CNS (2019) model answers

Unit 6 Security

What is the Need of security?

- Cyber security is crucial because it protects all types of information from theft and loss. (Loss of money, assets)
- Social reputation of person or business
- internet is being used by millions of users because most Financial services, payments, health services, etc are all connected via internet, on a daily basis.
- To ensure critical infrastructure system do not collapse under any situation.
- To ensure Business continuity.
- To protect Individual's rights and privacy.

Threats and Vulnerabilities

- Vulnerability refers to a weakness in your hardware, software, or procedures. (it's a way hackers could easily find their way into your system.) And risk refers to the potential for lost, damaged, or destroyed assets
- A threat takes advantage of a vulnerability and can damage or destroy an asset.
- Threat can be
  a)destruction of information;
  b) corruption or modification of information;
  c) theft of information;
  d) disclosure of information; and
  e) interruption of services.

What is Network security (CIA triad)

- Security ensures that only authorized users (confidentiality) have access to accurate information (integrity) when required (availability).
- it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility(CIA) of computer networks and data using both software and hardware technologies.
- Cyber security is the practice of protecting systems, networks, and programs from digital attacks
- It is different than physical attack on room where server , data center is kept , or system administrator.

Explain the three Key Principles of Security (CIA triad)

- **Confidentiality**

  Means the data is only available to authorized parties. Confidentiality not only applies to the storage of the information, it also applies to the transmission of information.

- **Integrity:**

  Guarantee that the data is not modified during transmission , either intentional or unintentional by unauthorized persons.

- **Availability:**

  This means that the information is available to authorized users when it is needed (eg denial of service (DOS) attack

What is attack ? explain different types of attackes.

three goals of security(CIA) can be threatened by security **attacks**

following are the types of attacks:

1. Snooping
2. Traffic Analysis
3. Modification
4. Masquerading (spoofing)
5. Replaying
6. Repudiation

- **Snooping** Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit.

  it can be prevented by encryption

- **Traffic Analysis** encryption of data makes it unusable for the intruder , but she can obtain some other type information by monitoring online traffic.

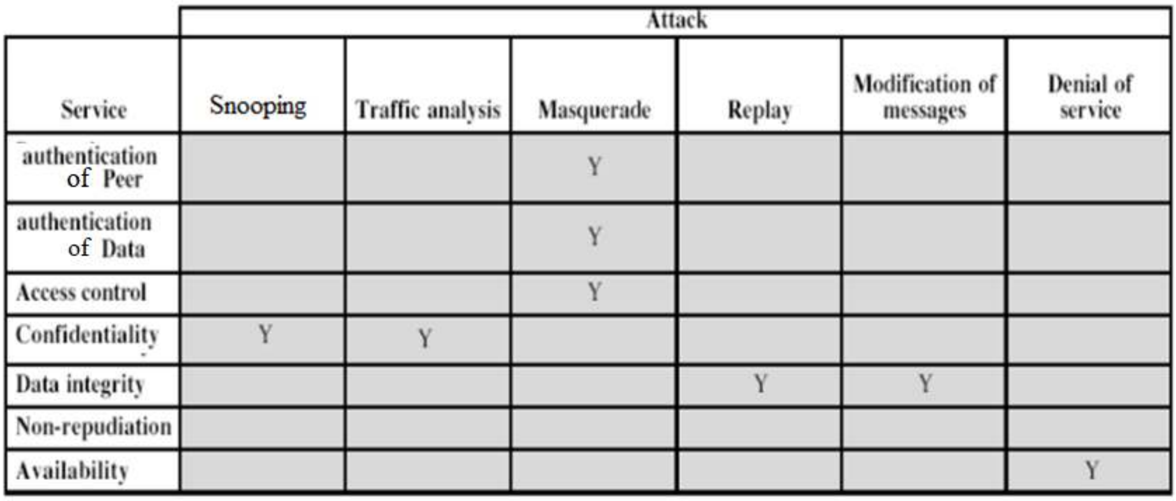
- **Modification** After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself or destructive

- **Masquerading** (spoofing) happens when the attacker impersonates somebody else to the legitimate user. Eg pretend as bank for a customer , or pretend as customer for a bank

- **Replaying** The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive repeat payment from the bank

- **Repudiation** is not by third party but is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message. Eg online shopping deny that payment has been made by customer.

Which service is is threatened by which attack:



	Attack					
Service	Snooping	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
authentication of Peer			Y			
authentication of Data			Y			
Access control			Y			
Confidentiality	Y	Y				
Data integrity				Y	Y	
Non-repudiation						
Availability						Y

Cyber-attacks can also be classified into the following categories:

Web based   & system based

- **Web-based attacks**

These are the attacks which occur on a website or web applications

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Another way of classifying network attacks:

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.

  Types of passive attacks

  1. Traffic analysis.
  2. Eavesdropping. ...
  3. Footprinting. ...
  4. Spying. ...
  5. War driving. ...
  6. Dumpster diving.

- **Active:** Attackers not only gain unauthorized access but also modify or delete or encrypts data being send

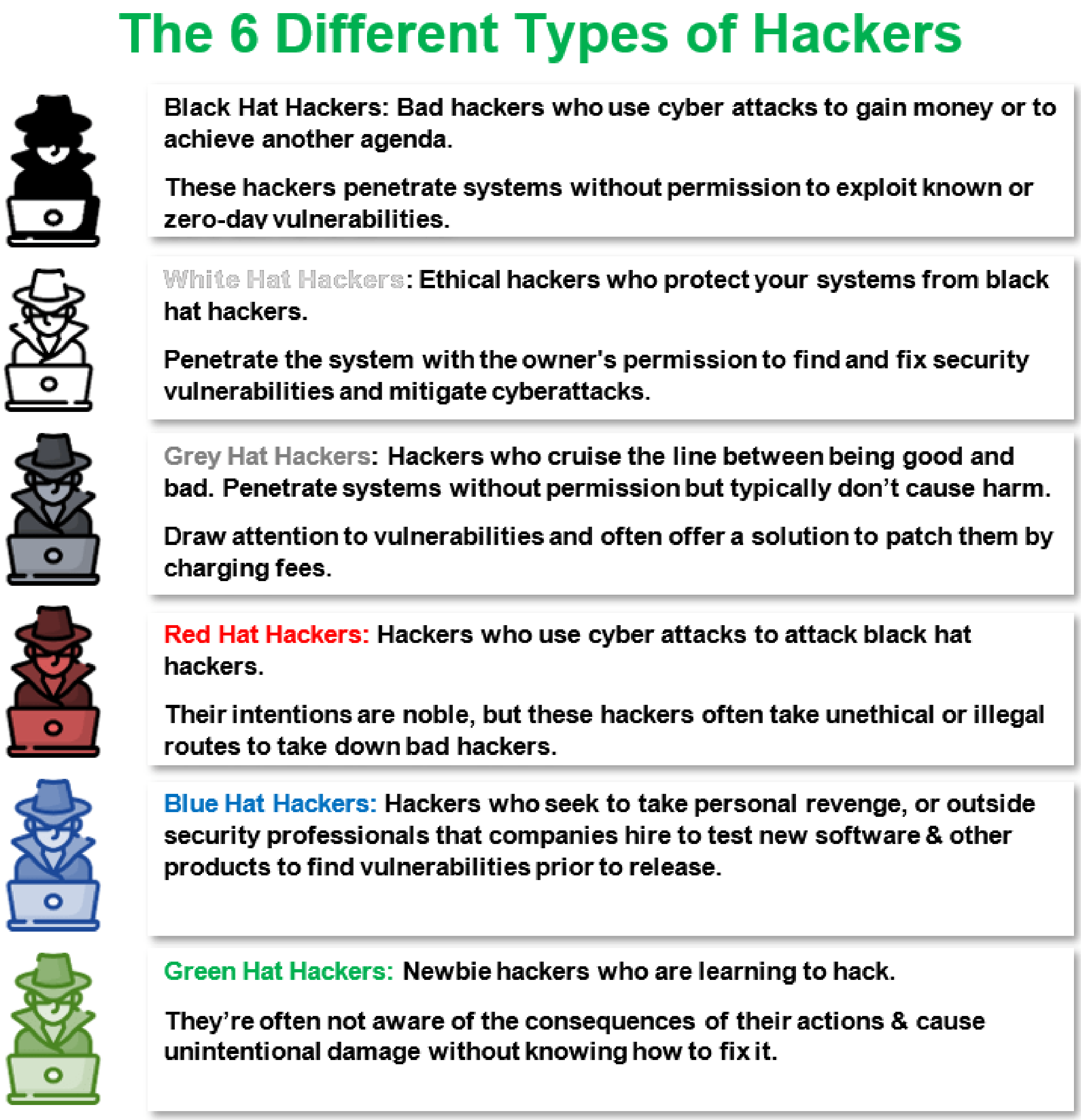
1. Session Hijacking Attack: in which the attacker will take over your internet session. ...
2. Masquerade Attack ...
3. Denial-of-Service Attack ...

