Chapter 2

NETWORK AND SYSTEM SECURITY

2.1 TYPES OF ATTACKS

- GENERAL POINT OF VIEW
- TECHNICAL POINT OF VIEW
- IMPLEMENTATION POINT OF VIEW

2.2 DIGITAL SIGNATURES

- WHAT IS DIGITAL SIGNATURE?
- PROPERTIES OF DIGITAL SIGNATURE
- WORKING OF DIGITAL SIGNATURE

2.3 PRETTY GOOD PRIVACY (PGP)

- INTRODUCTION - PGP
- E MAIL AUTHENTICATION USING PGP

2.4 SECURE SOCKET LAYER AND TRANSPORT LAYER SECURITY

- SECURE SOCKET LAYER
- TRANSPORT LAYER SECURITY

2.5 IPSEC

- INTRODUCTION – IPSEC
- IP SECURITY ARCHITECTURE

2.6 HTTPS (CONNECTION INITIATION & CONNECTION CLOSURE)

- INTROCUTION – HTTPS
- WORKING OF HTTPS
- DIFFERENCE BETWEEN HTTP AND HTTPS
- ADVANTAGES USING HTTPS

2.7 MALICIOUS SOFTWARE

- WHAT IS MALWARE?
- COMMON TYPES OF MALWARES
  THREATS (TROJAN, ROOTKIT, BACKDOORS, KEYLOGGER ETC...)

2.1 TYPES OF ATTACKS

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

A security attack is an activity or act made upon a system with the goal to obtain unauthorized access to information or resources. It is usually carried out by evading security policies that are in place in organizations or individual devices.

Thus, attack is any action that compromises the security of information owned by an organization.

Security attacks can be classified in three ways:

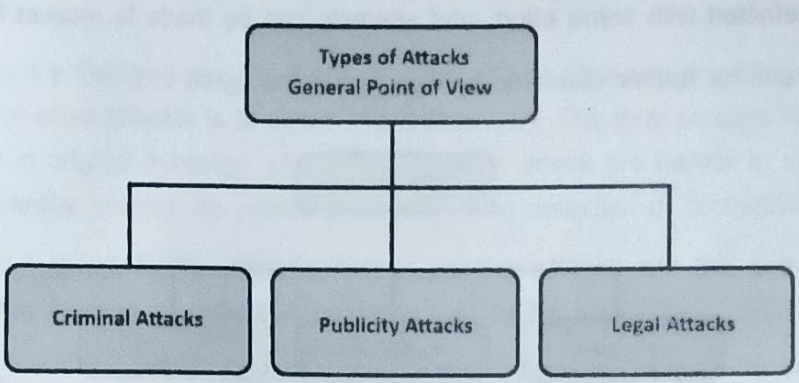
- General point of view
- Technical point of view
- Implementation point of view

2.1.1 General point of view

As a common non-technical person point of view security attacks can be classified into three types as depicted in the figure 2.1.

1. Criminal Attack

The main aim of attacker in criminal attack is to maximize financial gain or harm to other or their systems. Some of the examples of criminal attacks are: fraud, scams, identity theft, intelligent property theft, brand theft etc...



[Fig. 2.1 : Types of Attacks: General point of View]

2. Publicity Attack

The sole aim of an attacker in publicity attack is to get publicity instead of financial gain. Generally, this type of attackers are not usually hardcore criminals. They are people like students or employees who tries to get publicity through applying new approach of attack. Example of such attack is damage or hijacking web page of popular web site.

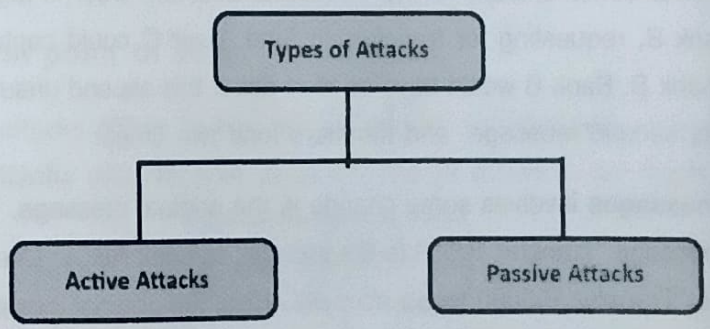
3. Legal Attack

The aim of the attacker is to exploit the weakness of the judge and the jury in technological matters. This form of attack is quite new and unique in which the attacker tries to convince the judge and the jury that there is inherent weakness in the computer system and he is not responsible for any wrongful activity.

Ex. Attacker excuse that he has just clicked as the system asked. He done nothing.

2.1.2 Technical point of view

As a technical point of view, attacks can be grouped into two types: passive attacks and active attacks, as shown infigure 2.2.



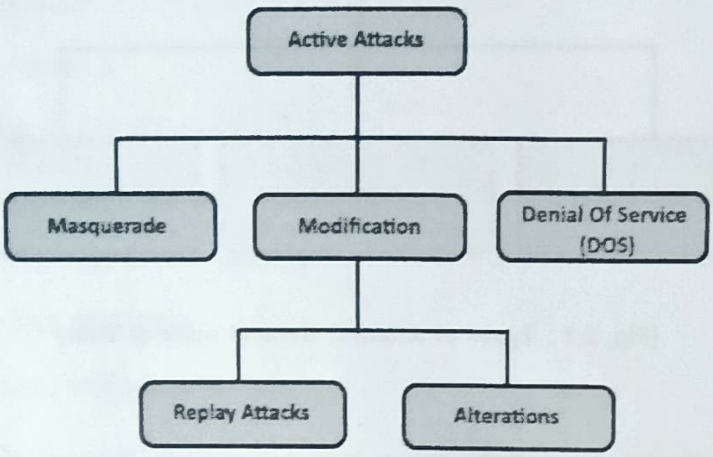
[Fig. 2.2 : Types of Attacks: Technical Point of View]

1. Active Attacks

Active attacks are the attacks in which attacker not only observes traffic but also tries to modify the original message or creates false message. These kinds of attacks cannot be easily prevented. Such kind

of attacks can be detected with some effort, and attempts can be made to recover from it.

These attacks can be further classified as depicted in the figure 2.3.



[Fig. 2.3 : Types of Active Attacks]

- **Masquerade** – Pose as another entity.

  When an attacker tries to pretends to be another entity, then attack is called masquerade attack. User C might pose himself as user A and send a message to user B. User B might be led to believe that the message indeed came from user A and he work as on message. Generally, masquerade attacks embedded with some other kind of active attacks

- **Modification** – Change of original message.

  Modification attacks are that kind of attacks in which attacker tries to modify the original message. These attacks are further classified as : **Replay attack** and **alteration attack**.

  In a **replay attack**, a user captures a message, and re-sends them. For example, suppose user A wants to transfer some amount to user C's bank account. User A might send an electronic message to bank B, requesting for transferring fund. User C could capture this message, and send again to bank B. Bank B would have no idea about this second unauthorised message, and would treat it as second message, and transfers fund two times.

  Alteration of messages involves some change in the original message. For example, suppose user A sends message "Transfer 10000 to B's account" to bank ABCL. User C might capture this, and change it to "Transfer 100000 to B's account". Here the original message is altered in terms of amount.

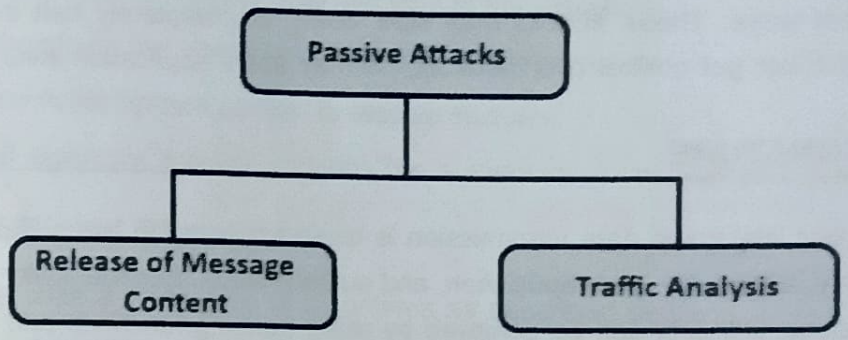
- **Denial Of Service (DOS) attacks.**

  Denial Of Service (DOS) attack attempts to make resources unavailable to its legitimate users. For example, an attacker sends thousands of requests to the server and make it busy. So, server can's response to legitimate user.

2. Passive Attacks

Passive attacks are those attacks in which the attacker just observes or monitors message during transmission. The aim of an attacker is to obtain information only. The term passive indicates, no attempt for any modification in original message. Due to this passive attack are harder to detect. To deal with passive attacks preventive actions are carried out, rather than detection or corrective actions.

Below Figure 2.4 shows further classification of passive attacks into two sub-categories. These categories are, namely **release of message contents** and **traffic analysis.**



[Fig. 2.4 : Types of Passive Attacks]

- **Release of message Content**

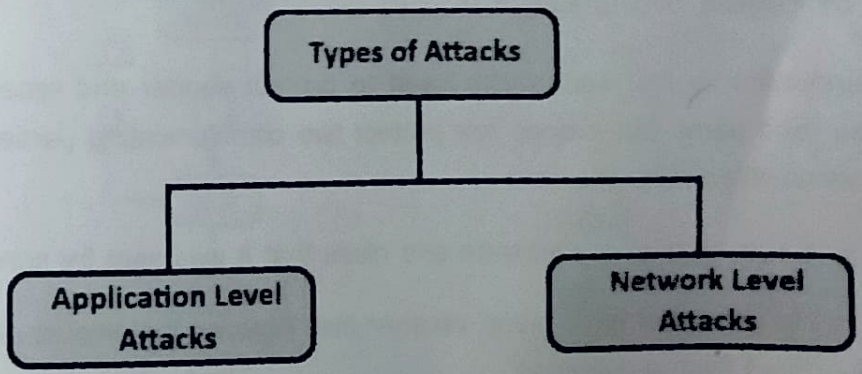
  Release of message contents attack is very simple to understand. Suppose sender wants to send confidential message to recipient without being released to any else. But an attacker accesses this message by somehow. We can prevent release of message attack with encryption like security mechanism.

- **Traffic Analysis**

  Sometime passive attacker collects large number of messages passing through network and figure out similarities between and sort out some pattern. Such attempt of analysing encrypted messages to find out original messages is called traffic analysis.

2.1.3 Implementation point of view

All the discussed attacks above can be further can be classified with implementation point of view as **Application-level attacks** and **Network level attacks** as shown in the figure 2.5.



[Fig. 2.5 : Types of Attacks: Implementation point of view]

1. **Application-level Attacks.**

These are the attacks in which an attacker attempts to access, modify, or prevent access to information of a particular application, or the application itself.

Examples: Access someone's credit-card information, or change the amount in a transaction.

2. **Network-level Attacks.**

Network level attacks are usually applied to the networks with the aim to reduce the capabilities of a network by different ways. These attacks may slow down, or completely halt the computer system network. Once an attacker get control over network, he may apply application-level attacks also.

2.2 DIGITAL SIGNATURE

As we know online electronic data transmission is carried out on the basic important elements like Confidentiality, integrity, availability, non-repudiation, and authentication. Confidentiality is achieved by using cryptographic techniques. Integrity can be achieved by using hashing functions and algorithms like SHA Algorithm and MD5 Message Digest. With the use of various activities by network administrator availability can be maintain. But how can authenticate that a particular message, data, software or document is from specific sender. That is the case where digital signature plays an important role.

2.2.1 What is Digital Signature ?

A ***digital signature*** is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software.

It is the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, digital signatures are considered legally in the same way as traditional handwritten document signatures.

2.2.2 Properties of Digital Signature ?

Message Authentication is the mechanism used to protect sender and receiver of digital data transmission from the third party. But it does not protect two communicating parties from each other. Several disputes between them arise like below.

- Receiver may forge an original message and claim that it was sent by sender.

  E. g. Electronic fund transfer takes place, receiver may increase the amount and claims that larger amount had arrived from the sender.

- Sender may deny about sent message.

  E.g. A stockholder sends an instruction to his stockbroker, and then pretends that he never sent such instruction.

In such situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature.

The digital signature must have the following **properties** :

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

Thus, the digital signature function includes the authentication as well as integrity functions.

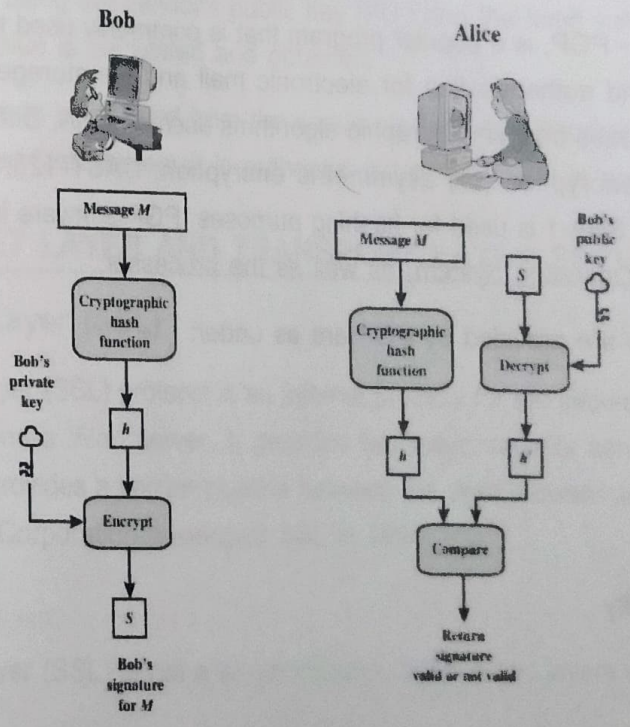
2.2.3 Working of Digital Signature ?

