentication:** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
3. **Detection of Tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
4. **Provide for Non-repudiation:** Digitally signing a message is similar to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages:

1. **Public Keys should/must be Authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

2. **Slow and Time Consuming:** Public key encryption is slow compared to symmetric encryption. Calculating the ciphertext from plaintext using the long keys takes a lot of time.
3. **Uses more Computer Resources:** It requires a lot more computer supplies compared to single-key encryption.
4. **Widespread Security Compromise is Possible:** If an attacker determines a person's private key, his or her entire messages can be read.
5. **Loss of Private Key may be Irreparable:** The loss of a private key means that all received messages cannot be decrypted.

6.6 SUBSTITUTION TECHNIQUES

- In substitution cipher technique, the characters of plaintext messages are replaced by other characters, numbers or symbols.
- A substitution cipher is a one in which each character in the plaintext is substituted for another character in the ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.
- In this section we study various types of substitution ciphers like Caesar, Playfair, Mono-alphabetic etc.

6.6.1 Caesar Cipher

- In this technique, the characters of a plaintext message are replaced by other characters. The method is named after Julius Caesar, who used it in his private correspondence.
- A Caesar cipher, or the shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- In Caesar cipher each alphabet of plaintext is replaced by an alphabet obtained by shifting three (3) letters from it.
- For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

Example:

- The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by 3 places. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

- When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

  Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

  Ciphetext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

- Deciphering is done in reverse, with a right shift of 3.

Algorithm to break Caesar Cipher:

Step 1: Read each alphabet in the ciphertext message, and search for it in the second row of the replacement table.

Step 2: When the match is found, replace that alphabet in the ciphertext message with the corresponding alphabet in the same column but first row of the table.

Step 3: Repeat the process for all alphabets in the message.

Example:

Ciphertext	L		O	R	Y	H		B	R	X
Plaintext	I		L	O	V	E		T	E	A

Modified version of Caesar Cipher:

- Let us assume that the ciphertext alphabets corresponding to the original plaintext alphabets may not necessarily be three places down the order, instead any places down the order. For example, Letter A in plaintext would not necessary replace by D, but by any letter (i.e. B through Z).
- For each alphabet there are 25 possibilities of replacement (letter itself cannot be replace).
- The attacker attempts to use all possible permutations and combinations, is called brute –force attack.
- To break the ciphertext, under each letter of the ciphertext, the entire alphabet is written out in reverse starting at that letter. This attack can be accelerated using a set of strips prepared with the alphabet written down in reverse order. The strips are then aligned to form the ciphertext along one row, and the plaintext should appear in one of the other rows. (See the following example).
- To break this version of Caesar cipher the following Algorithm used:

  Step 1: Let K = 1

  Step 2: Read ciphertext message.

  Step 3: Replace each alphabet in the ciphertext with an alphabet that is n position down the order.

  Step 4: K=K+1.

  Step 5: If K<26, goto step 2, else stop.

- **Disadvantage:** There an easy attack that consists of trying, by "brute force", all the possible 26 keys. This is no smart analysis of the encryption algorithm: the problem is the (very) small number of keys.

Example:

- Consider ciphertext "KWUMPMZN". The output produce by the above algorithm to break the cipher message "KWUMPMZN" is shown in the table. The 18th attempt is the correct plaintext "come here".

Ciphertext	K	W	U	M		P	M	Z	M
Attempt Number (Value of k)									
1	L	X	V	N		Q	N	A	N
2	M	Y	W	O		R	O	B	O
3	N	Z	X	P		S	P	C	P
4	O	A	Y	Q		T	Q	D	Q
5	P	B	Z	R		U	R	E	R
6	Q	C	A	S		V	S	F	S
7	R	D	B	T		W	T	G	T
8	S	E	C	U		X	U	H	U
9	T	F	D	V		Y	V	I	V
10	U	G	E	W		Z	W	J	W
11	V	H	F	X		A	X	K	X
12	W	I	G	Y		B	Y	L	Y
13	X	J	H	Z		C	Z	M	Z
14	Y	K	I	A		D	A	N	A
15	Z	L	J	B		E	B	O	B
16	A	M	K	C		F	C	P	C
17	B	N	L	D		G	D	Q	D
18	C	O	M	E		H	E	R	E
19	D	P	N	F		I	F	S	F
20	E	Q	O	G		J	G	T	G
21	F	R	P	H		K	H	U	H
22	G	S	Q	I		L	I	V	I
23	H	T	R	J		M	J	W	J
24	I	U	S	K		N	K	X	K
25	J	V	T	L		O	L	Y	L

6.6.2 Transposition Cipher

- In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.
- Transposition cipher changes the location of characters in plaintext to from the ciphertext. In this cipher, there is no substitution of characters and thus, the order of characters in the plaintext is no longer preserved in the ciphertext.

