Network Security and Applications

Syllabus

At the end of this unit, you should be able to understand and comprehend the following syllabus topics :

- Network security basics
- TCP/IP vulnerabilities (Layer wise)
  - Packet Sniffing
  - ARP spoofing
  - Port scanning
  - IP spoofing
  - Denial of Service (DoS)
    - Classic DoS attacks
      - ICMP flood
      - SYN flood
      - UDP flood
    - Distributed Denial of Service (DDoS)
    - Defences against Denial of Service Attacks
- Internet Security Protocols
  - SSL
  - IPSEC
- Secure Email
  - PGP
  - S/MIME
- Firewalls
- Intrusion Detection Systems (IDS)
  - Host based
  - Network based

5.1 Network Security Basics

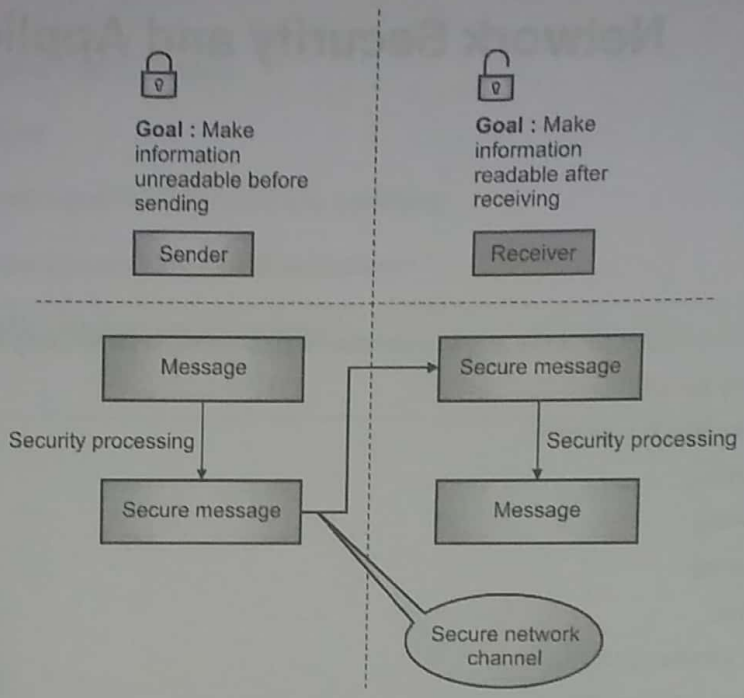


Fig. 5.1.1 : Transmitting a Message Securely over a Network

Network channel and protocols play a crucial role in information security. The information is not very useful when just stored locally on a computer. It must move to different devices in its lifetime to be useful. The way information is transferred from one device to another depends on several networking parameters. **Look at the simplistic diagram here.**

The network channel is the core mechanism to ensure that the message is transferred securely. If there are network vulnerabilities, as you will learn in this chapter, the information cannot be reliably sent.

You might have a question – if you are already securing the message before sending, why do you need a secure channel as well? The answer is that if the message can be intercepted (picked up) from the channel, the secure message can be attacked such that to make it insecure. Consider an example. You seal your letter in an envelope. But, if the person carrying the envelope is not reliable enough, would you still send the envelope with her? Not really, right? Same way, the network medium (or channel) should be secure enough to transfer the message to the destination reliably.

5.2 TCP/IP Vulnerabilities (Layer Wise)

Recall from our previous discussion on OSI model that you can conceptually view the networking as seven layers that inter-operate. Each of these layers have their respective vulnerabilities and requires appropriate protection mechanism. Some of these attacks and vulnerabilities are highlighted in the Table 5.2.1.

Table 5.2.1 : TCP/IP Vulnerabilities (Layer Wise)

Layer Number	Layer Name	Attacks / Vulnerabilities
7	Application	Layer 7 DoS attacks (HTTP flood) SQL Injection Cross-site scripting DNS Spoofing
6	Presentation	Malicious SSL requests Inspecting SSL encryption packets
5	Session	Session Hijacking SSH downgrade Session sniffing
4	Transport	SYN Flood UDP Flood Port Scanning Other DoS attacks
3	Network	IP Spoofing Source Address Spoofing ICMP Flood Packet Sniffing Teardrop attack Other DoS attacks
2	Data Link	ARP Flooding ARP Spoofing MAC flooding DHCP Spoofing
1	Physical	Wire-cuts Disrupting the signal Any other media transmission disturbance

Let's learn a few of these in detail.

5.2.1 Packet Sniffing

Definition : *Packet Sniffing is the act of intercepting (capturing) of network traffic and logging it for further analysis.*

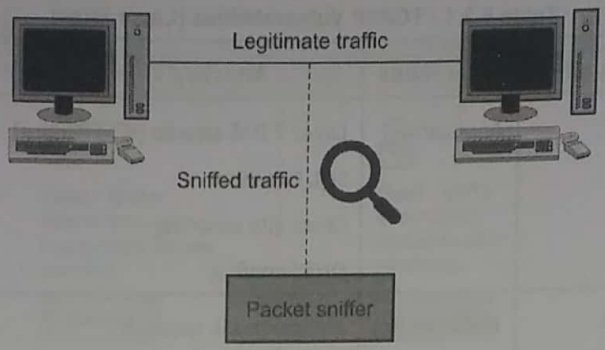


Fig. 5.2.1 : Packet Sniffing

Packet sniffing is carried out using either software programs or hardware devices. These are called packet analysers or just packet sniffers. Wireshark is one of the most widely used Packet Sniffing program.

Common Attacks

Some of the common attacks carried out using packet sniffing technique are as following:

- Capturing sensitive information.
- Analyse communication patterns.
- Learn about the network infrastructure.
- Exploit network vulnerabilities.

Protection

You cannot, to a great extent, avoid network sniffing attempts since it is external to the network and mostly beyond your control. For example, how do you protect someone with Wi-Fi analysing device to capture your Wi-Fi packets? However, some of the common protection mechanisms to reduce the impact from sniffing are as follows:

- **Encryption :** Use TLS, VPN tunnels or application level encryption wherever possible to avoid sending and receiving data in plaintext.
- **Use secure protocols :** Discourage the use of protocols such as HTTP, FTP, TELNET, RPC and prefer using secure protocols such as HTTPS, FTPS, SSH, etc.
- **Isolate and Segment Networks :** Design your network in such a way that the sensitive systems are adequately segmented from rest of the network.

5.2.2 ARP Spoofing

✍ ***Definition :*** *ARP spoofing is a technique by which the attacker associates her MAC address with the IP address of a legitimate device.*

It is also called ARP cache poisoning or ARP poison routing.

During network communication, a device, when wishes to interact with another target device, requires mapping the IP address of the target to the MAC address of the target. In ARP spoofing, the attacker maliciously provides MAC address of her device so that the wrong mapping of target IP address to target MAC is created.

ARP Table (Expected)	
Target IP Address	Target MAC Address
10.12.92.56	AA:00:FE:12:E4:56
ARP Table (Spoofed)	
Target IP Address	Target MAC Address
10.12.92.56	BB:11:FE:12:F7:84

Once the attacker's MAC address is linked to the target IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol (ARP).

Common Attacks

Some of the common attacks carried out using ARP spoofing technique are as following:

- **Denial-of-service attacks :** DoS attacks often use ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.
- **Session hijacking :** Session hijacking attacks can use ARP spoofing to steal session IDs and thus granting attackers access to private or sensitive data.
- **Man-in-the-middle attacks :** MITM attacks can use ARP spoofing to intercept and modify traffic between victims and carry out further attacks.

Protection

Some of the protection mechanisms for ARP spoofing are as follows:

- **Static ARP entries :** You could create static ARP entries so that any MAC entries are approved for use.
- **ARP spoofing detection software :** You could use software to detect ARP spoofing attacks and prevent spoofed MAC entries.

5.2.3 Port Scanning

Q. What is Authentication Header (AH)? How does it protect against replay attacks? MU - May 19, 5 Marks

In computer networking terminology,

✍ ***Definition :*** *A port is an endpoint of communication that serves the service requests.*

Each service on the OS requires a port to communicate with any other service or device on the network. Hence, indirectly, if you can find out which ports are open for connection on a particular system, it is as good as knowing which services are running on the system. Once you know which services are running on the system, you can further craft attacks on the system exploiting vulnerabilities in those services.

Hence,

✍ ***Definition :*** *Port scanning is a technique using which you can identify the state of ports and indirectly know about the running services that could be exploited.*

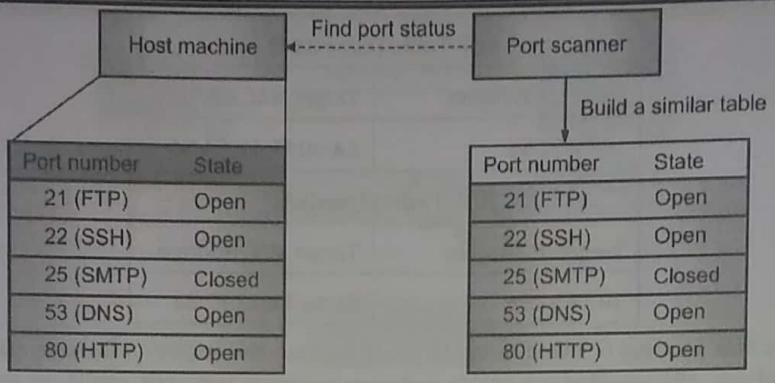


Fig. 5.2.2 : Port Scanning

5.2.3(A) Port Scanning Techniques

There are several port scanning techniques. The following techniques are commonly used.

1. Connect Scan
2. SYN Scan
3. FIN Scan
4. NULL Scan

Let's learn about them.

1. **Connect Scan :** This is the simplest of all the port scanning techniques. The port scanner utilizes the OS network functions to identify any open ports. It tries to establish the connection to all the ports serially one after the another. The ports that are open would complete the 3-way TCP handshake and ports which are not open would not.
2. **SYN Scan :** In this technique, the port scanner sends the SYN packet to the ports it desires to test openness for. Ports that are open respond with SYN-ACK packet and ports that are not open respond with RST packet.
3. **FIN Scan :** In this technique, the port scanner sends the FIN packet to the ports it desires to test openness for. Ports that are open ignore the packet and ports that are not open respond with RST packet.
4. **NULL Scan :** In this technique, the port scanner sends a TCP packet with no TCP flags set. Ports that are open ignore the packet and ports that are not open respond with RST packet.

Protection

1. **Close unnecessary ports :** Close unnecessary ports on the system. Any service that you are not using and is installed and running could be vulnerable to attacks.
2. **Firewalls :** Firewalls can stop scanning or connection establishment from any non-approved devices. They can filter various ports and avoid providing the state of the ports to any unauthorized port scanners.
3. **Intrusion Detection Systems :** Intrusion Detection Systems can identify port scanning attempts and can raise notifications accordingly.

5.2.4 IP Spoofing

Q. Write in brief about - IP spoofing. MU - Dec. 15, 5 Marks

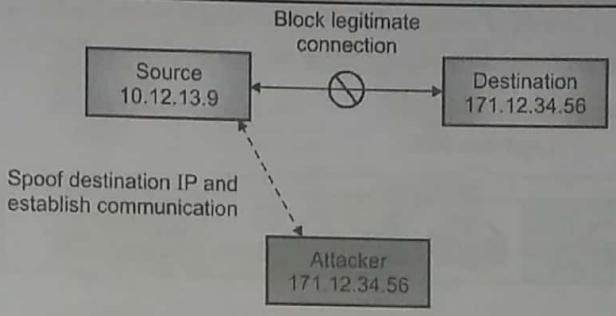


Fig. 5.2.3 : IP Spoofing

IP addresses are, in a way, identities of the systems that are communicating over a network.

✍ ***Definition :*** *IP Spoofing is a technique whereby an attacker impersonates (tries to steal the identity of) another machine by manipulating IP packets.*

The goal of the attacker is to get unauthorized access to communication by manipulating her IP address as the actual target IP address.