Digital signature uses a three kind of algorithms as described below.

Key Generation Algorithms : Digital signatures are electronic signatures that guarantee a certain sender sent the message. The algorithms which are used to generate keys are called key generation algorithms.

Signing Algorithms : To create a digital signature, hashing algorithms are used create a one-way hash of the electronic data which is to be transmitted. The signing algorithm then encrypts the hash value using the sender's private key (signature key). This encrypted hash value along with original data is known as the digital signature.

Signature Verification Algorithms : Digital signature Verifier receives Digital Signature along with the original data. Verifier then uses Verification algorithm to verify the received digital signature.



[Fig. 2.6 : Digital Signature process Step by Step]

The steps followed in creating digital signature and verifying signature are :

1. Hash value is computed by applying hash function on the message and then hash value is encrypted using private key of sender (Bob) to form the digital signature.

   digital signature = encryption (private key of sender, Hash Value) and

   Hash Value = Hashing algorithm(message).

2. Digital signature is then transmitted with the original message.

   (original message + digital signature is transmitted)

3. Receiver decrypts the digital signature using the public key of sender. (This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).

4. The receiver now has the Hash value from the sender side.

5. The receiver can also compute the hash value from the original message. (actual message is sent with the digital signature).

6. The hash value computed by receiver and the hash value received from the sender (got by decryption on digital signature) need to be same for ensuring integrity.

Digital signatures are used in various financial or business transactions like legal documents and contracts, sales and purchase contracts, financial documents, health data, shipping documents etc...

2.3 PRETTY GOOD PRIVACY(PGP)

2.3.1 Introduction - PGP

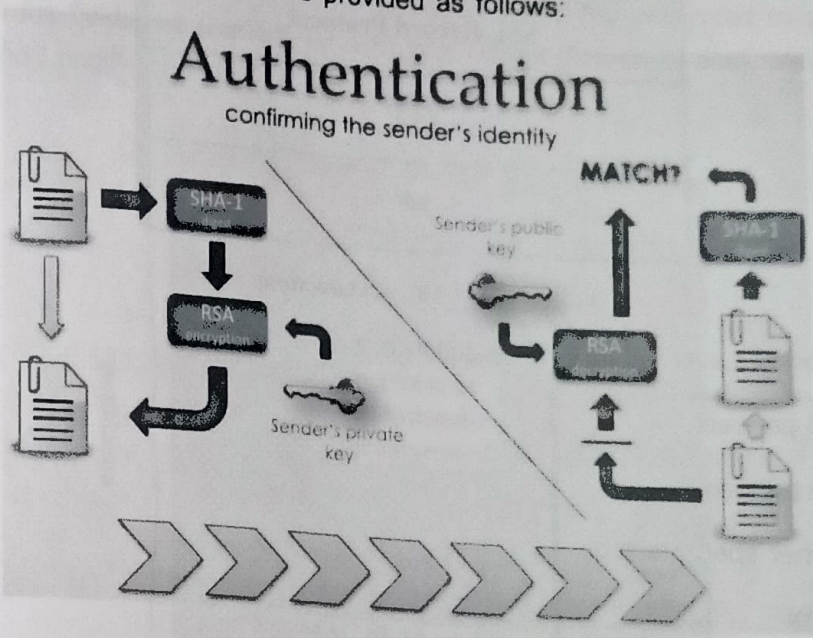
Pretty Good Privacy - PGP, is a popular program that is commonly used to provide two fundamental services confidentiality and authentication for electronic mail and file storage. It was designed by **Phil Zimmermann** in 1991. It uses best cryptographic algorithms such as RSA, Diffie-**Hellman** key exchange, DSS for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA is used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open-source software and independent of OS (Operating System) as well as the processor.

The various services are provided by PGP are as under:

- Authentication
- Confidentiality
- Compression
- Email Compatibility
- Segmentation

2.3.2 E mail Authentication using PGP

Authentication of an email is nothing but to check whether it actually came from the person it says or not. The Authentication service in PGP is provided as follows:



[Fig. 2.7 : E mail Authentication service with PGP]

As shown in the above figure 2.7, the hashing algorithm SHA-1 is used and it produces a 160-bit output hash value. Then, with use of sender's private key (KP_a), hash value is encrypted and it's called as Digital Signature. The Message is then appended to the signature. Then the message is compressed to reduce the transmission cost and is sent to the receiver.

At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key (PU_a) and the hash value is obtained. From the message again the hash value is calculated and obtained.

Both the hash values, one is received from the sender and another is calculated at receiver side are compared. If both are same, then the email is authenticated email else it is not.

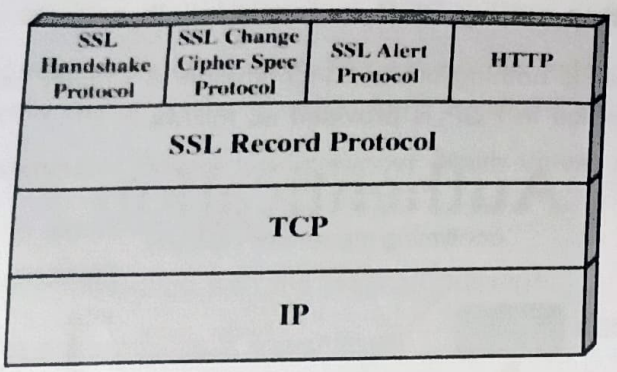
2.4 SECURE SOCKET LAYER AND TRANSPORT LAYER SECURITY

2.4.1 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) protocol is an Internet protocol for the secure exchange of information between a Web browser and a Web server. It provides two basic security services: authentication and confidentiality. Logically, it provides a secure pipeline between the Web browser and the Web server during communication. Netscape Corporation developed SSL in 1994.

SSL Architecture:

The Secure socket layer (SSL) is not a single protocol, but it is two layers of protocols as illustrated in below figure 2.8.



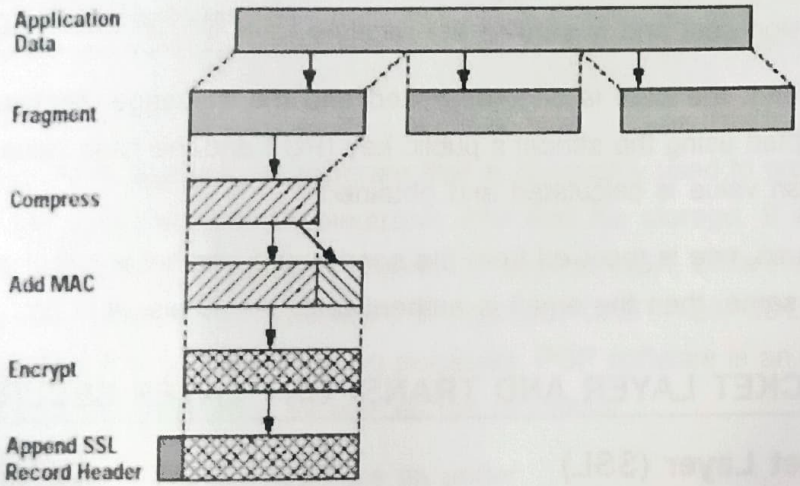
[Fig. 2.8 : SSL Architecture]

The Secure Socket Layer (SSL) is a collection of below protocols.

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Record Protocol

The SSL record protocol provides two fundamental security services: Confidentiality and Message Integrity.

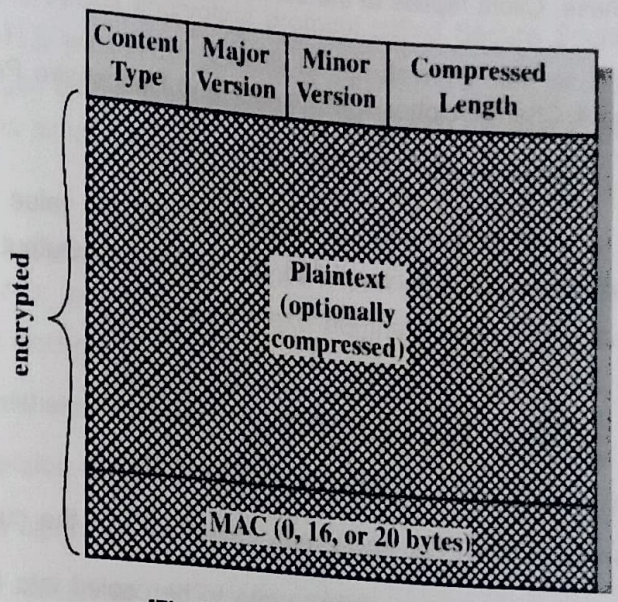


[Fig. 2.9 : SSL Record Protocol Operation]

The SSL Record Protocol operation is as under:

- *Fragmentation* : the original data is fragmented into blocks of 214 Bytes or less.
- *Compression* : each fragment is compressed. This is optional. Compression must be lossless.
- *Appending MAC Code* : Message Authentication Code is appended to fragment.

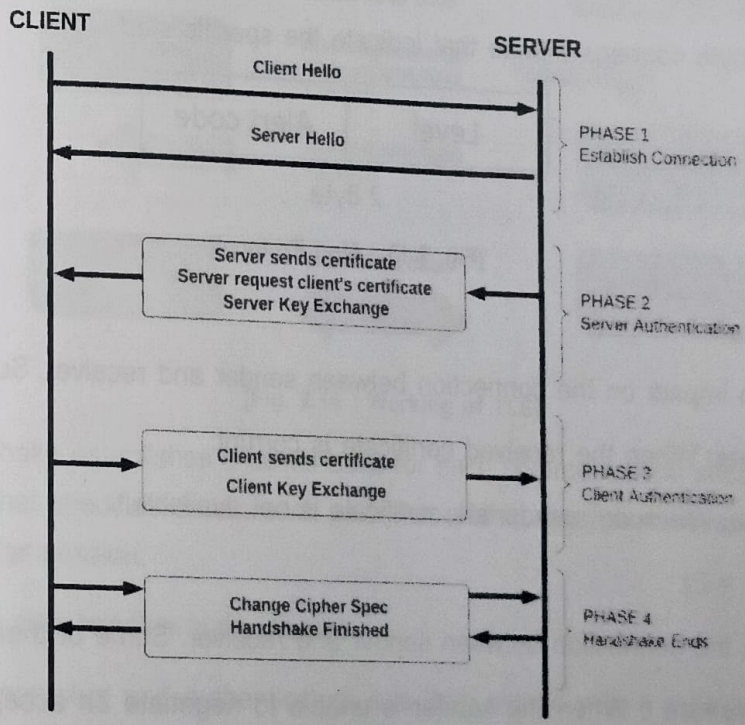
- *Encryption* : The compressed message with appended MAC Code is encrypted using symmetric encryption algorithms like AES, DES, 3DES etc...
- *Add SSL header* : Finally, SSL header is appended to the encrypted fragment. The header consists of the fields like Content Type (8 bits), Major Version (8 bits), Minor Version (8 bits), Compressed Length (16 bits).



[Fig. 2.10 : SSL Record Format]

SSL Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

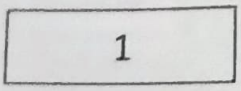


[Fig. 2.11 : SSL Handshake Protocol]

- **Phase-1** : In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2** : Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3** : In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4** : In Phase-4 Change-cipher suite occurs and Handshake Protocol ends.

Change Cipher Protocol

This protocol consists of a single message of single byte with the value 1. It uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state.



1 Byte

[Fig. 2.12 : Change Cipher Spec Protocol]

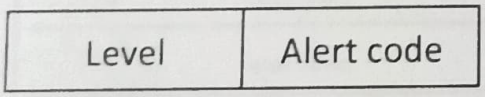
After the handshake protocol, the Pending state is converted into the current state.

This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol

The Alert protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol consists of 2 bytes.

- The first byte indicates the severity of the message by value warning (1) and fatal (2).
- The second byte contains s code that indicate the specific alert.



2 Byte

[Fig. 2.13 : Alert Protocol]

Warning Error (Level = 1) :

This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad certificate:** When the received certificate is corrupt.
- **No certificate:** When an appropriate certificate is not available.

Fatal Error (level = 2):

This Alert breaks the connection between sender and receiver. Some of them are :

- **Handshake failure :** When the sender is unable to negotiate an acceptable set of security parameters given the options available.

- **Decompression failure:** When the decompression function receives improper input.

2.4.2 Transport Layer Security (TLS)

The Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols are currently the two most used ones for delivering security at the transport layer.

