3.8 INFORMATION THEFT

GQ. What is Credential theft? Which malwares are used for credential theft?

OR

GQ. How keyloggers and spyware are used for information theft?

- In some payloads, malware try to gather the data from the infected system so that this data can be further used by the attacker. **Credential theft** (stealing login and password) is the common target. Credential theft is a cybercrime which involves the unlawful attainment of an organizations' or individual's password with the intent to access critical data and information. Credential theft can be considered as often an early stage of a cyber-based attack. It enables attackers to reset passwords and wreak havoc within an organization and remain undetected throughout a network. An organization's resources can be compromised by credential theft even if those resources haven't been directly targeted.
- For stealing the credentials, different methods can be used. One of them is using Keylogger. **Keyloggers** are a type of monitoring software designed to record keystrokes made by a user. Though your password is complex, these keystroke loggers record the information you type into a website or application and send to back to a third party. It is one of the oldest forms of cyber threat. Criminals use keyloggers to steal personal or financial information such as banking details. This information, they can then sell or use for profit. However, there are legitimate uses of keylogging within businesses to troubleshoot, improve user experience, or monitor employees. There are many legitimate software which are designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computer. Law enforcement and intelligence agencies also uses keylogging for surveillance purposes.
- Spyware is another malware which secretly records information about a user and forwards it to third parties. It secretly observes activity on a device and send those observations to a snooper. That data can be used to track your activity online and that information can be sold to marketers. The information gathered may cover files accessed on the computer, a user's online activities or even user's keystrokes. Spyware can also be used to steal personal information, such as account passwords and credit card numbers, which can result in identity theft and fraud.

Module 3

3.9 PHISHING AND IDENTITY THEFT

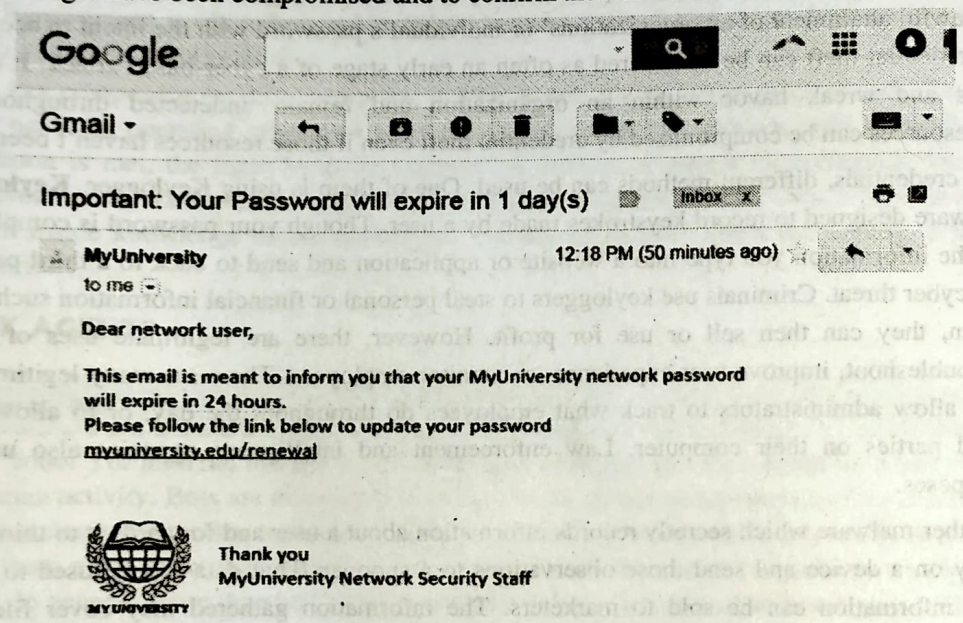
GQ. Explain Phishing attack with example.

- **Identity theft** is tricking consumers into disclosing their personal and financial information credit card or bank account numbers. Such schemes perpetrated through the Internet are called "phishing" for information. **Phishing** is a cyber-attack that uses concealed email as a weapon. The goal is to trick the email recipient into believing that the message is something they want, maybe a request from their bank or a note from someone in their company and to click a link or download an attachment. The recipient is tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system or the revealing of sensitive information.
- The victim usually encounters the link attached in email or a webpage being browsed by him in the following examples:

(1) Apparently, a spoofed email from myuniversity.edu is mass-distributed to many faculty members as shown in Fig. 3.9.1. The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours. After clicking on the link, the user is redirected to myuniversity.edurenewal.com, a fake webpage appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker is monitoring the page, hijacks the original password to gain access to secured areas on the university network.

(2) You have received a friend request from someone who has the same Facebook friends as you. You do not immediately recognize the person but assume the request is legitimate because of the common friends. This new friend then sends you a Facebook message with a link to a video which when clicked installs malware on your computer and potentially the network of your company.

(3) The attacker knows that the victim has made a recent purchase at Apple for example. The attacker sends an email disguised to look like it is from Apple customer support. The email tells the victim that their credit card information might have been compromised and to confirm their credit card details to protect their account.



(1C2)**Fig. 3.9.1 : An example of phishing attempt**

3.10 STEALTHING

GQ. Explain trapdoor and rootkits. How are they used for stealthing?

Stealth indicates malware will use certain techniques to hide its presence on the infected system to avoid detection by antivirus software. And then to provide covert access to that system. This type of payload also attacks the integrity of the infected system.

Trapdoor

- **Trapdoor** is a secret means of bypassing security (normal authentication methods) to gain access to a restricted part of a computer system. Therefore, it is also known as **Backdoor**. It is kind of a secret entry point into a program that allows anyone gain access to any system without going through the usual security access procedures. For example, a hacker may insert a piece of code that would allow them access to a computer or secure area using a password that only they know. Cybercriminals can use a backdoor to steal personal and financial data, install malware, and hijack devices.
- Programmers use Trapdoor legally to debug and test programs. Programmers usually remove trapdoors during program development once the work is done. However, trapdoors can persist in production programs because the programmers may forget to remove them, intentionally leave them in the program for testing, intentionally leave them in the program for maintenance of the finished program, or intentionally leave them in the program as a secret means of access to the component after it becomes an accepted part of a production system.

- Trap doors turns to threats when any dishonest programmers try to gain illegal access. Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoors of the non-criminal variety are useful for helping customers who are locked out of their devices or for troubleshooting and resolving software issues.
- Auditors sometimes request trapdoors in production programs to insert fictitious but identifiable transactions into the system. Then, the auditors trace the flow of these transactions through the system. However, trapdoors must be documented, access to them should be strongly controlled, and they must be designed and used with full understanding of the potential consequences.

Rootkits

- A **rootkit** is a covert computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit". Root refers to the Admin account on Unix/Linux systems, and kit refers to the software components that implement the tool. Originally, a rootkit was a collection of tools that enabled admin level access to a computer/network. But today, rootkits are generally associated with malware. This malicious software alters the regular functionality of an OS on a computer in a stealthy manner. The altering helps the hacker to take full control of the system and the hacker acts as the System administrator on the victim's system. Almost all the rootkits are designed to hide their existence. Since rootkits have complete control over the system, they can modify software and antivirus that could detect rootkits.
- There are also good uses of rootkits like in a honeypot to detect attacks, to enhance emulation software, to enhance security software, for digital rights management enforcement and device anti-theft protection. It is really difficult to detect rootkits. There are no commercial products available that can find and remove all known and unknown rootkits. For rootkit detection, behavioral-based methods can be used where strange behaviour on a computer system can be observed. As well as signature scanning and memory dump analysis can be used. Many times, the only option to remove a rootkit is to completely rebuild the compromised system.

Module 3

3.11 DENIAL OF SERVICE ATTACK

UQ. Explain different types of Denial of Service attacks. MU - Dec. 18

UQ. Define DoS attack. Show the different ways by which this attack can be mounted at various layers. MU - Dec. 19

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources. An attacker, or attackers, attempt to make it impossible for a service to be delivered by interrupting the device's normal functioning. Services affected may include email, websites, online accounts, or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host/network with traffic or sending it information until the target cannot respond or simply crashes, preventing access for legitimate users. A DoS attack is characterized by using a single computer to launch the attack. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

3.11.1 General Methods of DoS Attacks

DoS attacks typically fall in two categories:

(1) Buffer overflow attacks

This is the most common DoS attack targeted at **application layer** of OSI model. In this attack, a memory buffer overflow causes a machine to consume all available hard disk space, memory, or CPU time because more traffic/HTTP requests to a network address is sent than the programmers have built the system to handle. This form of exploit often results in sluggish behaviour, system crashes, or other harmful server behaviours, resulting in denial-of-service.

- When operating in **tunnel mode**, special gateways perform cryptographic processing in addition to the source and destination hosts. Here, many tunnels are created in series between gateways, establishing gateway-to-gateway security.
- When using either of these modes, it's important to provide all gateways with the ability to verify that a packet is real and to authenticate the packet at both ends. Any invalid packets must be dropped.

4.1.1(B) Applications of IPSec

Given below are some applications of IPSec:

1. **Secure remote internet access :** With IP security, we can make a call to our ISP (Internet Service Provider) so as to connect to our organization network in a secure manner. We can also access corporate network facilities or remote servers/desktops.
2. **To Set up communication with other organizations :** As IP security allows connection between various branches of the organization, it can also be used to connect the networks of various organizations in a secure manner.
3. **Secure branch office connectivity :** It allows an organization to set an IPSec enabled network to securely connect all its branches over the internet. This feature reduces the expense of the organization that needs for connecting the organization branches across the cities or countries.

4.1.1(C) Benefits of IPSec

Following are some of the benefits of IPSec:

- It allows fast traveling to have secure access to the corporate network.
- It allows interconnectivity between branches of the organization in a secure and inexpensive manner.
- It works at the network layer, therefore there is no need for changes in the upper layers i.e application layer and transport layer.
- It is transparent to end-users. There is no need for user training, key issuance, and revocation.
- It is also used in a firewall to protect the incoming and outgoing traffic.
- When IP security is configured to work with the firewall, it becomes only an entry-exit point for all traffic to make it extra secure.