1. Rail-Fence Technique:

- In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out.
- The message is then read off in rows. For example, if we have 3 "rails" and a message of 'WE ARE DISCOVERED FLEE AT ONCE', ciphertext writes out:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E .R .D .S .O .E .E .F .E .A .O .C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

- Now read the text row by row. The ciphertext is: WECRLTEERDSOEEFEAOCAIVDEN

2. Simpler Columnar Transposition Techniques:

(i) Basic Techniques:

- The message is written out in row by row of a fixed length. Then read out the message column by column, and the columns are chosen in some scrambled order, i.e. it can be any order such as 3, 2, 4 etc. The message thus obtained is ciphertext message.

Example:

- Consider the plaintext message " Hello I am here", Now this message can be transform into cipher as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
h	E	l	l	o
i	A	m	h	e
r	E			

- Let us consider 5 columns. Now, decide the order of columns (random), say, 3, 4, 2, 5, 1 and read the text in this order. We get ciphertext as **lmlheaeoehir.**

(ii) Simpler Columnar Transposition Techniques with Multiple rounds:

- **A single columnar transposition could be attacked by guessing possible column lengths.**

- To improve the above technique, we can have the basic technique, but to do it more than once.
- The ciphertext produce by Simpler Columnar Transposition Techniques with Multiple rounds is much more complex and hard to crack.

Procedure:

Step 1: Write the plaintext row by row. Read the message column by column in random order.

Step 2: The message obtained is the ciphertext of round one.

Step 3: Repeat the steps 1 and 2 as many times as desire.

Example:

- Let us consider same plaintext message " Hello I am here" , which generate ciphertext in round 1 as lmlheaeoehir .
- Now, Repeat the same process on the cipher for further round as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
l	M	l	h	e
a	E	o	e	h
i	R			

- Now, use the same order of column as 3, 4, 2, 5, 1 and read the text in this order. We get ciphertext as lohemerehlai
- Repeat this process with more number of times if desire, otherwise stop.

3. Vernam Cipher/ One-Time Pad (OTP):

- In Cryptography, the One-Time Pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad).
- One-time pad (OTP), also called Vernam-cipher or the perfect cipher.
- Once, an input ciphertext for transposition is used, it is never been used again for any other message.
- The length of the input ciphertext and the original plaintext should be the same.

Procedure:

Step 1: Consider each character in the plaintext as a number i.e. A=0, B=1 ..., Z=25.

Step 2: Add each number corresponding to the plaintext alphabet to the corresponding input ciphertext alphabet number.

Step 3: If the sum produced is greater than 26, subtract 26 from it.

Step 4: Translate each number of the sum back to the corresponding letter, which results the output ciphertext.

Example:

- Consider the plaintext "How are you", using one-time-pad NCBTZQARX.
- We will discuss to produce a ciphertext message as follows:

Plaintext	H	o	w	a	r	e	y	o	u	
	7	14	22	0	17	4	24	14	20	
One-time Pad	N	C	B	T	Z	Q	A	R	X	**SUM**
	13	2	1	19	25	16	0	17	23	
Initial total	20	16	23	19	42	20	24	31	43	
Subtract 26	20	16	23	19	16	20	24	5	17	
Ciphertext	U	Q	X	T	Q	U	Y	F	R	

6.7 FIREWALL (W-18, W-22, S-23)

- Firewalls can be used to protect a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
- Firewalls exist both as software (software firewalls are installed on the computers) that run on a hardware (hardware firewalls are standalone products).

6.7.1 Need of Firewall

- For most of the organization, the Internet is the virtual backbone of their enterprise network, interconnecting an organization's corporate network and those of its business partners and customers.
- Every organization needs internet access, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization.
- To protect confidential information from those who do not explicitly need to access it and its resources from malicious users & accidents that originate outside of our network.

6.7.2 What is Firewall?

- **Definition:** A firewall is defined as a single choke point that keeps unauthorized users out of trusted or protected network, prohibits potential vulnerable services from entering and leaving the network and provides protection from various kinds of IP spoofing and routing attacks.
- A firewall is inserted between premises of the network connects and the Internet. This location permits the firewall to provide authentication and other security services to remote users in order to prevent unauthorized users from logging in to the network.