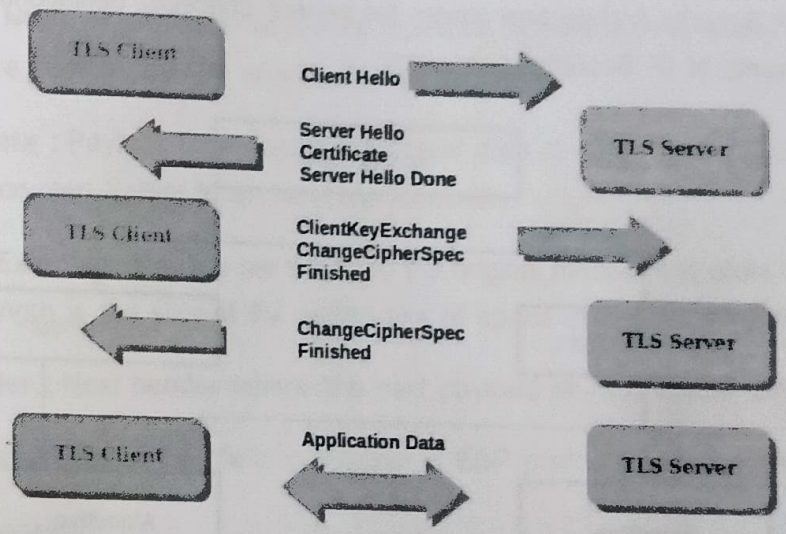
TLS evolved from a previous encryption protocol called Secure Sockets Layer (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

Working of TLS

A TLS connection is initiated using a sequence known as the TLS handshake. When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the client device) and the web server.

During the TLS handshake, the user's device and the web server:

- Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use.
- Decide on which cipher suites (see below) they will use.
- Authenticate the identity of the server using the server's TLS certificate.
- Generate session keys for encrypting messages between them after the handshake is complete.



[Fig. 2.14 : Working of TLS]

The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session.

The handshake also handles authentication.

Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data.

2.5 IPSEC

2.5.1 Introduction - IPsec

IPsec (Internet Protocol Security) is a large set of protocols and algorithms. The Internet Engineering Task Force (IETF), developed the IPsec protocols for the purpose of providing security at the IP layer through authentication and encryption of IP network packets.

Originally, it was defined with two protocols for securing the IP packets which were Authentication Header (AH) and Encapsulating Security Payload (ESP). The former protocol i.e. AH provides data integrity and non-replay services, and the latter protocol i.e. ESP encrypts and authenticates data.

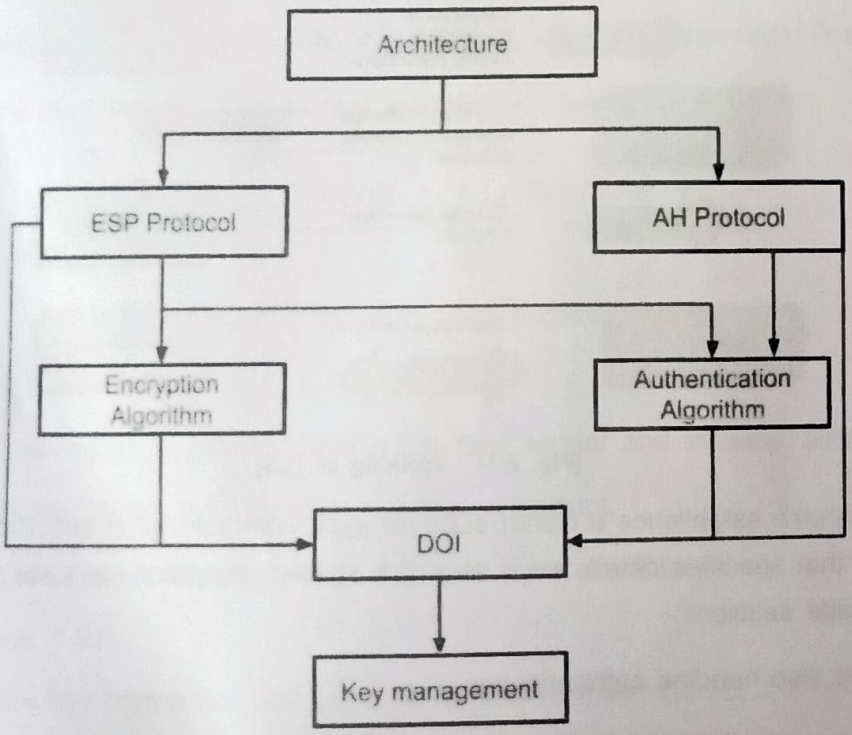
Thus, IPsec provides the basic services as listed below:

- Confidentiality
- Authentication
- Integrity
- Non-Replay

2.5.2 IP Security Architecture

1. Architecture:

Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.

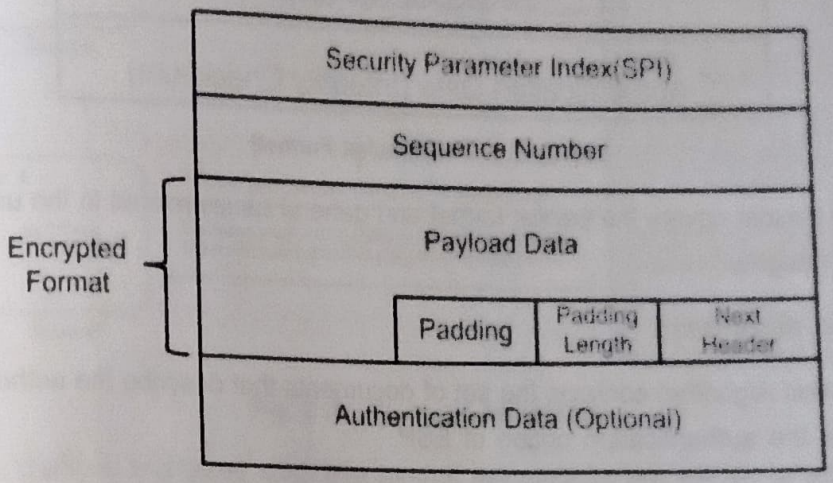


[Fig. 2.15 : IP Security Architecture]

2. ESP Protocol :

ESP (Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.



[Fig. 2.16 : ESP Packet Format]

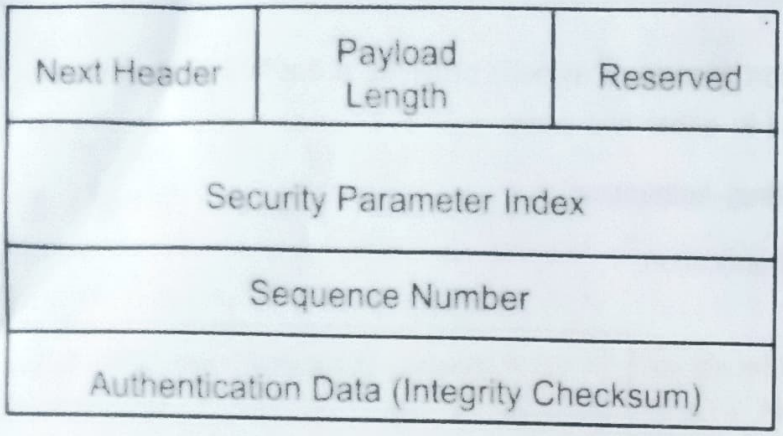
- **Security Parameter Index (SPI) :** This parameter is used by Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number :** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data :** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
- **Padding :** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- **Next Header :** Next header means the next payload or next actual data.
- **Authentication Data:** This field is optional in ESP protocol packet format.

3. Encryption algorithm :

The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.

4. AH Protocol :

AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



[Fig. 2.17 : AH Packet Format]

Authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.

5. Authentication Algorithm :

The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.

6. DOI (Domain of Interpretation) :

DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management :

Key Management contains the document that describes how the keys are exchanged between sender and receiver.

2.6 HTTPS (CONNECTION INITIATION & CLOSURE)

2.6.1 Introduction - HTTPS

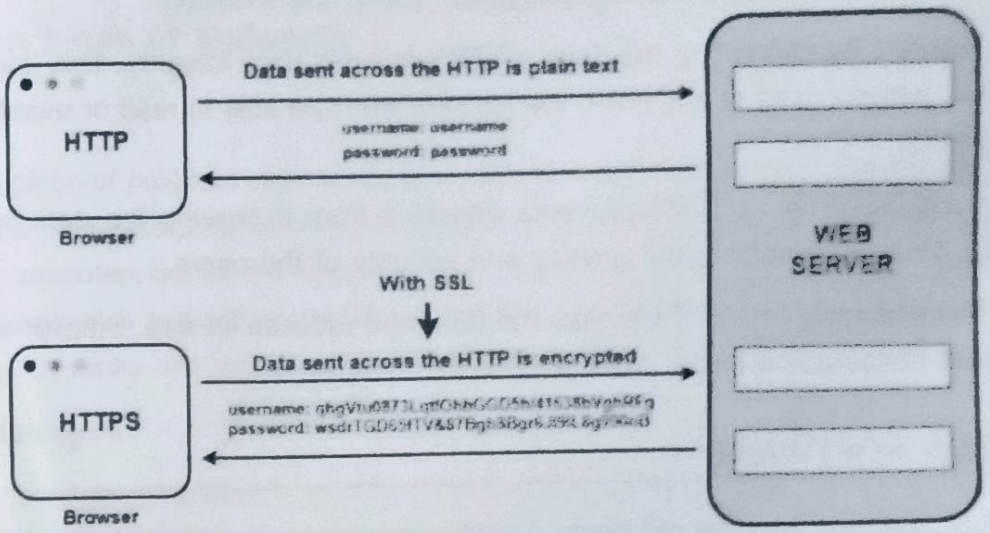
Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is particularly important when users transmit sensitive data, such as by logging credentials for a bank account, email service, or health insurance provider.

In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are.

2.6.2 Working of HTTPS

HTTPS uses an encryption protocol to encrypt the communication data. The protocol used for this encryption is called Transport Layer Protocol (TLS), formerly it was known as Secure Socket Layer (SSL). This protocol uses an asymmetric public key infrastructure. It uses two different keys: the private key and the public key.

When information is sent over regular HTTP, the information is broken into packets of data that can be easily "sniffed" using free software. This makes communication over the an unsecure medium, such as public Wi-Fi, highly vulnerable to interception.



[Fig. 2.18 : Working with HTTPS]

With HTTPS, traffic is encrypted such that even if the packets are sniffed or otherwise intercepted, they will come across as nonsensical characters.

2.6.3 Difference between HTTP and HTTPS

HTTP	HTTPS
The full form of HTTP is Hypertext Transfer Protocol	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It operates on application layer.	It operates at the transport layer.
The data is transferred in plain text form.	The data is transferred in encrypted form, i.e., ciphertext.
By default, this protocol operates on port number 80.	By default, this protocol operates on port number 443.
The URL start with http://	The URL start with https://
This protocol does not need any certificate.	But this protocol requires an SSL (Secure Socket Layer) certificate.
Communication carried out without encryption.	Communication carried out with encryption.
Faster than HTTPS.	Slower than HTTP.
It is un-secure.	It is highly secure.
Examples of HTTP websites are Educational Sites, Internet Forums, etc.	Examples of HTTPS websites are shopping websites, banking websites, etc.

2.6.4 Advantages of using HTTPS

- **Secure Communication** : HTTPS establishes a secure communication link between the communicating system by providing encryption during transmission.
- **Data Integrity** : By encrypting the data, HTTPS ensures data integrity. This implies that even if the data is compromised at any point, the hackers won't be able to read or modify the data being exchanged.
- **Privacy and Security** : HTTPS prevents attackers from accessing the data being exchanged passively, thereby protecting the privacy and security of the users.
- **Faster Performance** : HTTPS encrypts the data and reduces its size. Smaller size accounts for faster data transmission in the case of HTTPS.

2.7 MALICIOUS SOFTWARE

The number of internet users are increased due to improvement in internet technology, reduced cost of hardware, and advancement of mobile technology. So, people are dependent because of their professional, social and personal activities. With the use of internet, they can perform so many tasks online with clicks in seconds. But there is also another side of coin.

There are so many people who attempts to damage our Internet-connected computers, violate our privacy and make unavailability of the Internet services. Such people are called attackers and they use malwares for such activities.

2.7.1 What is Malware ?

Malware – "A short name of malicious software, is an umbrella term that describes any malicious program or code that is harmful to systems. It is specifically designed to disrupt, damage, or gain unauthorized access to a computer system."

How can malware affect your system ?

- Your computer slows down.
- Your screen is inundated with annoying ads.
- Your system crashes.
- You notice a mysterious loss of disk space.
- There's a weird increase in your system's Internet activity.
- Your browser settings change.

  homepage changed or you have new toolbars, extensions, or plugins installed etc.
- Your antivirus product stops working and you cannot turn it back on, leaving you unprotected against the malware that disabled it.
- You lose access to your files or your entire computer.

Adware, Spyware, Virus, Worms, Trojans, Ransomware, Rootkit, keylogger etc are the various forms of malware. Each of these have different working method and affects our system or network very differently.

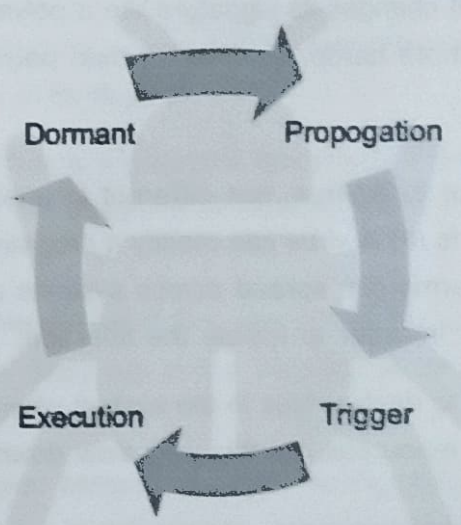
2.7.2 Common types of Malwares :

1. Virus

A virus is a piece of program code (malicious software) that attaches itself to legitimate program code, and runs when the legitimate program runs. It can then infect other programs in that computer, or programs that are in other computers but on the same network. Virus is capable to delete all the files from the current user's computer, and virus can self-propagate by sending its code to all other users whose email addresses are stored in the currently infected computer system.