Common Attacks

Some of the common attacks carried out using IP spoofing technique are as following:

- Steal sensitive information by impersonating as the legitimate IP address.
- Bypass authentication in networks where machines are trusted by their IP addresses.
- Carry out of Denial of Service (DoS) attacks by manipulating that the traffic is coming from a legitimate source.

Protection

Some of the protection mechanisms for IP spoofing are as follows:

- Do not trust IP addresses for authentication. Use stronger form of authentication such as certificates.
- Use packet filtering to reject packets with private (internal) IP addresses.
- Monitor network using controls such as network monitoring tools, IDS, etc.

5.2.5 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Q. What is a Denial of service attack? What are the different ways in which an attacker can mount a DOS attack on a system? MU - Dec. 15, May 17, 10 Marks

Q. Write in brief about Denial of service attacks. MU - May 16, 5 Marks

Q. Explain briefly with example, How the following Denial of service attacks occurs. MU - Dec. 16, Dec. 17, 5 Marks

Q. Explain different types of Denial of Service attacks. MU - May 19, 10 Marks

Remember our discussion on availability – one of the CIA triads? DoS and DDoS are attacks on the availability triad.

✍ ***Definition :*** *Denial of Service (DoS) is an attack from a single source such that the resources are exhausted on the target beyond its serving capacity.*

✍ ***Definition :*** *Distributed Denial of Service (DDoS) is an attack from multiple sources such that the resources are exhausted on the target beyond its serving capacity.*

Let's understand these using quick examples.

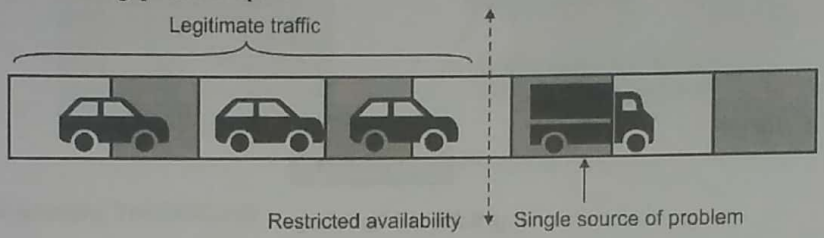


Fig. 5.2.4 : Analogy for DoS

In this example, a single source (truck – the attack) is blocking the road (resources) for all other vehicles (legitimate traffic) behind it.

The vehicles behind the truck have limited mobility and the road (resources) is exhausted (full capacity being consumed by the truck). This is what is DoS in the typical sense. A single source of attack exhausts all target resources such that the target is unavailable to serve the legitimate requests.

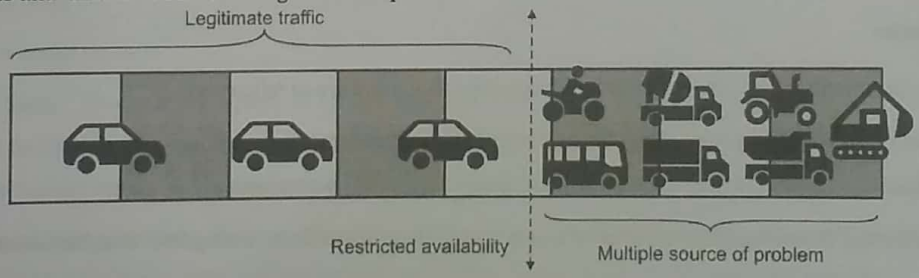


Fig. 5.2.5 : Analogy for DDoS

In the second example, there are multiple sources of jam (attacks) that have completely blocked the road (resources) despite that the road is wider this time when compared with the previous example. This is what is typically Distributed Denial of Service (DDoS).

Note : These days computer and other equipment have large capacities. So, it is not very effective to carry out DoS attack (the resources are sufficient to not cause any availability problem). Instead, attackers choose DDoS to attack the target such that to exhaust its capacity (such that even a larger capacity does not help to protect availability to a great extent). Hence, in our discussion, we can use the terms DoS and DDoS to actually mean just DDoS. Any DDoS attack is actually a DoS attack which is amplified (multiplied) using various sources of attack.

5.2.5(A) Botnet

Understanding botnet (robot networks) is crucial to understating DDoS attacks.

✍ ***Definition :*** *A botnet refers to a group of computers which have been infected by an attacker and is under her complete control.*

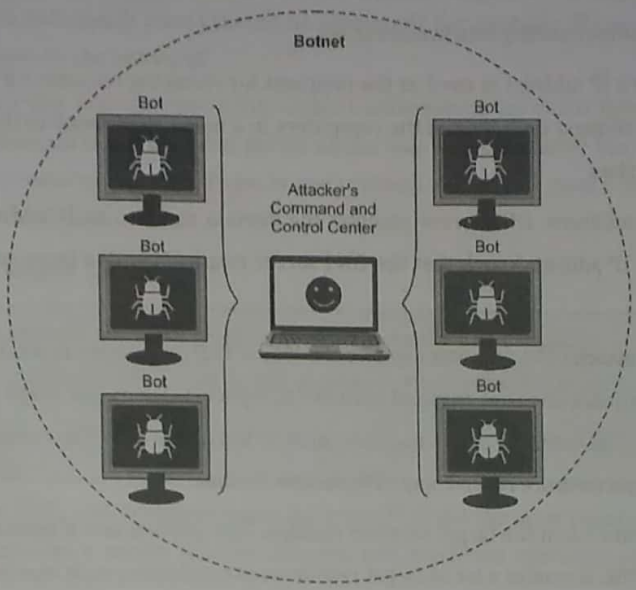


Fig. 5.2.6 : Botnet

These are the computers that the attacker uses to carry out DDoS attacks. All the computers in the group work together under the command of the attacker to hit a particular target and bring down its availability.

5.2.5(B) Types of DDoS Attacks

There are various types of DDoS attacks. Some of them are outlined here.

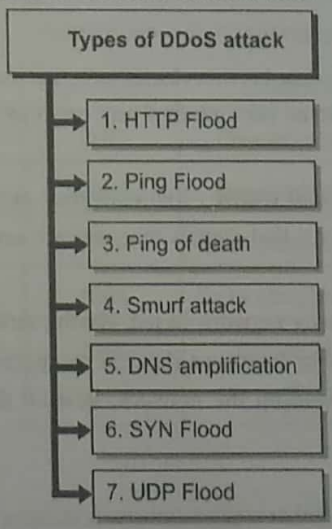


Fig. 5.2.7 : Types of DDoS Attacks

1. **HTTP flood :** HTTP flood is similar to you hitting refresh on your browser several times. It is just that it is done at a much large scale to crash the webserver and restrict the legitimate users from reaching the webserver.
2. **Ping (ICMP) Flood :** In this attack, the target machine is sent so many ping requests that it is overwhelmed and fails to respond.

3. **Ping of Death :** In this attack, the target machine is sent malformed packets such that the system is unable to understand and process them resulting into system crash.
4. **Smurf attack :** The victim's IP address is used as the recipient for receiving responses from broadcast communication. The attacker then crafts a request such that all the computers in a network respond to the victim's IP address such that it is overwhelmed and crashes.
5. **DNS Amplification :** As you know, DNS server resolves the domain name to an IP address. The attacker crafts a DNS request (with the target's IP address) such that the DNS server responds with a large amount of data and crashes the target.
6. **SYN Flood :** In SYN flood attacks, the attacker exploits the way a TCP connection is established. After sending the SYN packet to the target, the attacker does not respond with the ACK packet. The target keeps on waiting for the ACK until it runs out of the resources. The attacker sends multiple such SYN packets until the resources on the target are totally consumed and the target can no more receive any SYN packets further.
7. **UDP flood :** UDP flood occurs when the target receives multiple UDP packets and it needs to check if there are any UDP ports listening for UDP traffic. It wastes a lot of target resources in conducting such searches for port numbers and thus the target becomes too busy to serve any legitimate traffic thus impacting its availability.

5.2.5(C) Preventing DDoS Attacks

Here are some ways to potentially prevent DDoS attacks.

1. **Reduce attack surface area :** By reducing the attack surface area we mean reducing the number of points exposed for attacks. These could be network ports, number of services running, open networks, unrestricted administrative access, unpatched OS or applications or anything else that could be exploited.
2. **Plan for scale :** DDoS attacks target the limited resources. If you have resources spread over a large scale (or say cloud computing), the DDoS attack impact could be very minimal and could be absorbed by the large resource pool without impacting availability.
3. **Know what is a normal and an abnormal traffic :** Knowing your network traffic patterns would let you plan for action if you see any change in the pattern that signals that you are under attack. You can then appropriately take actions to remedy any impact from DDoS.
4. **Deploy firewalls :** DDoS attacks are mostly network based. Having stringent (strong) firewall rules, such that only appropriate traffic is allowed, is a great way to ensure that the resources are not wasted in serving the DDoS traffic. Only the traffic that is legitimate is allowed on the network. Rest all the traffic is dropped without impacting the resources.

5.3 Internet Security Protocols

World Wide Web or just web is a collection of web servers that run several websites that hold the desired information. The Internet as a whole is a collection of such servers and various communication devices and protocols. You mostly use browsers (such as Chrome, Firefox, Internet Explorer, Safari, etc.) or applications (for example, Mobile Apps) to browse the web and fetch the desired information or just complete a desired interaction such as making a purchase.

Let me pause you here and ask a simple question. Don't you feel that your interaction with the Internet (which generally is an insecure and unsafe place) should be protected? For example, if you type your Facebook password, should it be available to everyone on the network?

To make a purchase when you provide your bank account information, isn't that information very confidential and requires secure handling as you pass it through your device all the way to the website? Yes, I am sure you understand that your interaction with the web requires security. There is one protocol that we all need – SSL (obsolete now) followed by TLS (currently used). Let's learn about it.

5.3.1 Secure Socket Layer (SSL)

Q. List the functions of the different protocols of SSL. Explain the handshake protocol. **MU - Dec. 15, 5 Marks**

Q. What are the different protocols in SSL? How do the client and server establish an SSL connection ? **MU - Dec. 17, 5 Marks**

Q. What is the need of SSL? **MU - May 19, 4 Marks**

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the most widely use web security protocol. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network.

✍ ***Definition :*** *A Secure Socket Layer (SSL) is a cryptographic protocol designed to protect communication between two entities.*

SSL underwent several revisions and is now followed by a more secure protocol called TLS. The Table 5.3.1 is a quick version history of SSL/TLS.

Table 5.3.1 : History of SSL/TLS

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Obsoleted in 2011
SSL 3.0	1996	Obsoleted in 2015
TLS 1.0	1999	To be obsolete in 2020
TLS 1.1	2006	To be obsolete in 2020
TLS 1.2	2008	Currently good
TLS 1.3	2018	Currently good

Goals of SSL

1. **Cryptographic Security :** Establish and provide a secure connection between two parties.
2. **Interoperability :** Two unrelated applications should be able to establish SSL connection.
3. **Extensibility :** Provides a framework for using various algorithms and methods without changing the protocol.
4. **Efficiency :** Performance enhancement mechanism to avoid overloading the system when protocol is in use.

5.3.1(A) Overview of SSL Protocol

SSL protocol works in layers. At each layer, messages may include fields for length, description, and content. SSL takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. On the other side, received data is decrypted, verified, decompressed, and reassembled and then delivered to higher level clients.

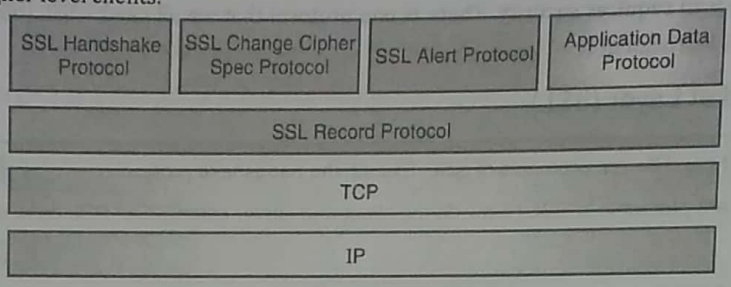


Fig. 5.3.1 : Overview of SSL protocol

Let's learn about each one of them in detail.