- It is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on defined set of security rules it accept, reject or drop that specific traffic.
- Technically, Firewall is specialized version of a router.
- It provides a location for monitoring security related events and provides convenient platform for several internet functions such as NAT, internet usage audit or logs.
- A firewall can serve as platform for IPsec to implement VPN.
- Firewall must immune itself to penetration since it will be target of attack.
- The following Fig. 6.27 illustrates a firewall-controlled access to the enterprise network from the Internet.

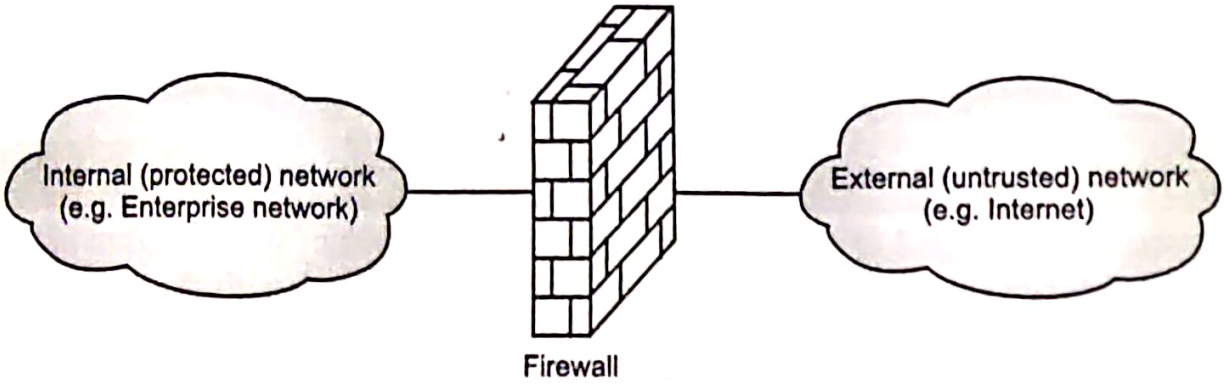


Fig. 6.27: Firewall controlled access from Internet

6.7.3 Design Goals of Firewall

- The following are the design goals of a firewall.
  1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.
  2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
  3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.
- There are four essential controls exercised by a firewall:
  - **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
  - **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec.
- **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

6.7.4 Limitations of Firewall

- Firewalls have their limitations, including the following:
  1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
  2. The firewall does not protect against internal threats, such as an unhappy employee or an employee who unwittingly cooperates with an external attacker.
  3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

6.7.5 Types of Firewall

- The following figure 6.28 shows types of firewall.

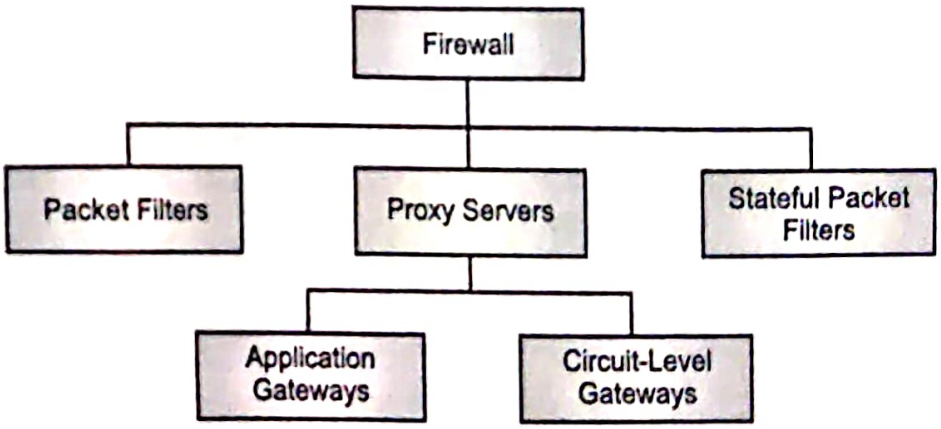


Fig. 6.28: Types of firewall

6.7.5.1 Packet Filters Firewall

- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

- The router is typically configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a network packet: Source and destination IP address protocols and ports.
- It analyses traffic at the transport protocol layer.
- Packet firewalls treats each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic.
- Only it can allow or deny the packets based on unique packet headers.
- Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded.

Advantages:

1. Packet filters are fast and can be easily implemented in existing routers.
2. Transparency to the user is the users need not know about the presence of the firewall and this is also typically high speed.