- **Virus Lifecycle**

During its lifetime, a virus goes through four phases as depicted in the below figure.



[Fig. 2.19 : Virus Life Cycle]

(a) Dormant Phase : During this phase the virus is in idle mode.

(b) Propagation Phase : In this phase, a virus propagate itself by copying self-code, and each copy starts creating more and more copies of itself.

(c) Triggering Phase : A dormant virus is triggered based on a certain action or event (e.g. certain key press, a certain date or time is reached, etc).

(d) Execution Phase : The actual work of the virus starts in this phase, which could be harmless (just display some message on screen) or destructive (delete a file or corrupt a file).

- **Types of Viruses**

Viruses can be classified into different categories on the base of their working and implementation method:

(a) **Parasitic Virus :** Such a virus attaches itself to executable files and keeps replicating. When an infected file is executed, the virus attaches to other executable files. This is the most common type of virus.

(b) **Memory-resident Virus :** This virus resides in main memory and then infects every executable program that is executed.

(c) **Boot sector Virus :** That infects the master boot record of the disk and spreads on the disk during booting process of the computer.

(d) **Stealth Virus :** This virus has an in-built intelligence, due to which it can prevent anti-virus software programs from detecting it.

(e) **Polymorphic Virus :** Such virus continuously changes its signature (identity) on every execution, so it makes difficult to detect it.

(f) **Metamorphic Virus :** It changes its signature like a polymorphic virus, and also rewrites itself. So, it becomes even more harder to detect it than polymorphic virus.

2. Worms

Worms are Similar in concept to a virus, but different in implementation point of view. The big difference between virus and worm is (1) A virus can modify a program to which it is attached but a worm, does not modify a program. (2) Worms can spread across systems on their own, whereas viruses need some triggering action from a user in order to initiate the infection.

Thus, the basic aim of virus is to destroy files in the system whereas aim of worm is to replicate itself repeatedly and consuming system resources, by this way slow down system or network performance.

3. Keyloggers

Keyloggers, also known as keystroke loggers or keyboard capturing software, are tools or programs designed to record and monitor keystrokes on a computer or mobile device.

Applications of keyloggers

Keyloggers can be used for legitimate purpose as well as malicious.

1. Legitimate purpose :

- System Monitoring: Keyloggers are sometimes used by system administrators or employers to monitor and track computer usage within an organization for security or productivity purposes.
- Parental Control: Keyloggers can be employed by parents to monitor their children's online activities and ensure their safety.
- Law Enforcement: Keyloggers may be used by law enforcement agencies during investigations to gather evidence or track suspect activities with proper legal authorization.

2. Malicious purpose :

- Information Theft: Malicious keyloggers are designed to capture sensitive information, such as usernames, passwords, credit card details, or personal data, entered by users on a compromised system. Attackers can use this information for identity theft, financial fraud, or unauthorized access to accounts.
- Credential Harvesting: Keyloggers can be used to capture login credentials for various online services, including email accounts, social media platforms, or banking websites. These stolen credentials can be sold on the dark web or used for further unauthorized activities.
- Remote Access: Some keyloggers allow attackers to remotely access the compromised system and monitor keystrokes in real-time, providing unauthorized access to sensitive data or control over the system.

3. Types of keyloggers

There are several types of keyloggers, each with its own characteristics and methods of operation. Here are some common types of keyloggers :

1. Hardware Keyloggers: Hardware keyloggers are physical devices that are physically attached between the keyboard and the computer or inserted into the USB port. They record keystrokes directly from the keyboard.
2. Software Keyloggers: Software keyloggers are programs or malicious software installed on a computer or mobile device. They run in the background and record keystrokes, capturing the information entered by the user.
3. Memory-Injection Keyloggers: Memory-injection keyloggers inject malicious code into running processes or the memory of a target system. They intercept and record keystrokes by hooking into the operating system's keyboard events.
4. Form Grabbing Keyloggers: Form grabbing keyloggers target web browsers and capture information submitted through online forms.

4. Trojan horse

A Trojan, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install other forms of malware, often ransomware.

5. Rootkit

Rootkit is a form of malware that provides the attacker with administrator privileges on the infected system, also known as "root" access. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.

6. Adware

Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser. Typically, it uses an underhanded method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device.

7. Spyware

Spyware is malware that secretly observes the computer user's activities without permission and reports it to the software's author.

8. Backdoors

Backdoor allows someone to enter your house, not from the legal way that is the front door. In technical terms, the backdoor is any sort of method which allows hacker, or even government to access your system without your permission. A Backdoor can be installed on your system by hackers in the form of some malware application or using your device's software vulnerabilities.

All the malware like rootkits, trojans, spyware, keyloggers, worms and even ransomware are considered to be backdoors if installed in user's devices without their permission or knowledge.

2.8 FIREWALL

2.8.1 Need of Firewall

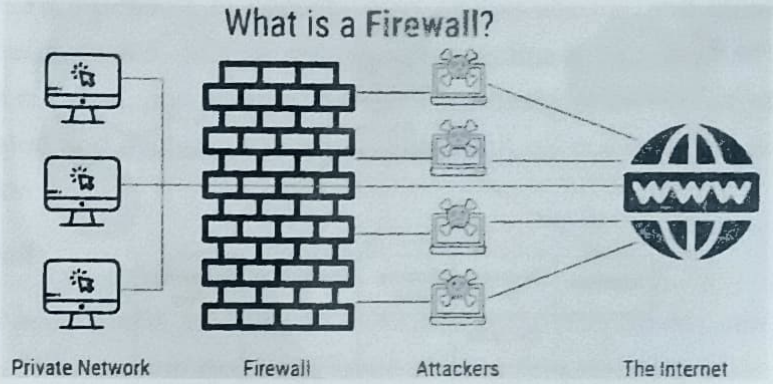
The unparalleled improvement in the internet technology has opened the possibilities to connect any computer with any other computer in the world. It's a great advantage for the individual as well as business houses or organisations. But the problems with the large organisations are: (1) They have large amount of confidential data that must be keep secret from their business rivals. (2) They must have mechanism that can protect these valuable and confidential information from outsider. Firewall is a such mechanism which protects individual or corporate network from outside attacker.

2.8.2 What is Firewall ?

A firewall is a network security device or software that acts as a barrier between an internal network and external networks or the internet. Its primary purpose is to monitor and control incoming and outgoing network traffic based on predetermined security rules.

Conceptually, a firewall can be compared with a security person standing outside a house of nation's president. He physically checks every person who enters into or exit from the house. If security person finds a suspicious person, he stops that person. Firewall also works like security person and checks every data packet enters or exits from the private network.

Firewalls are designed to prevent unauthorized access to a network by filtering and blocking potentially harmful or malicious traffic while allowing legitimate communication to pass through. They examine network packets, which are small units of data, and apply rules to determine whether the packets should be allowed or blocked.



[Fig. 2.20 : Firewall working Architecture]

Firewalls play a crucial role in network security by protecting against various threats, such as unauthorized access attempts, malware infections, distributed denial-of-service (DDoS) attacks, and data breaches. They are an essential component of a comprehensive security strategy and are commonly used in both home networks and large-scale enterprise environments.

2.8.3 Types of Firewalls

Firewalls can be implemented in various forms. On the base of implementation firewalls can be classified in two categories.

- Network Based Firewall
- Host Based Firewall

1. Network Based Firewall

Network Firewalls are the devices that are used to prevent private networks from unauthorized access. The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

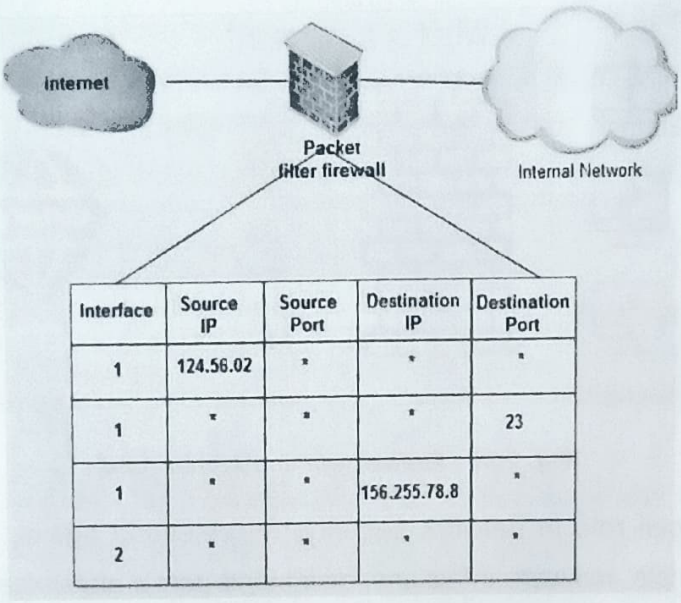
Types of Network based firewalls

- **Packet filtering firewall (First Generation firewall)**

  As the name suggest Packet filtering firewall is used to monitor incoming and outgoing packets, and decide whether to allow them or stop based on protocols, ports, source and destination IP addresses, and other factors. Every packet is handled separately by packet firewalls. Packet filtering firewalls are also known as static firewall.

  Working of packet filter firewall

  (a) Receive each incoming packet to the packet filter node which is also called **filtering router** or **screening router.**



Interface	Source IP	Source Port	Destination IP	Destination Port
1	124.56.02	*	*	*
1	*	*	*	23
1	*	*	156.255.78.8	*
2	*	*	*	*

[Fig. 2.21 : Filtering Rule Table]

(b) Apply set of predefined rules on each packet, If there is a match with one of the set rules, decide whether to accept or discard the packet based on that rule. For example, a rule could specify: disallow all incoming traffic from an IP address 157.28.19.14

(c) If there is no match with any rule, take the default action. The default can be discarding all packets or accept all packets.

- **Stateful Inspection Firewall (Second generation Firewall)**

Stateful inspection firewalls include both packet filtering and TCP handshake verification, making stateful inspection firewalls superior to packet-filtering firewalls.

When a user establishes a connection and requests data, the firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

In most cases, stateful inspection firewalls are implemented as additional security levels. Advantage of this firewall is more secure than stateless firewall. The disadvantage is it increases the load and puts more pressure on computing resources. So, it leads to slower transfer rate for data packets than other solutions.

- **Next Generation Firewalls**

Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

2. Host Based Firewall

These are software applications installed on individual computers or devices to control traffic to and from that specific device. They provide an added layer of security, especially when devices are connected to untrusted networks.

2.8.4 Advantages and Disadvantages of Firewalls

Advantages of using Firewall

1. **Preventing unwanted access :** By restricting incoming traffic from specific IP addresses or networks, firewalls can stop hackers and other bad actors from getting easy access to a system or network. safeguarding against unauthorized access.
2. **Avoiding malware and additional dangers :** Prevention of malware and other threats: Firewalls can be configured to stop traffic that is connected to known malware or other security issues, helping to thwart these types of attacks.
3. **Control of network access :** Firewalls can be used to restrict access to specific servers or applications, as well as to specific network resources or services, by limiting access to designated persons or groups.
4. **Network activity monitoring :** Firewalls can be configured to log and monitor every activity on the network.
5. **Regulation compliance :** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation :** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **Complexity :** Set up of firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of devices.
2. **Limited Visibility :** Firewalls can only observe and manage traffic at the network level.
3. **False sense of security :** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.

4. **Limited adaptability :** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
5. **Performance impact :** Network performance can be significantly impacted by firewalls, particularly in the case of lot of traffic.
6. **Limited scalability :** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
7. **Limited VPN support :** Some firewalls might not allow complex VPN features like split tunnelling, which could restrict the experience of a remote worker.
8. **Cost :** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

2.9 PROXY SERVER

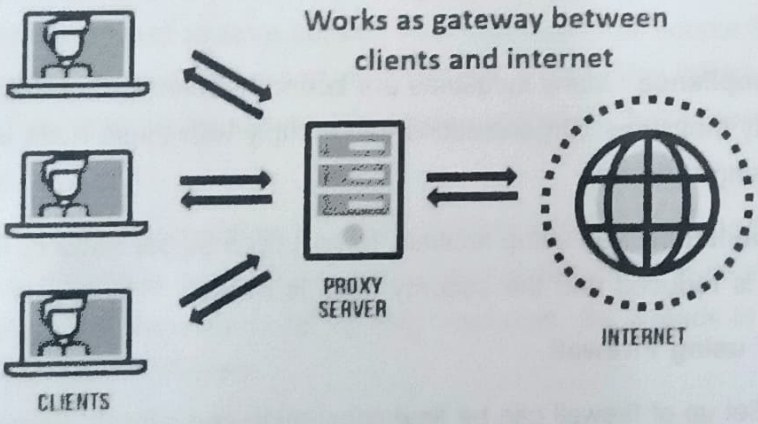
2.9.1 Proxy servers and its working

The proxy server is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It plays an intermediary role between users and targeted websites or servers.

There are two main purposes of proxy server:

- To keep the system behind it anonymous.
- To speed up resource access using concept of caching.