Session and Connection States

An SSL session is stateful which means that parameters negotiated during the session establishment persist (stay the same) until the session is terminated. The SSL handshake protocol coordinates the states of the client and server. It is thus important to preserve Session and Connection States.

The Table 5.3.2 summarizes a Session State.

Table 5.3.2 : Session State

Fields	Purpose
Session Identifier	A session ID chosen by the server to identify an active or resumable session state.
Peer Certificate	X.509 Certificate of the other party in the communication.
Compression method	The algorithm used to compress data prior to encryption.
Cipher Specification	Chosen encryption algorithm such as AES and a hash algorithm such as SHA.
Master Secret	48-byte secret shared between the client and server.
Is resumable	A Boolean flag indicating whether a session ID can be used to initiate new connections.

The Table 5.3.3 summarizes a Connection State.

Table 5.3.3 : Connection State

Fields	Purpose
Server and client random	Byte sequences for establishing connection.
Server write MAC secret	The secret used in MAC operations on data written by the server.
Client write MAC secret	The secret used in MAC operations on data written by the client.
Server write key	The bulk cipher key for data encrypted by the server and decrypted by the client.
Client write key	The bulk cipher key for data encrypted by the client and decrypted by the server.
Initialization vectors	Random number to initialize encryption operation.
Sequence numbers	Sequence numbers for transmitted and received messages for each connection.

5.3.1(B) SSL Record Layer Protocol

Definition : *The SSL Record Layer is the last protocol that receives the raw data from the higher application layers and other SSL protocols such as handshake.*

Its core function is to facilitate (perform) data transfer. The basic unit of data in SSL is a record. Each record consists of a five-byte record header, followed by data.

There are four types of records in SSL.

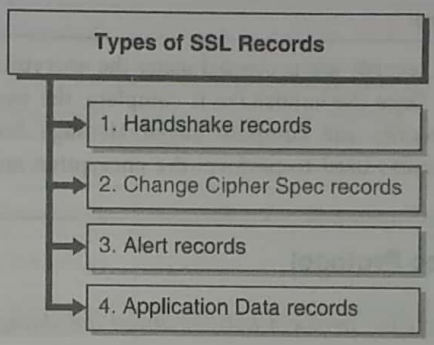


Fig. 5.3.2 : Types of SSL records

The five-byte format of an SSL Record Header shown in Fig. 5.3.3.

SSL record type (1-byte)	SSL Major Version (1-byte)	SSL Minor Version (1-byte)	Length of data in the record (2-bytes)

Fig. 5.3.3 : Format of an SSL record header

A simplistic block diagram of steps involved in the SSL Record Protocol shows in Fig. 5.3.4.

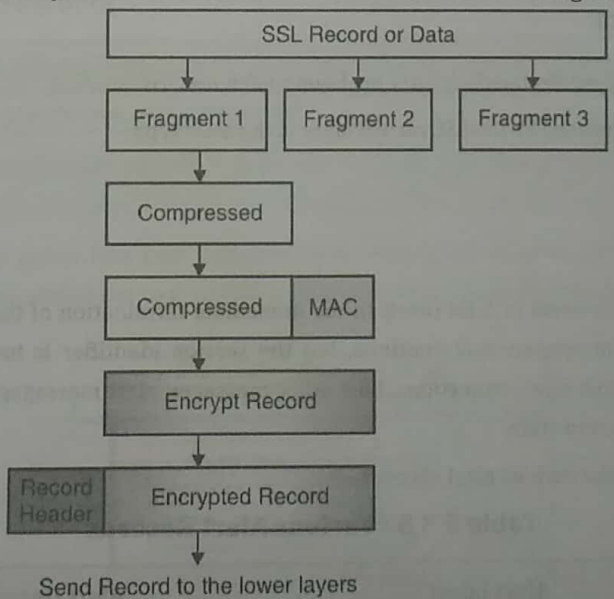


Fig. 5.3.4 : Block diagram of SSL record

At a high level the SSL Record Protocol performs three operations as shown in the Table 5.3.4.

Table 5.3.4 : Operations of SSL Record Protocol

Operation Performed	Purpose
Fragmentation	Break original data into SSL Plaintext records of 2^{14} bytes or less.
Compression and Decompression	All SSL Plaintext records are compressed using the compression algorithm defined in the current session state. The compression algorithm translates an SSL Plaintext structure into an SSL Compressed structure.
Payload Protection	All SSL Compressed records are protected using the encryption and MAC algorithms defined in the current CipherSpec. Once the handshake is complete, the two parties have shared secrets that are used to encrypt records and compute keyed Message Authentication Codes (MACs) on their contents. The techniques used to perform the encryption and MAC operations are defined by the CipherSpec.

5.3.1(C) SSL Change Cipher Spec Protocol

✍ ***Definition :*** *The Change Cipher Spec protocol notifies about the changes in cipher parameters.*

The protocol consists of a single message, which is encrypted and compressed. The Change Cipher Spec Protocol notifies the communicating parties about any change in the previously negotiated Cipher Specifications or Keys.

The keys or the algorithms need to be changed at times for reasons such as renewing the session or resuming the session. The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the just-negotiated CipherSpec and keys.

5.3.1(D) SSL Alert Protocol

✍ ***Definition :*** *The SSL Alert Protocol signals problems with an SSL session.*

One of the content types supported by the SSL record layer is the alert type.

Alert messages notify the;

- Severity of the alert and,
- A description of the alert

Alert messages with a severity level of *fatal* result in the immediate termination of the connection. In this case, other connections corresponding to the session may continue, but the session identifier is invalidated, preventing the failed session from being used to establish new connections. Like other messages, alert messages are encrypted and compressed, as specified by the current connection state.

The Table 5.3.5 summarizes the various alert records.

Table 5.3.5 : Various Alert Records

Alert Code	Alert Message	Alert Level	Alert Description
0	close_notify	1 (Warning)	Notifies the recipient that the sender will not send any more messages on this connection.
10	unexpected_message	2 (Fatal)	An inappropriate message was received.

Alert Code	Alert Message	Alert Level	Alert Description
20	bad_record_mac	2 (Fatal)	A record is received with an incorrect MAC.
30	decompression_failure	2 (Fatal)	The decompression function received improper input.
40	handshake_failure	2 (Fatal)	The sender was unable to negotiate an acceptable set of security parameters given the options available.
41	no_certificate	1 (Warning)	Sent in response to a certification request if no appropriate certificate is available.
42	bad_certificate	1 (Warning)	A certificate was corrupt.
43	unsupported_certificate	1 (Warning)	A certificate was of an unsupported type.
44	certificate_revoked	1 (Warning)	A certificate was revoked by its signer.
45	certificate_expired	1 (Warning)	A certificate has expired or is not currently valid.
46	certificate_unknown	1 (Warning)	Some other (unspecified) issues.
47	illegal_parameter	2 (Fatal)	A field in the handshake was out of range or inconsistent with other fields.

The alert record consists of 2 bytes of information from the Table 5.3.5.

Alert Level (1-byte)	Alert Code (1-byte)

Fig. 5.3.5 : Alert record

5.3.1(E) SSL Handshake Protocol

Q. Write in brief about SSL handshake protocol. **MU - May 16, 5 Marks**

Q. Explain all phases of SSL Handshake protocol in detail. **MU - May 19, 6 Marks**

✍ ***Definition :*** *The cryptographic parameters of the session state are produced by the SSL handshake protocol.*

When an SSL client and the server first start communicating, they need to agree upon certain parameters. There are also several steps that need to be carried out to establish a secure session. At a high level, Fig. 5.3.6 shows the four steps are carried out.

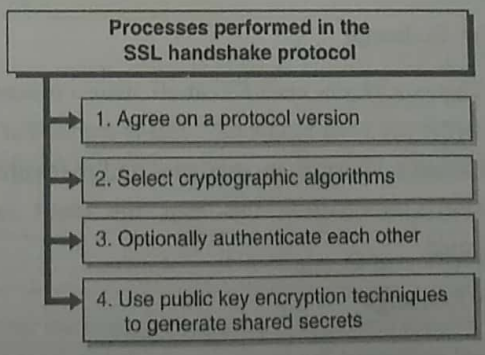


Fig. 5.3.6 : Processes performed in the SSL Handshake Protocol

The steps can be detailed shown in the Fig. 5.3.7 simplistic handshake process.

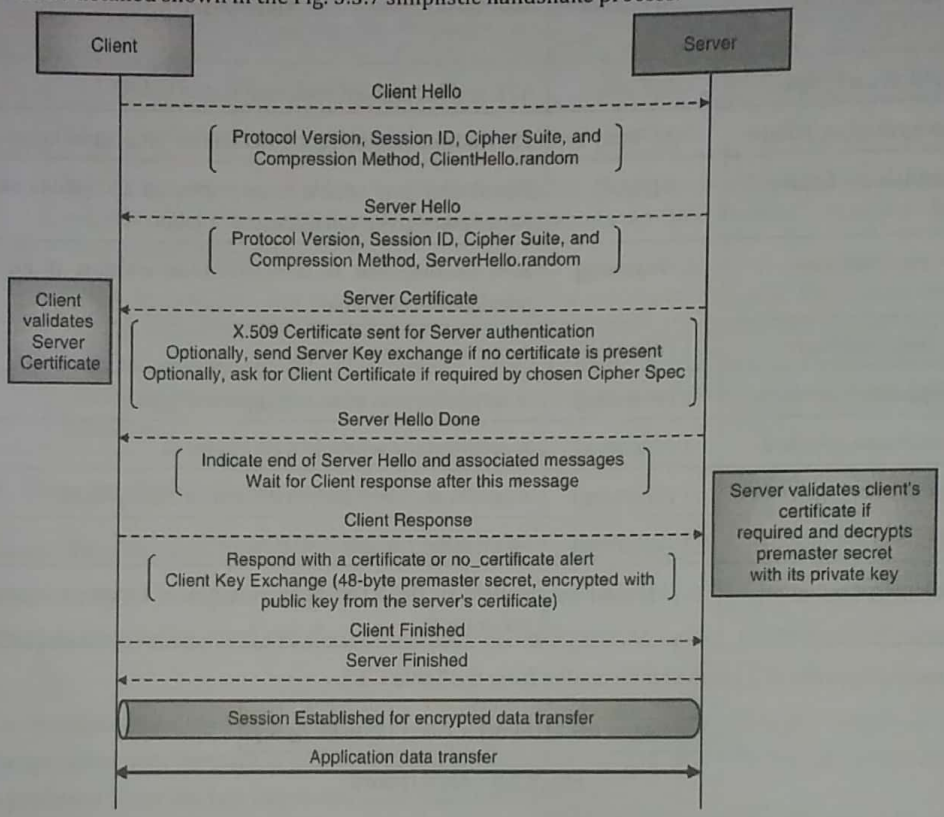


Fig. 5.3.7 : Handshake Process Diagram

Step 1 : Hello messages (Establish security capabilities)

The hello phase messages are used to exchange security enhancement capabilities between the client and server.

1. Client Hello : When a client first connects to a server it is required to send the client hello as its first message. The client can also send a client hello in response to a hello request or on its own initiative in order to renegotiate the security parameters in an existing connection. The list of parameters sent are shown in Fig. 5.3.7.
2. Server Hello : The server processes the client hello message and responds with server hello message. The list of parameters sent are in the diagram.

Step 2 : Server Authentication and Key Exchange

This is the most important step. This is why you need SSL at all. Before proceeding to interact with the server you should find out "Is this really the server you want to talk to?". This is crucial. For example, if you want to do a banking transaction, before providing your account information, username and password, you MUST validate that the website you are on (server behind the website) is legitimate. In this step, the client validates the server certificate. Any certificate related errors are highlighted.