4. Distributed Denial-of-Service Attack ...

5. Trojans ...

What is hacking?

also known as cyber attacking, Is the practice of intentionally exploiting weaknesses in an organization's computer systems.



The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don’t cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

Green Hat Hackers: Newbie hackers who are learning to hack.

They’re often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

Hackers are good people who hack devices and systems with good intentions. They might hack a system for a specified purpose or for obtaining more knowledge out of it.

Crackers are people who hack a system by breaking into it and violating it with some bad intentions.

What is Ethical hacking ?

involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them

compare Hacker with Cracker

Hacker	**Cracker (black hat hackers)**
The good people who hack for knowledge purposes.	The evil person who breaks into a system for personal benefits .
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organisation to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organisations .
Hackers share the knowledge and never damages the data.	If they found any loop hole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benifit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for there cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as there motive is to stay annonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers.

What are the System-based attacks?

These are the attacks are on computer software (client or server).

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

ITU-T X.800 Security Architecture for OSI

(ITU-T: International Telecommunications Union – Telecommunications Sector)

It Defines security requirements and providing those security requirements

ITU-T X.800 Security Architecture for OSI

The following concepts are used:

- **Security attack:** Any actions that compromises thesecurity of information owned by an organization (or aperson)

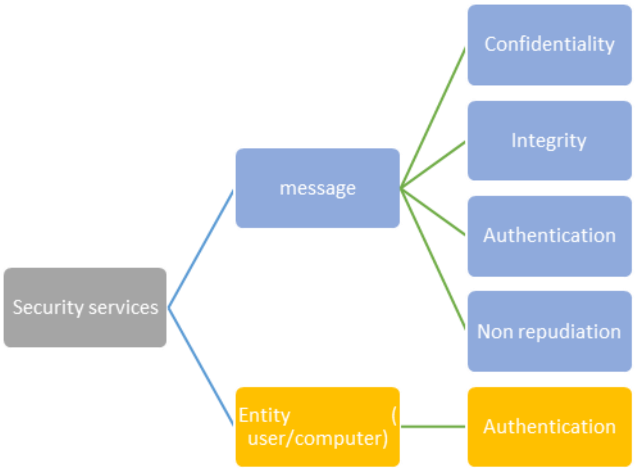
• **Security mechanism:** a mechanism that is designed todetect, prevent, or recover from a security attack

• **Security service:** a service that enhances the security ofthe information of an organization. The security services make use of one or more security mechanisms to provide the service

In short , security services make use of security mechanisms to reduce the effects of security attacks

Types of security attacks

(ITU-T defines 5 attacks CIA + non repudiation & authentication)



- Message Confidentiality
  The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.

- Message Integrity
  Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000.

- Message Authentication
  Message authentication is a service beyond message integrity. In message authenticationthe receiver needs to be sure of the sender's identity and that an imposter has not sent themessage.

- Message Nonrepudiation
  Message nonrepudiation means that a sender must not be able to deny sending a message
  that he or she, in fact, did send. The burden of proof falls on the receiver. For example,
  when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

- Entity Authentication
  In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example)

Security mechanisms

1. *Encipherment*
2. *Digital signature*
3. *Access control*
4. *Data integrity*
5. *Authentication exchange*
6. *Traffic padding*
7. *Routing control*
8. *Notarization*

Service	**Mechanism**							
	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
authentication	Y	Y	·	·	Y	·	·	·
Access control service	·	·	Y	·	·	·	·	·

confidentiality	Y	·	·	·	·	·	Y	·
Integrity	Y	Y ·	·	Y	·	·	·	·
Non-repudiation.		Y	·	Y	·	·	·	Y

Operational Model of Network Security

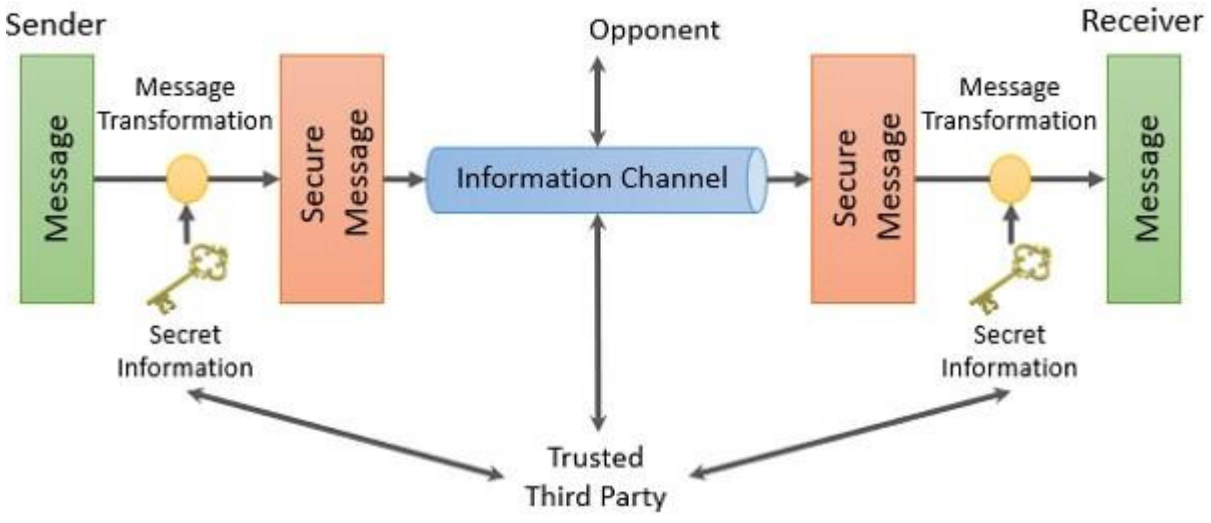
A Network Security Model shows how the security service has been designed over the network to prevent the opponent from causing a threat to the CIA of the information that is being transmitted through the network.
Any security service would have the **three components** :

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the **secret information** between sender and receiver of which the opponent must not any clue. i.e. the **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

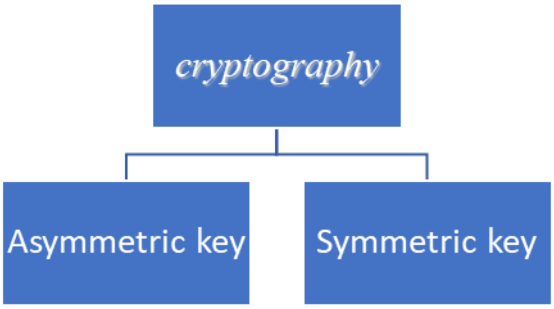
3. There must be a **trusted third party** which should take the responsibility of **distributing the secret information** (key) to both the communicating parties and also prevent it from any opponent.