Working mechanism of proxy server :



[Fig. 2.22 : Working of proxy server]

The proxy server accepts the request from the client and produces a response based on the following conditions :

1. If the requested data or page already exists in the local cache, the proxy server itself provides the required data or page to the client.

2. If the requested data or page does not exist in the local cache, the proxy server forwards that request to the destination server.

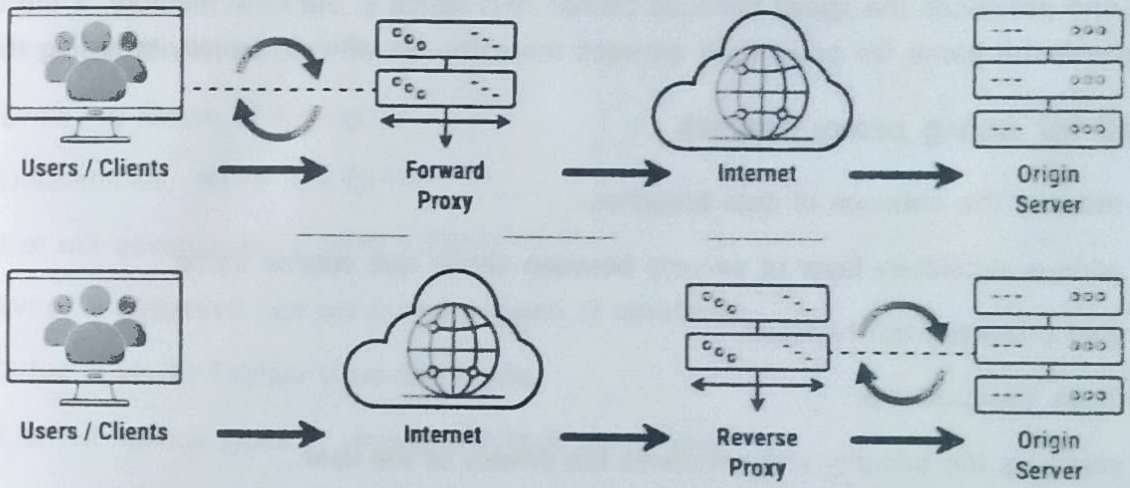
3. The proxy servers transfer the replies to the client and also being cached to them.

Therefore, it can be said that the proxy server acts as a client as well as the server.

2.9.2 Types of proxy servers

Open or Forward Proxy Server :

Forward proxy server refers to those sorts of intermediaries that get demands from web clients and afterward peruse destinations to gather the mentioned information. After collecting the data from the sites, it forwards the data to the internet users directly. It bypasses the firewall made by authorities. The following image shows forward proxy configuration.



[Fig. 2.23 : Forward Proxy V/s Reverse proxy]

Reverse Proxy Server :

It is a proxy server that is installed in the neighbourhood of multiple other internal resources. It validated and processes a transaction in such a way that the clients do not communicate directly. The most popular reverse proxies are **Varnish** and **Squid**. The above image shows the reverse proxy configuration.

Transparent Proxy :

It is a proxy server that does not modify the request or response beyond what is required for proxy authentication and identification. It works on port 80.

Non-Transparent Proxy :

It is an intermediary that alters the solicitation reaction to offer some extra types of assistance to the client. Web demands are straightforwardly shipped off the intermediary paying little mind to the worker from where they started.

Web Proxy Server : The proxy server targeted to the WWW is called a web proxy server.

Public Proxy :

A public proxy is available free of cost. It is perfect for the user for whom cost is a major concern while security and speed are not. Its speed is usually slow. Using a public proxy puts the user at high risk because information can be accessed by others on the internet.

Residential Proxy :

It assigns an IP address to a specific device. All requests made by the client channelled through that device. It is ideal for the users who want to verify ads that display on their websites. Using the residential proxy server, we can block unwanted and suspicious ads from competitors. In comparison to other proxy servers, the residential proxy server is more reliable.

HTTP Proxy :

HTTP proxies are those proxy servers that are used to save cache files of the browsed websites. It saves time and enhances the speed because cached files reside in the local memory. If the user again wants to access the same file proxy itself provides the same file without actually browsing the pages.

2.9.3 Need for using proxy servers

- It reduces the chances of data breaches.
- It adds a subsidiary layer of security between server and outside traffic.
- It also protects from hackers.
- It filters the requests.
- It improves the security and enhances the privacy of the user.
- It hides the identity (IP address) of the user.
- It controls the traffic and prevents crashes.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What do you mean by attack? List out various types of attacks.

(2) Differentiate Active attacks Vis Passive attacks.

(3) Explain types of attacks in general point of view.

(4) Explain types of attacks in technical point of view.

(5) Explain types of attacks with implementation point of view.

(6) What is Digital Signature?

(7) List out properties of Digital Signature.

(8) Write down steps to create Digital Signature and its verification.

(9) What is PGP ? List out various services provided by PGP.

(10) Explain e-mail authentication process using PGP.

(11) What is SSL? List of various protocols of SSL.

(12) Draw the architecture of SSL.

(13) Draw the SSL Record format.

(14) Explain Change Cipher protocol and alert protocol.

(15) what is TLS? How it is different than SSL?

(16) What is IPsec? List out various services provided by IPsec.

(17) Draw the architecture of IPsec.

(18) Draw the format of ESP Packet.

(19) Draw the format of AH Packet.

(20) Differentiate: HTTP V/s HTTPS

(21) List out advantages of using HTTPS.

(22) What is Malware? List out common types of Malwares.

(23) What is virus? Explain Virus Life Cycle.

(24) List out various types of viruses with their properties.

(25) Define : Worm, Trojan Horse, Ransomware, Rootkit, Keyloggers, Adware, Spyware, Backdoors

(26) What is Firewall? Explain with simple real-life example.

(27) List out various types of firewalls.

(28) Explain advantages of using firewalls.

(29) What is proxy server? List out various types of proxy server.

Q. 2 Explain the below questions :

(1) What is Attack? Explain various types of attacks in detail.

(2) Explain working of Digital Signature with its creation and verification.

(3) Short note on : PGP

(4) Explain SSL Record protocol.

(5) Explain SSL Handshake protocol.

(6) Explain working of Transport Layer Security (TLS) Protocol.

(7) Explain an Architecture of IP Security.

(8) What is HTTPS? Explain working of HTTPs

(9) What is Virus? Explain with its lifecycle and types.

(10) What are keyloggers? Explain its applications.

(11) Explain all about different types of keyloggers.

(12) What is firewall? Explain Packet filtering firewall in detail.

(13) Explain advantages and disadvantages of using firewalls.

(14) What is Proxy server? Explain working of proxy server.

(15) Explain various types of proxy servers in detail.

* * *

Chapter 3

CYBER CRIME

3.1 OVERVIEW OF CYBERCRIME

- INTRODUCTION TO CYBER CRIME
- INTRODUCTION TO CYBER CRIMINAL

3.2 CLASSIFICATION OF CYBER CRIMES

- ORGANISATIONAL CLASSIFICATION
- INDIVISUAL BASED CLASSIFICATION
- SOCIAL BASED CLASSIFICATION
- PROPERTY BASED CLASSIFICATION

3.3 CHALLENGES AND PREVENTIONS OF CYBER CRIME

- CHALLENGES OF CYBER CRIME
- PREVENTION OF CYBER CRIME

3.4 CYBER LAW

- THE INFORMATION TECHNOLOGY ACT, 2000
- THE INFORMATION TECHNOLOGY ACT, 2008
- SECTION 65 : TAMPERING WITH COMPUTER SOURCE DOCUMENTS
- SECTION 66 : COMPUTER RELATED OFFENCES
- SECTION 67 : PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM

○ **Self - Assessment**

3.1 OVERVIEW OF CYBERCRIME

The topic of most discussion in the twenty-first century is cybercrime. The number of people using smartphones and the internet is increasing, which is worrisome for the privacy and security of consumers in the technology industry globally. Because of this, it is imperative that all users understand cybercrime and security. According to this perspective, students should have knowledge about cybercrime and be ready to deal with impacts of it.

3.1.1 Introduction to cyber crime

Cybercrime is a risky attack that can happen to a business or a person. In numerous instances, a cyberattack has resulted in significant losses for both the organization and the person as a result of a data breach. Our day is driven by technology, and computers are now the source of all knowledge. Attacks on computers and other electronic devices are a part of cybercrime. These cyberattacks could be dangerous not just for personal or organizational but also for the country. Currently, there are several instances of cyberattacks in India and around the world, which calls for increased security. If not stopped at the outset, these attacks are also having an impact on the nation's economy.

Everybody thinks that only stealing someone's private data is Cyber Crime. But in defining terms we can say that

"Cyber Crime refers to the use of an electronic device (computer, laptop, etc.) for stealing someone's data or trying to harm them using a computer."

It comprises a wide range of crimes such as cyber fraud, financial scams, cybersex trafficking, ad scams, etc. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories :

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Some Notable Cases :

- One of the most high-profile banking computer crimes happened in 1970. The top teller at New York's Union Dime Savings Bank's Park Avenue branch stole over $1.5 million from hundreds of accounts.
- A hacker organization known as **MOD (Masters of Deception)** is accused of stealing passwords and technical data from Pacific Bell, Nynex, and other telephone providers, as well as six major credit bureaus and two major colleges.
- In January 2012, Zappos.com suffered a security breach that exposed up to 24 million customers' credit card details, personal information, and billing and delivery addresses.
- Unlawful access to camera sensors, microphone sensors, phonebook contacts, all internet-enabled apps, and metadata on mobile phones running Android and iOS appears to have been allowed by Israeli spyware, which was determined to be in use in at least 46 countries across the world.

3.1.2 Introduction to Cybercriminal

"Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit."

Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.

How cybercriminals are different than Hackers and threat actors :

Hacking does not necessarily count as a cybercrime; as such, not all hackers are cybercriminals. Cybercriminals hack and infiltrate computer systems with malicious intent, while hackers only seek to find new and innovative ways to use a system, be it for good or bad.

Cybercriminals also differ greatly from threat actors in various ways, the first of which is intent. Threat actors are individuals who conduct targeted attacks, which actively pursue and compromise a target entity's infrastructure. Cybercriminals are unlikely to focus on a single entity, but conduct operations on broad masses of victims defined only by similar platform types, online behaviour, or programs used.

Secondly, they differ in the way that they conduct their operations. Threat actors follow a six-step process, which includes researching targets and moving laterally inside a network. Cybercriminals, on the other hand, are unlikely to follow defined steps to get what they want from their victims.

Comparison between Hackers and Cybercriminals

Hackers	Cybercriminal
Hackers are computer programmers who use their skills to breach digital systems	Cybercriminals, on the other hand, are people who use computers to commit crimes
The intension of hackers not always bad. E.g. Ethical hackers, use their knowledge to improve security practices.	The intension of Cyber criminals is always to commit crime.
The most common types of hackers are White hat, Black hat, and Grey hat Hackers.	The common types of Cybercriminals are Hacktivists,Script Kiddies, Insider Threats, Cybercrime Groups
The primary goal of hackers is not a financial aid.	The primary goal of the cybercriminal is financial aids.

3.2 CLASSIFICATION OF CYBERCRIMES

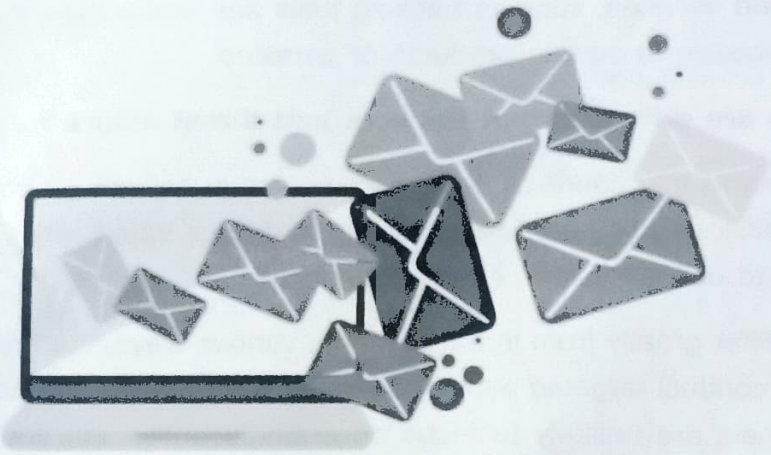
Hacking does not necessarily count as a cybercrime; as such, not all hackers are cybercriminals. Cybercriminals hack and infiltrate computer systems with malicious intent, while hackers only seek

3.2.1 Organizational Classification

A. E mail Bombing

An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial-of-service attack.

An email bomb is also known as a **letter bomb.**



[Fig. 3.1 : E Mail Bombing]

There are three ways to create an email bomb:

- Mass mailing: involves sending numerous duplicates of the same email to one email address. Because of the simplicity of this attack, it can be easily detected by spam filters. To be done on a massive scale, an attacker can use a bot net or zombie net, computers across the globe which are under the attacker's control due to some form of malware such as Trojans, and then instructing the bot net to send millions of emails to a single or a few addresses at once in order to perform a denial-of-service attack. This is harder for spam filters to detect since each email would be coming from a unique source.
- List linking: The technique involves subscribing the email address of victim for attack to different email list subscriptions so it would always receive spam mail from these lists. The user then has to manually unsubscribe from each list.
- ZIP bombing: the latest twist on email bombing using ZIP archived attachments. Mail servers always check email attachments for viruses, especially zip archives and .exe files. The idea here is to place a text file with millions or billions of arbitrary characters or even a single letter repeated millions of times so that the scanner would require a greater amount of processing power to read each one. Combining this with mass mailing techniques ups the potential for a denial-of-service attack to succeed.