Step 3 : Client authentication and Key Exchange

If the certificate is found valid, client exchanges the keying material that would be subsequently used to encrypt the messages. The client generates a 48-byte premaster secret, encrypts it using the public key from the server's certificate and sends the result in an encrypted pre-master secret message.

Step 4 : Connection establishment and data transfer

Once all the connection parameters are negotiated and exchanged, a connection between the server and the client is established. Once the connection is established, the data transfer begins between the server and the client. The data is encrypted based on the negotiated terms.

5.3.2 Transport Layer Security (TLS)

As you learnt earlier, SSL is obsolete. TLS replaced SSL in 1999. The underlying working of TLS is very similar to SSL.

TLS is more efficient and secure than SSL. It provides stronger message authentication, key-material generation and supports pre-shared keys, secure remote passwords, elliptical-curve keys and Kerberos. TLS and SSL are not interoperable, but TLS provides backward compatibility for devices using SSL.

HTTPS

Now that you learnt how SSL works, let's learn about one of its implementations – HTTPS application protocol.

✍ ***Definition :*** *HTTPS establishes a secure SSL / TLS tunnel before beginning data transfer.*

The Hypertext Transfer Protocol (HTTP) is an application protocol used to transfer data on distributed and connected systems. HTTPS is the secure version of HTTP. The 'S' at the end of HTTPS stands for 'Secure'. It means that all the communications between your client (browser, mobile apps) and the server (website, web application) is encrypted. HTTPS is often used to protect confidential online interactions such as online banking.

Conceptually, HTTPS is very simple. Simply use HTTP over TLS (previously SSL) instead of HTTP. The use of TLS (previously SSL) ensures that the adequate protection mechanisms such as encryption, server authentication, hashing, and optionally client authentication are effectively applied, and the communication is adequately protected.

Comparison between HTTP and HTTPS

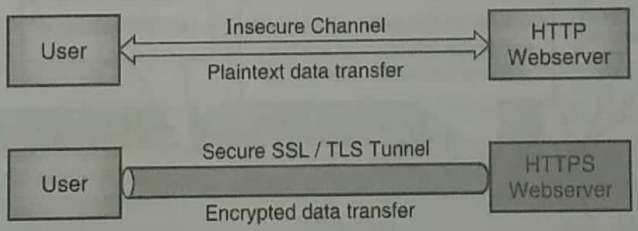


Fig. 5.3.8 : Comparison between HTTP and HTTPS

Table 5.3.6 : Comparison between HTTP and HTTPS

HTTP	HTTPS
Data transfer in plaintext	Data transfer in ciphertext
Default port is 80	Default port is 443
Does not require SSL/TLS or Certificates	Requires SSL/TLS implementation with Certificates
URL has http://	URL has https://
Should be avoided	Should be preferred
Search engines do not favour the insecure websites	Improved reputation of the website in search engine
Users worried about their data	Users confident about the security of their data

Motivation / Benefits of using HTTPS

1. **Increasing sensitivity of data :** With the proliferation (widespread use) of internet, a lot of sensitive communication such as online banking, ticketing, shopping, etc. is taking place over the Internet. There is an ever increasing need to ensure that the communication is secure (confidentiality and integrity of the information is enforced). Information such as your password or credit card number is not transferred in plaintext that can potentially be captured and then misused.
2. **Authentication :** One of the critical use cases that HTTPS serves is that using it you can potentially authenticate a website or a business. HTTPS connection is established using X.509 certificates and certificate authorities do proper business or website validation before issuing certificates. Certificates help you prove that a website is indeed legitimate, and you are indeed interacting with the right website. This avoids several online frauds where a similar looking banking or e-commerce site can capture your confidential details.
3. **Privacy requirements :** Often times, the nature of communication is private even if it is not confidential.

   For example, your health reports, your chats, your location details, etc. require that they are adequately protected when transferred over the network. Use of HTTPS ensures that encryption is applied to all data seamlessly and the private information is adequately protected during transfer.

Format, Port Number and Representation

Typical format of HTTPS is https://www.example.com. It works over port 443 by default. You would have seen various websites with HTTPS enabled. These days browsers show green colour in the URL for HTTPS protected websites and warning for non-HTTPS websites.

An example of a HTTPS protected website is shown in Fig. 5.3.9.

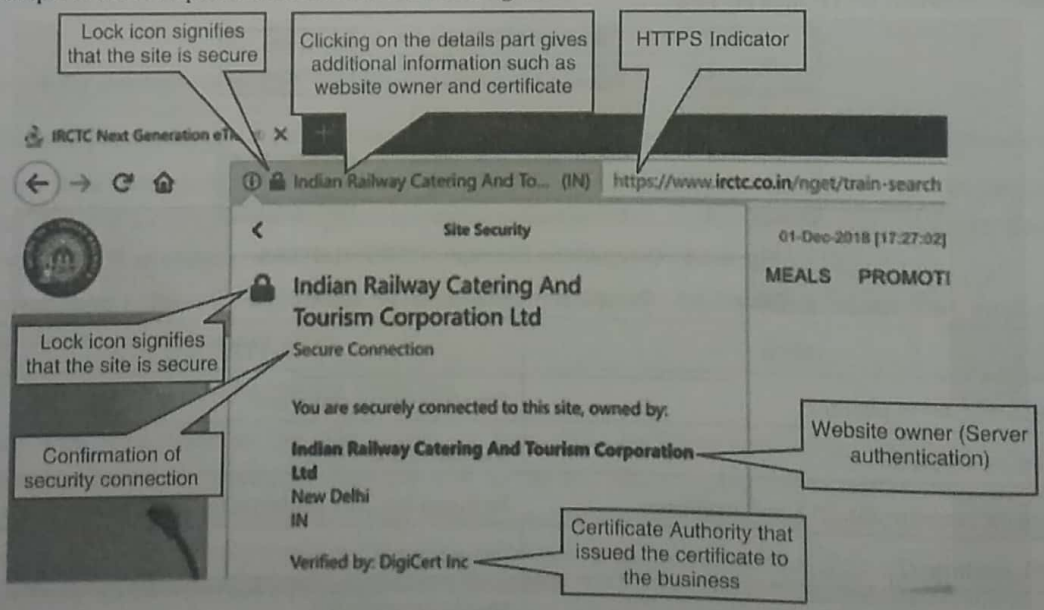


Fig. 5.3.9 : HTTPS protected website

An example of a non-HTTPS website in shown in Fig. 5.3.10.

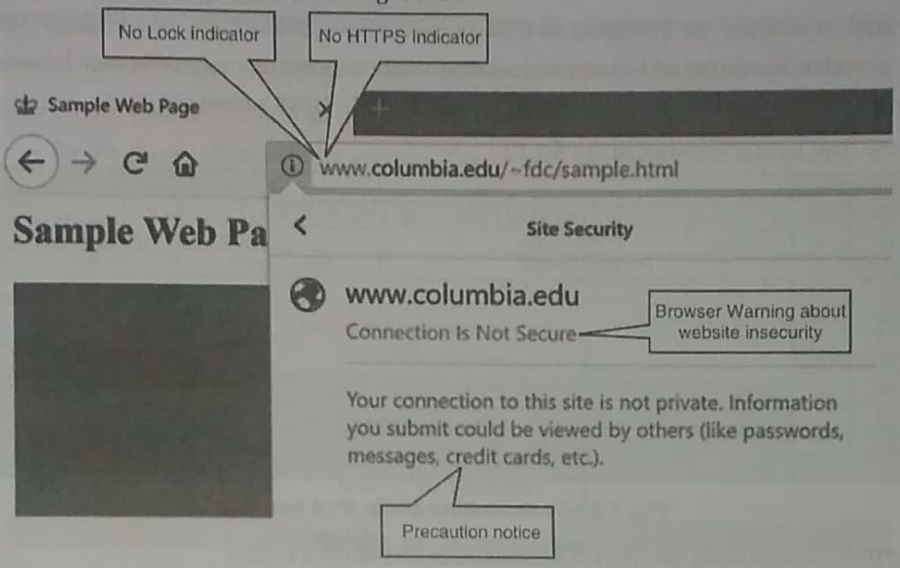


Fig. 5.3.10 : Non-HTTPS website

5.3.3 Internet Protocol Security (IPSec)

Q. Write in brief about IPSec protocols for security. **MU - May 16, 5 Marks**

IP stands for Internet Protocol. IP defines a set of protocols that can be used for communication between any two devices on the network. A network protocol is a standard set of rules that determines how systems will communicate across networks. Two different systems that use the same protocol can communicate and understand each other very similar to how two people can communicate and understand each other by using the same language.

IP provides addressing and routing mechanisms for each packet of data that needs to move across the network. Each device on the network must have a unique IP address to communicate with any other device on the network.

Note : It is assumed that you have a general understanding of computer networking. While this section does not dive deeper into computer networks, it focuses on specific security topics around networking.

IPv4 : IPv4 is IP version 4. This is the most common IP addressing scheme used today despite certain challenges. It is 32-bit long and thus has an address space of 2^{32} = 4,294,967,296. This means you can maximally have 4,294,967,296 (approximately 4.3 billion) IPv4 addresses. There are many more devices than the number 4,294,967,296. An outline of the IPv4 header is shown in Fig. 5.3.11.

Offsets Octet	Octet	0								1								2								3							
	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Fig. 5.3.11 : An outline of the IPv4 header

An example of IPv4 address looks like 121.56.78.214.

IPv6

IPv6 was created to address the limitation of IPv4 to have only 4,294,967,296 IP addresses due to 32-bit length. IPv6 more or less provides the similar addressing and routing capabilities but one core difference between IPv4 and IPv6 is the address space. IPv6 address is 128-bit long and thus you can have 2^{128} IPv6 addresses!

An outline of the IPv6 header is shown in Fig. 5.3.12.

Offsets Octet	Octet	0								1								2								3							
	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source IP Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination IP Address																															
28	224																																
32	256																																
36	288																																

Fig. 5.3.12 : An outline of the IPv6 header

An example of IPv6 address looks like 2001:0:9d38:6abd:2c37:10da:8554:4234.

Definition : *IPSec is a suite of protocols that protects IP traffic.*

IP does not have any integrated security mechanisms by itself and hence IPSec (short form for IP Security) is additionally used to provide security for IP traffic. The IPSec suite consists of following security protocols.

Table 5.3.7 : Security protocols/ Services Provided by IPSec

Protocol Name	Functionality Provided
Authentication Header (AH)	• Data Integrity • Data Origin Authentication • Protection from replay attacks.
Encapsulating Security Payload (ESP)	• Confidentiality • Data Origin Authentication • Data Integrity.
Internet Security Association and Key Management Protocol (ISAKMP)	Framework for Authentication and Key Exchange.
Internet Key Exchange (IKE)	Authenticated keying material for use with ISAKMP.

Note here that IPSec is a framework. It does not mandate which hashing and encryption algorithms should be used or how keys should be exchanged between the communicating devices. Key management can be handled manually or automated by a key management protocol such as ISAKMP.

5.3.3(A) Security Association

Q. What are security associations ? **MU - Dec. 17, 4 Marks**

Security Association (SA) is a fundamental concept with respect to IPSec.

Definition : *Security Association (SA) holds several information that determines how security services would be consumed by the communicating devices.*

IPSec provides many options for performing security services such as encryption, integrity and authentication.

The network devices that wish to establish an IPSec connection, must negotiate and arrive at exactly which algorithms and parameters to use for the chosen IPSec security services. The security association is a mechanism to hold all the agreed terms (algorithms, parameters, etc.) for a given IPSec communication session.

5.3.3(B) Modes of Operation

IPSec can work in two modes.