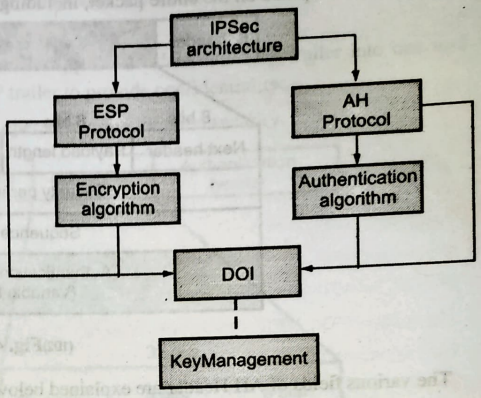
4.1.2 IPSec Architecture

- IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

  (1) Confidentiality (2) Authentication (3) Integrity

- The IPsec specification is scattered across dozens of RFCs and draft IETF documents that can be categorized into the following groups.
  - **IPSec Architecture** : Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.
  - Encapsulating Security Payload (ESP) : ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/ authentication.
  - Authentication Header (AH) : AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated.

- **Internet Key Exchange (IKE) :** This is a collection of documents describing the key management schemes for use with IPsec.
- **Cryptographic algorithms :** This category encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.
- **Domain of Interpretation (DOI) :** DOI contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.



(1D1)**Fig. 4.1.1 : IPSec Architecture**

4.1.3 Protection Mechanism

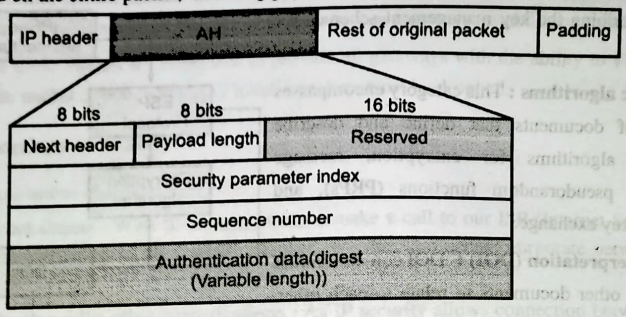
- IPsec provides two security protocols for protecting data:
  (1) Authentication Header (AH)
  (2) Encapsulating Security Payload (ESP)
- An AH protects data with an authentication algorithm. An ESP protects data with an encryption algorithm. Optionally, an ESP protects data with an authentication algorithm. Each implementation of an algorithm is called a **mechanism**.

4.1.3(A) The Authentication Header (AH) Mechanism

Module 4

- The Authentication Header information is added into the packet which is generated by the sender, right between the Network (Layer 3) and Transport (Layer 4) Layer.
- Authentication protects your network, and the data it carries, from tampering. Tampering might be a hacker sitting between the client and server, altering the contents of the packets sent between the client and server, or someone trying to impersonate either the client or server, thus fooling the other side and gaining access to sensitive data.
- To overcome this problem, IPSec uses an *Authentication Header* (AH) to digitally sign the entire contents of each packet. This signature provides 3 benefits:
  (1) **Protection against replay attacks :** If an attacker can capture packets, save them and modify them, and then send them to the destination, then they can impersonate a machine when that machine is not on the network. This is what we call a replay attack. IPSec will prevent this from happening by including the sender's signature on all packets.
  (2) **Protection against tampering :** The signatures added to each packet by IPSec means that one can't alter any part of a packet undetected.
  (3) **Protection against spoofing:** Each end of a connection (e.g. client-server) verifies the other's identity with the authentication headers used by IPSec.

- The AH is computed on the entire packet, including payload (upper layers - 4,5,6,7) and headers of each layer.



(1D2)**Fig. 4.1.2 : AH Header**

- The various fields of AH Header are explained below.

(1) **Next Header :** The Next Header is an 8-bit field that identifies the type of the next payload after the Authentication Header.

(2) **Payload Length :** Specifies the length of AH in 32-bit words.

(3) **Reserved :** 16-bit field is reserved for future use. It must be set to "zero".

(4) **Security Parameter Index (SPI) :** The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the Security Association for this datagram.

(5) **Sequence Number Field :** This unsigned 32-bit field contains a monotonically increasing counter value (sequence number). It is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA.

(6) **Authentication Data :** This is a variable length field that contains the Integrity Check Value (ICV) for this packet. The field must be an integral multiple of 32 bits in length.

☞ AH ALGORITHMS

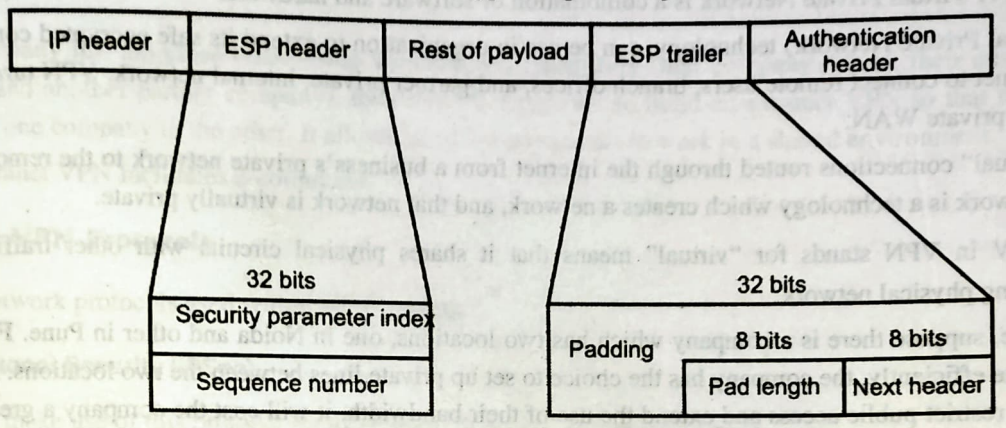
- For point-to-point communication (e.g. client to server), suitable authentication algorithms include keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g. DES) or on one-way hash functions (e.g. MD5 or SHA-1).
- For multicast communication (e.g. between a group of routers), one-way hash algorithms combined with asymmetric signature algorithms are usually used, but they are also more CPU intensive.

4.1.3(B) The Encapsulating Security Payload - ESP

- The Authentication Header (AH) we spoke about will protect your data from tampering, but it will not stop people from seeing it.
- For that, **IPSec** uses an encryption which provides the *Encapsulating Security Payload* (ESP).
- ESP is used to encrypt the entire payload of an **IPSec** packet (Payload is the portion of the packet which contains the upper layer data).
- ESP is a bit more complex than AH because *alone* it can provide authentication, replay-proofing and integrity checking.
- It accomplishes this by adding 3 separate components:

(1) An ESP header (2) An ESP trailer and (3) An ESP authentication block.

- Each of these components contains some of the data needed to provide the necessary authentication and integrity checking.
- To prevent tampering, an ESP client has to sign the ESP header, application data, and ESP trailer into one unit, of course ESP is used to encrypt the application data and the ESP trailer to provide confidentiality.
- The combination of this overlapping signature and encryption operation provides good security.



(1D3)**Fig. 4.1.3 : ESP Header and Trailer**

☞ **ESP Header**

ESP Header consists of two fields, namely, Security Parameter Index and Sequence Number.

- **Security Parameter Index (SPI) :** The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the Security Association for this datagram.
- **Sequence Number :** This unsigned 32-bit field contains a monotonically increasing counter value (sequence number).

☞ **ESP Trailer**

ESP trailer consists of three fields, namely, Padding, Pad Length and Next Header.

- **Padding (for encryption) :** This field ranges from 0 to 2040 bits. It takes different values depending upon the encryption algorithm used.
- **Pad Length :** This is 8-bit field which indicates the number of pad bytes immediately preceding it.
- **Next Header :** The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data Field.

☞ **ESP Authentication**

The Authentication data is a variable length field that contains the Integrity Check Value (ICV) computed over ESP packet minus the Authentication Data.

⏭ 4.2 TRANSPORT LEVEL SECURITY

Transport-level security is a well-known and often used mechanism to secure HTTP Internet and intranet communications. Transport level security can be used to secure web services messages. This section begins with a discussion of VPN, the general requirements for Web security, and then focuses on three standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer: SSL/TLS, HTTPS, and SSH.

4.2.3 Secure Socket Layer (SSL) Architecture

UQ. Write short note on: SSL/TLS. **MU – Nov. 18**

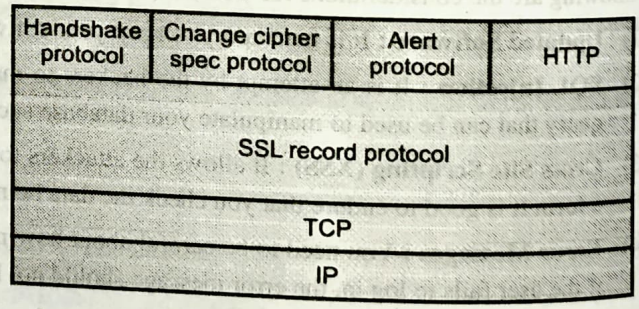
UQ. A user wishes to do online transactions with Amazon.com. Discuss a protocol which can be used to set up a secure communication channel and provide server side and client side authentication. Show the steps involved in the handshake process. **MU – May 19**

- SSL is the secure communications protocol of choice for a large part of the Internet community.
- There are many applications of SSL in existence, since it is capable of securing any transmission over TCP.
- Secure HTTP, or HTTPS, is a familiar application of SSL in e-commerce or password transactions.
- The current version of SSL is version 3.0, released by Netscape in 1999.
- The Internet Engineering Task Force (IETF) has created a similar protocol in an attempt to standardize SSL within the Internet community.
- The need to send sensitive information over the Internet is increasing, and so is the necessity to secure information in transit through the Internet.
- A common application of SSL with a web system is an online store where a client machine is sending a request to a merchant's server.
- In order to apply the SSL protocol to a web system, some requirements must be met. Since the SSL protocol is integrated into most web browsers, and those browsers are normally used to access web applications, no further configuration is required from the client's side of the SSL connection.

(1) Configuration is relatively simple from the server side of the communication equation. First, the web server administrator must acquire a digital certificate. This can be obtained from a Certification Authority (CA) such as VeriSign or RSA Data Security. CAs require that certificates be renewed after a set length of time, as a mechanism for ensuring the identity of the owner of the application's server.

(2) The second requirement is the proper configuration of the web server to allow SSL connections. For example, the iPlanet Web Server has the capability to store multiple certificates for multiple sites on one web server. This capability allows the administrators to prove the identity of each application hosted by this server, and allows the application users to correctly identify each application separately.

(3) The third requirement is to add an accelerator to the web server. SSL accelerators are PCI cards sold by several companies (Cisco, Broadcom, etc.) to speed up the processing actions required to encrypt information for secure communications. SSL connections do slow communications, mostly due to the exchanging of keys and other information during the startup phase of the session. The use of public key cryptography requires a "sizeable amount of information" to be passed between the client and server machines.