Network Security Model

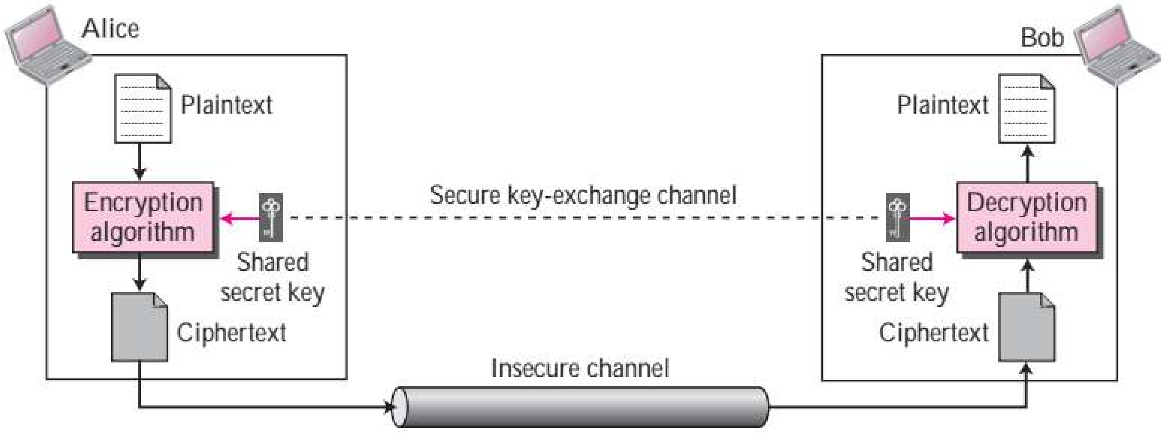
cryptography

- *The word cryptography in Greek means "secret writing."*
- *The term today refers to the science and art of transforming messages to make them secure and immune to attacks.*
- *Cryptography can be implemented by two techniques*



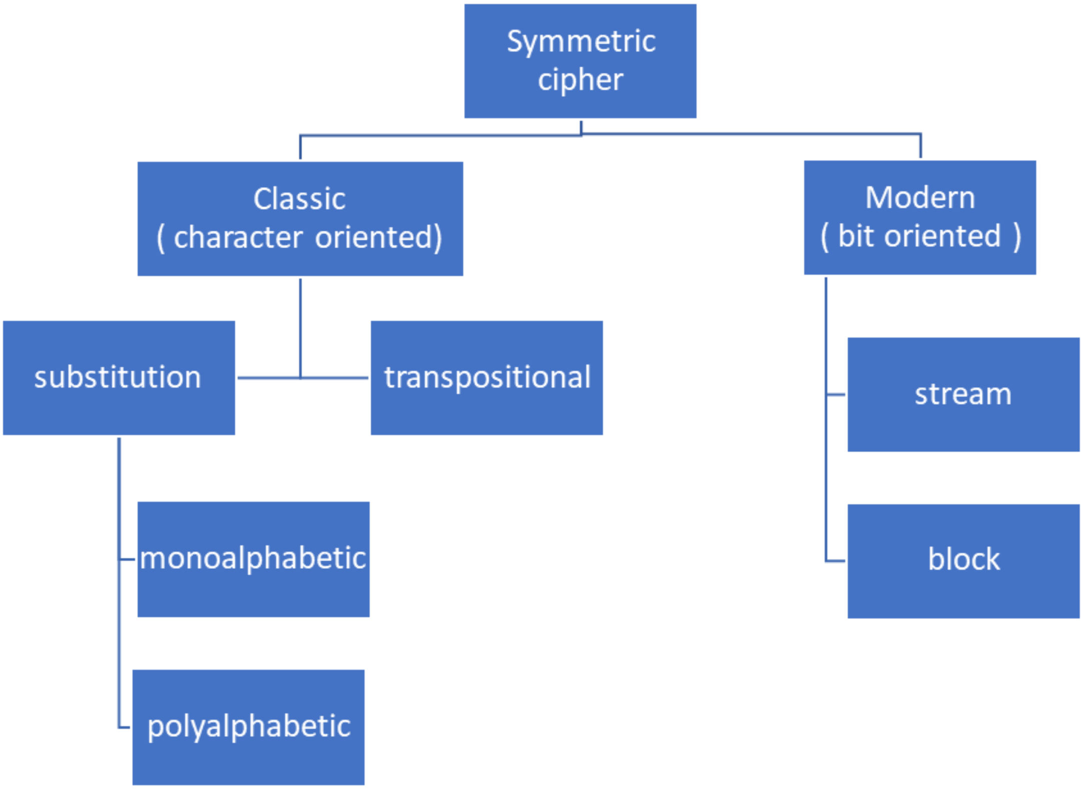
symmetric-key ciphers

- These are Traditional ciphers
- Also called as secret-key ciphers
- symmetric-key means the same key is used for encryption by sender and decryption by receiver
- The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To get back the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key used by Alice.
- encryption and decryption algorithms are called as ciphers . A key is a set of values (numbers) that the cipher (algorithm) uses to create cipher text



- If P is the plaintext, C is the ciphertext, and K is the key, the encryption algorithm E*k*(*x*) creates the ciphertext from the plaintext; the decryption algorithm D*k*(*x*) creates the plaintext from the ciphertext.
- So Encryption: C = E*k*(P)   Decryption: P = D*k*(C)
- We assume that E*k*(*x*) and D*k*(*x*) are inverses of each other: they cancel the effect of each other if they are applied one after the other on the same input D*k*(E*k*(*P*)) = E*k*(D*k*(*P*)) = *P*.
- *In symmetric cryptography, the encryption/decryption algorithms are public; the key is secret.*
- This means that Alice and Bob need separate secured channel, to exchange the secret key. That secured channel can be face-to-face exchange of the key or They can also trust a third party to give them the same key.
- **Key**
  Encryption is similar to putting the message in a locker; decryption is similar to unlocking the locker. In symmetric-key encipherment, the same key locks and unlocks .

Classification of symmetric Key ciphers



Substitution Ciphers

A substitution cipher replaces one symbol with another

Subtypes : monoalphabetic ciphers & polyalphabetic ciphers.

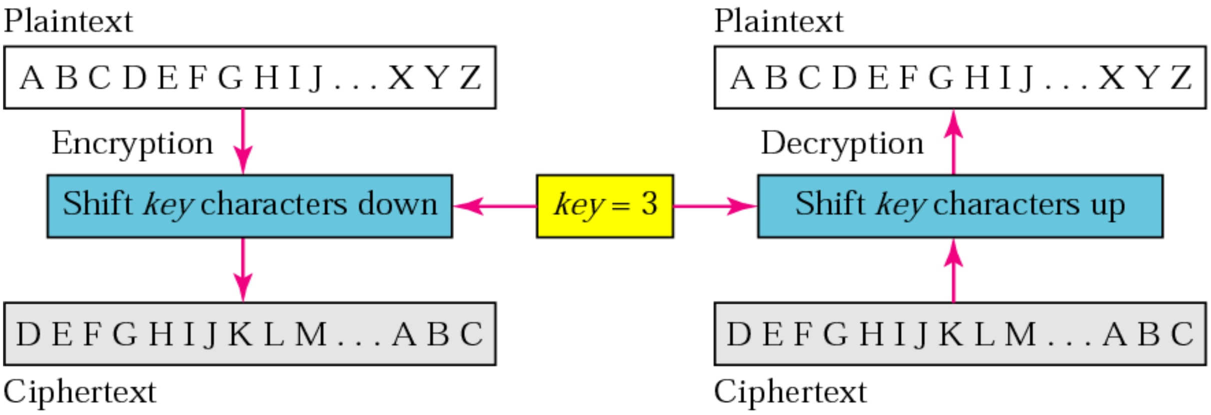
Monoalphabetic Ciphers

In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext

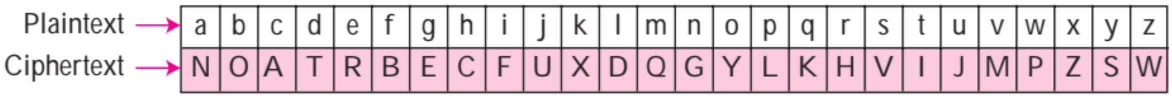
The simplest monoalphabetic cipher is the additive cipher or shift cipher or Caesar cipher

Example 1

eg for key =3 . Every letter is replaced with third letter


Plaintext
A B C D E F G H I J . . . X Y Z
Encryption
Shift key characters down
key = 3
D E F G H I J K L M . . . A B C
Ciphertext
Plaintext
A B C D E F G H I J . . . X Y Z
Decryption
Shift key characters up
D E F G H I J K L M . . . A B C
Ciphertext

- Disadvantage of monoalphabetic cipher is it can be easily decrypted by using all keys from 1 to 25. (this technique is called brute-force attacks)
- Solution is **keyless** monoalphabetic cipher
- It uses some predetermined substitution which is not having fixed distance (key).



Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Polyalphabetic Ciphers

In polyalphabetic substitution, each occurrence of a character has a different substitute for every occurence

- For example, “a” could be enciphered as “d” in the first occurrence in the text, but as “n” in next occurrence
- So frequency statistic can’t be used to break the cipher
- In this many keys are used,
- Eg plain text is P = P1 P2 P3 cipher text is C = C1C2C3 & keys are k= (k1, P1, P2, ..)

Transposition Ciphers

A transposition cipher does not substitute one symbol by another, but it changes
the location of the symbols.

- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext. A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext.
- In other words, a transposition cipher reorders (transposes) the symbols

bit-oriented ciphers.

The traditional symmetric-key ciphers that we have studied so far are character-oriented ciphers.

- With the advent of the computer, we need bit-oriented ciphers. because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
- It is convenient to convert these types of data into a stream of bits, & to encrypt the stream.
- A modern cipher can be either a block cipher or a stream cipher.

Advantages of Symmetric Key Cryptography

- Much faster (less computations) than asymmetric systems.
- Hard to break if using a large key size.

Disadvantages of Symmetric Key Cryptography

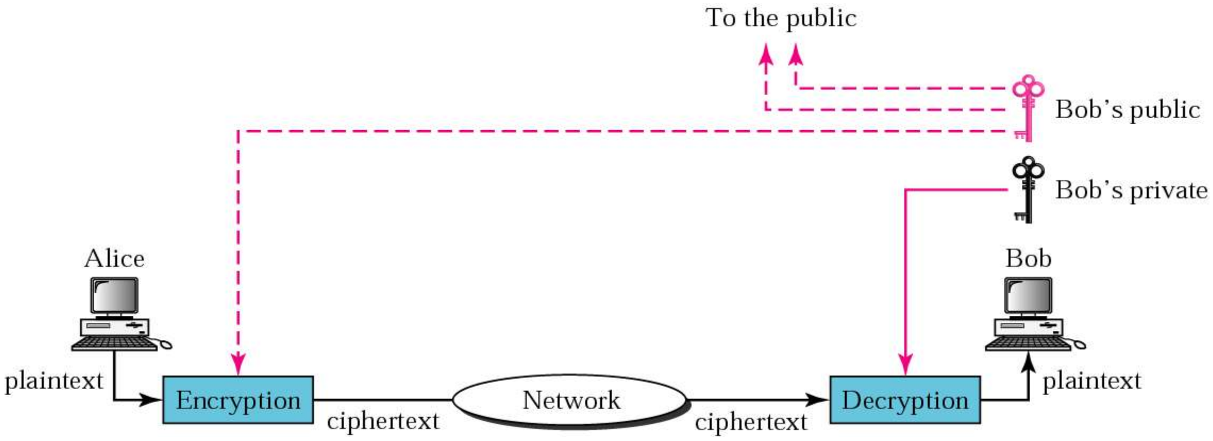
• Requires a secure mechanism to share the secret key.
• Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management difficult.
• Provides confidentiality but not authenticity or nonrepudiation.

Examples of Symmetric Key Cryptography

RC4, AES, DES, 3DES, and QUAD.

Asymmetric-key Cryptography

- Also called as public key cryptography
- It uses two keys : public & private key
- Every party has two keys. Public key is shared , private key is secret. Sender uses receiver's public key to encrypt . Receiver uses its private key for decryption of the ciphertext. Ciphertext can't be decrypted by public key.



Each entity in the community should create its own private and public keys.
Alice needs *n* public keys to communicate with *n* entities in the community, one public key for each entity. In other words, Alice needs a ring of public keys. Thus each entity will have one private key (its own) & n public keys (shared by others).

Examples of asymmetric encryption include:

- Rivest Shamir Adleman (RSA)
- the Digital Signature Standard (DSS), which incorporates the Digital Signature Algorithm (DSA)
- Elliptical Curve Cryptography (ECC)
- the Diffie-Hellman exchange method
- TLS/SSL protocol

Which one is preferred ? Symmetric or Symmetric

- the advent of asymmetric key (public-key) cryptography does not eliminate the need for symmetric-key (secret key) cryptography.
- One complements the other.
- The reason is that asymmetric-key, is much slower than symmetric key. For encipherment of large messages, symmetric-key cryptography is still needed. On the other hand, the speed of symmetric-key cryptography does not eliminate the need for asymmetric-key cryptography.
- Asymmetric-key cryptography is still needed for authentication, digital signatures, and secret-key exchanges.
- This means that, to be able to use all services of security today, we need both symmetric-key and asymmetric-key cryptography.
- One complements the other.

Compare Symmetric Encryption with Asymmetric Encryption

Symmetric Encryption	**Asymmetric Encryption**
A single key is used to encrypt and decrypt data. Called as secret key	A key pair is used for encryption and decryption. These keys are known as public key and private key.
based on substitution and permutation of symbols (characters or bits) . the plaintext and ciphertext are thought of as a combination of symbols	based on applying mathematical functions to numbers. the plaintext and ciphertext are numbers
simpler method	more complex process.
So faster and requires less computational power.	So Slower and requires more computational power.
For n people, $n(n - 1)/2$ shared secrets are needed	*For n* personal secrets are needed
Smaller key lengths (e.g., 128-256-bit)	longer keys (e.g. 1024-4096-bit)
Ideal for applications where a large amount of data needs to be encrypted.	Ideal for applications where a small amount of data is used by ensuring authentication.
Algorithms include . RC4, AES, DES, 3DES, and QUAD.	algorithms include RSA, Diffie-Hellman, ECC, El Gamal, and DSA.
Symmetric encryption is primarily used for confidentiality.	used for confidentiality.,authentication, and non-repudiation.

Network layer security

Why We need security at the network layer

for three reasons.

1. not all client/server programs are protected at the application layer.
2. not all client/server programs at the application layer use the services of TCP (which can use SSL or TLS for security); some programs use the service of UDP (which does not have security).
3. many applications, such as routing protocols, directly use the service of IP; they need security services at the IP layer.

IP Security (IPSec)

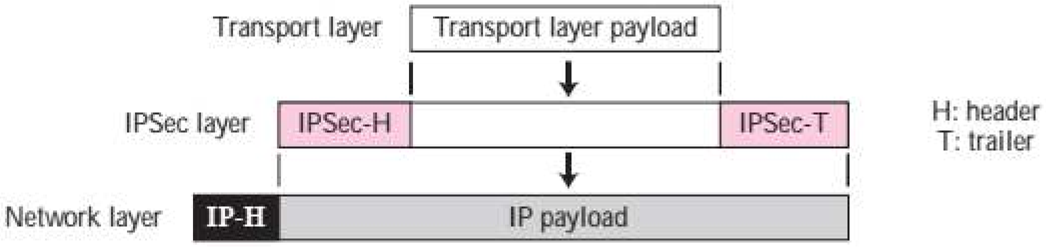
is a collection of protocols , provide security for a packet at the network level.
IPSec helps create authenticated and confidential packets for the IP layer.

Two Modes

IPSec operates in one of two different modes: transport mode or tunnel mode.