Some of the **prevention methods** from e mail bombing are as :

- Strong Email Filters: Implementing robust email filtering solutions can help in identifying and blocking mass email sign-ups and suspicious influxes of emails.
- Monitoring and Alerts: Setting up monitoring systems to alert when there is an unusual spike in email traffic can help in quickly identifying an email bomb attack.
- Regular Security Audits: Conducting regular audits of email systems can help in identifying potential vulnerabilities that could be exploited for email bombing.

- Educating Employees: In organizations, educating employees about email bombs and related Email Security Threats is crucial. Awareness can lead to quicker identification and response to such attacks.
- Backup Communication Channels: Establishing alternative communication channels can ensure continuity of operations in case the primary email system is compromised.
- Collaboration with Email Providers: Working closely with your email service provider can be beneficial. Some providers offer specialized services to mitigate the effects of email bombing.

B. Salami Attack

A Salami Attack, also known as a Salami Slicing Attack, is a fraudulent method where a cybercriminal commits a series of minor, inconspicuous actions or thefts that, when combined, can lead to significant harm or a considerable compromise of data, resources, or assets.

The name "Salami Attack" originates from the idea of a cybercriminal metaphorically slicing off small, seemingly insignificant pieces of data or assets, much like slicing salami thinly.

These attacks are insidious because they are typically carried out in a way that each individual action remains inconspicuous, making it challenging for security systems to detect a breach until significant damage has already occurred.

Types of Salami Attacks

- Financial Salami Attack: This is the most common type, where attackers steal small amounts of money over time, often from multiple accounts or transactions. Attackers may round down transactions or subtly manipulate bank account balances to avoid immediate detection.

  A bank employee programs a system to round down interest calculations and deposits the fractions of a cent into a personal account.

- Data Salami Attack: Attackers gradually steal or manipulate small pieces of data from the database that are not immediately noticeable but lead to large-scale breaches or long-term integrity issues.

  A cybercriminal hacks into a company's database and extracts small portions of customer data (e.g., email addresses or phone numbers) to build a spam list or launch targeted phishing attacks.

- Resource Salami Attack: Attackers consume small amounts of computing resources or network bandwidth from multiple users or organizations to create a larger network for malicious purposes.

  A botnet operator uses thousands of infected devices to launch Distributed Denial of Service (DDoS) attacks on a website, consuming a small portion of each device's bandwidth, but the cumulative effect is a devastating attack.

Some of the **prevention methods** from Salami Attacks are as :

- Regular Audits: Implement comprehensive and frequent audits. These should be unpredictably timed and thoroughly check transaction logs and data records.

- Enhanced Transaction Monitoring: Use advanced monitoring software to detect anomalies in transaction patterns, no matter how small.
- Employee Training: Educate employees about salami attacks, including how to recognize and report suspicious activities.
- Data Validation and Integrity Checks: Regularly validate data and check for integrity to spot any discrepancies that might indicate a salami slicing technique in play.

Salami Attacks may appear inconspicuous and minor in isolation, but when executed systematically, they can lead to significant damage and losses.

C. Logic Bomb

A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs. When this condition is met, the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives.

Logic bombs are small bits of code contained in other programs. Although they might be malicious, they are not technically malware. Common types of malwares include viruses and worms, which can contain logic bombs as part of their attack strategy. A logic bomb virus would then be a virus that has a logic bomb in its code.

The defining characteristics of a logic bomb are:

- It lies dormant for a specific amount of time.
- Its payload is unknown until it triggers. A payload is the component that carries out the malicious activity.
- It's triggered by a certain condition. The detonator of the logic bomb is the condition that must be met. It's this feature that lets logic code bombs go undetected for long periods of time. Logic bombs with triggers related to dates or specific times are also known as **time bombs**.

D. Trojan Horse

A Trojan, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install other forms of malware, often ransomware.

A Trojan is sometimes called a Trojan virus or Trojan horse virus, but those terms are technically incorrect. Unlike a virus or worm, Trojan malware cannot replicate itself or self-execute. It requires specific and deliberate action from the user.

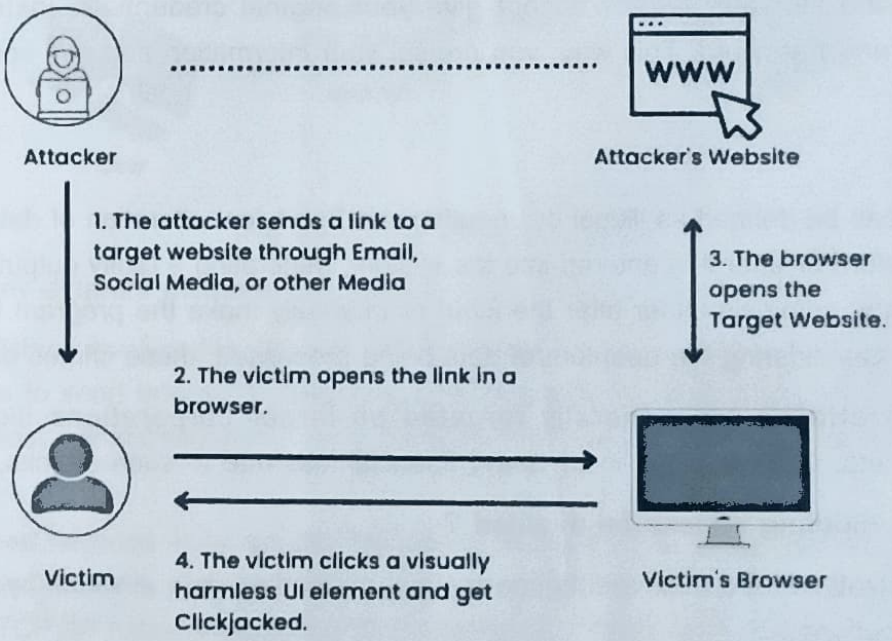
Trojans are malware, and like most forms of malware, Trojans are designed to damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system. Trojans may delete, block, modify, leak or copy data, which can then be sold back to the user.

E. Web Jacking

Among the several Cyberattacks; Web Jacking in Cyber Security is one of the most prominent.

Web Jacking is a type of phishing attack which frequently used to obtain user information, such as credit card numbers and login information, in Cyber Security.

In simplest terms, when attackers illegally gain control of an organisation's or individual's website is known as Web Jacking. The hackers implant a fake website, which, when you open it, takes you to another fraudulent website, where the attackers try to extract sensitive information. This crucial data can range from simple account passwords to credit card details.



[Fig. 3.2 : Web Jacking Working Model]

Following are the steps generally followed by attackers in Web Jacking.

- *Fake Website Creation* : Firstly, the hacker creates a fake web page using the same domain name as the targeted web application.
- *Hosting* : The second step is to host it on your computer or shared hosting.
- *Sending link* : This step involves the hacker sending the fake website's link to the victim. The success of the hacker's mission depends fully on whether the victim falls for it.
- *Entering details* : If the victim clicks on the link, it directs them to the malicious website. As the victim enters sensitive information like their login credentials or credit card details, the hacker gets all of it. The attacker can use these freshly retrieved details for nefarious reasons.

How one can be safe from Web Jacking

It is essential that you remain vigilant whenever something unfamiliar enters your system. You never know when you could become a victim of web jacking. This suggests that it is vital to remember a few pointers that can maintain cyber security.

- Avoid clicking suspicious links: The first tip to keep in mind is to avoid clicking on suspicious links that make their way to you via emails or messages.
- Check the legitimacy of the link: Always check the legitimacy of the link by pasting the URL on the address bar. Your first hint at a fraudulent link could be the difference between the URL and the intended website.
- Use of anti-Phishing detection browsers: Make use of browsers with anti-phishing detection.
- Confirm Spellings: If your links include company or institution names, confirm the original spelling.
- Provide fake Data: Another tip to keep in mind is that if or when you come across a shady website that is asking for your details, do not give your original credentials. Instead, put in a fake username and password. This way, you protect your information and can confirm the website's legitimacy.

F. Data Diddling

Data Diddling can be defined as illegal or unauthorized fraudulent alteration of data. It is the process of modifying data before or after it is entered into the system, generating a faulty output. While processing large amounts of data, criminals either alter the input or internally make the program that processes the data to malfunction. Considering the quantum of data being processed, these crimes are difficult to track.

Data Diddling attacks are generally targeted on larger corporations like power supply, telecommunications etc. Organisations incur heavy financial loss due to such attacks.

How can data diddling attacks be avoided ?

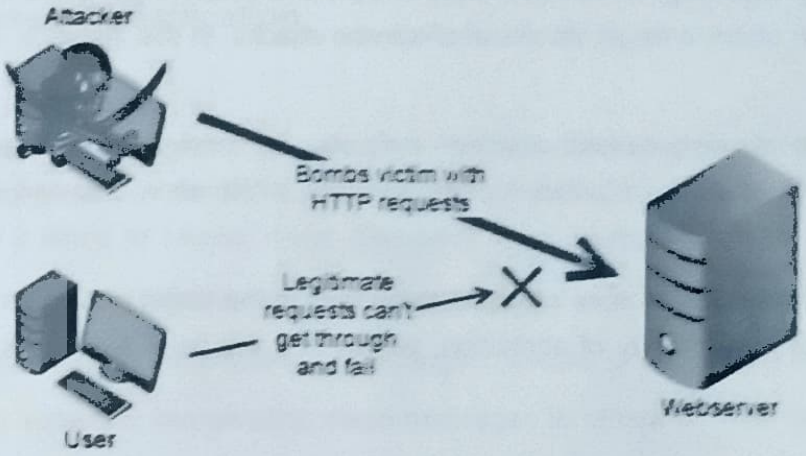
Financial organizations and their clients can prevent misleading data assaults by utilizing a number of countermeasure options:

- Consumers ought to routinely review their monthly statement and transaction history to look for any unusual activity. They can look over these transactions to find any strange credit card charges. If they see anything strange, they should notify their financial institution right away.
- The OWASP (Open Web Applications Security Project) principles must be adhered to in order to guarantee that no application contains undesired or harmful code.
- You should flag an email as phishing and delete it if it contains an attachment or asks for your bank account details or for you to click on a link to reset your password. Global organizations are still being impacted by phishing assaults, which include spear, email, barrel, and whale phishing. Security teams persist in allocating both organizational financial resources and human capital towards impeding data diddling and other related kinds of data theft.

G. Denial of Service / Distributed Denial of Service

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.

A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

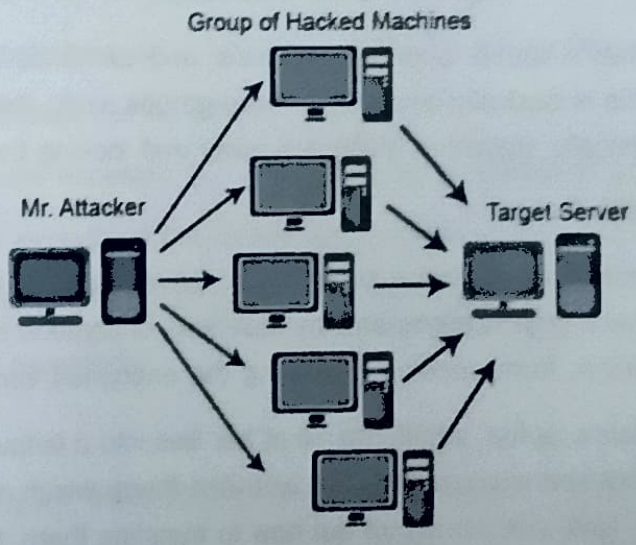


[Fig. 3.3 : Denial of Service Attack]

There are many different methods for carrying out a DoS attack.

- **A Smurf Attack** involves the attacker impersonating the target machine and using its faked source IP address to send Internet Control Message Protocol broadcast packets to several hosts. The targeted host will subsequently get a barrage of responses from the recipients of these spoof packets.
- **A SYN flood** happens when an attacker tries to connect to the target server by sending a request, but fails to finish the connection through the three-way handshake—a Transmission Control Protocol (TCP)/IP network technique that establishes a connection between a local host/client and server. The connected port is left in an occupied state and is not available for new requests due to the unfinished handshake. All open ports will be flooded with requests from an attacker, making it impossible for authorized users to connect.