(1D5)**Fig. 4.2.2 : SSL Protocol Stack**

- The various protocols in the SSL Protocol Stack are explained below.

(1) Record Layer

- The record layer formats the Alert, Change Cipher Spec, Handshake and application protocol messages.
- This formatting provides a header for each message, and a hash, generated from a Message Authentication Code (MAC) at the end.

- The fields that comprise the five-byte header of the Record Layer are: Protocol Definition (1 byte), Protocol Version (2 bytes) and the Length (2 bytes).
- The protocol messages that follow the header cannot be longer than 16,384 bytes, as specified by the SSL protocol.

(2) ChangeCipherSpec Protocol

- The ChangeCipherSpec layer is composed of one message that signals the beginning of secure communications between the client and server.
- Though the ChangeCipherSpec Protocol uses the Record Layer format, the actual ChangeCipherSpec message is only one byte long, and signals the change in communications protocol by having a value of '1'.

(3) Alert Protocol

- This protocol sends errors, problems or warnings about the connection between the two parties.
- This layer is formed with two fields: Severity Level and Alert Description.
- **Severity Level:**
  - The Severity Level sends messages with a '1' or '2' value, depending on the level of concern.
  - A message with a value of '1' is a cautionary or warning message, suggesting that the parties discontinue their session and reconnect using a new handshake.
  - A message with a value of '2' is a fatal alert message, and requires that the parties discontinue their session.
- **Alert Description**
  - The Alert Description field indicates the specific error that caused the Alert Message to be sent from a party.
  - This field is one byte, mapped to one of twelve specific numbers, and can take on one of the following meanings.
  - Those descriptions that always follow a "fatal" alert message are underlined.

CloseNotify	HandshakeFailure	CertificateRevoked
UnexpectedMessage	NoCertificate	CertificateExpired
BadRecordMAC	BadCertificate	CertificateUnknown
DecompressionFailure	UnsupportedCertificate	IllegalParameter

Module 4

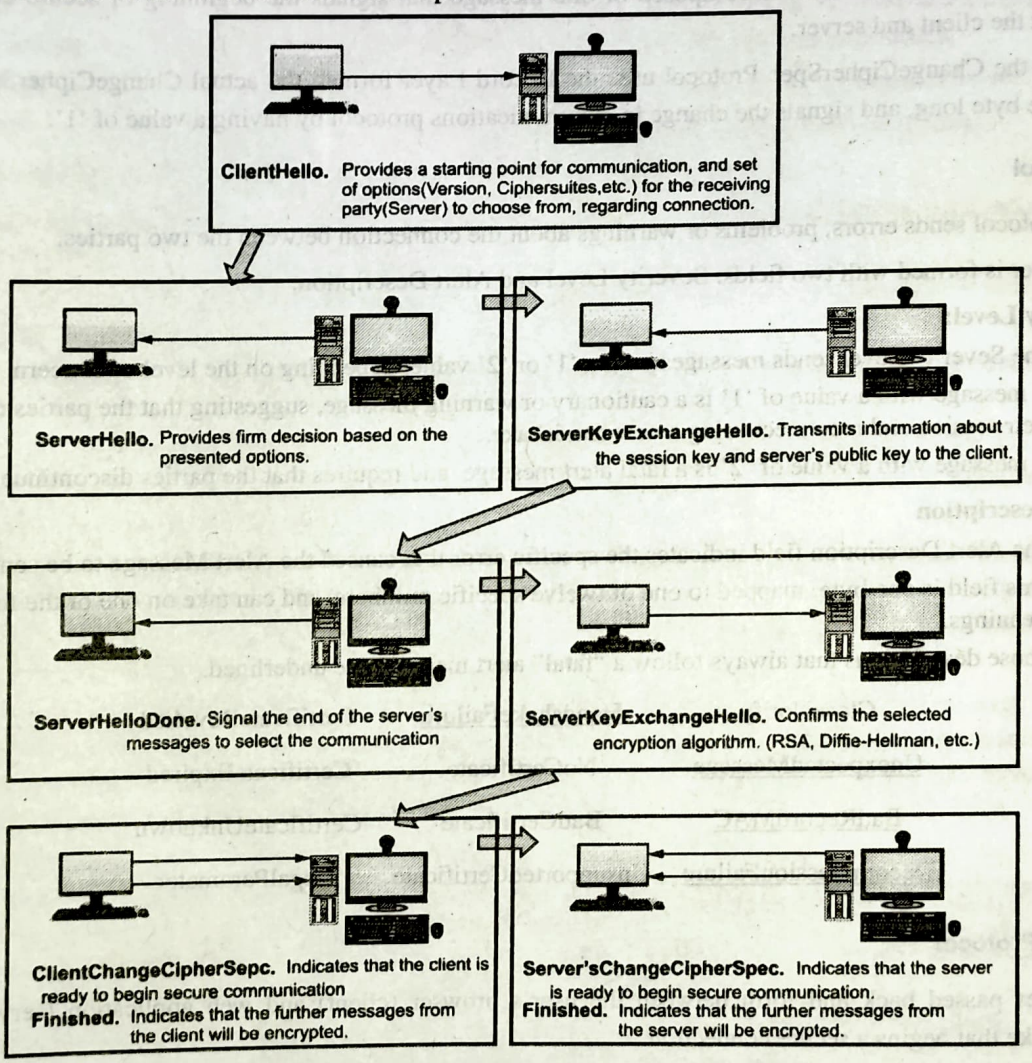
(4) Handshake Protocol

- Messages passed back and forth between the user's browser (client) and web application (server) establish a handshake that begins a secure connection.
- The messages that compose this handshake are: ClientHello, ServerHello, ServerKeyExchange, ServerHelloDone, ClientKeyExchange, ChangeCipherSpec, Finished, ChangeCipherSpec, Finished.
- A visual explanation of the Handshake Protocol is given.
- At the end of this handshake process, the user will see a lock icon in the corner of his/her browser to indicate that a secure protocol has been agreed upon, and is in use by his/her browser and the web e-mail server.
- Each of the message in handshake process is explained in detail.

(a) ClientHello

- The first message is the ClientHello. Since the client machine is requesting the secure communication session, this message involves a set of options that the client is willing to use in order to communicate with the server.

- The option categories are: Version of SSL to be used, CipherSuites supported by the client, and Compression methods used by the client.
- Other information that is included in this message is a 32-byte Random Number that assists the client in establishing encrypted communications, and a SessionID field that is blank.
- This message is generated by the client in the web e-mail example when our user wants to check her email and clicks on the "secure connection" option that is made available on many websites.



(1D6)**Fig. 4.2.3 : Handshake Process in SSL**

(b) ServerHello

- The second message of the SSL handshake is the ServerHello. In this message, the server makes choices based on the ClientHello message.
- The server returns five fields, just like the ClientHello message, but fills in the SessionID, and makes firm decisions on the Version of SSL to be used, the Compression Method and CipherSuite.
- The date and time stamp replaces four bytes of the Random Number field to avoid repeated random values.

(c) ServerKeyExchange

- Now that the server has made decisions for the transmission of data, information must be passed between the parties to determine how data will be encrypted.

- Since no algorithm has been previously agreed upon, this information is sent with no encryption. This means that all communication for this segment must already be in the public domain.
- The server's public key is used to encrypt a separate session key to be maintained for this secure communication. Both the client and server will use this same key to encrypt data to be transmitted.
- To ensure that the communicating parties are who they claim to be, digital certificates are used to provide electronic identification.
- Digital certificates combine the public key and connect it to the name of the certificate owner. Additionally, these certificates contain public keys to certification authorities like RSA Security or VeriSign and an expiration date so that the person receiving the digital certificate can verify the link between the certificate owner and the certification authority.
- The certificate only contains the public key, and should never include the private key, else the private key would be compromised, and the entire purpose of having the digital certificate would be voided.

(d) ServerHelloDone

- Once the Server has completed the ServerKeyExchange message, the client receives a ServerHelloDone message to indicate that the server is through with its messages.
- It is similar to a two-way radio conversation when the sending party says "OVER" to announce that he is done sending a message, and signals the receiving party to acknowledge the message that was sent.

(e) ClientKeyExchange

- Since SSL does not require a client to have public and private keys in order to establish a SSL session, the ClientKeyExchange message contains information about the key that the client and server will use to communicate.
- This is the point where the "man in the middle" attack is mitigated since a masquerader must know the server's private key in order to decrypt this message.
- This message completes the negotiation processes between the client and the server.

Module 4

(f) ChangeCipherSpec

- The two ChangeCipherSpec messages signal the change of data transmission from an insecure state to a secure state.
- As each computer sends the ChangeCipherSpec message, it changes its side of the connection into the agreed-upon secure state.

(g) Finished

- The two messages signaling the final messages of the SSL handshake ensure that three things are verified before the initial handshake is complete.
- These are key information, contents of all previous SSL handshake messages exchanged by the systems and a special value indicating whether the sender is a client or server.

4.2.4 Transport Layer security (TLS)

- TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.
- It is an IETF standard intended to prevent eavesdropping, tampering and message forgery.
- Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP.

(3) **SNMPv3 :** It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

5.1.1 SNMPv3

- The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network.
- Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415.
- **Security Features in SNMP Version 3 :** The security features provided in SNMPv3 are as follows:

(1) **Message integrity :** Ensures that a packet has not been tampered with during transit.

(2) **Authentication :** Determines that the message is from a valid source.

(3) **Encryption :** Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

- SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides.
- Security level is the permitted level of security within a security model.
- A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

Table 5.1.1 : SNMP Version 3 Security Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication.
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

- **Security Threats and SNMPv3 Protection :** Secure management with SNMPv3 protects against five threats:

Threat	SNMPv3 Protection
Masquerade	Verifies the identity of the message's origin by checking the integrity of the data.
Modification of Information	Thwarts accidental or intentional alterations of in-transit messages by checking the integrity of the data, including a time stamp.
Message Stream Modification	Thwarts replay attacks by checking message stream integrity, including a time stamp.
Disclosure	Prevents eavesdropping by protocol analysers, etc., by using encryption.
Unauthorized Access	Verifies operator authorization and protects critical data from intentional and/or accidental corruption by using an access control table (part of policy-based management).

Module 5

- **SNMPv3 Message Format :** The SNMPv3 message consists of the following fields.

(1) ***msgVersion :*** This field contains the SNMP message version. A value 0 is an SNMPv1 message, 1 is an SNMPv2c message, 2 is an SNMPv2 message, and 3 is an SNMPv3 message. The value of message version is used to choose between the different message processing models (SNMPv1, SNMPv2c, or SNMPv3) available in the SNMP engine/entity.