Transport Mode

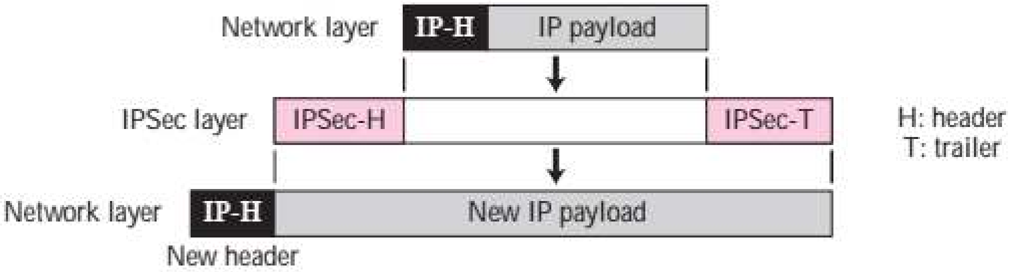
In transport mode, IPSec protects what is sent from the transport layer to the network layer.
i.e. IPSec in transport mode does not protect the IP header;
it only protects the information coming from the transport layer.



Transport mode is normally used when we need host-to-host (end-to-end) protection of data

Tunnel Mode

In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header, as shown

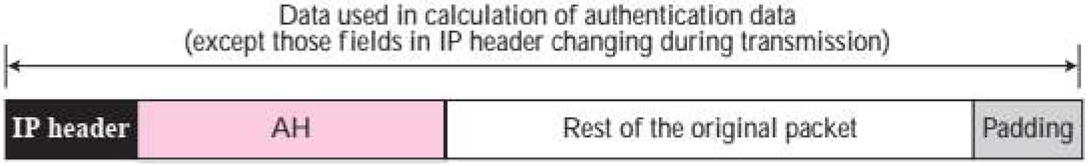


Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host,. The entire original packet is protected from intrusion between the sender and the receiver, as if the whole packet goes through an imaginary tunnel.

IPSec defines two protocols
the Authentication Header (AH) Protocol (for authentication) and the Encapsulating Security Payload (ESP) Protocol (for encryption) for packets at the IP level.

Authentication Header (AH)

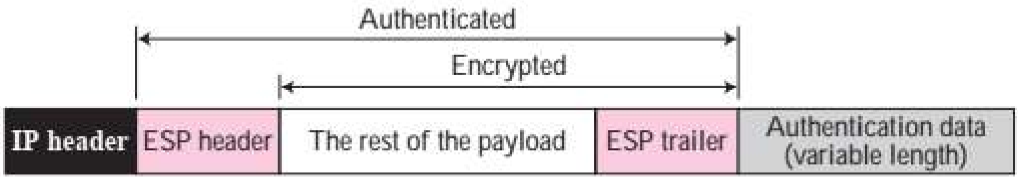
is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
The AH protocol does not provide confidentiality (privacy).
The protocol uses a hash function and a symmetric (secret) key to create a message digest; the digest is inserted in the authentication header.
The AH is then placed in the appropriate location, based on the mode (transport or tunnel).


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding

Encapsulating Security Payload (ESP)

The AH protocol only source authentication and data integrity but does not provide confidentiality. IPSec later defined an alternative protocol, Encapsulating Security Payload (ESP), that provides source authentication, integrity, and confidentiality.

ESP adds both , a header and trailer. ESP's authentication data are added at the end of the packet, which makes its calculation easier.



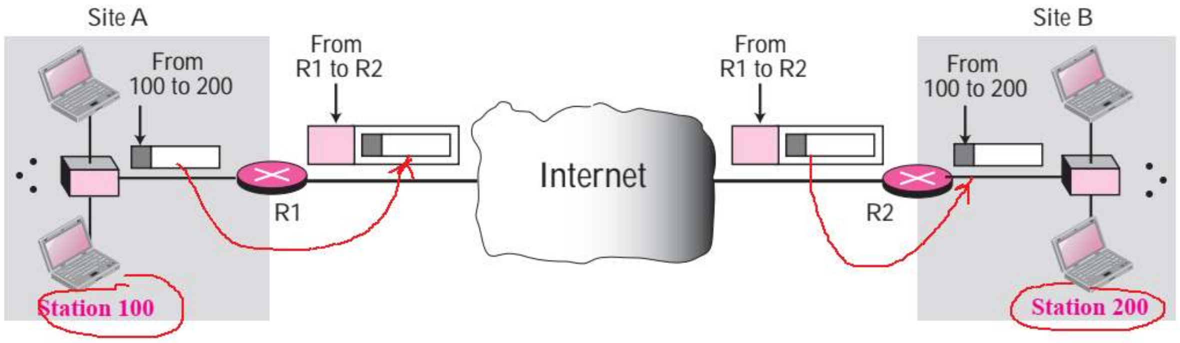
applications of IPsec

is in virtual private networks.

A virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the public Internet for communication, but require privacy in their intra-organization communication.

VPN is a network that is private but virtual.

It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs but uses public WAN i.e. internet;

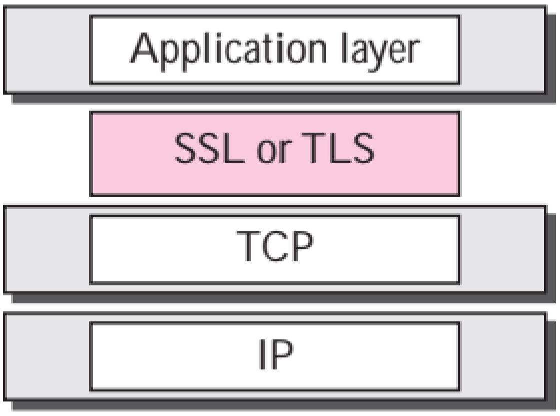


TRANSPORT LAYER SECURITY

Two protocols for providing security at the transport layer:

the Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol.

TLS is very similar to SSL. Figure shows the position of SSL and TLS in the Internet model



TLS or SSL provide CIA i.e. data confidentiality, and data integrity, & server and client authentication.

SSL was deprecated(stopped) in 2015

Transport Layer Security (TLS) is upgraded version of SSL. TLS is a more secure and efficient protocol

SSL Services
SSL provides several services on data received from the application layer.

❑ Fragmentation. First, SSL divides the data into blocks of 214 bytes or less.

❑ Compression. Each fragment of data is compressed using one of the lossless compression methods negotiated between the client and server. This service is optional.

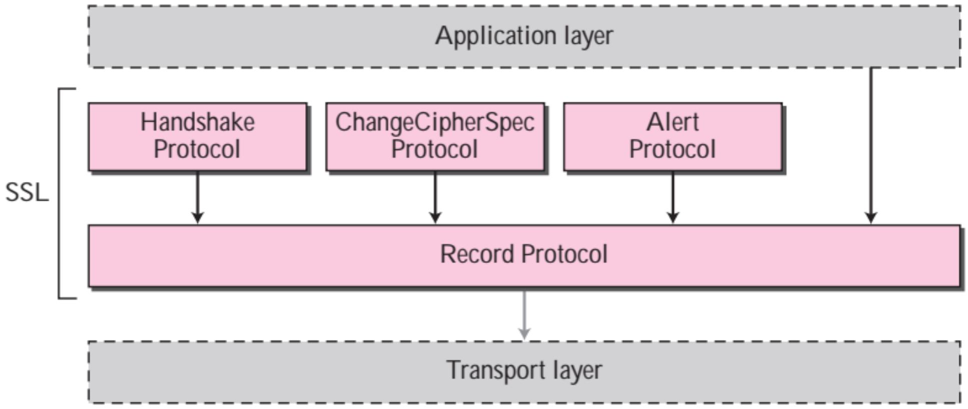
❑ Message Integrity. To preserve the integrity of data, SSL uses a keyed-hash function to create a MAC (see Chapter 29).

❑ Confidentiality. To provide confidentiality, the original data and the MAC are encrypted using symmetric-key cryptography.