Distributed Denial of Services Attack



[Fig. 3.4 : Distributed Denial of Service Attack]

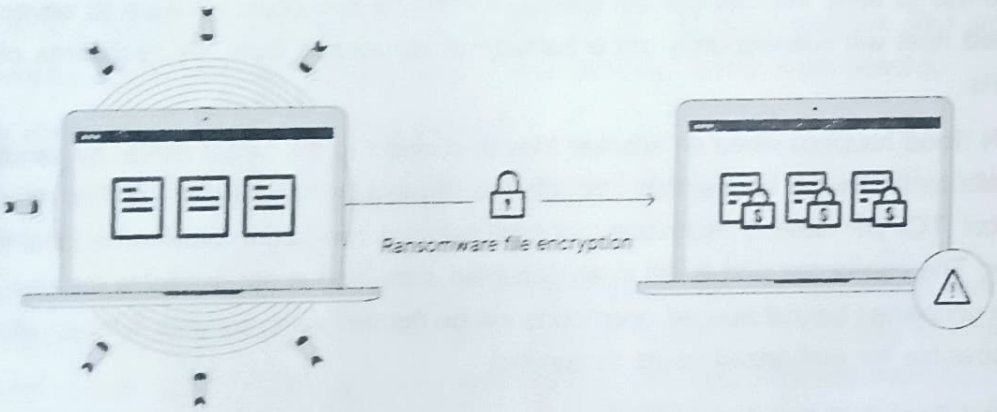
A distributed denial-of-service (DDoS) assault happens when several computers collaborate to attack a single target. A botnet is a collection of compromised internet-connected devices that is frequently used by DDoS attackers to launch massive attacks. Attackers use command and control software to take over many devices by taking advantage of security flaws or device shortcomings. Once in command, a hacker can direct their botnet to attack a target via denial-of-service attacks. In this instance, the attack also affects the infected devices.

Botnets—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to "attack-for-hire" services, which allow unskilled users to launch DDoS attacks.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

G. Ransomware

Malicious software known as ransomware encrypts files and demands payment for their release. Ransomware has the ability to spread swiftly throughout an entire network, and in certain instances, an infection has extended to networks owned by other businesses. Only when the victim pays the ransom can the individual or organization in possession of the malware unlock the files.



[Fig. 3.5 : Ransomware Attack]

Assume Ronak takes Rahi's laptop, puts it in his safe, and demands 20000 Rs. from her before allowing her to get it back. This is basically how ransomware groups work; the only difference is that they do it digitally rather than physically snatching machines away and locking them up.

How Ransomware works ?

Encryption is a vital component of online security and privacy and is frequently utilized for legal purposes. However, ransomware organizations employ malicious encryption to keep everyone, even the rightful owners of the information, from opening and using the encrypted versions of their files.

Now, instead of taking Rahi's laptop, transforms all of her files into a language she is illiterate in. Rahi still has access to the data, but she is unable to view or utilize them, which is comparable to encryption in the context of ransomware. Until she can figure out how to translate them, the files are effectively lost.

However, without the encryption key, decrypting data is nearly impossible, in contrast to interpreting a language.The attacking party keeps the key to themselves, which is why they have the leverage they need to demand payment.

3.2.2 Individual Based Classification

A. Cyber bullying

Cyberbullying is the use of digital communication tools (like the internet and cell phones) to make another person feel angry, sad, or scared. Online bullying is like in-person bullying in two key ways. It's done on purpose. And it tends to happen more than once. The examples include:

- Spreading lies about or posting embarrassing photos or videos of someone on social media.
- Sending hurtful, abusive or threatening messages, images or videos via messaging platforms.
- Impersonating someone and sending mean messages to others on their behalf or through fake accounts.

Cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.

B. Cyber Stalking

Cyberstalking uses the internet and other technologies to harass or stalk another person online, and is potentially a crime. Cyberstalking is an extension of cyberbullying and in-person stalking, can take the form of e-mails, text messages, social media posts, and more.

Even when the recipient says they're not happy or requests them to stop, the conversations usually go on. The content directed at the target is often inappropriate and sometimes even disturbing, which can leave the person feeling fearful, distressed, anxious, and worried.

Here are some examples of things people who cyberstalk might do:

- Post rude, offensive, or suggestive comments online.
- Follow the target online by joining the same groups and forums.
- Send threatening, controlling, or lewd messages or emails to the target.
- Use technology to threaten or blackmail the target.
- Tag the target in posts excessively, even if they have nothing to do with them.
- Comment on or like everything the target posts online.
- Create fake accounts to follow the target on social media.
- Message the target repeatedly.

C. Cyber Defamation

Defamation means giving an "injury to the reputation of a person" resulting from a statement which is false.

Cyber defamation is a new concept but it virtually defames a person through new medium. The medium of defaming the individual's identity is through the help of computers, internet or other digital technologies. If any individual posts or publishes some false statement about the other individual through internet or emails the individual having the defamatory statement with the intention to defame the other about whom the statement has been made would amount to cyber defamation.

D. Phishing

Phishing is a type of cybercrime in which criminals pose as a trustworthy source online to lure victims into providing personal information such as usernames, passwords, or credit card numbers. The goal of any phishing scam is always **stealing personal information**, there are many different types of phishing attacks as described below.

The various types of phishing attacks are: Email Phishing, Spear Phishing, Whaling, Smishing, Vishing, Business Email Compromise (CEO Fraud), Clone Phishing etc....

E. Cyber Fraud and Cyber Theft

Cyber fraud

Cyber fraud involves using online services and software with access to the internet to defraud or take advantage of victims. The term "Cyber fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

Cyber theft

Cybercrime is one of the most crucial problems faced by the countries across the globe these days. It includes unauthorized access of information and break security like privacy, password, etc. of any person with the use of internet. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet. The most common types of cyber theft include identity theft, password theft, theft of information, internet time thefts etc.

- Identity theft: Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit. It is the commonest form of cyber theft.
- Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.
- Intellectual property (IP) theft: Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy.

F. Spyware

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. Spyware collects information like user's internet usage,

credit card, and bank account details, or steal credentials. It sends such collected information to advertisers, data collection firms, or malicious actors for a profit.

The common types of spywares are :

- *Adware* : It enters in a device and monitors users' activity then sells their data to advertisers and malicious actors.
- *Infostealer* : It scans device for specific data and instant messaging conversations.
- *Keyloggers* : Keyloggers (Key Stroke logger) are a type of infostealer spyware. They record the keystrokes that a user makes on their infected device, then save the data into an encrypted log file. This spyware method collects all of the information that the user types into their devices, such as email data, passwords, text messages, and usernames.
- *Rootkits* : These enable attackers to deeply infiltrate devices by exploiting security vulnerabilities or logging into machines as an administrator. Rootkits are often difficult and even impossible to detect.
- *Red Shell* : It installs itself onto a device while a user is installing specific PC games, then tracks their online activity. It is generally used by developers to enhance their games and improve their marketing campaigns.
- *System monitors* : These also track user activity on their computer, capturing information like emails sent, social media and other sites visited, and keystrokes.
- *Tracking cookies* : Tracking cookies are dropped onto a device by a website and then used to follow the user's online activity.
- *Trojan Horse Virus* : This brand of spyware enters a device through Trojan malware, which is responsible for delivering the spyware program.

G. E-mail Spoofing

Email spoofing is a technique that is used in spamming and phishing attacks which involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email. This way, the protocols think it came the real sender.

E.g. The SMTP (Simple Mail Transport Protocol) doesn't make any provision to authenticate email addresses. So, hackers take advantage of this weakness to fool unsuspecting victims into thinking the mail is coming from someone else.

Difference between E mail Spoofing and Phishing

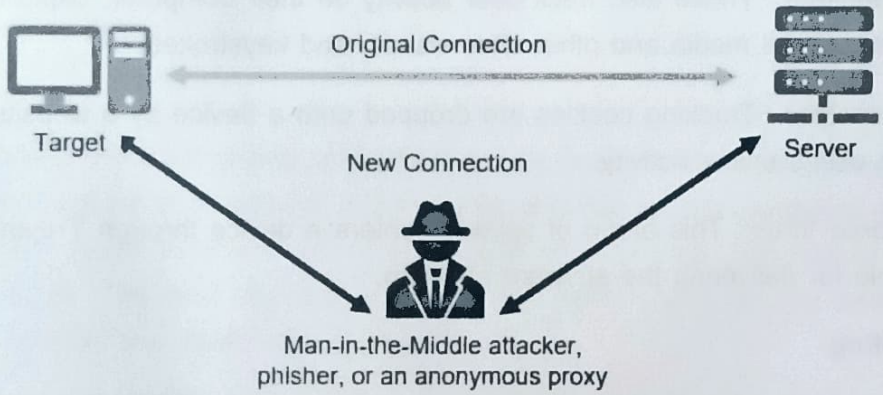
Spoofing	Phishing
Spoofing refers to a form of identity theft where someone uses the identity of a real user.	Phishing involves someone stealing sensitive information such as bank or credit card details.
Spoofing can involve phishing.	Phishing is not an element of spoofing.
With spoofing, the target has to download malware.	Phishing uses social engineering.
Spoofing is used to acquire identity information.	Phishing is aimed at extracting confidential information.

(H) Man in the middle attack

Man-in-the-middle attacks (MITM) are a common type of security attack which allows attackers to manipulate both communicating parties and achieves access to the data that the two parties were trying to deliver to each other.

The attack takes place in between two legitimately communicating parties, allowing the attacker to "listen" to a conversation they should normally not be able to listen to, hence the name "Man-In-The-Middle."

Working of Man In The Middle (MITM) Attack :



[Fig. 3.6 : Man In The Middle Attack]

Regardless of the specific techniques and technologies, the MITM attacks can be carried out with the below work flow order.

1. Sender A sends message to the recipient B.
2. The MITM attacker intercepts the message without sender(A) or receiver(B) knowledge.
3. The MITM attacker changes the message content or removes the message altogether, again, without the knowledge of sender and receiver.

In computing terms, a MITM attack works by exploiting vulnerabilities in network, web, or browser-based security protocols to divert legitimate traffic and steal information from victims.

Some of the Man InThe Middle (MITM) attack types are : *Email Hijacking, Wi-Fi Eavesdropping, DNS Spoofing, Session Hijacking, Secure Sockets Layer (SSL) Hijacking, ARP Cache Poisoning, IP Spoofing, Stealing Browser Cookies*

3.2.3 Social Based Classification

Some of the social based classification are as under :

A. Cyber Pornography

Pornography is a criminal offence which has been considered as one of the corrupt demonstrations causing harm to people. Cyber pornography means an act by using cyberspace to create, display, distribute, import, or publish obscene materials, especially materials related to children who are engaged in sexual acts with adults.

Sexually explicit content has seemingly become a bigger problem than one could have imagined it to be because of technological advancements and easy access of cyberspace.

B. Cyber Terrorism

Cyber Terrorism attack is defined as a "cybercrime that may be used intentionally to cause harm to people on large scale using computer programs and spyware."

Hackers with extensive experience and talent can seriously harm government systems and force a nation to flee out of fear of further attacks. Since this is a sort of terrorism, the goals of such terrorists may be political or ideological.

C. Cyber Spying

Cyber spying, also known as cyber espionage, is a form of Cyber Attack where an attacker obtains information without authorized permission or knowledge by the information holder in a digital setting.

Various methods can be employed to spy digitally: account hacking, tracking behaviour with cookies or keylogging, or implementing malware onto devices such as Trojan horses and spyware are frequently used spying tactics on users. Though pervasive spying in any sense is considered illegal, this does not stop the practice from being carried out on a massive scale through loopholes, especially by those in high power.

D. Social Engineering Attack

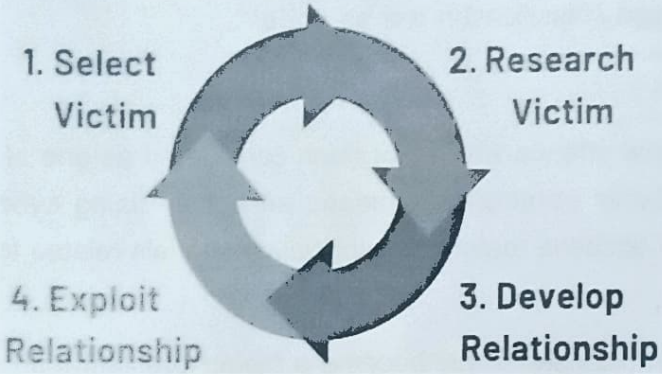
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Steps of a Social Engineering Attack

Social engineering attacks typically follow these simple steps :

1. **Research :** The attacker identifies victims and chooses a method of attack.

2. **Engage**: The attacker makes contact and begins the process of establishing trust, appealing to greed, helpfulness, or curiosity, and creating a sense of urgency.
3. **Attack**: The attack commences and the attacker collects the payload.
4. **The Gateway**: The attacker covers their tracks and concludes the attack.



[Fig. 3.7: Social Engineering Life Cycle]

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

E. Online gambling

Government authorities prohibits individuals from betting on sports or gambling contests using a "wire communication facility," which includes the Internet. Yet the Internet allows immediate and anonymous communication that makes it difficult to trace gambling activity. Internet sites can be altered or removed in a matter of minutes. For these reasons organized crime operates internet gambling sites.

Operators alter gambling software to be in their favour so the customer always loses. Unlike real casinos that are highly regulated, Internet gambling is unregulated and dangerous. Individuals gambling on the Internet risk providing credit card numbers and money to criminal gambling operators. Further, minors can gamble on the sites since the Internet is unaware of the age of its users.

3.2.4 Property Based Classification

A. Credit Card Fraud

Credit card fraud is a type of financial crime that involves the unauthorized use of someone else's credit card information to make purchases or access funds. This illicit activity can take various forms, and criminals use different techniques to obtain or use credit card details fraudulently. Here are some common types and aspects of credit card fraud:

- *Stolen Cards* : Criminals may physically steal credit cards from individuals or intercept new cards sent through the mail.