Disadvantages:

1. It may be difficult to set up the packet filter in rules.
2. Lack of authentication and less secure: cryptographic technique is not used anywhere. So that here attacks like IP spoofing can be carried out where someone can change the IP address of a network of the machine and can get some unwanted advantage or authorization which otherwise that person is not allowed to have.

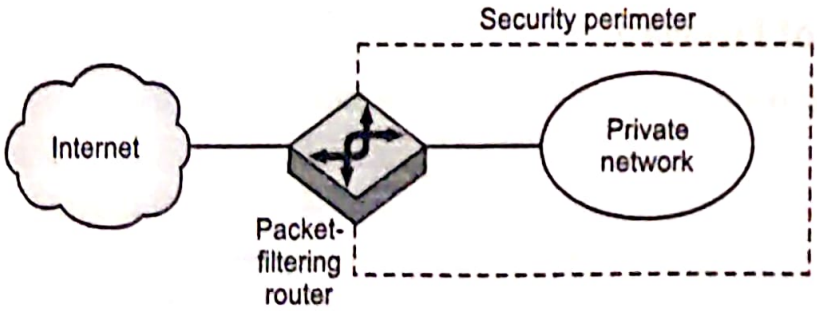


Fig. 6.29: Packet-Filtering

6.7.5.2 Stateful Inspection Firewall

- Stateful packet firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient.
- It keeps track of the state of networks connection travelling across it, such as TCP streams.
- A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.

- There is an entry for each currently established connection.
- The stateful packet firewall will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

Advantages:

- The connection table greatly reduces the chance that a packet will be spoofed to appear as it were part of an existing connection.
- It has the ability to look into the data of certain packet types.

Disadvantages:

- It does not protect the internal hosts to the same degree as an application layer firewall.
- It does not act as proxy or setup a separate connection on behalf of the source.

6.7.5.3 Proxy Servers (S-22)

- A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy.
- All communication between a user and the actual server occurs through the proxy server.
- A proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions.
- Proxy servers can operate at either the application layer or the transport layer.
- There are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

1. Application Level Gateway:

- An application gateway is a proxy server that provides access control at the application layer.
- It acts as an application-layer gateway between the protected network and the untrusted network. Because it operates at the application layer, it is able to examine traffic in detail and, therefore, is considered the most secure type of firewall.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.
- It can also log all network activities according to applications for both accounting and security audit purposes.
- Application layer firewalls can also be used as Network Address Translator.

Advantages:

- Application level gateways tend to be more secure than packet filters.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application level gateway need only scrutinize a few allowable applications.
- It is easy to log and audit all incoming traffic at the application level.

Disadvantages:

- Prime disadvantage of the application level gateway is the additional processing overhead on each connection. In effect there are two spliced connections between the end users with the gateway at the splice point and the gateway must examine and forward all traffic in both directions.

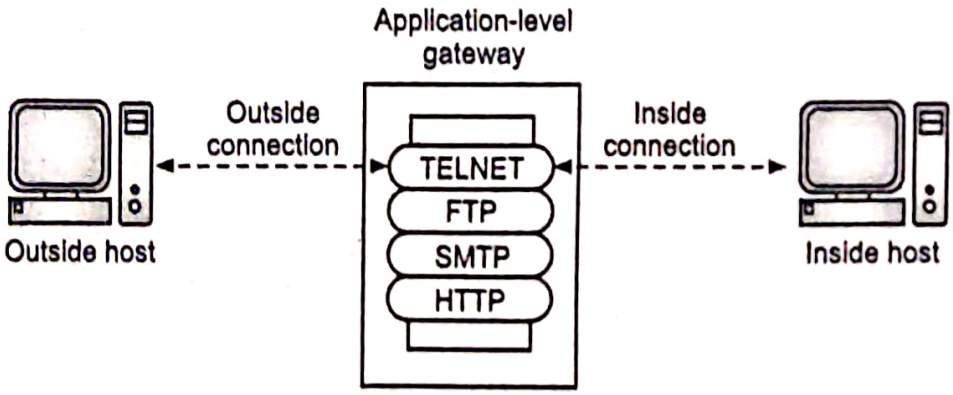


Fig. 6.30: Application-level Gateway

1. Circuit-level Gateways:

- A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied.
- A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.
- A circuit-level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders.