The following fields are part of the SNMPv3 message and are not available in the SNMPv1 or SNMPv2c message.

(2) ***msgID*** **:** This field contains the SNMP message identifier. This is the unique ID associated with the message. The msgID field is different from the reqID field available in the PDU. It is possible that a received PDU that is part of a message cannot be decoded due to security parameters between the SNMP entities. The msgID is used to relate the request with a response during a transaction.

(3) ***msgMaxSize*** **:** This field gives the maximum size of the message which the requesting SNMP entity can accept.

(4) ***msgFlags*** **:** This field contains the message security level. The bit 0 of msgFlags indicates whether a message is authenticated. The bit 1 indicates whether a message uses privacy. The bit 2 indicates whether a report PDU is expected for the message (in case the message is dropped or a response cannot be generated).

(5) ***msgSecurityModel*** **:** This field indicates the security model used to generate the message. It has a value of 3 when USM is used.

(6) ***msgEngineID :*** This field has the SNMPEngineID of the authoritative SNMP entity involved in the transaction. When a request PDU is generated from an SNMP engine, the remote peer (agent for Get request and manager for Trap request) is the authoritative SNMP entity.

(7) ***msgEngineBoots*** **:** This field indicates the number of times the authoritative SNMP entity has booted. This field is used in authenticated message to validate the timeliness of a message.

(8) ***msgEngineTime*** **:** This field indicates the time since the authoritative SNMP entity has been rebooted. This field is used in authenticated messages to validate the timeliness of a message.

(9) ***msgUserName*** **:** This field contains the principal who originated the request. The fields msgUserName and the msgEngineID are used to locate the security data associated with the message from the USM database. This security data is used to authenticate and process the message.

(10) ***msgSecurityParams*** **:** This field contains the security parameters that are security model dependent. It contains the authentication parameters and the privacy parameters for USM. For an AuthPriv message, the authentication parameter has the digest computed for the message using the authentication protocol applicable for the USM entry and the privacy parameter has the salt generated, while encrypting the message using the privacy protocol applicable to the USM entry.

(11) ***contextEngineID*** **:** Within an administrative domain, the contextEngineID uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName.

(12) ***contextName :*** A contextName is used to name a context. Each contextName must be unique within an SNMP entity.

(13) ***PDU*** **:** The SNMP PDU (Protocol Data Unit) is used for communication between the SNMP entities. PDU encapsulates the SNMP request ID, error status, variable bindings, and so on. There are different types of PDUs, such as GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, Response-PDU, SetRequest-PDU, Trap-PDU, InformRequest-PDU, SNMPv2-Trap-PDU, and Report-PDU. The exact format of the PDU depends on the type of the PDU.

Table 5.1.2 : Comparison of SNMPv1, SNMPv2 and SNMPv3

Sr. No.	SNMPv1	SNMPv2c	SNMPv3
1.	It was the first version of SNMP introduced in 1988.	It was second version of SNMP introduced in 1993. It has three flavours SNMPv2p, v2u and v2c where SNMPv2c (C stands for community) is the most commonly used.	It is the latest version of SNMP available currently exist. It was introduced in early 2000.
2.	It supports 32-bit counter architecture.	It supports 64-bit counter architecture.	It supports 64-bit counter architecture.
3.	It does not have any encryption algorithm for sending any critical data in encrypted format. It sends the data as clear text.	It also has the same issue.	It has the optional data encryption mechanism in place, which can be used to encrypt the critical data.
4.	It uses community strings for authentication. Most devices supporting SNMPv1 comes with default community string set to public, which can later be changed to any customized value.	It also uses community string for authentication same as SNMPv1.	SNMPv3 uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.
5.	It has 4 SNMP commands/messages i.e. GET, GETNEXT, RESPONSE, SET and TRAP for communication between SNMP Manager and Agent.	It Introduced 2 more commands/messages i.e. GETBULK and INFORM which are being used along with existing commands.	It also used all 6 commands/messages same as SNMPv2c.
6.	It is easy to setup and configure.	It is also easy to setup and configure.	It is complex to setup and configure.

5.2 NETWORK ACCESS CONTROL (NAC)

- Network access control (NAC) is a security software that businesses can use to control the amount and level of access to their networks.
- According to Wi-Fi engineers and IT security professionals, NAC is the most recommended solution to solve the security challenges of today's Bring Your Own Device (BYOD) and IoT-filled network environments.
- The top benefits of network access control include increasing network visibility, reducing cyber threats, and drastically improving network performance.
- NAC verifies users logging into the network and decides what data they can access and actions they are allowed to perform.
- The user's machine or mobile device (the endpoints) is also examined by NAC.

Module 5

5.2.1 Principle Elements of NAC

NAC systems deal with three categories of components

(1) Access Requestor (AR)

- ARs are also referred to as supplicants, or simply, clients.

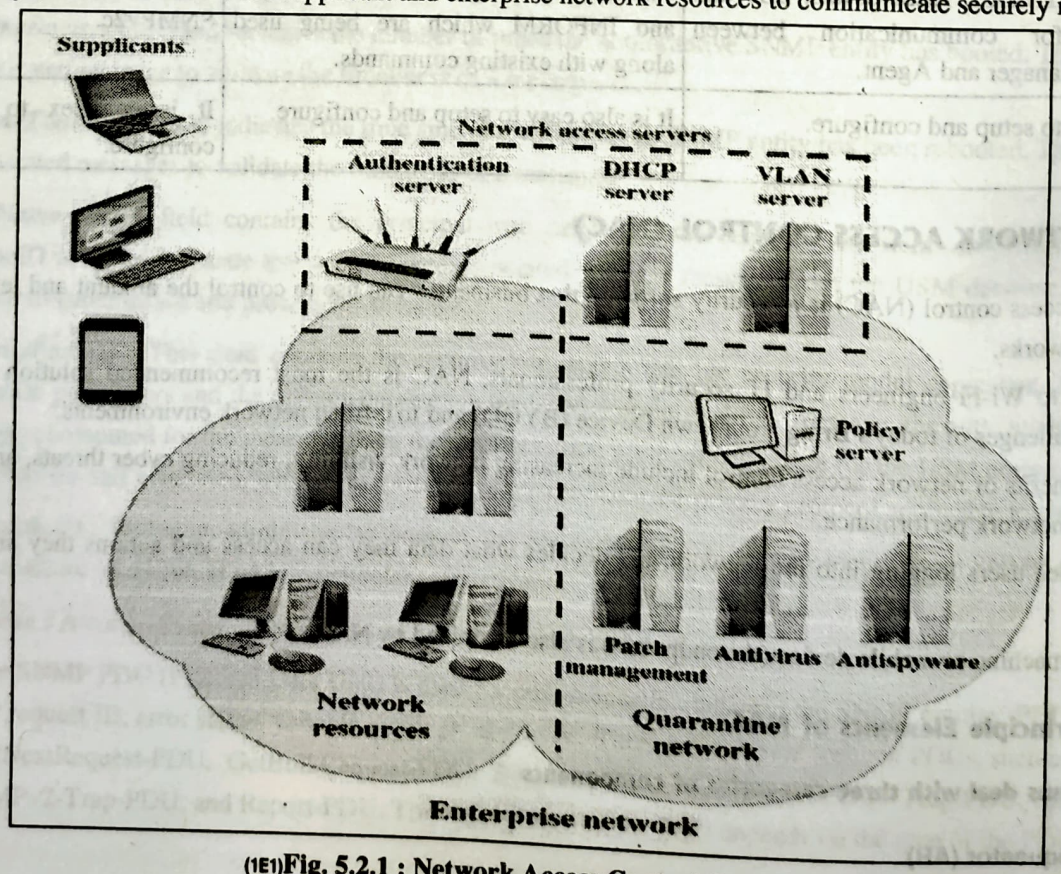
- The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices.

(2) Policy Server

- The policy server decides what access should be given based on the AR's posture and an enterprise's existing policy.
- To assess the host's state, the policy server often consults backend systems such as antivirus, patch management, or a user directory.

(3) Network Access Server (NAS)

- The NAS serves as an access control point for users connecting to an enterprise's internal network from remote locations.
- An NAS is also known as a media gateway, a remote access server (RAS), or a policy server.
- NAS can have its own authentication services or depend on one provided by the policy server.
- Multiple ARs refer to various types of NAS in order to gain access to an enterprise network. Authenticating the AR is usually the first move. Authentication usually entails the use of cryptographic keys and a secure protocol. The NAS can perform authentication or act as a middleman in the authentication process. In the latter case, authentication occurs between the supplicant and an authentication server that is either part of the policy server or can be accessed by the policy server.
- The authentication procedure is used for a variety of reasons. It verifies a supplicant's asserted identity, allowing the policy server to decide if the AR has any access privileges. The authentication exchange can result in the creation of session keys, which will allow the supplicant and enterprise network resources to communicate securely in the future.



(1E1)**Fig. 5.2.1 : Network Access Control Context**

6.2 FIREWALLS

UQ. What is a firewall? Explain different types of firewall. **MU- Nov. 18**

UQ. What is a firewall? Explain different types of firewalls and list their advantages. **MU- May 19**

- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
- Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
- A firewall can be hardware, software, or both.
- It is shown in Fig. 6.2.1.

6.2.1 Working of Firewall

- Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks.
- Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.
- For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."
- Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all. Then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

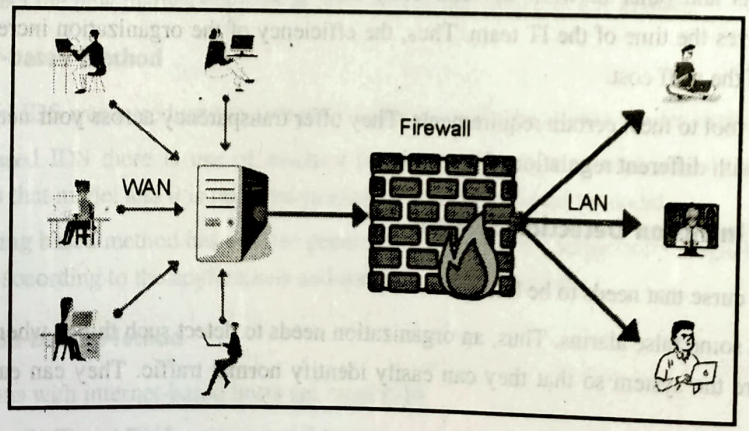


Fig. 6.2.1 : Firewall

6.2.2 Firewall Design Principles

Information systems in companies, government agencies and other organizations have undergone a continuous evolution.