❑ Framing. A header is added to the encrypted payload. The payload is then passed to a reliable transport layer protocol

For authenticated and confidential message, SSL uses Key Exchange Algorithms & Encryption/Decryption Algorithms
To provide message integrity (message authentication) SSL uses hash algorithms

The combination of key exchange, hash, and encryption algorithms defines a cipher suite for each SSL session.
To provide all above services SSL defines four protocols in two layers, as shown



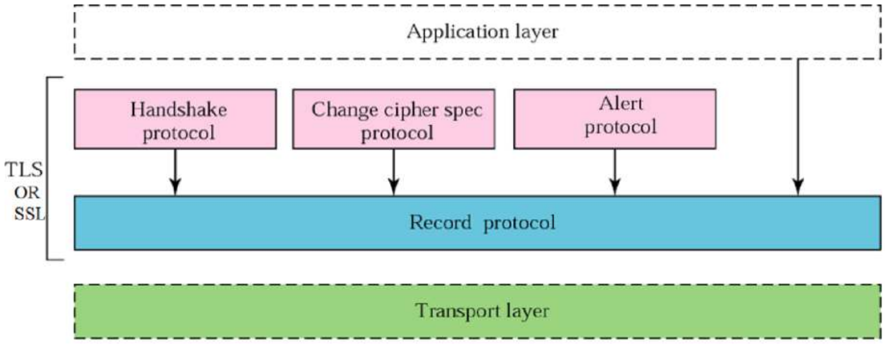
SSL provides security services on data received from the application layer.

- Message Integrity (message Authentication)
- Confidentiality of data (by encryption)
- Authentication (of web server by checking its SSL certificate)

To provide these security , SSL uses:

Key Exchange Algorithms,
the client and the server each need a set of cryptographic secrets. However, to create these secrets, one pre-master secret must be established between the two parties. SSL defines several key-exchange methods to establish this pre-master secret.
Encryption/Decryption Algorithms
The client and server also need to agree to a set of encryption and decryption algorithms.
Hash Algorithms
SSL uses hash algorithms to provide message integrity (message authentication).
Cipher Suite:
The combination of key exchange, hash, and encryption algorithms defines a cipher suite for each SSL session
SSL accomplishes its tasks , by using four protocols in two layers,

SSL Protocol Stack:



Summary of four protocols :

The Record Protocol is the carrier. It carries messages from three other protocols as well as the data coming from the application layer. Messages from the Record Protocol is sent to the transport layer, normally TCP.

The Handshake Protocol provides security parameters for the Record Protocol. It establishes a cipher suite. It also authenticates the server to the client and the client to the server (if needed.)

The ChangeCipherSpec Protocol is used for signalling the readiness of cryptographic secrets.

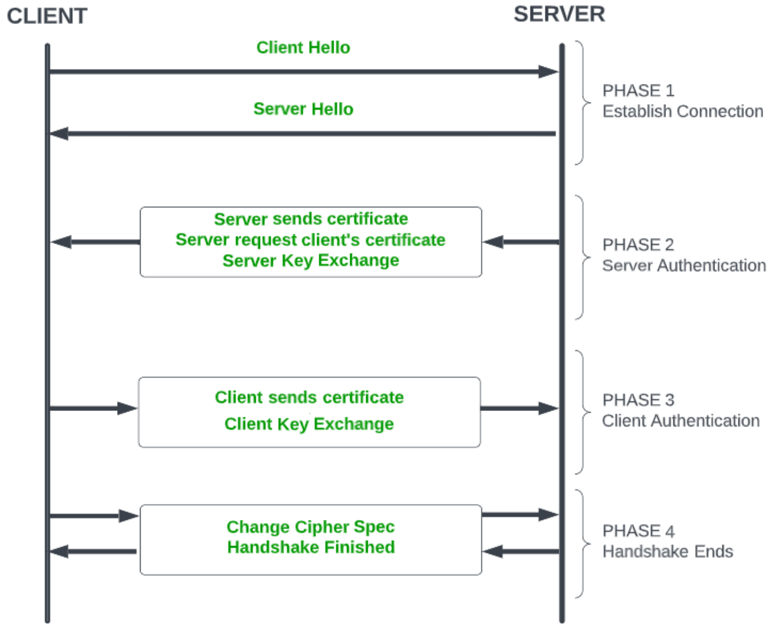
The Alert Protocol is used to report abnormal conditions.

Details of four protocols

Handshake Protocol:

It is used to establish sessions. It allows the client and server to authenticate each other by sending a series of messages to each other. It uses four phases.

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



SSL HANDSHAKE PROTOCOL

SSL Record Protocol:

provides two services to SSL connection.

- Confidentiality

- Message Integrity

In this , data is divided into fragments. Each fragment is compressed (optional)and then encrypted MAC (Message Authentication Code) is generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) ,it is appended to each fragment. After that a SSL header is appended to it.

Change-cipher Protocol:

The “Change Cipher Spec” message lets the other party know that, it has generated the session key and is going to switch to encrypted communication.

Alert Protocol:

This protocol is used to send SSL-related alerts by server to client or vice versa.

Warning (level = 1):

This Alert does not close the connection between sender and receiver. Eg.

Bad certificate: When the received certificate is corrupt.
No certificate: When certificate is not available.
Certificate expired: When a certificate has expired.
Certificate unknown: When some other unspecified issue arose in processing the certificate.
Close notify: It notifies that the sender will no longer send any messages in the connection.

Fatal Error (level = 2):

This Alert terminates the connection between sender and receiver.

Application of SSL

Application-layer protocols, such as HTTP become HTTPS when it uses TLS or SSL in TCP , to encapsulate their data in SSL packets. Then URL can be https://... instead of http://...

What is Hypertext Transfer Protocol Secure (HTTPS)?

HTTPS is the secure version of HTTP.

Hypertext Transfer Protocol Secure (HTTPS) is a protocol that secures communication and data transfer between a user's web browser and a website. The protocol protects users against eavesdroppers and man-in-the-middle (MitM) attacks. It also protects legitimate domains from domain name system (DNS) spoofing attacks.

As noted in the previous section, HTTPS works over SSL/TLS with public key encryption to distribute a shared symmetric key for data encryption and authentication. It uses port 443 by default, whereas HTTP uses port 80. All secure transfers require port 443, although the same port supports HTTP connections as well.

Before a data transfer starts in HTTPS, the browser and the server decide on the connection parameters by performing an SSL/TLS handshake. The handshake is also important to establish a secure connection.

Here's how the entire process works:

1. The client browser and the web server exchange "hello" messages.
2. Both parties communicate their encryption standards with each other.
3. The server shares its certificate with the browser.
4. The client verifies the certificate's validity.
5. The client uses the public key to generate a pre-master secret key.
6. This secret key is encrypted using the public key and shared with the server.
7. The client and server compute the symmetric key based on the value of the secret key.
8. Both sides confirm that they have computed the secret key.
9. Data transmission uses symmetric encryption.

(i.e. operation of TLS)
Even if HTTPS is more secure than HTTP, it may be vulnerable to the following malicious activities:
Cryptanalysis or protocol weakness.: Threat actors may use cryptanalysis or exploit potential weaknesses to compromise the HTTPS connection.
Attacks on the client computer: Attackers may install a malicious root certificate into the client computer or browser trust store, thereby compromising the HTTPS connection.
Manipulating a certificate authority: Attackers can manipulate or compromise a certificate authority to obtain a rogue certificate that is mistakenly trusted by major browsers.

Application of HTTPS

in securing websites that handle or transfer sensitive data, eg online banking services, email providers, online retailers, healthcare providers and more.
In other words , any website that requires login credentials or involves financial transactions should use HTTPS

Compare HTTP with HTTPS

HTTP	**HTTPS**
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It is written in the address bar as http://.	It is written in the address bar as https://.
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
It is an application layer protocol.	It is an application layer which uses TLS /SSL at transport layer.
It does not use SSL.	It uses SSL that provides the encryption of the data.
Google does not give the preference to the HTTP websites.	Google gives preferences to the HTTPS as HTTPS websites are secure websites.
The page loading speed is fast.	The page loading speed is slow as compared to HTTP because of the additional feature that it supports, i.e., security.