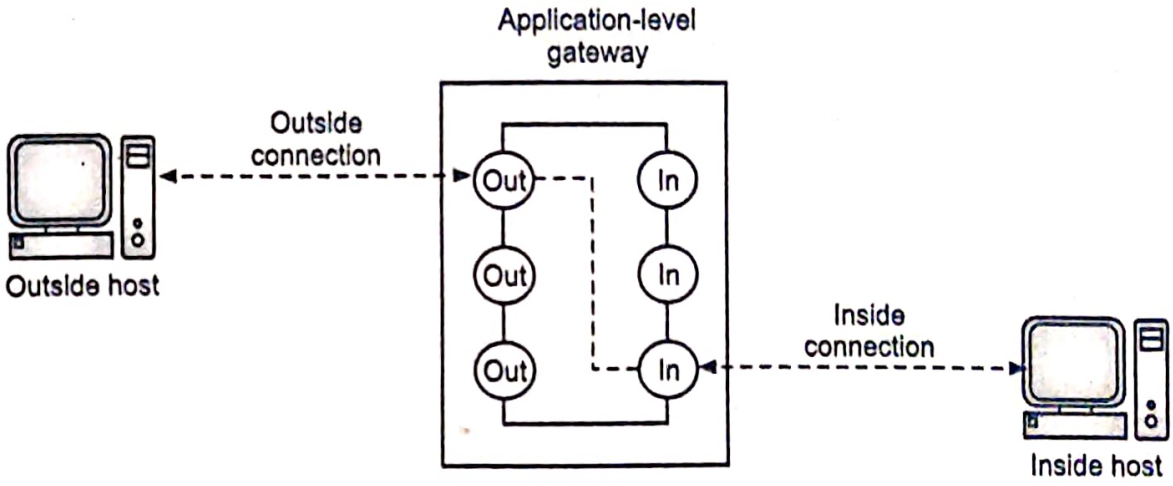


Fig. 6.31: Circuit-level Gateway

Advantages:

- Private network data hiding.
- Avoidance of filtering individual packets.
- Flexible in developing address schemes.
- Don't need a separate proxy server for each application.
- Simpler to implement.

Disadvantages:

- A circuit level gateway cannot examine the data content of the packets it relays between a trusted network and an untrusted network. The potential exists to slip harmful packets through a circuit level gateway to a server behind the firewall.
- It can only handle TCP connections – new extensions proposed for UDP.
- TCP/IP stacks are mandatorily be modified by vendor for using CL Gateways.

6.8 STEGANOGRAPHY (S-23)

- Steganography is a technique that facilitates hiding of message that is to be kept secret inside other messages. It is also known as stego.
- The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

- Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.
- Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.
- For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.
- In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.

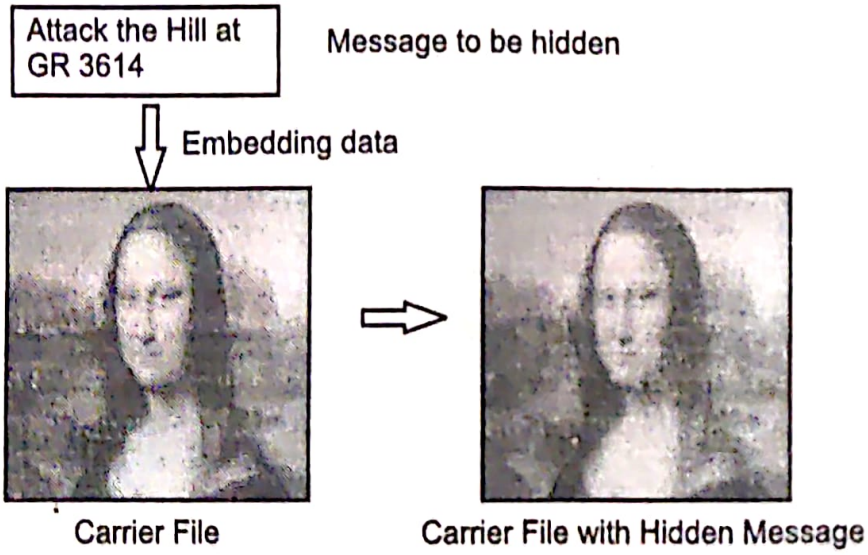


Fig. 6.32: Example of Steganography

6.9 COPYRIGHT (W-22, S-23)

- Copyright refers to the legal right of the owner of intellectual property. In simpler terms, copyright is the right to copy. This means that the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work.
- With the ceaseless usage of web and other online services, it has turned out that copying, sharing, and transmitting digital media over the Internet are amazingly simple.