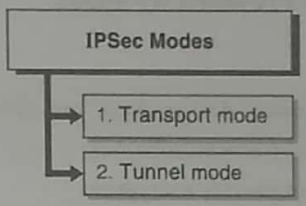


Fig. 5.3.13 : IPSec Modes

1. **Transport Mode :** In this mode, only the payload (data) part of the information is protected. The addressing and routing information is not protected. It is like a sealed envelope with address on it. The message inside the envelop is protected whereas the source and destination addresses are not.

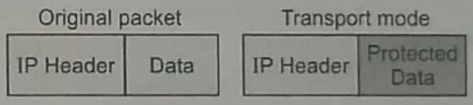


Fig. 5.3.14 : Transport Mode

2. **Tunnel Mode :** In this mode, both the payload (data) as well as the addressing information is protected. In this mode, the entire packet is protected, and a new IP header is added by IPSec. The original IP header information along with the payload information is protected. Tunnel mode provides more security than the transport mode.

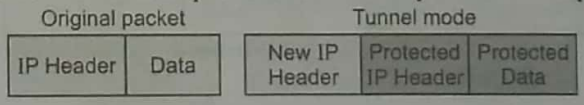


Fig. 5.3.15 : Tunnel Mode

5.3.3(C) Applications / Benefits / Usage of IPSec

1. **Establish Virtual Private Network (VPN) :** IPSec is predominantly used to establish VPN connection. VPN connections are generally used to access private networks over the internet. For example, you can access your college or your organization's network from home over the internet.
2. **Connecting two or more branch networks :** IPSec can be used to extend or connect branch networks. For example, if you have two branches of office each using its own network, the branches can be connected using IPSec. The network traffic then can securely move between the branches.
3. **General Security Benefits :** IPSec adds general security benefits to the core IP protocol. It provides benefits such as data confidentiality, data integrity, data origin authentication and protection from several attacks on the core IP protocol.

5.3.3(D) How does IPSec work?

Overall, communication over IPSec has 5 broad steps.

1. **Initiate IPSec process :** IPSec communication begins with the identification of traffic that requires IPSec security.
2. **IKE Phase 1 :** In this phase, the IKE SAs are negotiated and agreed.
3. **IKE Phase 2 :** In this phase, next set of SAs for actual data transfer are negotiated and agreed.
4. **Data Transfer :** Data is transferred between the communicating entities.
5. **Termination :** The IPSec connection is terminated once the data transfer is complete.

5.3.3(E) Security Protocols/ Services Provided by IPSec

1. Authentication Header (AH)

✍ ***Definition :*** *The Authentication Header (AH) protocol provides data integrity and data original (source address) authentication over the network communication.*

It also provides replay protection. It does not provide encryption.

AH calculates the Integrity Check Value (ICV) over non-changing fields of the IP header:

- Next Header
- Payload Len
- Reserved
- Security Parameter Index (SPI)
- Sequence number
- Padding bytes

ICV is a hash value which is often computed using SHA-1 or other hashing algorithms.

(i) Transport mode for AH, Fig. 5.3.16 is show before and after applying AH.

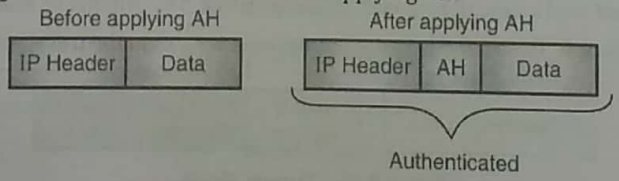


Fig. 5.3.16 : Transport mode for AH

(ii) Tunnel mode for AH, Fig. 5.3.17 is show before and after applying AH.

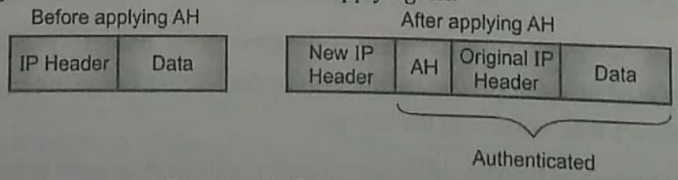


Fig. 5.3.17 : Tunnel mode for AH

If you recall our previous discussion on hash values, hash values provide integrity. AH uses hashing algorithms to find out hash value of the IP header and attaches it with the IP header. This way it not only provides data integrity (since hash is calculated on payload as well) but also data origin integrity or authentication (since source address is part of the IP header as well).

2. Encapsulating Security Payload (ESP)

✍ ***Definition :*** *The Encapsulating Security Payload (ESP) protocol is designed to provide confidentiality (through encryption), data integrity and data origin authentication over network communication.*

ESP can be applied with AH or without AH. Note here that ESP can itself provide integrity. It does not need AH for integrity. You have an option to additionally calculate integrity using AH. ESP in transport mode encrypts the actual payload (data) so that it cannot be read by an unauthorized entity. In tunnel mode, the IP header information is encrypted as well.

If you choose integrity service, the Integrity Check Value (ICV) is calculated on the following fields in the IP header.

- Security Parameter Index (SPI)
- Sequence Number
- Payload Data
- ESP trailer

If you choose confidentiality service, the ciphertext consists of the following fields in the IP header.

- Payload (Data)
- ESP trailer

(i) Transport mode for ESP, Fig. 5.3.18 shows before and after applying ESP.

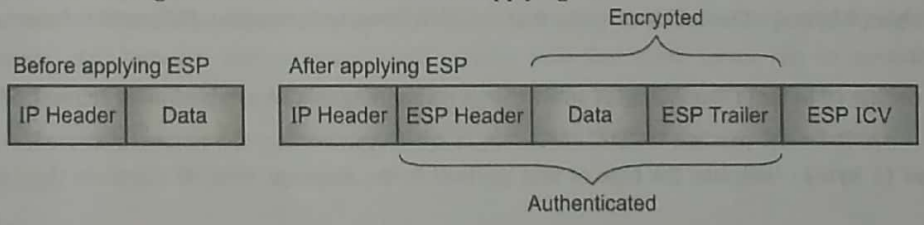


Fig. 5.3.18 : Transport mode for ESP

(ii) Tunnel mode for ESP, Fig. 5.3.19 shows before and after applying ESP.

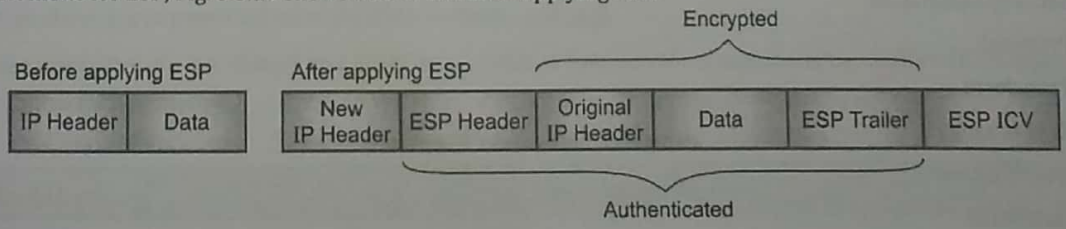


Fig. 5.3.19 : Tunnel mode for ESP

3. Internet Security Association and Key Management Protocol (ISAKMP)

✍ ***Definition :*** *Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange.*

ISAKMP does not define the exact algorithms to be used. It is just a framework within which various exchange protocols can work.

ISAKMP defines the procedures for;

- Authenticating communication devices
- Creation and management of Security Associations (SA)
- Key generation techniques
- Threat mitigation

ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework. ISAKMP header is shown in Fig. 5.3.20.

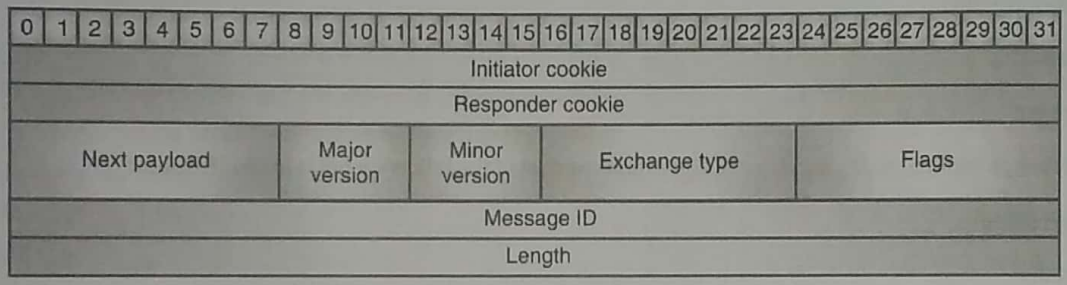


Fig. 5.3.20 : ISAKMP header

- **Initiator cookie (8 bytes) :** The cookie of entity that initiated Security Association (SA) establishment, SA notification, or SA deletion.
- **Responder cookie (8 bytes) :** The cookie of entity that is responding to a SA establishment request, SA notification, or SA deletion.
- **Next Payload (1 byte) :** Indicates the type of first payload in the message. ISAKMP supports the following payload types :
  - None
  - SecurityAssociation
  - Proposal
  - Transform
  - KeyExchange
  - Identification
  - Certificate
  - CertificateRequest
  - Hash
  - Signature
  - Nonce
  - Notification
  - Delete
  - VendorID
  - NAT Discovery Payload

- NAT Original Address Payload
- Reserved
- PrivateUse

- **Major version (4-bits) :** Major version of the ISAKMP protocol in use.
- **Minor version (4-bits) :** Minor version of the ISAKMP protocol in use.
- **Exchange Type (1 byte) :** The type of exchange in a given ISAKMP session. The primary difference between exchange types is the ordering of the messages and the payload ordering within each message.
- **Message ID (4 bytes) :** The unique message identifier.
- **Length (4 bytes) :** The length, in bytes, of the total message (header + payloads).

ISAKMP offers two phases of negotiation :

- **Phase 1 :** In the first phase, two entities agree on how to protect further negotiation traffic between themselves, establishing an ISAKMP SA.
- **Phase 2 :** The second phase of negotiation is used to establish security associations for other security protocols. This second phase can be used to establish many security associations. The security associations established by ISAKMP during this phase can be used by a security protocol to protect many message/data exchanges.

4. Internet Key Exchange (IKE)

Definition : *Internet Key Exchange (IKE) is the protocol used to set up a Security Association (SA) in the IPsec protocol suite.*

Recall from our earlier discussion on security association – A security association is a set of negotiated terms (algorithms, parameters, etc.) between two communicating entities such that these terms can be used in successive communication.

The following attributes are used by IKE and are negotiated as part of the ISAKMP Security Association :

- Encryption algorithm
- Hashing algorithm
- Authentication method
- Information about a group over which to do Diffie-Hellman exchange.

All of these attributes are mandatory and MUST be negotiated between the communicating entities. IKE supports the following attributes for negotiation.

Table 5.3.8 : IKE negotiated attributes

Attribute For	Supported Attributes
Encryption algorithm	DES, IDEA, Blowfish, 3DES, CAST, RC5, AES
Hashing algorithm	MD5, SHA, TIGER
Authentication method	Pre-shared key, DSS Signature, RSA Signature, Encryption with RSA, Revised encryption with RSA
Group information	MODP (modular exponentiation group), ECP (elliptic curve group over GF[P]), EC2N (elliptic curve group over GF[2^N])

IKE works in two phases :

In Phase 1, following functions are carried out :

- Mutual authentication of the communicating entities.
- Negotiating cryptographic parameters.
- Creating session keys.

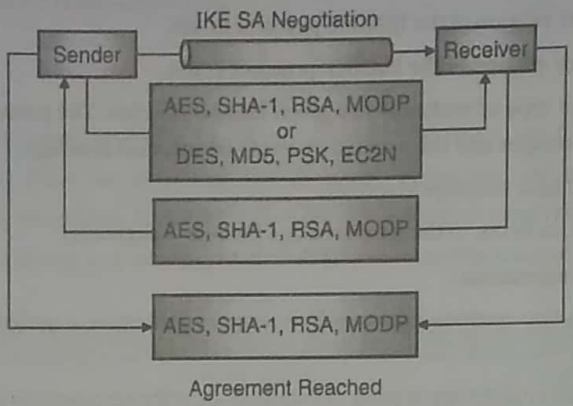


Fig. 5.3.21 : IKE Agreement Process

In Phase 2, an IPSec tunnel is negotiated by creating keying material for the IPSec tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange).