Here are some noteworthy developments :

- Centralized data processing system, with a central mainframe supporting a number of terminals connected directly.
- PCs and terminals are connected to each other and to the mainframe through local area networks (LANs).

- A premise network is made up of many LANs that connect PCs, servers, and possibly a mainframe or two.
- Multiple, geographically dispersed premises networks are linked by a private wide area network (WAN) to form an enterprise-wide network.
- Internet access, in which all of the premises networks are linked to the Internet and can or may not be connected by a private WAN.
- The following are the design goals for a firewall :
- All traffic from inside to outside and vice versa must flow through the firewall. This is achieved by physically blocking all access to the local network except through the firewall.
- Only authorized traffic, as defined by the local security policy, be allowed to let through the firewall. Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is impenetrable. This implies the use of a reliable system with a secure operating system.

6.2.3 Firewall Characteristics

Firewalls use four general techniques to manage access and implement the site's security policy, which are listed below.

(1) **Service control :** Determines whether inbound or outbound Internet resources can be accessed. The firewall can filter traffic based on IP address, protocol, or port number; provide proxy software that receives and interprets each service request before passing it on; or host the server software, such as a Web or mail service, itself.

(2) **Direction control :** Determines the path in which specific service requests are permitted to be initiated and flow through the firewall.

(3) **User control :** Controls access to a service based on the customer who is trying to use it. This functionality is usually only available to users who are within the firewall perimeter (local users). It can also be used to protect incoming traffic from external users, but this includes the use of secure authentication technologies like IPsec.

(4) **Behavioral control :** Controls how specific programs are used. The firewall, for example, may filter e-mail to prevent spam, or it may allow external access to only a portion of the information on a local Web server.

Firewalls strengths / capabilities

(1) They are excellent at enforcing corporate security policies.

(2) They are used to restrict access to specify services.

(3) The majority of firewalls can even provide selective access via authentication functionality.

(4) Firewalls are singular in purpose and do not need to be made between security and usability.

(5) They are excellent auditors.

(6) Firewalls are very good at altering appropriate people of specified events.

Firewalls weakness / limitations

(1) Firewalls cannot protect against what has been authorized.

(2) It cannot stop social engineering attacks or an unauthorized user intentionally using their access for unwanted purposes.

(3) Firewalls cannot fix poor administrative practices or poorly designed security policies.

(4) It cannot stop attacks if the traffic does not pass through them.

(5) They are only as effective as the rules they are configured to enforce.

6.2.4 Types of Firewalls

- A firewall may act as a packet filter.
- It can act as a positive filter, allowing only packets that meet certain criteria to pass through, or as a negative filter, refusing any packet that meets certain criteria.
- Depending on the type of firewall, each packet may be examined for one or more protocol headers, the payload, or the pattern created by a sequence of packets.
- The different configurations of firewalls explained in this section are shown in Fig. 6.2.2.

6.2.4(A) Packet Filtering Firewall

- As the most "basic" and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch.
- Packet filtering firewall is a network security technique that is used to control data flow to and from a network.
- It is a security mechanism that allows the movement of packets across the network and controls their flow on the basis of a set of rules, protocols, IP addresses, and ports.
- The packet filtering firewall analyses for the source and destination IP addresses, source, and destination port numbers, and protocol IDs of IP packets as per an access control list (ACL). The firewall checks for the information contained in the IP, TCP, or UDP header, and then it decides to accept or drop the packet depending upon the ACL.
- The firewall can allow the fragment type packets after comparing the information with the ACL.
- Additionally, it has a default method, set by users, that allows the packets to pass even if these do not qualify with the ACL.
- **Default = discard :** That which is not expressly permitted is prohibited.
- **Default = forward :** That which is not expressly prohibited is permitted.

Advantages

(1) It is fast because it operates on IP addresses and TCP/UDP port numbers alone, ignoring the data contents (payload) of packets.

(2) Due to the fact that packet payload is ignored, application independence exists.

(3) Least expensive than other types of firewalls.

(4) Packet filtering rules are relatively easy to configure.

(5) There are no configuration changes necessary to the protected workstations.

Disadvantages

(1) Packet filtering firewall offers the least security because they allow a direct connection between endpoints through the firewall.

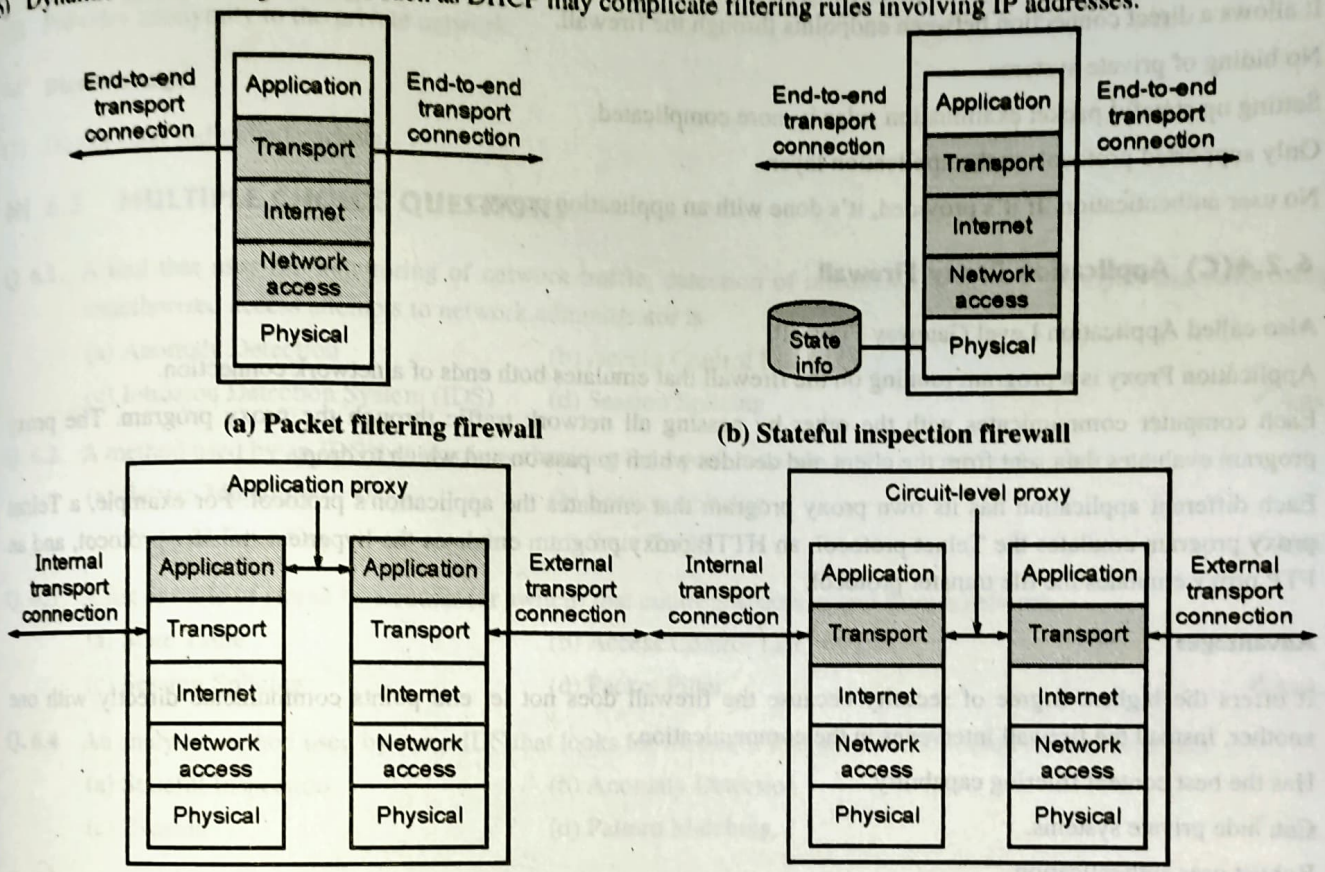
(2) There is no screening of packet payload available. It is impossible to block users from visiting web sites deemed off limits, for example.

(3) Logging of network traffic includes only IP addresses and TCP/UDP port numbers, no packet payload information is available, and IP spoofing can penetrate this firewall.

(4) Complex firewall policies are difficult to implement using filtering rules alone.

(5) There is a reliance on the IP address for authentication rather than user authentication.

(6) Dynamic IP addressing schemes such as DHCP may complicate filtering rules involving IP addresses.



(a) Packet filtering firewall (b) Stateful inspection firewall

(c) Application proxy firewall (d) Circuit-level proxy firewall

Fig. 6.2.2 : Different Configurations of Firewalls

6.2.4(B) Stateful Inspection Firewall

- This approach examines the contents of packets rather than just filtering them, that is, to consider their contents as well as their addresses.
- This type of firewall employs an inspection module, applicable to all protocols, that understands data in the packet intended for other layers, from the network layer (IP headers) up to the application layer.
- Intelligent filtering can effectively combine with the ability to do network-session tracking, to use information about the beginning and end of sessions in filtering decisions and this is known as session filtering.
- The filter uses smart rules, thus enhancing the filtering process and controlling the network session rather than controlling the individual packets.

Advantages

(1) Offers improved security over basic packet filters due to packet examination.

(2) Offers a degree of application independence, based on level of stateful packet examination.

(3) Better logging of activities over basic packet filters.

(4) Good performance.

(5) Configuration changes to the protected workstations are unnecessary.

Disadvantages

(1) It allows a direct connection between endpoints through the firewall.

(2) No hiding of private systems.

(3) Setting up stateful packet examination rules is more complicated.

(4) Only supported protocols at the application layer.

(5) No user authentication. If it's provided, it's done with an application proxy.

6.2.4(C) Application Proxy Firewall

- Also called Application Level Gateway Firewall.
- Application Proxy is a program running on the firewall that emulates both ends of a network connection.
- Each computer communicates with the other by passing all network traffic through the proxy program. The proxy program evaluates data sent from the client and decides which to pass on and which to drop.
- Each different application has its own proxy program that emulates the application's protocol. For example, a Telnet proxy program emulates the Telnet protocol, an HTTP proxy program emulates the hypertext transfer protocol, and an FTP proxy emulates the file transfer protocol.

Advantages

(1) It offers the highest degree of security because the firewall does not let end points communicate directly with one another, instead the firewall intervenes in the communication.

(2) Has the best content filtering capability.