- Since the text is one of the main available data sources and most widely used digital media on the Internet, the significant part of websites, books, articles, daily papers, and so on is just the plaintext.
- Therefore, copyrights protection of plaintexts is still a remaining issue that must be improved in order to provide proof of ownership and obtain the desired accuracy.
- Major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting.
- Watermarking hides copyright information within a watermark by overlaying files not easily detected by the naked eye. This prevents fraudulent actions and gives copyright protected media extra protection.
- During the last decade, digital watermarking and steganography techniques have been used as alternatives to prevent tampering, distortion, and media forgery and also to protect both copyright and authentication.
- Digitally marking a file with a text or with an image is known as Digital Watermarking. It is commonly used for the purpose of authenticating a digital file and for copyright protection. By placing a watermark in a digital file, can ensure copyright protection and authenticity of the digital file.
- Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can use the fingerprint to identify which customer violated the license agreement by distributing a copy of the file.

Applications:

- Text watermarking techniques are applicable in many applications. The following points are the most important watermarking applications.

(i) **Digital Copyright Protection (Proof of Ownership):** Text watermarking provides passive protection tools for digital documents so that the text content cannot be illegally copied or replicated. For example, if someone copies a watermarked document/file (e.g., PDF, Docx, Latex, and RTF), then the reversibility of watermarking techniques can be used to prove the ownership of the copied documents

(ii) **Access Control (Copy Control):** Currently, the publishers and the content providers are seeking more reliable ways to control copy or access to their valuable documents, and simultaneously, they want to make the documents accessible on the Internet in order to obtain more revenue. The text watermarking is a desirable technique on the online systems that provide access control to prevent illegal copy or restrict the number of times of copying the original text.

(iii) **Tamper Proofing:** These days a huge number of text documents are available online for selling or reading for users. Therefore, these documents are prone to be exposed to a number of attacks (e.g., unauthorized access, copy, and redistribution). In this case, text watermarking can be used as a fragile tool for tamper proofing of the watermarked texts against attacks. In general, a fragile watermark is embedded into text documents, and if any type of alterations has been made, then it fails to detect the watermark.

(iv) **Text Content Authentication:** The online publishing of articles and newspapers in form of plaintext documents has brought several issues related to authenticating the integrity of these documents. Text watermarking can be applied as an authentication tool to verify the integrity of plaintext documents.

(v) **Forgery Detection (Prevention):** Plagiarism and reproduction of text documents are serious forgery activities and are rapidly increasing. Text watermarking can be used as a forgery detection tool by embedding a watermark in the original text before the online publishing. Thus, it can prove the plagiarism and reproduction of the watermarked texts.

Summary

- Network security is the security provided to a network from unauthorized access and risks. It measures are needed to protect data during their transmission and to guarantee that data transmissions are authentic.
- One of the key aspects of cryptography and network/Internet security is authentication. Authentication helps establish trust by identifying the particular user/system. Authentication ensures that the claimant is really who he/she claims to be. This is process of establishing the legitimacy of anode or user before allowing access to requested information.
- The main types of authentication available are Password based authentication, Token based authentication, Biometric based authentication and Image based authentication.
- Attacks are typically categorized based on the action performed by the attacker. Thus an attack can be passive or active.
- Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.
- Data integrity is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently.

- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
- Encryption key is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- Decryption key is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it.
- Substitution and transposition ciphers are two categories of ciphers used in cryptography.
- In the substitution-cipher technique, the characters of a plain-text message are replaced by other characters, numbers or symbols.
- A transposition cipher is methods of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.
- A firewall is defined as a single choke point that keeps unauthorized users out of trusted or protected network, prohibits potential vulnerable services from entering and leaving the network and provides protection from various kinds of IP spoofing and routing attacks.
- Firewalls are classified into three common types namely packet filters, circuit level gateways and application level gateways.
- Packet filters firewalls processes network traffic on a packet-by-packet basis. A packet filter's main function is to filter traffic from a remote.
- The circuit level gateway represents a proxy server that statically defines what traffic will be forwarded. Circuit proxy's always forward packets containing a given port number if that port number is permitted by the rule set. A circuit level gateway operates at the network level of the OSI model. This gateway acts as an IP address translator between the Internet and the internal system. The main advantage of a proxy server is its ability to provide NAT.
- The application-level gateway represents a proxy server, performing at the TCP/IP application level, that is set up and torn down in response to a client request, rather than existing on a static basis. Application proxies forward packets only when a connection has been established using some known protocol.
- Steganography is a technique that facilitates hiding of message that is to be kept secret inside other messages.
- Major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting,