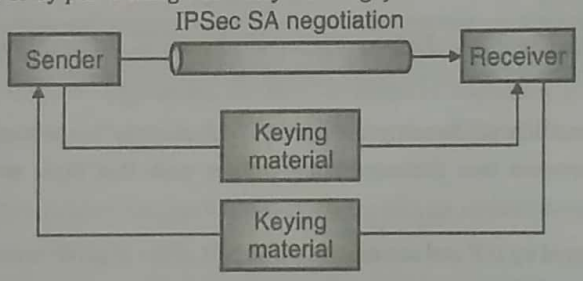


Fig. 5.3.22 : IPSec Tunnel Negotiation

5.4 Secure Email

Q. Write in brief about Email security. **MU - May 16, 5 Marks**

Around billions of emails are sent across the globe every day. Emails have become the primary source of official communication. With such a wide use of emails, attackers are inclined and motivated to intercept emails and get the message and at times modifying the messages before the recipient gets it. It is important that you secure the email communication as any other form of communication. In this section, you will learn about a couple of email security standards that you could use.

5.4.1 Pretty Good Privacy (PGP)

Q. How does PGP achieve confidentiality and authentication in emails? **MU - Dec. 15, 5 Marks**

✍ ***Definition :*** *Pretty Good Privacy (PGP) is an email security program that was developed in 1991. It is based on public key cryptography.*

1. Web of Trust

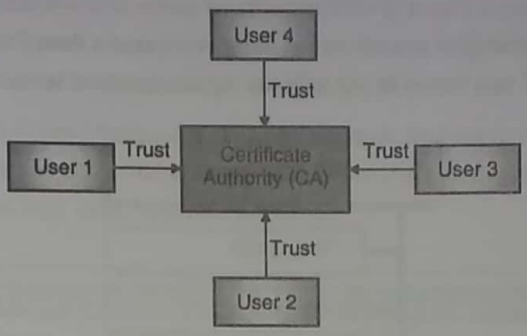


Fig. 5.4.1 : Trust using Public Key Cryptography

In Public Key Cryptography system that depends upon a third-party Certificate Authorities (CAs) to establish trust, there is no mutual trust amongst the users.

Each user trusts a reputed CA and thus CA plays a predominant role in establishing the trust so that communication can happen between users. If there is no CA, the trust relationship is not established and thus the communication may not happen.

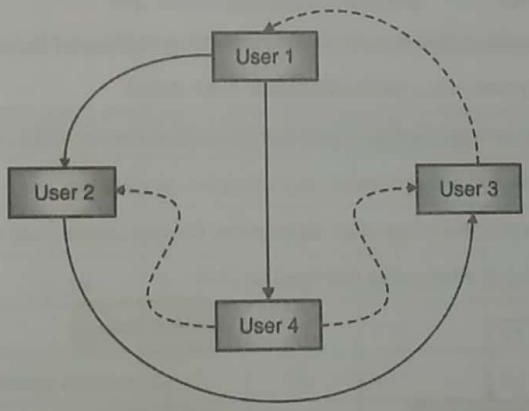


Fig. 5.4.2 : Web of Trust

Unlike the traditional Public Key Cryptography system that depends upon a CA to establish trust amongst the users, the earlier implementations of PGP did not use the regular CAs for issuing certificates. It used "Web of Trust" where each user generates and distributes his or her public key, and users sign each other's public keys, which creates a community of users who trust each other. This is different from the CA approach, where no one trusts each other; they only trust the CA.

So, basically, PGP is a system of "I don't know you, but my friend Alice says that you can be trusted, so I will trust you on her words". In the Fig. 5.4.2, as you understand, there is a trust relationship (User 1, User 2) and (User 2, User 3). Now, when User3 needs to communicate with User 1, it establishes a trust inherited from its prior trust on User 2. There is no third-party involved in this scenario. Each user keeps in a file, referred to as a key ring, a collection of public keys he has received from other users. Each key in that ring has a parameter that indicates the level of trust assigned to that user and the validity of that particular key.

5.4.1(A) PGP Services

PGP provides the following services. You can use one or more services at a time. For example, if you intend to use only encryption service, you can do so. If you intend to use only the digital signature service, you can do so. Let's learn a brief about these services.

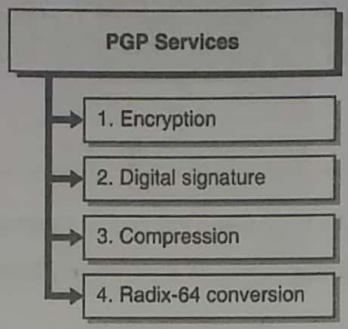


Fig. 5.4.3 : PGP Services

1. Encryption

(a) The sender creates a message.

(b) PGP generates a random number that is used as symmetric key to encrypt it.

(c) The symmetric key is encrypted using receiver's public key.

(d) Encrypted message and the encrypted symmetric key are sent to the receiver.

(e) The receiver decrypts the encrypted symmetric key using her private key.

(f) Once the receiver gets the symmetric key after decryption, the key can be used to decrypt the message.

Fig. 5.4.4 illustrates steps involved in encryption followed by PGP.

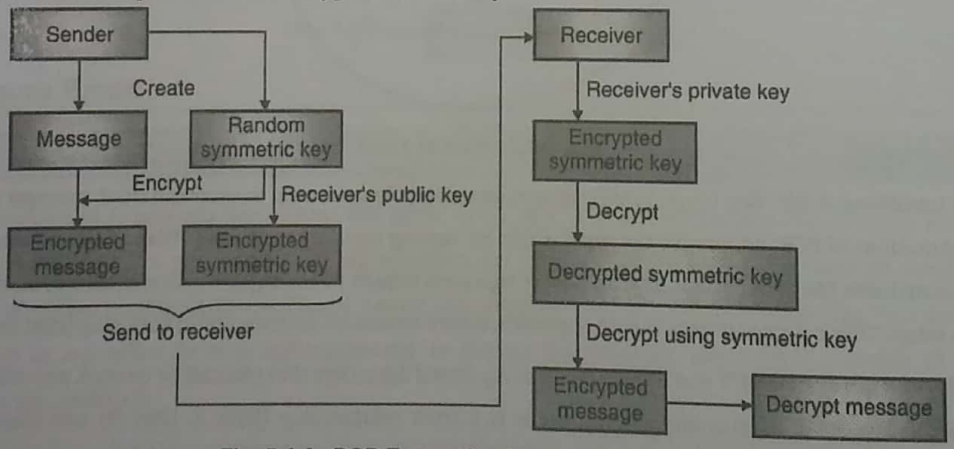


Fig. 5.4.4 : PGP Encryption / Decryption Process

2. Digital Signature : The digital signature uses a hash code or message digest algorithm, and a public-key signature algorithm. You have already learnt digital signature in detail in Chapter 2. Refer it for a quick refresher.

3. Compression : PGP compresses the message after applying the signature but before encryption. Compression has the added side effect that some types of attacks can be avoided by the fact that even the slightly altered, compressed data does not decompress without errors. This side security benefit is operationally useful.

4. **Radix-64 conversion :** R64 conversion is useful for compatibility of emails across varied systems. PGP's underlying native representation for encrypted messages, signature certificates, and keys is a stream of arbitrary octets. Some systems only permit the use of blocks consisting of seven-bit, printable text.

So, for transporting PGP's native raw binary octets through channels that are not safe to raw binary data, a printable encoding of these binary octets is needed. PGP provides the service of converting the raw 8-bit binary octet stream to a stream of printable ASCII characters, called Radix-64 encoding.

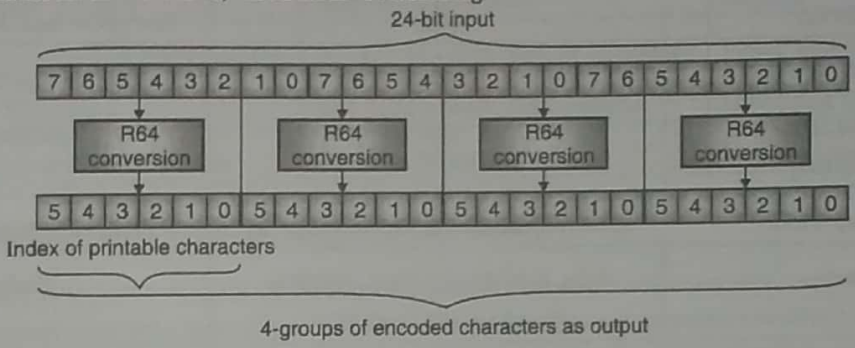


Fig. 5.4.5 : Radix-64 encoding

Each 6-bit group is used as an index into an array of 64 printable characters as shown in Table 5.4.1.

Table 5.4.1 : Encoding Map

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v	(pad)	=
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

5.4.1(B) PGP Algorithms

The Table 5.4.2 is a summary of various PGP services and algorithms they support.

Table 5.4.2 : Summary of various PGP services and Algorithms

PGP Service	Supported Algorithm	Purpose
Public Key	RSA	Encrypt or Sign (Symmetric Key)
Public Key	Elgamal	Encrypt (Symmetric Key)
DSA (Digital Signature Algorithm)	DSS	Sign (Message)
Symmetric Key	IDEA, TripleDES, CAST5, Blowfish, AES	Bulk encryption (message)
Hash	MD5, RIPEMD160, SHA1, SHA256, SHA384, SHA224, SHA512	Hashing
Compression	ZIP, ZLIB, BZip2	Compress messages

5.4.2 S/MIME

✍ ***Definition :*** *S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data (emails).*

It is based on certificates (Public Key Cryptography) and works as you have learnt in previous sections and units.

5.4.2(A) S/MIME Services

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

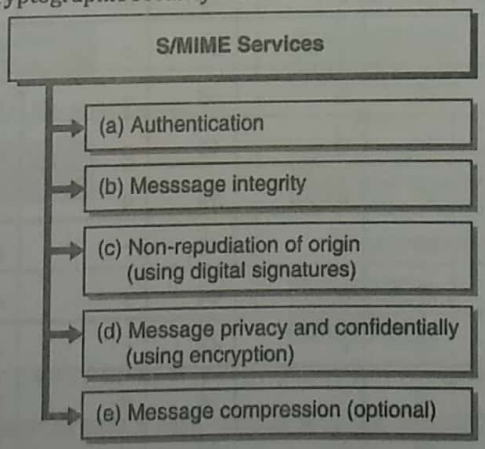


Fig. 5.4.6 : S/MIME Services

These services are provided using same techniques as you have learnt in the previous sections and units.

5.4.2(B) S/MIME Algorithms

Summary of various S/MIME services and algorithms they support are shown in The Table 5.4.3.

Table 5.4.3 : S/MIME Supported services and algorithms

Sr. No.	S/MIME Service	Supported Algorithms	Purpose
1.	Message Integrity	SHA-256, SHA-1, MD5	Hashing
2.	Non-repudiation, Authentication	RSA and DSA with Hashing algorithms	Digital Signature
3.	Key Encryption	RSA, RSAES-OAEP, Diffie-Hellman	Encrypting Symmetric key
4.	Privacy and Confidentiality	AES, DES, Triple DES	Message Encryption

5.4.2(C) S/MIME Cryptographic Message Syntax (CMS)

S/MIME standard describes a protocol for adding cryptographic signature and encryption services to MIME (email) data. The MIME standard provides a general structure for the content of Internet messages and allows extensions for new content-type-based applications. The S/MIME specification defines how to create a MIME (email) body part that has been cryptographically enhanced according to the Cryptographic Message Syntax (CMS).