(3) Can hide private systems.

(4) Robust user authentication.

(5) Offers the best logging of activities.

(6) Policy rules are usually easier than packet filtering rules.

Disadvantages

(1) Performance around 100 Mbps, which tends to be the worst type of firewalls.

(2) Must have a proxy for every protocol. Failure to have a proxy may prevent a protocol from being handled correctly by the firewall.

(3) TCP is the preferred transport. UDP may not be supported.

(4) Limited transparency, clients may need to be modified. Setting up the proxy server in a browser, for example.

(5) No protection from all protocol weaknesses.

6.2.4(D) Circuit Gateway Firewall

- This can be a stand-alone system or it can be the specialized functions performed by an application-level gateway for certain applications.
- It does not permit end-to-end TCP connection; rather, the gateway sets two TCP connections.
- A typical use of the circuit-level gateway is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level for outbound connections.

Advantages

(1) Comparatively inexpensive.

(2) Provides anonymity to the private network.

Disadvantage

(1) Do not filter individual packets.

6.3 MULTIPLE CHOICE QUESTIONS

Q. 6.1 A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator is

(a) Anomaly Detection (b) Access Control List (ACL)

(c) Intrusion Detection System (IDS) (d) Session Splicing ✓**Ans. (c)**

Q. 6.2 A method used by an IDS that involves checking for a pattern to identify unauthorized activity is

(a) Pattern Matching (b) Session Splicing

(c) Protocol Decoding (d) State Table ✓**Ans. (a)**

Q. 6.3 A list or table of stored by a router (or switch) that controls access to and from a network.

(a) State Table (b) Access Control List (ACL)

(c) Session Splicing (d) Packet Filter ✓**Ans. (b)**

Q. 6.4 An analysis method used by some IDS that looks for instances that are not considered normal behavior.

(a) Stateful Inspection (b) Anomaly Detection

(c) Evasion (d) Pattern Matching ✓**Ans. (b)**

Q. 6.5 What are the different ways to classify an IDS?

(a) Zone based (b) Host & Network based

(c) Network & Zone based (d) Level based ✓**Ans. (b)**

Q. 6.6 What are the characteristics of anomaly based IDS?

(a) It models the normal usage of network as a noise characterization

(b) It doesn't detect novel attacks

(c) Anything distinct from the noise is not assumed to be intrusion activity

(d) It detects based on signature ✓**Ans. (a)**

Q. 6.7 What are the characteristics of signature based IDS?

(a) Most are based on simple pattern matching algorithms

(b) It is programmed to interpret a certain series of packets

(c) It models the normal usage of network as a noise characterization

(d) Anything distinct from the noise is assumed to be intrusion activity ✓**Ans. (a)**

- Since no algorithm has been previously agreed upon, this information is sent with no encryption. This means that all communication for this segment must already be in the public domain.
- The server's public key is used to encrypt a separate session key to be maintained for this secure communication. Both the client and server will use this same key to encrypt data to be transmitted.
- To ensure that the communicating parties are who they claim to be, digital certificates are used to provide electronic identification.
- Digital certificates combine the public key and connect it to the name of the certificate owner. Additionally, these certificates contain public keys to certification authorities like RSA Security or VeriSign and an expiration date so that the person receiving the digital certificate can verify the link between the certificate owner and the certification authority.
- The certificate only contains the public key, and should never include the private key, else the private key would be compromised, and the entire purpose of having the digital certificate would be voided.

(d) ServerHelloDone

- Once the Server has completed the ServerKeyExchange message, the client receives a ServerHelloDone message to indicate that the server is through with its messages.
- It is similar to a two-way radio conversation when the sending party says "OVER" to announce that he is done sending a message, and signals the receiving party to acknowledge the message that was sent.

(e) ClientKeyExchange

- Since SSL does not require a client to have public and private keys in order to establish a SSL session, the ClientKeyExchange message contains information about the key that the client and server will use to communicate.
- This is the point where the "man in the middle" attack is mitigated since a masquerader must know the server's private key in order to decrypt this message.
- This message completes the negotiation processes between the client and the server.

(f) ChangeCipherSpec

- The two ChangeCipherSpec messages signal the change of data transmission from an insecure state to a secure state.
- As each computer sends the ChangeCipherSpec message, it changes its side of the connection into the agreed-upon secure state.

(g) Finished

- The two messages signaling the final messages of the SSL handshake ensure that three things are verified before the initial handshake is complete.
- These are key information, contents of all previous SSL handshake messages exchanged by the systems and a special value indicating whether the sender is a client or server.

Module 4

4.2.4 Transport Layer security (TLS)

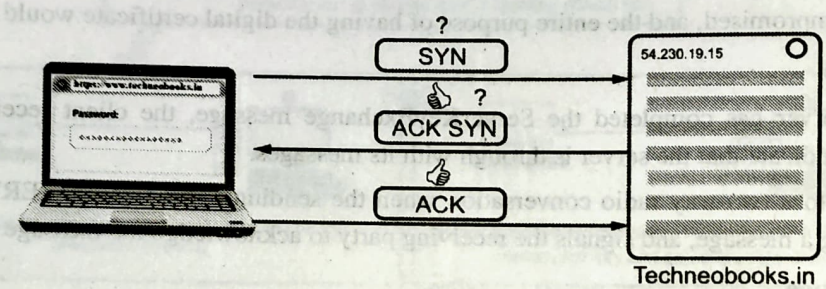
- TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.
- It is an IETF standard intended to prevent eavesdropping, tampering and message forgery.
- Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP.

- The Transport Layer Security (TLS) protocol adds a layer of security on top of the TCP/IP transport protocols.
- TLS uses both symmetric encryption and public key encryption for securely sending private data, and adds additional security features, such as authentication and message tampering detection.
- TLS adds more steps to the process of sending data with TCP/IP, so it increases latency in Internet communications. However, the security benefits are often worth the extra latency.

4.2.4(A) Working of TLS

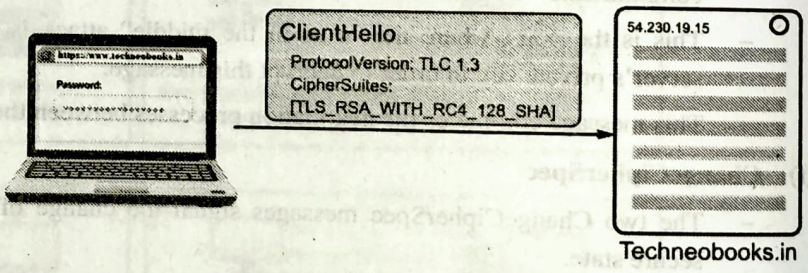
Let's step through the process of securely sending data with TLS from one computer to another. We'll call the sending computer the **client** and the receiving computer the **server**.

(1) **TCP handshake :** Since TLS is built on top of TCP/IP, the client must first complete the 3-way TCP handshake with the server.



(1D7)**Fig. 4.2.4 : TLS Handshake Process**

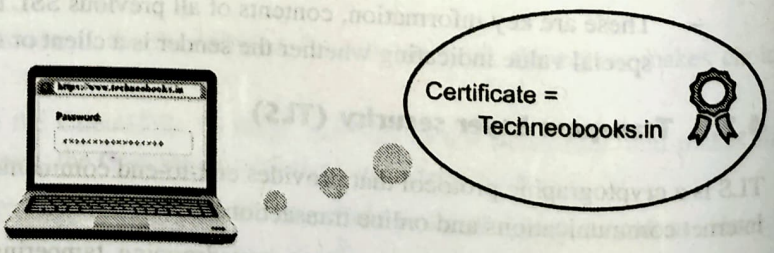
(2) **TLS initiation :** The client must notify the server that it desires a TLS connection instead of the standard insecure connection, so it sends along a message describing which TLS protocol version and encryption techniques it'd like to use.



(1D8)**Fig. 4.2.5 : TLS Initiation**

(3) **Server confirmation of protocol :** If the server doesn't support the client's requested technologies, it will abort the connection. That may happen if a modern client is trying to communicate with an older server. As long as the server does support the requested TLS protocol version and other options, it will respond with a confirmation, plus a digital certificate that contains its public key.

(4) **Certificate verification :** The server's digital certificate is the server's way of saying "Yes, I really am who you think I am". If the client doesn't believe the certificate is legit, it will abort the connection, since it doesn't want to send private data to an imposter. Otherwise, if the client can verify the certificate, it continues on to the next step.



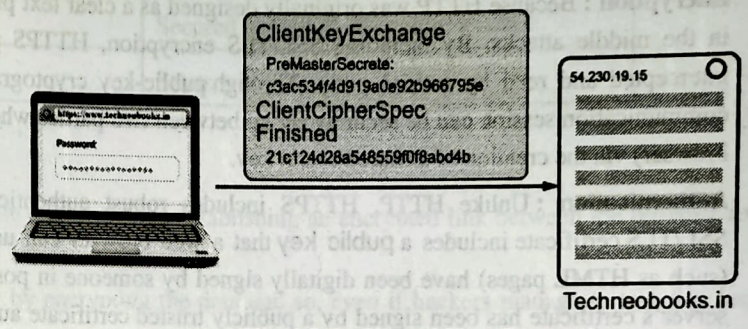
(1D9)**Fig. 4.2.6 : Digital Certificate Verification**

(5) Shared key generation

The client now knows the public key of the server, so it can theoretically use public key encryption to encrypt data that the server can then decrypt with its corresponding private key.

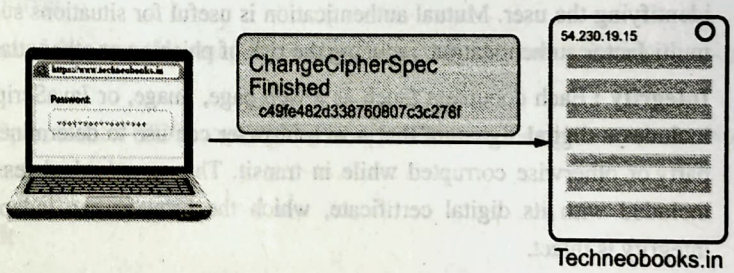
However, public key encryption takes much more time than symmetric encryption due to the more difficult arithmetic operations involved. When possible, computers prefer to use symmetric encryption to save time. Fortunately, they can! The computers can first use public key encryption to privately generate a shared key, and then they can use symmetric encryption with that key in future messages.

The client starts off that process by sending a message to the server with a pre-master key, encrypted with the server's public key. The client computes the shared key based on that pre-master key (as that is more secure than sending along the actual shared key) and remembers the shared key locally. The client also sends a "Finished" message whose contents are encrypted with the shared key.