APPLICATION LAYER SECURITY

eg providing security for application layer progrma such as email
two protocols providing security services for e-mails: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME)

(S/MIME)

Secure/Multipurpose Internet Mail Extension
It is provides security for electronic mail . The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol

MIME

It is a protocol that allows non-ASCII data to be sent through e-mail.eg. various language scripts Marathi ,Chinese, and Japanese etc & to send binary files or video or audio data.
S/MIME (Secure/Multipurpose internet Mail Extensions) is a protocol for sending digitally signed and encrypted emails.
Another protocol for similar function is PGP .
S/MIME works based on asymmetric encryption. This means that there are two keys involved to encrypt and decrypt an email.
When an email is sent, the sender encrypts the email using the recipient's public key and the recipient decrypts the email using the private key. S/MIME also attaches a digital signature to an email. This ensures that the sender is authorized to send emails from a certain domain.

S/MIME provides the following cryptographic security services for electronic messaging applications:

- Authentication (verifying the identity of a user)
- Message integrity (a message has not been tampered with or altered)
- Non-repudiation of origin (using digital signatures) (Assurance that the sender can’t deny ownership of message)
- Privacy (safeguarding of user identity)
- Data security (safeguarding of data using encryption)

An S/MIME certificate is installed on the email clients of both the recipient and the sender S/MIME certificates encrypt emails using asymmetric encryption. When you send an secured email to your friend, you can use a public key to encrypt your email. This public key can be accessed by anyone However, no one except your friend can access the contents of the email without the private key. Only the intended recipient, your friend, can access the private key and decrypt and access the email. This is how a S/MIME certificate works.
To sign and encrypt your email, you will need an email signing certificate – which you can purchase from a certificate authority. You can use this certificate to digitally sign your email. Once you purchase this certificate, it will get attached to your email automatically.

the private key is used to generate the digital signature, the public key is used for authentication. The public and private keys are the two keys with which the digital signature is associated. The digital signature shows that the email sent is unaltered and not accessible to anyone else other than the intended recipient.

Features and Benefits of S/MIME Certificates

- S/MIME certificates make sure the emails you send are accessible only by the recipient and not by any other third party.
- These certificates use asymmetric encryption.
- Public and private keys will be used to encrypt and decrypt emails so that you can be assured that the emails you send cannot be accessed by anyone else other than the recipient.
- S/MIME certificates secure emails and make sure hackers do not access the contents of the email or make changes to it.
- Digital signatures, as well as encryption, are both offered.

- While asymmetric encryption lets you keep your data confidential, digital signatures offer authentication and message integrity.
- S/MIME certificates are installed on email clients.

Uses of S/MIME

- S/MIME can be used to
- Make sure the email you sent has not been altered by any third party.
- Create digital signatures to sign your emails.
- Encrypt all your emails.
- Verify the email client you use.

Document signing and client authentication are two of the additional features S/MIME certificates come with.

- Document Signing

Similar to email signing, you can sign documents using a digital signature. You can use your private key to sign your documents digitally. Using the unique digital signature, the recipient will be able to verify that the document was signed by you with your digital signature and that it has not been tampered.

If someone happens to tamper with the document you sent, the recipient will receive a warning message.

- Client Authentication

This feature helps users to secure apps, servers, and the network using certificate-based authentication. This feature will let you grant access to servers and apps to only authorized users. Only the users who have a client certificate installed will be able to access important data and the servers. Securing servers with passwords may not be a great option as passwords can be cracked.

Special settings have to be done in email clients to install S/MIME certificates (which we need to purchase) in email clients such as gmail , outlook etc.

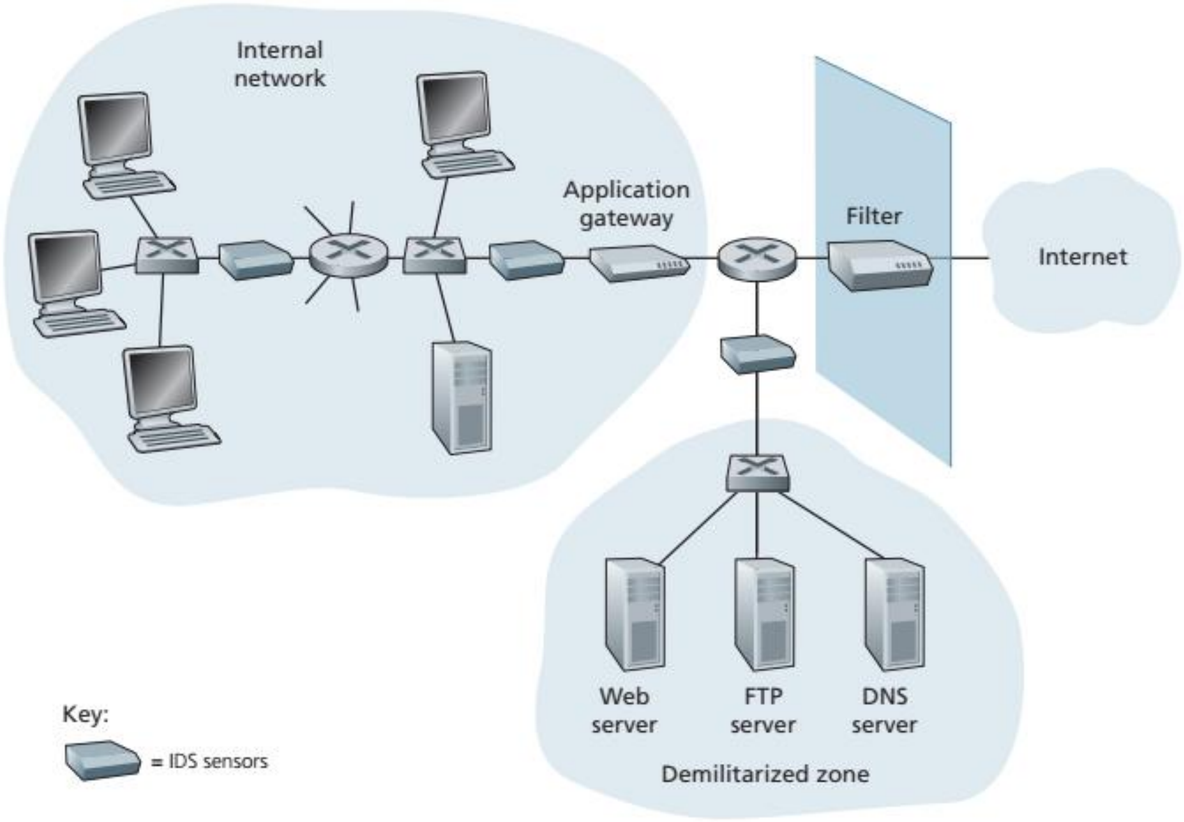
An Intrusion Detection System (IDS)

is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

Any malicious activity or violation is reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms (false alarms means IDS gives alarm for correct activity).

a device that not only examines the headers of all packets passing through it (like a packet filter), but also performs deep packet inspection (unlike a packet filter). When such a device observes a suspicious packet, or a suspicious series of packets, it prevents those packets from entering the organizational network. Or, because the activity is only deemed as suspicious, the device could let the packets pass, but send alerts to a network administrator, who can then take a closer look at the traffic and take appropriate actions.

A device that filters out suspicious traffic is called an intrusion prevention system (IPS)
An IDS can be used to detect a wide range of attacks, including network mapping (emanating, for example, from nmap), port scans, TCP stack scans, DoS bandwidth-flooding attacks, worms and viruses, OS vulnerability attacks, and application vulnerability attacks.
Examples of IDS systems : Cisco, Check Point & Snort (free)



Classification of Intrusion Detection System:
IDS are classified into 5 types:

Network Intrusion Detection System (NIDS):
are set up at a planned point within the network to examine traffic from all devices on the network. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

Host Intrusion Detection System (HIDS):
run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.

Protocol-based Intrusion Detection System (PIDS):
comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream

Application Protocol-based Intrusion Detection System (APIDS):
is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System :
is made by the combination of two or more approaches of the intrusion detection system Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.