There are 4 types of CMS used in S/MIME :

1. **Data Content Type :** This is the original plaintext form of the email message. It has an identifier that is referred whenever it is compressed, encrypted or digitally signed.
2. **SignedData Content Type :** SignedData content type is used when a sender needs to apply a digital signature to a message. Applying a signature to a message provides authentication, message integrity, and non-repudiation of origin.
3. **EnvelopedData Content Type :** This content type is used to apply data confidentiality (via encryption) to a message. A sender needs to have access to a public key (for encrypting the symmetric key used for actual encryption of the message) for each intended message recipient to use this service. At the receiver's end, the receiver uses her private key to decrypt the symmetric key used for encrypting the original message. Once the symmetric key is available, it can be used to decrypt the encrypted message and thus read the email message.
4. **CompressedData Content Type :** This content type is used to apply data compression to a message. This content type does not provide authentication, message integrity, non-repudiation, or data confidentiality. It is only used to reduce the size of the message.

5.4.3 Firewalls

Q.	What is a firewall ? What are the firewall design principles ?	MU - May 16, 5 Marks
Q.	What are firewals ?	MU - Dec. 16, 3 Marks

Your computer is connected to the internet. How do you protect it from someone trying to access it over the internet? How do you prevent some rogue programs on your computer to send information to the attacker? Firewalls could be a mechanism.

✍ ***Definition :*** *Firewalls are network security systems that protect the computing resources on a trusted network from unauthorized access.*

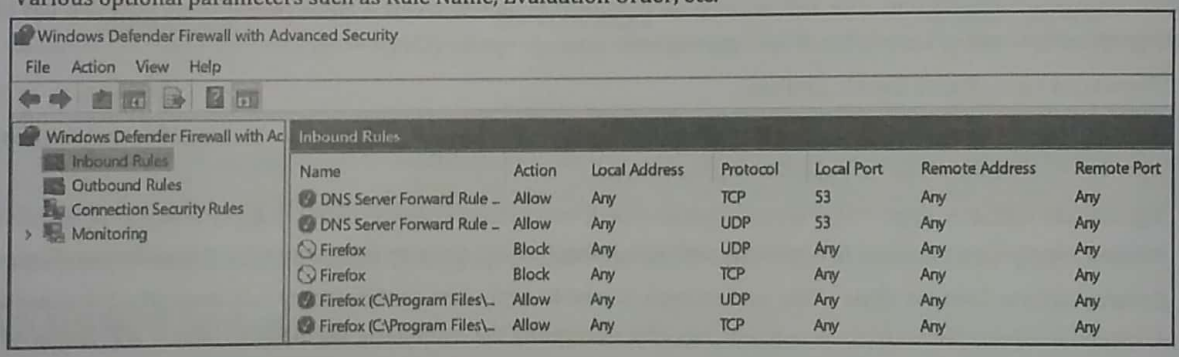
For example, you can access google.com website but not it's webserver's operating system. If you try connecting to the webserver except over the HTTP or HTTPS, the connection would be denied. That's what a firewall does at a high level.

You need to define various rules, as per your security requirements, in the firewall and the firewall evaluates those rules before granting or denying access to the requested resource.

5.4.3(A) Components of a Firewall Rule

Typically, a firewall rule consists of the following parameters :

1. Source IP address or hostname.
2. Destination IP address or hostname.
3. Source Port number.
4. Destination Port number.
5. Direction of communication [inbound or outbound].
6. Protocol name [TCP, UDP, ICMP or various others].
7. Action [allow, deny, log, etc.].
8. Various optional parameters such as Rule Name, Evaluation Order, etc.



This is a snapshot of Microsoft® Windows® Firewall.

5.4.3(B) Classification of Firewalls

Q. Explain the different types of firewalls and mention the layer in which they operate. MU- Dec. 16, 7 Marks

Q. What are the types of firewalls ? MU- May 17, 5 Marks

Firewalls can be classified based on various attributes. Let's learn about their types.

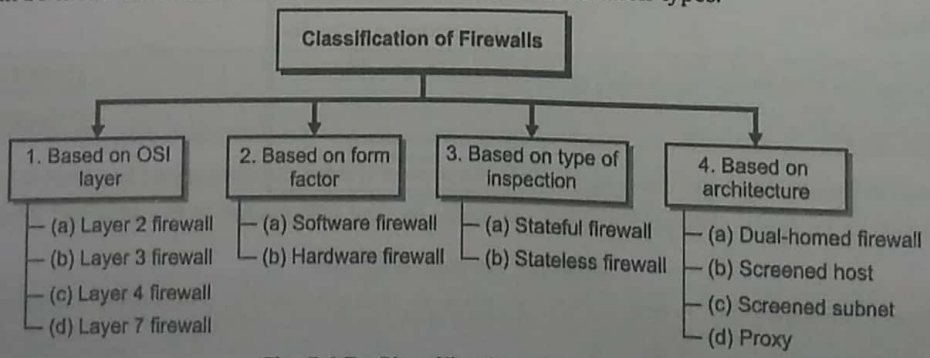


Fig. 5.4.7 : Classification of Firewalls

1. **Based on the OSI Layer :** As you understand, OSI is a conceptual networking model. Based on the various layers, firewalls can be classified as following :

   (a) **Layer 2 Firewall :** These firewalls work at the "Data Link" layer of the OSI model. These firewalls require MAC, VLAN or device hardware level information to operate. One of the greatest advantage of these types of firewalls is that they are not IP dependent.

   (b) **Layer 3 Firewall :** These firewalls work at the "Network" layer of the OSI model. These filter traffic based on source/destination IP, port, and protocol. These are one of the most prevalent types of firewalls in use today. These are also called as Stateless firewalls. These are also called first-generation firewalls.

   (c) **Layer 4 Firewall :** These firewalls work at the "Transport" layer of the OSI model. These firewalls do everything that a Layer 3 firewall does and additionally track the active network connections and allow/deny traffic based on the state of those connections. These can effectively stop DoS attacks such as the ones based on TCP SYN/ACK as these are aware of the state of connection. These are also called as Stateful firewalls. These are also called second-generation firewalls.

   (d) **Layer 7 Firewall :** These firewalls are called Layer 7 but can work at three layers – Session, Presentation and Application. For simplicity, these are just called Layer 7 firewalls. Layer 7 firewalls do everything that a Layer 4 firewall does and additionally include the ability to intelligently inspect the contents of the network packets passing through them.

   For example, a Layer 7 firewall could deny all the HTTP requests from Korean IP addresses. They have the actual packet content level visibility and are the most advanced types of firewall in use today. These are also called third-generation firewalls.

2. **Based on the form factor :** Form factor or the footprint is the way the firewall is actually packaged and deployed. They can be classified as,

   (a) **Software Firewalls :** These firewalls work as a software program and require an operating system to run them. All the implementation logic is coded in software and they are installed, patched, upgraded and maintained like a regular computer software. These firewalls could work at any of the OSI layers as discussed before.

   (b) **Hardware Firewalls :** Firewalls can also be deployed as a hardware device. Hardware firewall may have better performance and they come packaged in a ready to use hardware device. Like any other firewall, you need to configure it as per your security requirements.

3. **Based on the type of inspection :** Firewalls can keep track of connections or just work based on the configured rules. Based on their inspection types, these can be classified as,

   (a) **Stateful Firewalls :** These firewalls keep track of the state of connections apart from the defined firewall rules. These precisely understand various handshake protocols and can effectively stop attacks that try to manipulate connection establishment or maintenance process.

   (b) **Stateless Firewalls :** Stateless firewalls typically work at the Layer 3 and take decisions based on the defined rule parameters such as IP, Port and Protocol. These do no track connection states and cannot effectively protect against attacks that manipulate connection processes.

4. **Based on architecture :** Firewalls can be deployed in many ways. They have special properties that make them suitable for one deployment type over the another. Based on the deployment possibilities, firewalls can be classified as,

   (a) **Dual-homed Firewalls :** A Dual-Homed Firewall has two interfaces - one facing the external network and the other facing the internal network. It receives the external packets on one of its interfaces, evaluates firewall rules, and passes on the traffic to the designated internal resources via the second interface. The two interfaces are kept separate to isolate the external traffic with the internal traffic physically.

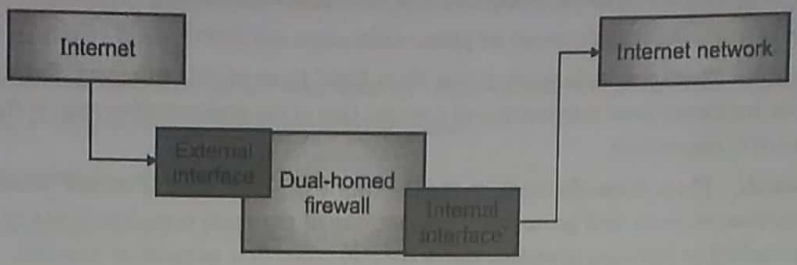


Fig. 5.4.8 : Dual-homed Firewalls

(b) Screened Host : In a screened host firewall, all internet (and other regulated) traffic goes through the firewall, no matter what. The internet router device first screens (filters) all the packets that are relevant to the network and then passes it to the Screened Host firewall for further inspection and applying rules.

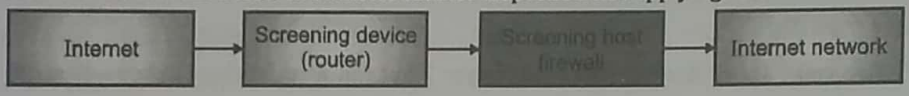


Fig. 5.4.9 : Screened Host

(c) Screened Subnet : In screened subnet architecture, two firewalls are used. One just after the external network and the one just before the internal network. Any network that lies between the two firewalls is called a demilitarized zone (DMZ). You place your public facing servers such as webservers, email servers etc. in DMZ. An attacker would have to bypass both the firewalls before she can hit the internal network. This kind of architecture is commonly used in the industry today.

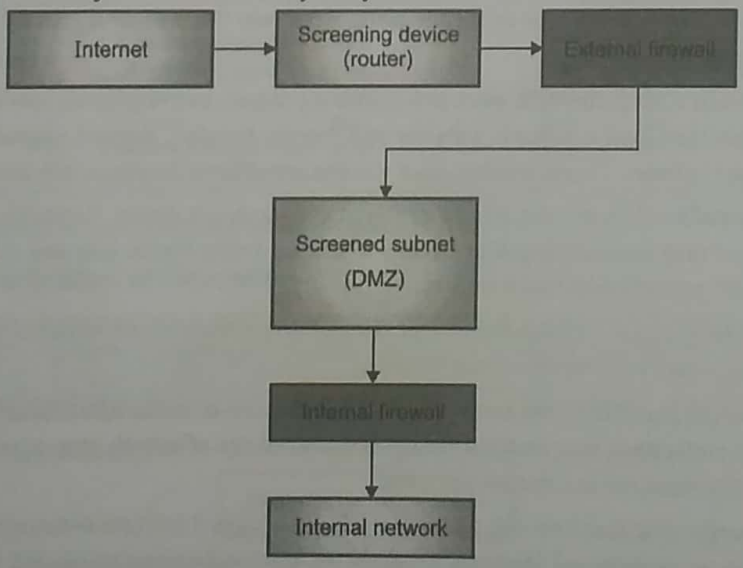


Fig. 5.4.10 : Screened Subnet

(d) Proxy firewall : A proxy firewall stands between the trusted and the untrusted network and takes allow or deny decisions after careful inspection of what is being passed along. Like a regular proxy, the proxy firewall breaks the connection between the source and the destination. After examining the traffic, it self-establishes a connection with the destination and passes the intended traffic to the destination as if the packets were originating from it.