(1D10)**Fig. 4.2.7 : Shared Key Generation**

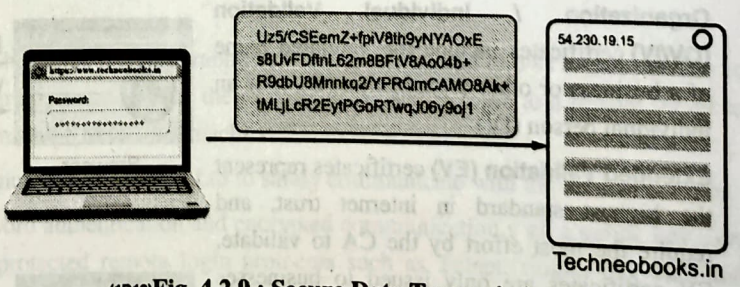
(6) Server confirmation of shared key: The server can now compute the shared key based on the pre-master key, and attempt to decrypt the "Finished" message with that key. If it fails, it aborts the connection. As long as the server can successfully decrypt the client's message with the shared key, it sends along a confirmation and its own "Finished" message with encrypted contents.



(1D11)**Fig. 4.2.8 : Server Confirmation of Shared Key**

(7) Send secure data : Finally, the client securely sends the private data to the server, using symmetric encryption and the shared key.

- Oftentimes, the same client needs to send data to a server multiple times, like when a user fills out forms on multiple pages of a website. In that case, the computers can use an abbreviated process to establish the secure session.
- In this way, both computers must go through many steps to set up secure communication with TLS.



(1D12)**Fig. 4.2.9 : Secure Data Transmission**

4.2.5 HTTPS

- **HTTPS (Hypertext Transfer Protocol Secure)** is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication.
- HTTPS is specified by RFC 2818 and uses port 443 by default instead of HTTP's port 80.

6.1 INTRUSION DETECTION SYSTEM (IDS)

- An intrusion detection system (IDS) is a software application or device that monitors network traffic for anomalous patterns.
- These patterns indicate potentially suspicious activity.
- An IDS also monitors for violations of established network policy (like the transmission of unusually large amounts of data).
- Upon detecting anomalies or violations, the IDS has two possible responses.

(1) **Send alerts :** Passive IDS solutions respond by raising alerts through email or text. They may also notify a security information and event management (SIEM) system. A SIEM will correlate the event with other security events to help determine if this is an issue or not.

(2) **Defensive action :** Active IDS also known as an intrusion prevention system (IPS), not only sends alerts, but also has extra security features. These features give active IDS solutions the ability to (a) modify access control lists on firewalls to block the suspicious traffic, (b) kill processes on the internal system involved in the communications, or (c) redirect traffic to a honeypot to further assess the threat.

- Fig. 6.1.1 depicts the intrusion detection system in the network.

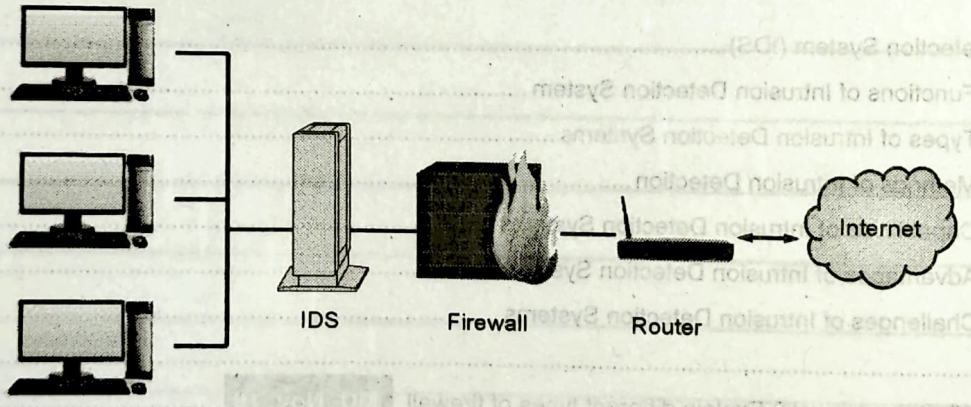


Fig. 6.1.1 : Intrusion Detection System

6.1.1 Functions of Intrusion Detection System

Following are the functions of IDS, which make it popular among its various clients.

- It keeps an eye on the functions of routers, firewalls, key management servers, and files.
- It provides continuous support to the users.
- Arranges the various audit trails and other logs.
- It generates an alarm when security breaches are detected.
- Once the suspicious activity is detected, they block the server immediately.

(5) Hybrid Intrusion Detection System

- Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system.
- In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.
- Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.
- Prelude is an example of Hybrid IDS.

6.1.3 Methods of Intrusion Detection

There are three methods to detect the intrusion in the network.

(1) Signature-based Method	(2) Anomaly-based Method
(3) Reputation-based Method	

(1) Signature-based Method

- Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's 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.
- Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

(2) Anomaly-based Method

- Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.
- In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.
- Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

(3) Reputation-based Method

- Communications with internet-based hosts are monitored.
- The external host's IP and DNS are compared against a reputation database of potentially malicious hosts.
- External hosts with low reputation scores can be blocked from connecting with your network.

6.1.4 Capabilities of Intrusion Detection Systems

Security teams use one or more of the following IDS capabilities to detect potential intrusion:

(1) **Deep packet inspection :** Network traffic is inspected in detail and is used in conjunction with signature-based detection. This level of inspection requires network traffic to be decrypted.

(2) **File integrity monitoring :** Data files on critical endpoints and servers are monitored for changes, which may indicate malware is being installed or security configurations are being modified.

(3) **System call monitoring :** Applications, processes, and system libraries can be monitored to determine if activity is sanctioned or not.

(4) **Configuration monitoring :** Agents can be used to monitor the configuration of specific systems, watching for changes that may alter the networking security state of the system.

(5) **User-friendly data parsing :** The details about the state of the network traffic and system are almost always compiled in a format that's difficult to decipher. IDS solutions parse this data to provide IT and security teams with intelligible information that can be easily understood.

(6) **Data visualization:** Transforming data into visualizations in an intuitive user interface helps both experienced IT professionals and those without expertise to manage system security and make intelligent decisions.

(7) **Signature database :** Many vendors offer an extensive signature database of malware and other attacks that can be used by the IDS solution to find threatening activity.

(8) **Notifications :** Email, text, and event log-based alerts go to IT and security teams, informing them of potential, attempted, or in-progress malware infections, cyberattacks, and data breaches.

6.1.5 Advantages of Intrusion Detection Systems

The intrusion detection system provides a wide range of benefits to an organization.

- It keeps a check on all the incoming and outgoing network activity. It detects any signs of intrusion in the system. Its main function is to send an alert immediately when it identifies any activity in the system.
- It recognizes various security incidents. Also helps to examine the quantity and types of such suspicious attacks. It also detects bugs and issues relating to their network device configurations. An organization can use this information and fix the problem. They may change their security system or take some effective measures.
- IDS sensors identify hosts and other network devices. They tend to examine the data within the network and the operating system. This saves the time of the IT team. Thus, the efficiency of the organization increases. This will help the organization to cut off the staff cost.
- IDS can also be used as a tool to meet certain requirements. They offer transparency across your network. Thus, it helps the organization to meet with different regulations for security.

6.1.6 Challenges of Intrusion Detection Systems

IDS comes with a certain curse that needs to be known.

- At times they might send some false alarms. Thus, an organization needs to detect such things when they are first using it. They need to configure the system so that they can easily identify normal traffic. They can easily distinguish any malicious activity.
- Such false alarms sometimes can create some serious issues. IDS might skip a threat to such recognized traffic.
- In such a scenario, the IT teams have no sign that an attack might take place. Thus, they will fail to take any steps. Thus, it is advisable to be careful about such abnormal behaviors.
- IDS help to monitor the network. But they don't block or resolve such issues. The organization needs to hire the right personnel to look after such threats and take immediate action.
- IDS are suffering from a serious issue. They fail to detect a new suspected intrusion, as the new malware does not display the pattern of previous unusual behavior. Thus, the IDS must take steps to detect such new behavior. So that an organization can take immediate precautions to such a threat.

(3) **SNMPv3 :** It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

5.1.1 SNMPv3

- The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network.
- Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415.
- **Security Features in SNMP Version 3 :** The security features provided in SNMPv3 are as follows:
  (1) **Message integrity :** Ensures that a packet has not been tampered with during transit.
  (2) **Authentication :** Determines that the message is from a valid source.
  (3) **Encryption :** Scrambles the content of a packet to prevent it from being learned by an unauthorized source.
- SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides.
- Security level is the permitted level of security within a security model.
- A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

Table 5.1.1 : SNMP Version 3 Security Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication.
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

- **Security Threats and SNMPv3 Protection :** Secure management with SNMPv3 protects against five threats:

Threat	SNMPv3 Protection
Masquerade	Verifies the identity of the message's origin by checking the integrity of the data.
Modification of Information	Thwarts accidental or intentional alterations of in-transit messages by checking the integrity of the data, including a time stamp.
Message Stream Modification	Thwarts replay attacks by checking message stream integrity, including a time stamp.
Disclosure	Prevents eavesdropping by protocol analysers, etc., by using encryption.
Unauthorized Access	Verifies operator authorization and protects critical data from intentional and/or accidental corruption by using an access control table (part of policy-based management).

Module 5

Table 5.1.2 : Comparison of SNMPv1, SNMPv2 and SNMPv3

Sr. No.	SNMPv1	SNMPv2c	SNMPv3
1.	It was the first version of SNMP introduced in 1988.	It was second version of SNMP introduced in 1993. It has three flavours SNMPv2p, v2u and v2c where SNMPv2c (C stands for community) is the most commonly used.	It is the latest version of SNMP available currently exist. It was introduced in early 2000.
2.	It supports 32-bit counter architecture.	It supports 64-bit counter architecture.	It supports 64-bit counter architecture.
3.	It does not have any encryption algorithm for sending any critical data in encrypted format. It sends the data as clear text.	It also has the same issue.	It has the optional data encryption mechanism in place, which can be used to encrypt the critical data.
4.	It uses community strings for authentication. Most devices supporting SNMPv1 comes with default community string set to public, which can later be changed to any customized value.	It also uses community string for authentication same as SNMPv1.	SNMPv3 uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.
5.	It has 4 SNMP commands/messages i.e. GET, GETNEXT, RESPONSE, SET and TRAP for communication between SNMP Manager and Agent.	It Introduced 2 more commands/messages i.e. GETBULK and INFORM which are being used along with existing commands.	It also used all 6 commands/messages same as SNMPv2c.
6.	It is easy to setup and configure.	It is also easy to setup and configure.	It is complex to setup and configure.