- *Lost or Misplaced Cards* : If someone loses their credit card, it can be found by an unauthorized person who then uses it for fraudulent transactions.
- *Skimming* : Skimming involves using a small device (skimmer) to capture credit card information during a legitimate transaction. This often happens at ATMs, gas pumps, or point-of-sale terminals.
- *Phishing* : Cybercriminals use phishing techniques to trick individuals into providing their credit card information by posing as a trustworthy entity in emails, messages, or websites.
- *Carding* : Carding is a practice where criminals use stolen credit card information to make small online purchases to validate if the card is still active before making larger transactions.
- *Account Takeover* : Hackers may gain unauthorized access to online accounts where credit card information is stored, allowing them to make purchases using the victim's card.
- *Identity Theft* : In cases of identity theft, criminals may use stolen personal information, including credit card details, to open new credit card accounts in the victim's name.
- *Malware and Data Breaches* : Criminals use malware to infect computer systems or exploit vulnerabilities to gain access to large databases containing credit card information. Data breaches at businesses or financial institutions can result in the exposure of thousands or even millions of credit card records.
- *Social Engineering* : Fraudsters may use social engineering techniques to manipulate individuals into revealing their credit card information over the phone or online.

To prevent credit card fraud, individuals and businesses can take various measures, such as monitoring their accounts regularly, using secure and unique passwords, enabling two-factor authentication, and being cautious about sharing personal information.

B. Software Piracy

Software privacy refers to the illegal act of copying, distributing, using, or selling application without the permission or proper licensing from the rightful owners or publishers.

This practice violates intellectual property laws, specifically copyright laws, which are designed to protect the rights of creators and publishers.

Here are some common forms of software piracy :

- *Unauthorised Copying* : This involves installing and using application on multiple computers beyond the terms allowed by the purchased license. For example, using one license to install application on multiple office computers or sharing it with friends.
- *Counterfeiting* : This type of piracy involves creating and selling fake copies of application. These copies often appear legitimate but are illegal reproductions.
- *Internet Piracy* : This involves downloading application from the internet without paying for it or obtaining it through proper channels. It includes using torrent sites, file-sharing networks, or unauthorised download links.

- *Cracking Software* : This is the process of modifying application to remove or disable features that are considered undesirable by the person cracking it, often including copy protection features.
- *Corporate Piracy* : This occurs when businesses use unlicensed application or more copies than permitted by the license. It's a form of piracy that can involve significant financial losses for application companies.
- *OEM (Original Equipment Manufacturer) Unbundling* : This happens when OEM application, which is meant to be sold with specific hardware, is copied and sold separately without the hardware.
- *Softlifting* : This refers to purchasing a single licensed copy of application and then loading it onto several computers, contrary to the license terms.

C. Copyright Infringement

Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder. Copyright infringement means that the rights afforded to the copyright holder, such as the exclusive use of a work for a set period of time, are being breached by a third party. Music and movies are two of the most well-known forms of entertainment that suffer from significant amounts of copyright infringement.

Living in the digital era, it is becoming less common for authors to express their creative sparkle as physical embodiments. The digital form of expression carries many advantages but also opens some potential threats. One of them is vulnerability to cyberattacks and cybercrime. Some forms of copyrighted work are, by nature, conditioned to be in a digital (electronic) form, such as databases and computer software.

As a consequence, copyright infringement and cybersecurity-related issues are at the point of focus.

D. Trademarks violations

Trademark violations in cybersecurity occur when a company or individual uses a trademarked name, logo, or other intellectual property without proper authorization in the context of cybersecurity products, services, or marketing materials.

Trademark violation may happen in various ways:

1. Product Names : Companies may use trademarked names or terms to market their cybersecurity products or services without authorization from the trademark owner.
2. Domain Names : Registering domain names that include trademarked terms or brands to mislead users or divert traffic is another common form of trademark violation in cybersecurity.
3. Advertising and Marketing : Unauthorized use of trademarked logos, slogans, or other branding elements in advertising materials, online campaigns, or social media posts can constitute trademark infringement.
4. Cybersquatting : This involves registering domain names with the intent to profit from the goodwill associated with someone else's trademark.

5. False Endorsement : Using a trademarked name or logo in a way that suggests endorsement or affiliation with the trademark owner when no such relationship exists can lead to trademark violations.

Trademark violations in cybersecurity can result in legal action, including cease and desist letters, lawsuits for damages, and demands to transfer domain names. It's essential for businesses operating in the cybersecurity space to conduct thorough research and obtain proper authorization when using third-party trademarks to avoid potential legal consequences.

3.3 CHALLENGES AND PREVENTIONS OF CYBERCRIME

The incredible evolution of information society and its dependence on Internet usage in world and particularly in India is laterally accompanied by vulnerability of societies to cybercrime. Cybercriminals are not constrained by geographical limitations as cyberspace is a free-flowing, borderless and a global problem. These crimes can't be deterred by local laws. India to counter Cybercrime has engaged itself in various bilateral agreements like cyber agreement with Russia and a framework agreement with the US. Indo-Israel cyber framework is yet another effort of India to streamline its cyberspace. Even if this effort there are so many challenges of Cybercrime. These bilateral agreements have limited scope and are inadequate and ineffective to deal with cybercrime. Some of the challenges are as under:

3.3.1 Challenges of Cyber Crime

- **Poor awareness about their cyber rights :**

  Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

- **Anonymity :**

  Those who Commit cybercrime are anonymous for us so we cannot do anything with these people.

- **Less number of registered cases :**

  Every country in the world faces the challenge of cybercrime and the rate of cybercrime is increasing day by day because the people who even don't register a case of cybercrime and this is major challenge for us as well as for authorities as well.

- **Mostly Educated People are Involved :**

  Committing a cybercrime is not a cup of tea for every individual. The person who commits cybercrime is a very technical person so he knows how to commit the crime and not get caught by the authorities.

- **No Harsh Punishment :**

  In Cybercrime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment

for that individual. But in other cases, there is no harsh punishment so this factor also gives encouragement to that person who commits cybercrime.

- **Fragmented and complex regulations :**

  Different countries, and jurisdiction may have different rules regulations and provisions in regard cybercrime.

- **No procedural rules :**

  There are no separate rules of procedure for investigating cybercrime or computer crime. Electronic evidence is very different from traditional criminal evidence, so it is essential to establish standardized and consistent procedures for handling electronic evidence.

- **Shortage of technical staff :**

  There are minimal efforts by states to recruit technical personnel to investigate cybercrime. A regular police officer with a background in humanities and business administration may not understand the nuances of how computers and the Internet work.

  Additionally, the Information Technology (IT) Act of 2000 maintains that offences registered under the Act should be investigated by police officers, not below the rank of inspector. In practice, the number of police inspectors in the district is limited and most field investigations are conducted by deputy inspectors.

- **Lack of Infrastructure – Cyber labs :**

  State cyber forensics labs need to be upgraded as new technologies emerge. Cryptocurrency-related crime continues to be underreported due to the limited ability to solve such crimes. Most government cyber labs are well equipped to analyse hard drives and mobile phones, but many still employ "electronic evidence examiners" so they can provide an expert opinion on electronic records.

3.3.2 Prevention of Cyber Crime :

While it isn't possible to completely eradicate cybercrime and ensure complete internet security, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy using a defence in depth to securing systems, networks and data. Thus, to deal with cybercrime is very difficult but fortunately, there are many effective ways of preventing cybercrime, including:

- **Use Strong Passwords**

  For each account, keep a unique username and password combination; avoid writing them down. Complex passwords—those with a mix of letters, numbers, and special characters—are more difficult to crack than weak ones because weak passwords can be easily cracked using techniques like Brute force attacks and Rainbow Table attacks.

- **Use reliable antivirus software**

  For both personal computers and mobile devices, make sure to always utilize cutting-edge, reliable antivirus software. As a result, several virus attacks on devices are avoided.

- **Maintain privacy on social media**

  Make sure that only your friends have access to the data on your social media accounts. Additionally, be sure to limit your friend-making to people you know.

- **Always use updated software**

  Use the software on your device whenever you receive updates. This is because outdated versions of the program might occasionally be readily exploited.

- **Avoid Public Network / Use a secure network**

  Public Wi-Fi is not secure. Refrain from executing business or financial transactions over these networks.

- **Avoid opening attachments from scam emails**

  These can lead to malware infections and other types of online fraud on your machine. Never open an attachment that someone you do not know sent you.

- **Use updated operating systems**

  When it comes to internet security, software and operating systems should be updated frequently. This might become dangerous if hackers take advantage of holes in the system.

- **Use of Firewalls**

  Firewalls can control incoming and outgoing traffic on a computer network, blocking external threats from entering.

- **Use of Antivirus software**

  Antivirus software can detect, quarantine, and remove malicious and suspicious applications.

- **Intrusion detection and intrusion prevention systems (IDS/IPS)** monitor network traffic and system logs to identify and respond to potential threats.

Finally, organizations can hire dedicated cyber security professionals such as Computer hacking and forensics investigators, Ethical Hackers, Penetration testing professionals, Network security professionals, Incident responders and Cyber security technicians

3.4 CYBER LAW

3.4.1 The Information Technology ACT, 2000

The Indian IT Act 2000, also known as the Information Technology Act, 2000, is a legislation passed by the Indian government to provide legal recognition and guidelines for electronic transactions, digital signatures, cybersecurity, and the regulation of cyberspace in India. The Act was enacted to address emerging challenges and issues in the digital realm and to establish legal frameworks for electronic commerce, digital communication, and data protection.

Key provisions of the Indian IT Act 2000 include :

1. **Legal Recognition of Electronic Records :** The Act recognizes electronic records and digital signatures as legally valid and equivalent to their paper-based counterparts. This enables the use of electronic documents in legal proceedings.
2. **Offenses and Penalties :** The Act identifies various cyber offenses and prescribes penalties for activities such as unauthorized access to computers, data theft, hacking, identity theft, and spreading of computer viruses. It also covers offenses related to obscenity, pornography, and the protection of children online.
3. **Cybercrime Investigation and Law Enforcement :** The Act grants powers to law enforcement agencies to investigate and prevent cybercrimes. It outlines procedures for the collection and preservation of digital evidence and enables authorities to request assistance from service providers and intermediaries.
4. **Digital Signatures :** The Act recognizes and regulates the use of digital signatures, which serve as a secure method for verifying the authenticity and integrity of electronic records and transactions.
5. **Data Protection and Privacy :** The Act includes provisions related to the protection and privacy of personal data. It outlines guidelines for the collection, storage, and use of personal information by individuals and entities.
6. **Cyber Appellate Tribunal :** The Act established the Cyber Appellate Tribunal (CAT), which serves as an appellate authority for adjudicating appeals against orders issued by the Controller of Certifying Authorities and Adjudicating Officers under the Act.
7. **Network Service Providers' Liability :** The Act includes provisions related to the liability of network service providers, intermediaries, and internet companies for content hosted on their platforms. It provides certain exemptions to intermediaries for content posted by users but also requires them to comply with due diligence and take down objectionable content upon notification.

3.4.2 The Information Technology ACT, 2008

(Ref: https://www.indiacode.nic.in/bitstream/123456789/15983/1/the_information_technology_act%2c_2008.pdf)

The Indian IT Act 2000 has undergone amendments over the years to address emerging challenges in cyberspace, including the introduction of the Information Technology (Amendment) Act, 2008, which expanded the scope of cyber offenses and introduced additional provisions related to data protection and privacy.

Some of them amendments which expanded the scope of cyber offences are as under :

Section 65 : Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme,

computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Section 66 : Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two **three** years or with fine which may extend to five lakh rupees or with both.

Explanation : For the purpose of this section, -

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66 A. Punishment for sending offensive messages through communication service, etc.

(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,

(a) any **information** that is grossly offensive or has menacing character; or

(b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to two **three** years and with fine.

Explanation : For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66 B. Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66 C. Punishment for identity theft. (Inserted Vide ITA 2008)

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66 D. Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66 E. Punishment for violation of privacy. (Inserted Vide ITA 2008)

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation. - For the purposes of this section –

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that —

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66 F. Punishment for cyber terrorism

(1) Whoever, -

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Section 67. Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to **two three** years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to **five** years and also with fine which may extend to ten lakh rupees.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five** years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.

Exception : This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever, -

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees :

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form -

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation : For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67C. Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is Cyber Crime? List out two notable cases.

(2) Define the terms: Cybercrime, Cybercriminal.

(3) Differentiate: Hackers V/s Cybercriminals

(4) List out types of cybercrime in terms of Organizational classification.

(5) List out types of cybercrime in terms of Individual based classification.

(6) List out types of cybercrime in terms of Property classification.

(7) What is Salami Attack? List out various Salami Attacks.

(8) What is logic bomb? Why it is called time bomb?

(9) Define the terms : Web Jacking, Data Diddling, DOS Attack, DDOS Attack.

(10) Define the terms : Cyber bullying, Phishing, Spyware, E mail Spoofing.

(11) What is Cyber terrorism?

(12) List out any four challenges in cybercrime.

Q. 2 Explain the below questions:

(1) What is Cybercrime? Explain in detail with defining cybercrime and cybercriminals.

(2) Explain various types cybercrime under Organizational classification.

(3) Explain various types cybercrime under Individual classification.

(4) Explain various types cybercrime under Property classification.

(5) Explain e mail bombing in detail.

(6) Explain Web jacking in detail.

(7) Explain Salami attack in detail.

(8) Explain DOS Attack and DDOS attack. Also differentiate them.

(9) Explain Social based Classified Cybercrime in detail.

(10) Explain Section 65 in brief.

(11) Explain various challenges of Cyber Crime.

***