Check Your Understanding

1. The _____ is the original message before transformation.
   (a) ciphertext (b) plaintext
   (c) secret-text (d) none of the above
2. In an asymmetric-key cipher, the sender uses the _____ key.
   (a) private (b) public
   (c) either (a) or (b) (d) neither (a) nor (b)
3. A combination of an encryption algorithm and a decryption algorithm is called a _____
   (a) cipher (b) secret
   (c) key (d) none of the above
4. Proxy firewall filters _____.
   (a) physical layer (b) data-link layer
   (c) network layer (d) application layer
5. Technically, _____ is specialized version of a router.
   (a) Firewall (b) Bridge
   (c) Gateway (d) Modem

ANSWERS

1. (b)	2. (b)	3. (a)	4. (d)	5. (a)

Practice Questions

Q.I Answer the following questions in short.

1. What is meant by Network security?
2. What is plaintext and ciphertext?
3. What is attack? What are its types?
4. What is encryption and decryption?
5. Write names of substitution techniques?
6. What are types of Firewall?

Q.II Answer the following questions.

1. How proxy servers and firewalls help in maintaining network security? Explain.
2. Explain working of firewall.
3. Explain the devices used to maintain network security.
4. What is difference between substitution cipher and transposition cipher?
5. Distinguish between symmetric and asymmetric cryptography.

Q.III Define the following terms:

1. Firewall
2. Steganography
3. Copyright
4. Passive attack
5. Active attack

Previous Exams Questions

Winter 2018

1. Explain Firewall and its security features. 5M

Ans. Refer to section 6.7

SOLVED QUESTION PAPERS
WINTER 2022

Time : 2½ Hours] **[Max. Marks : 70**

Instructions to the candidates:

1) All questions are compulsory.

2) Neat diagrams must be drawn wherever necessary.

1. Attempt any three of the following: **[3 × 5 = 15]**

(a) Define Network Topology? Explain different types of topologies.

Ans.: Refer to Section 1.2

(b) Explain function of each layer of ISO-OSI reference model.

Ans.: Refer to Section 2.2.2

(c) What is wireless transmission? Explain any two media in detail.

Ans.: Refer to Section 3.3.3

(d) Define the bridge? Explain the types of bridge.

Ans.: Refer to Section 5.4

2. Attempt any three of the following: **[3 × 5 = 15]**

(a) Define Computer Network. Explain goals of Computer Network.

Ans.: Refer to Sections 1.1.1 and 1.1.2

(b) Explain different types of addresses.

Ans.: Refer to Section 2.6

(c) Explain propagation methods in detail.

Ans.: Refer to Section 3.3.2

(d) Explain Firewall and its Security Features.

Ans.: Refer to Section 6.7

3. Answer any Four the following: **[3 × 5 = 15]**

(a) Draw TCP/IP model and state the function of each layer.

Ans.: Refer to Section 2.3.2

(b) Compare connection oriented and connectionless service.

Ans.: Refer to Section 1.7.3

(c) What is Router? Explain its components.

Ans.: Refer to Section 5.6

(d) What is Ethernet? What are its types? Explain any one in detail.

Ans.: Refer to Section 4.2

4. Answer any Four the following: **[3 × 5 = 15]**

(a) Explain IEEE standards 802-11 in detail.

Ans.: Refer to Section 4.8.4

(b) Compare ISO-OSI reference model and TCP/IP model.

Ans.: Refer to Section 2.5

(c) What is cryptography? Explain encryption and decryption process.

Ans.: Refer to Section 6.5

(d) Explain Fiber optic cable in detail.

Ans.: Refer to Section 3.2.4

5. Write short note on any Two of the following: **[2 × 5 = 10]**

(a) Modes of Communication.

Ans.: Refer to Section 1.4

(b) Bluetooth Architecture.

Ans.: Refer to Section 4.9.2

(c) MAC sublayer with its Frame Format.

Ans.: Refer to Section 4.3

(d) Copyright

Ans.: Refer to Section 6.9

❖❖❖

SUMMER 2022

1. Attempt any three of the following: **[3 × 5 = 15]**

(a) What is networking? Explain different types of network.

Ans.: Refer to Section 1.1 and 1.3

(b) Explain TCP/IP protocol in details.

Ans.: Refer to Sections 2.4

(c) What is guided media? Explain types of guided media.

Ans.: Refer to Section 3.2

(d) Explain Active and Passive Hub.

Ans.: Refer to Sections 5.2.2 and 5.2.3

2. Attempt any three of the following: **[3 × 5 = 15]**

(a) What are repeaters? Explain different types of repeaters.