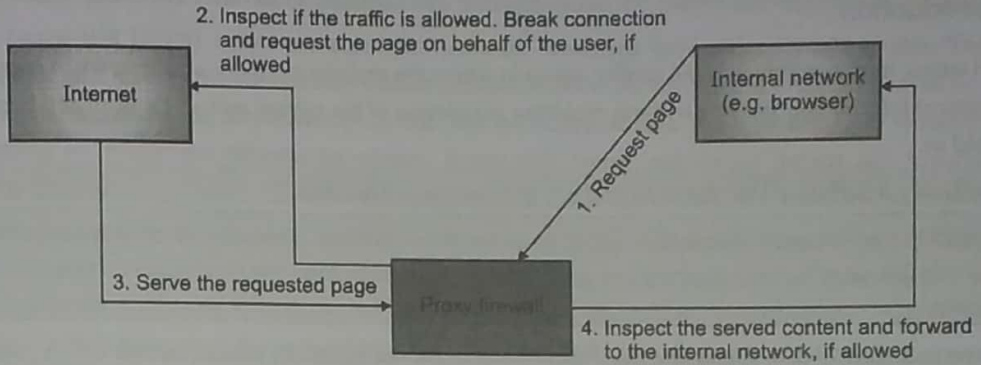


Fig. 5.4.11 : Proxy Firewell

5.4.3(C) Challenges in Managing and Deploying Firewalls

1. **Performance :** Since the traffic (as well as the content) needs to pass through the firewalls, there is a little performance degradation of the network. The adequate traffic examination may add up to a few milliseconds of latency on each packet.
2. **Business agility :** Firewall rules are usually manually added, edited or deleted. The pace of business might be too high to require several changes to the firewall rules frequently. Keeping up with these changes without making errors is difficult.
3. **Costs :** Modern (or advanced) firewalls that provide content and protocol level inspection may be cost-prohibitive for small or medium sized organizations.
4. **Insider attacks :** Firewalls are usually designed and deployed to protect a trusted network from an untrusted network. But, if there were other vulnerabilities (such as a missing OS security patch) that were exploited such that an attacker is already on the trusted network, firewalls might not be able to protect or limit damages to the other resources on the trusted network.
5. **Managing firewalls themselves :** Like your OS, printers or other software or hardware devices, firewalls need to be installed, patched, updated, etc. to remain operational. This adds a management overhead. Additionally, firewalls could have known vulnerabilities that need to be patched else a firewall that itself is lacking protection may not be very useful in providing you the required level of protection.

Note : Irrespective of what challenges or limitations firewalls may have, they are heavily used throughout the industry. You cannot just imagine any network without several firewalls in place to monitor, inspect and manage legitimate traffic and separate it from the illegitimate traffic. So, just know what some of the management or technical challenges are and do not worry too much about them.

5.4.4 Intrusion Detection Systems (IDS)

Q. Explain the significance of an Intrusion Detection System for securing a network. MU - May 16, 6 Marks

Q. Write short notes on IDS. MU - May 19, 4 Marks

Intrusion means to encroach (or to capture) a place. For example, suppose there is a vacant site and you manage to build a small hut there without seeking permission of the site owner, that is precisely what intrusion is. You, as an individual, are trying to intrude on someone's property.

5.4.4(A) Introduction

In digital terms, intrusion refers to the similar situation where the malicious code or attackers try to encroach (forcibly enter and capture) information systems without requiring permission of the system owner. An Intrusion Detection System (IDS) is defined as,

Definition : *A software that helps to find out if a system is breached.*

Note : Breach is a word used in information security domain to describe any form of attack or unauthorized actions. You can use this word to mean anything that refers to the undesired actions and outcomes with respect to information security.

So, in a nutshell, IDS can help you to find out if there were undesired actions or attacks carried out on your information systems. IDS works using various techniques as we will see later in this section. Note here that IDS does not help to prevent the attacks unlike anti-virus. It is only a system that can gather system information and find out if everything looks alright or not.

5.4.4(B) Need for IDS

IDS is one of the software-based security mechanisms that help to protect information system. At a high level, it is needed for the following reasons,

1. **Defense in Depth :** As you saw in the security architecture section, security is about minimizing the damage that can be possibly done. Defense in depth (or the layered approach) of security designing ensures that even if one of the controls is to fail, the overall security of the system would still be possibly healthy. IDS fulfils this need to bring an added layer of protection where any breaches or their possibilities can be identified quickly.
2. **Automate intrusion detection :** Imagine that you have a large set of machines, say 1,000 and more. How would you inspect each and every machine and find out if there were attacks or attempts to attack it? IDS helps you to automate this need and alert you when it detects any threat or likely a breach.
3. **Corrective actions :** Learning from threats or breaches that the IDS identifies, you can take corrective actions on your infrastructure design and could possibly strengthen its security. You might have some unprotected areas in your infrastructure that can be highlighted with the use of IDS.

5.4.4(C) Types of IDS

Broadly speaking, IDS can be classified based on **what** it monitors and **how** it monitors.

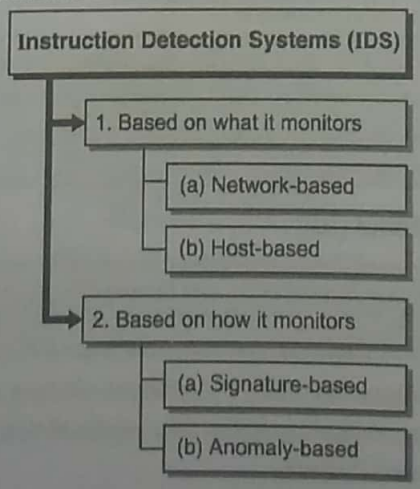


Fig. 5.4.12 : Types of IDS

1. **Based on what it monitors :** IDS can be classified into Network-based IDS (NIDS) and Host-based IDS (HIDS).

(a) **Network-based IDS (NIDS) :** Network-based IDS evaluate intrusions from the networking side. They watch all network traffic as it reaches the various information systems. If there are any alerting situations based on the network traffic analysis, it notifies the administrator to take the corrective actions. NIDS do not have visibility into what's actually going on within the information system. It can only watch and detect threats and breaches from the networking viewpoint.

(b) **Host-based IDS (HIDS) :** Host-based IDS are typically installed on the individual information systems and then they watch for suspicious activities occurring on the system. System entities such as system services and processes, system files, privileged user actions, downloads, etc. are closely monitored to detect any undesired activities. HIDS do not have visibility into what's going on at the networking side of the system. It can only watch and detect activities with respect to individual machines only.

2. **Based on how it monitors** : IDS can be classified into Signature-based and Anomaly-based.

(a) **Signature-based :** Like banks and other organizations use human signature to validate requests and transactions, similarly Signature-based IDS has a pre-loaded database of various attack signatures (patterns of a possible attack). When it watches the activities, it constantly compares the activities' patterns with that in the database. If a match is found, it raises an alert. If you notice, there are 3 things to understand here:

(i) Signature based IDS can only detect attacks if it already and historically knows about an attack pattern.

(ii) For new types of attack, signature-based IDS would not raise alerts.

(iii) It is important for you to update the signature definitions time to time (like how you do in anti-virus system).

(b) **Anomaly-based :** Anomaly typically means "deviation from routine". For example, if you wake up at 7 AM every day and one day you wake up at 4 AM, that is an anomaly situation. If I were to plot your wake-up time graph, 4 AM would show up away from your regular wake-up time. That 4 AM point on the graph is called outlier (or away from other samples).

Similarly, the Anomaly-based IDS first establishes the baseline (common routine) of activities. It might take up to 2-3 weeks to "learn" what's right for a system. Once the learning phase is over, it would watch out for any activities that are not part of that baseline and raise alerts. If you notice, there are 3 things to understand here as well :

(i) It does not require signature and hence can possibly detect new attacks.

(ii) It requires a learning period during which the system should have undergone all possible activities.

(iii) If you plan to use the system for other purposes, you need to retrain the IDS.

5.4.4(D) Limitations and Challenges of IDS

1. **Does not prevent attacks :** As you understand, IDS can only detect and raise alerts when it finds a likelihood of a breach. It cannot prevent or block the breach from happening.

2. **High rate of false alerts (noise) :** IDS might generate a lot of false alerts. It could happen so for example, when there is a new traffic from a source that IDS has not seen before. You need to spend your resources to take a note of each alert and appropriately deal with it – either fix it or ignore it.

3. **Complex systems :** IDS systems are typically complex in nature and require regular administrative actions and tuning for adequate operations.

4. **Bypassing IDS :** Advanced attackers know what actions and activities a version and brand of IDS can detect and what not. They tune their activities to bypass such detection mechanisms and go undetected.

Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

[A] Network Security Basics

Q. 1 Write a short note on network security. **(4 Marks)**

[B] TCP/IP Vulnerabilities (Layer wise)

Q. 2 Describe packet sniffing and protection against it. **(8 Marks)**

Q. 3 Describe ARP spoofing and protection against it. **(8 Marks)**

Q. 4 Describe port scanning, its techniques and protection against it. **(8 Marks)**

Q. 5 Describe IP spoofing and protection against it. **(8 Marks)**

Q. 6 Describe DNS spoofing and protection against it. **(8 Marks)**

Q. 7 Describe DDoS attack and protection against it. **(8 Marks)**

Q. 8 Describe the types of DDoS attacks. **(8 Marks)**

Q. 9 Write a short note on botnet. **(4 Marks)**

[C] Internet Security Protocols

Q. 10 What is SSL? List its goals. **(6 Marks)**

Q. 11 With a block diagram, give a brief Overview of SSL protocol. **(8 Marks)**

Q. 12 Describe SSL Record Layer Protocol. **(8 Marks)**

Q. 13 Describe SSL Alert Protocol. **(8 Marks)**

Q. 14 Describe SSL Handshake Protocol. **(8 Marks)**

Q. 15 What is HTTPS? Why do we need it? **(4 Marks)**

Q. 16 Compare HTTP and HTTPS. **(8 Marks)**

Q. 17 List the Motivation / Benefits of using HTTPS. **(6 Marks)**

Q. 18 Write a short note on Security Association. **(4 Marks)**

Q. 19 Describe IPSec modes of operation. **(8 Marks)**

Q. 20 List theapplicationsof IPSec. **(4 Marks)**

Q. 21 List the benefits of IPSec. **(4 Marks)**

Q. 22 List the usage of IPSec. **(4 Marks)**

Q. 23 List the steps involved in the working of IPSec. **(4 Marks)**

Q. 24 Describe IPSec Authentication Header (AH). **(8 Marks)**

Q. 25 Describe IPSec Encapsulating Security Payload (ESP). **(8 Marks)**

Q. 26 Describe Internet Security Association and Key Management Protocol (ISAKMP). **(8 Marks)**

Q. 27 Describe Internet Key Exchange (IKE). **(8 Marks)**

[D] Secure Email

Q. 28 What is Pretty Good Privacy (PGP)? Explain the concept of "Web of Trust". **(8 Marks)**

Q. 29 Describe PGP Services. **(8 Marks)**

Q. 30 Describe the Radix-64 conversion process in PGP. **(8 Marks)**

Q. 31 List the various algorithms used in PGP and their purpose. **(6 Marks)**

Q. 32 What is S/MIME? What services does it provide? **(6 Marks)**

Q. 33 List the various algorithms used in S/MIME and their purpose. **(4 Marks)**

Q. 34 Write a short note on S/MIME Cryptographic Message Syntax (CMS). **(4 Marks)**

[E] Firewalls

Q. 35 Write a firewall rule of your choice and describe its components. **(8 Marks)**

Q. 36 Classify firewalls based on the OSI Layer. **(4 Marks)**

Q. 37 Classify firewalls based on Form Factor. **(4 Marks)**

Q. 38 Classify firewalls based on the type of Inspection. **(4 Marks)**

Q. 39 Classify firewalls based on architecture. **(8 Marks)**

Q. 40 What are some of the major challenges in managing and deploying firewalls? **(6 Marks)**

[F] Intrusion Detection Systems (IDS)

Q. 41 What is Intrusion Detection Systems (IDS)? Why do you need it? **(6 Marks)**

Q. 42 Describe the types of Intrusion Detection Systems (IDS). **(8 Marks)**

Q. 43 Explain the limitations and challenges of IDS. **(4 Marks)**

❑❑❑