Detection Method of IDS:

Signature-based Method:
Signature-based IDS detects the attacks on the basis of the specific patterns in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

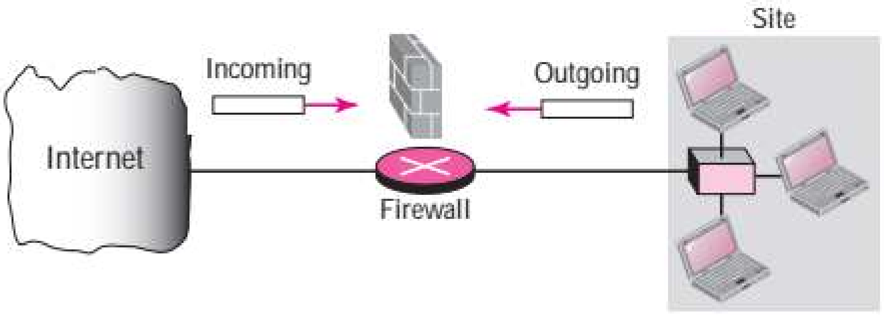
it is quite difficult to detect the new malware attacks as their pattern (signature) is not known. Also every packet must be compared with large collection of signatures, so the IDS can become overloaded and can make network slow.

Anomaly-based Method:
An anomaly-based IDS creates a traffic profile as it observes traffic in normal operation. It then looks for packet streams that are statistically unusual, for example, an large percentage of ICMP packets or a sudden exponential growth in port scans and ping requests.

Most IDS deployments are mainly signature-based.

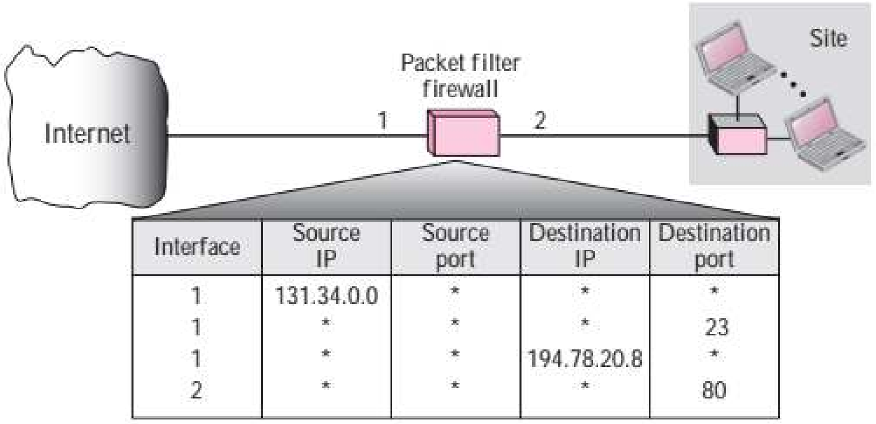
firewall

is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
Firewalls have been a first line of defense in network security.
They establish a barrier between secured and controlled internal networks (of an organization) that can be trusted and untrusted outside networks, such as the Internet.
A firewall can be hardware, software, or both.



Types of firewalls

Packet-Filter Firewall (also called stateless)
A stateless firewall inspects traffic on a packet-by-packet basis..
It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).
A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). Figure shows an example of a filtering table for this kind of a firewall.



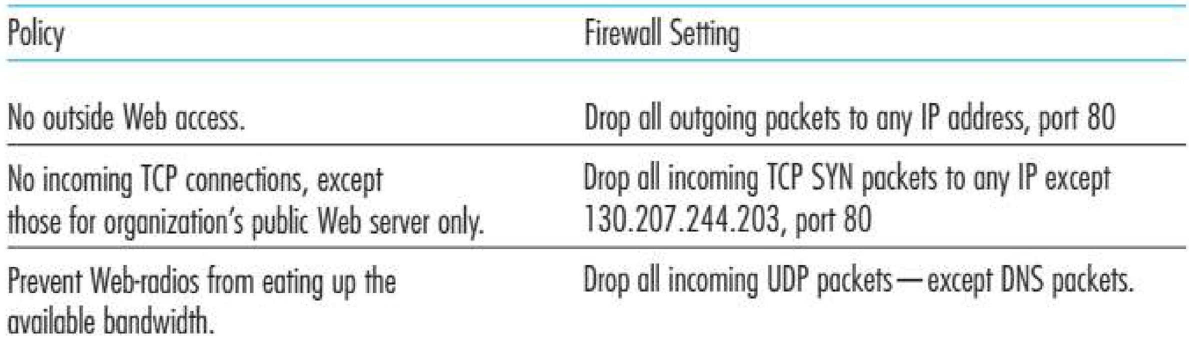
Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

* Means **any** host IP or process port address

According to the figure, the following packets are filtered(blocked):
1. Incoming packets from network 131.34.0.0. are blocked (security precaution).

2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets destined for internal host 194.78.20.8. are blocked. The organization wants this host for internal use only.
4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

Another example

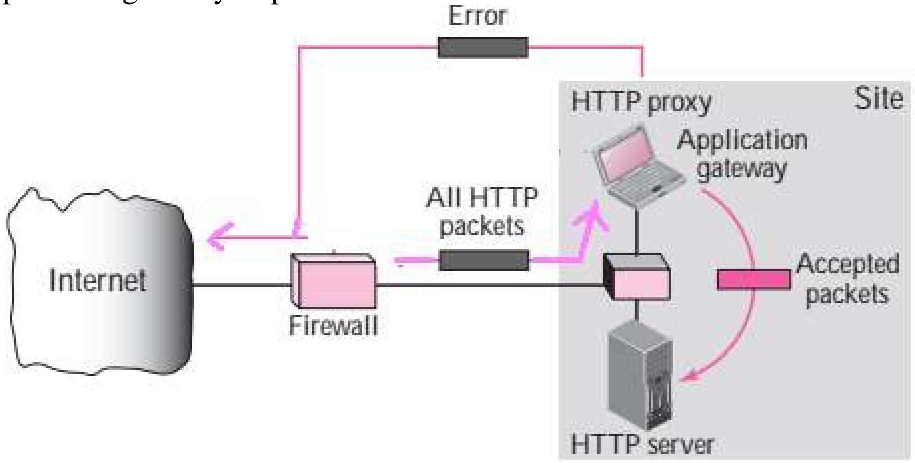


Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.

Since a packet-filter firewall checks only for IP addresses & port addresses , it works at the network & transport layer.

Proxy Firewall (application gateway)
The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCP/UDP). But, sometimes we need to filter a message based on the information available in the message itself (at the application layer).
As an example, an organization wants to implement the following policies regarding its Web pages: only those Internet users who have previously had business with the company can have access; access to other users must be blocked.
In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP) one from legitimate users & other from other users. So Testing must be done at the application level (using URLs).

When the user client process sends a message, the application receives the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user. In this way, the requests of the external users are filtered based on the contents at the application layer. Figure shows an application gateway implementation for HTTP



Stateful firewalls

Packet-Filter Firewall (also called stateless) inspects traffic on a packet-by-packet basis with no relation between them.

But Stateful firewalls in are designed to track details of all packets of a session from its beginning to its end. by tracking all ongoing TCP connections.

This is possible because the firewall can observe the beginning of a new connection by observing a three-way handshake (SYN, SYNACK, and ACK); and it can observe the end of a connection when it sees a FIN packet for the connection. These firewalls identify and block packets that don't make sense in context (such as a SYN/ACK packet sent without a corresponding SYN).

Different types of firewalls is based on how they are implemented.

1. Hardware Firewalls: These firewalls are implemented as a physical device kept in an organization's server room or data center.
2. Software Firewalls: Software firewalls are implemented as code on a computer.
3. Cloud Firewalls**:** Organizations are moving critical data and resources to the cloud, and they use cloud-native firewalls.

Comparison of IDS with Firewalls:

Firewall	IDS
A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.	An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network.
A firewall can block an unauthorized access to network (E.g. A watchman standing at gate can block a thief)	An IDS can only report an intrusion; it cannot block it (E.g. A CCTV camera which can alert about a thief but cannot stop it)
A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems
Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)	IDS are very difficult to be spotted in a network (especially stealth mode of IDS).