Ans.: Refer to Section 5.3

(b) What are different mode of communication? Explain with sketch.

Ans.: Refer to Section 1.4

(c) What is security services? Explain security mechanisms to provide the services.

Ans.: Refer to Section 6.3

(d) Explain Bluetooth in details.

Ans.: Refer to Section 4.9

3. Attempt any three of the following : **[3 × 5 = 15]**

(a) What is standard? What is their needs? Explain the two types of standard.

Ans.: Refer to Section 1.6.3

(b) What is Fast Ethernet? Explain categories of Fast Ethernet.

Ans.: Refer to Section 4.3

(c) Explain server based and peer to peer LANS.

Ans.: Refer to Sections 1.5.1 and 1.5.2

(d) Differentiate between fiber optic and twisted pair cable.

Ans.: Refer to Sections 3.2.3 and 3.2.4

4. Attempt any three of the following : **[3 × 5 = 15]**

(a) What is attack? Explain various types of attacks.

Ans.: Refer to Section 6.4

(b) Explain wireless transmission. Explain any one media in details.

Ans.: Refer to Section 3.3.3

(c) What is addressing? Explain different types of addresses.

Ans.: Refer to Section 2.6

(d) Explain IEEE standard 802.11 (WLAN) in details.

Ans.: Refer to Section 4.8.4

5. Write notes on (Any Two) : **[2 × 5 = 10]**

(a) Proxy server.

Ans.: Refer to Section 6.7.5.3

(b) Switch

Ans.: Refer to Section 5.5

(c) ISO-OSI Reference model.

Ans.: Refer to Section 2.2

(d) Line - of – sight

Ans.: Refer to Section 3.3.2.3

❖❖❖

SUMMER 2023

1. Attempt any eight of the following : **[8 × 2 = 16]**

(a) What is protocol?

Ans.: Refer to Section 1.1.7

(b) What is cladding?

Ans.: Refer to Section 3.2.4.2

(c) What is proxy server?

Ans.: Refer to Section 6.7.5.3

(d) What is meant by classless Addressing?

Ans.: Refer to Section 2.7.2

(e) What is transmission media?

Ans.: Refer to Section 3.1

(f) What is internetwork?

Ans.: Refer to Section 1.3.4

(g) Define stegnography?

Ans.: Refer to Section 6.8

(h) What is Hub?

Ans.: Refer to Section 5.2.1

(i) What is Standard Ethernet?

Ans.: Refer to Section 4.2

(j) What is Firewall?

Ans.: Refer to Section 6.7

2. Attempt any four of the following : **[4 × 4 = 16]**

(a) What is Computer Network? Explain Goals of computer Network.

Ans.: Refer to Sections 1.1.1 and 1.1.2

(b) Explain Function of each layer ISO-OSI reference model.

Ans.: Refer to Section 2.2

(c) What is wireless transmission? Explain any one media in detail.

Ans.: Refer to Section 3.3.3

(d) Explain IEEE standard 802.11 (WLAN) in detail.

Ans.: Refer to Section 4.8.4

(e) What is attack? Explain various types of attacks.

Ans.: Refer to Section 6.4

3. Attempt any four of the following : **[4 × 4 = 16]**

(a) What is Bridge? Explain types of bridges.

Ans.: Refer to Section 5.4

(b) Explain different modes of communication with sketch.

Ans.: Refer to Section 1.4

(c) Explain TCP/IP protocol in detail.

Ans.: Refer to Section 2.3.2

(d) What is guided media? Explain any one in detail.

Ans.: Refer to Section 3.2

(e) What is Fast Ethernet? Explain categories of Fast Ethernet.

Ans.: Refer to Section 4.3

4. Attempt any four of the following : **[4 × 4 = 16]**

(a) What is topology? Explain types of topology.

Ans.: Refer to Section 1.2

(b) What is addressing? Explain different types of addresses.

Ans.: Refer to Section 2.6

(c) Explain propagation method.

Ans.: Refer to Section 3.3.2

(d) What is copyright? Explain applications of copyright.

Ans.: Refer to Section 6.9

(e) What is Bluetooth? Explain its architecture.

Ans.: Refer to Section 4.9

5. Write short note on : any two : **[2 × 3 = 6]**

(a) Switch.

Ans.: Refer to Section 5.5

(b) Virtual LAN.

Ans.: Refer to Section 4.7

(c) Types of Network.

Ans.: Refer to Section 1.3

❖❖❖