5.2 NETWORK ACCESS CONTROL (NAC)

- Network access control (NAC) is a security software that businesses can use to control the amount and level of access to their networks.
- According to Wi-Fi engineers and IT security professionals, NAC is the most recommended solution to solve the security challenges of today's Bring Your Own Device (BYOD) and IoT-filled network environments.
- The top benefits of network access control include increasing network visibility, reducing cyber threats, and drastically improving network performance.
- NAC verifies users logging into the network and decides what data they can access and actions they are allowed to perform.
- The user's machine or mobile device (the endpoints) is also examined by NAC.

Module 5

5.2.1 Principle Elements of NAC

NAC systems deal with three categories of components

(1) Access Requestor (AR)

- ARs are also referred to as supplicants, or simply, clients.

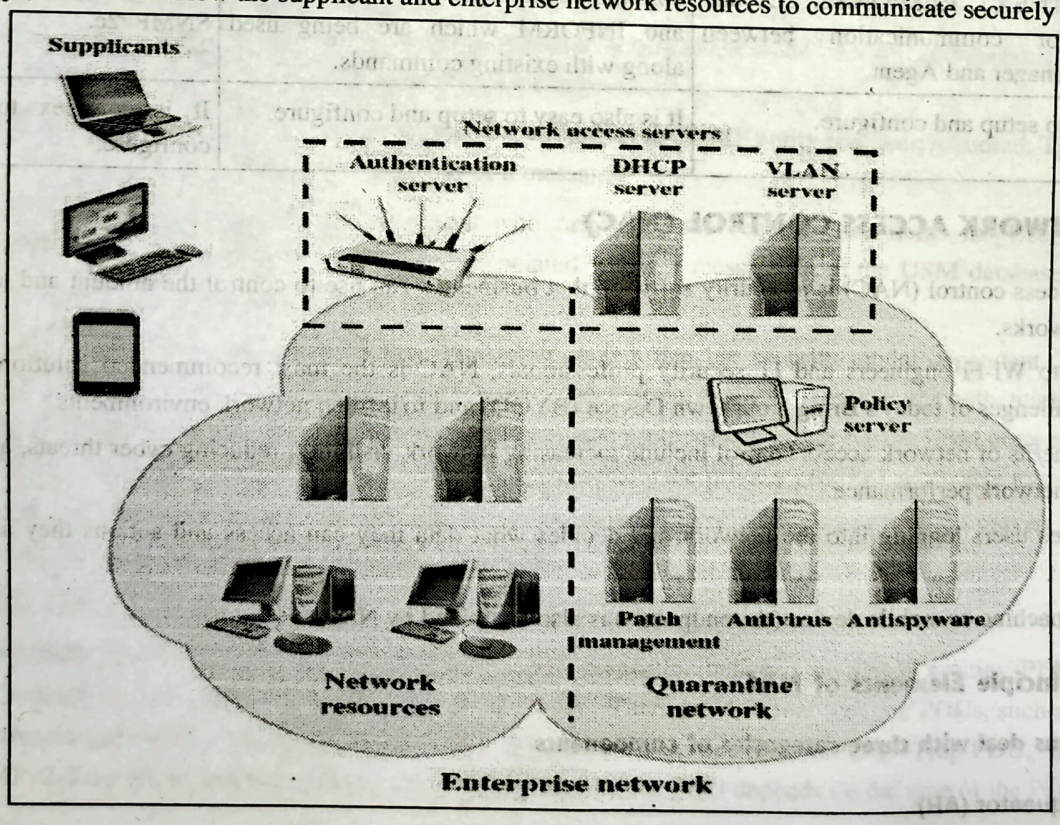
- The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices.

(2) Policy Server

- The policy server decides what access should be given based on the AR's posture and an enterprise's existing policy.
- To assess the host's state, the policy server often consults backend systems such as antivirus, patch management, or a user directory.

(3) Network Access Server (NAS)

- The NAS serves as an access control point for users connecting to an enterprise's internal network from remote locations.
- An NAS is also known as a media gateway, a remote access server (RAS), or a policy server.
- NAS can have its own authentication services or depend on one provided by the policy server.
- Multiple ARs refer to various types of NAS in order to gain access to an enterprise network. Authenticating the AR is usually the first move. Authentication usually entails the use of cryptographic keys and a secure protocol. The NAS can perform authentication or act as a middleman in the authentication process. In the latter case, authentication occurs between the supplicant and an authentication server that is either part of the policy server or can be accessed by the policy server.
- The authentication procedure is used for a variety of reasons. It verifies a supplicant's asserted identity, allowing the policy server to decide if the AR has any access privileges. The authentication exchange can result in the creation of session keys, which will allow the supplicant and enterprise network resources to communicate securely in the future.



(1E1)**Fig. 5.2.1 : Network Access Control Context**

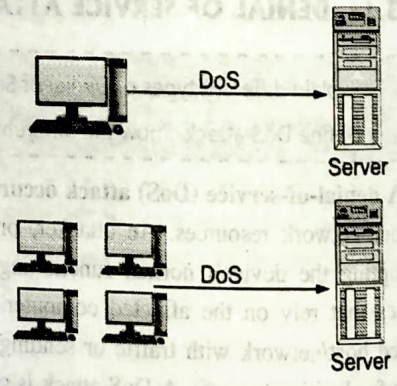
(2) Flood attacks

The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic and thus resulting in denial-of-service.

- **ICMP (Internet Control Message Protocol) flood :** This denial-of-service attack is based on crushing a target with ICMP (ping) packets. By flooding a target with more pings than it can respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack. This attack leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to intensify the traffic. This attack is also known as the **Smurf attack** or **Ping of death**.
- **SYN flood :** A three-way handshake method is used in TCP/IP network to create a connection between a local host/client and server. SYN flood attack occurs when an attacker sends a request to connect to the target server but never completes the handshake. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests for legitimate users. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

3.11.2 DoS and DDoS Attack

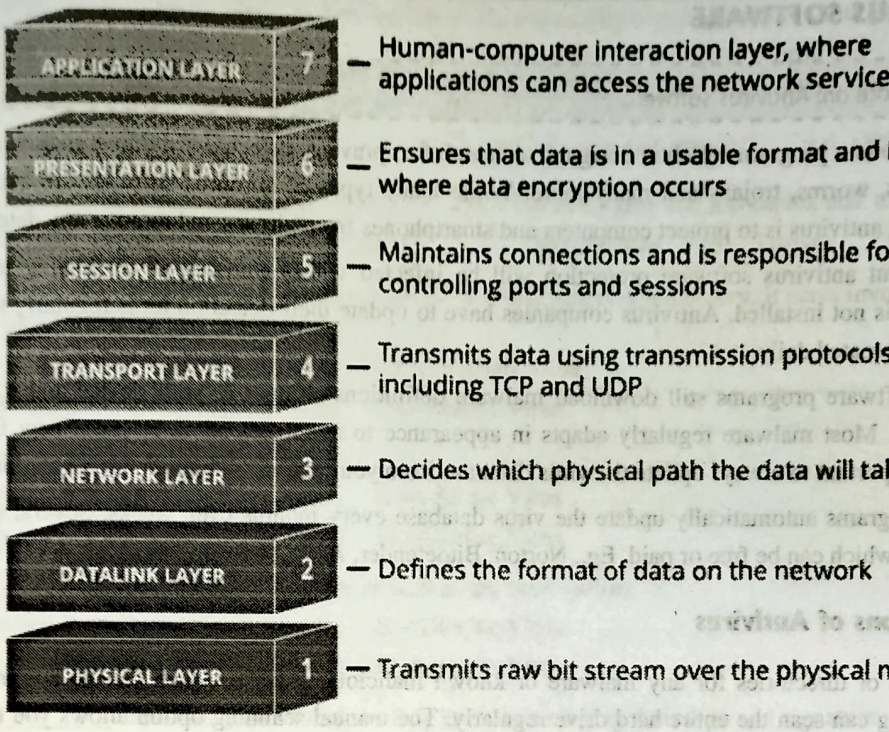
- An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. In a DoS attack, it's one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems at once.
- A DDoS attack occurs when multiple systems organize a synchronized DoS attack to a single target. DDoS attackers often leverage the use of a botnets. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software.
- Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.
- Since hosts are distributed, the attacker can leverage the greater volume of machine to execute a seriously disruptive attack. Also, the location of the attack is difficult to detect due to the random distribution of attacking systems. At the same time, the true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.



(1C3)Fig. 3.11.1: DoS attack and DDoS attack

3.11.3 DoS Attacks on Various Layers of OSI Model

The OSI model is a conceptual framework used to describe network connectivity in seven distinct layers. Let's discuss how DoS attacks can be mounted on every layer of OSI model.



Module 3

(1C4)**Fig. 3.11.2 : OSI reference model**

- **Application layer** protocols have two main categories: user protocols and support protocols. User protocols provide services to users directly, such as through HTTP, SMTP/POP, FTP, IMAP, XMPP, SSH, IRC, etc. Support protocols aim to provide common system functions. Such as DNS, NTP, SNMP, BOOTP/DHCP, TLS/SSL, RTP, SIP, etc. Any of these protocols can be a means or an object to launching a DoS attack. Buffer overflow attacks are the common approach to attack on this layer.
- DoS attacks at the **presentation layer** include malformed Secure Socket Layer (SSL) requests. SSL DDoS Attacks can be Protocol misuse attacks where the protocol being used is exploited or it can be SSL Traffic Floods. These attacks send a large amount of traffic over an established secure channel that results in exhausting the bandwidth and other resources.
- The **session layer** includes the synchronisation and termination of connections over the network. An attacker takes advantage of log-in and log-off protocols to launch DoS attacks in the session layer; for instance, launching a Telnet DoS attack. The attacks included are Telnet brute force attack and Telnet sniffing.
- **Layer 4** DoS attacks are based on transmission and generation of an enormous volume of traffic to deactivate or totally block the availability of services or resources in the network for legitimate clients. These attacks usually include misuse of TCP and UDP protocols for flooding resources in the network.
- **Layer 3** of the OSI model is responsible for data packets' routing and switching to various networks and LANs. It depends on IP, ARP, RIP and ICMP protocols, relying on routers. DoS attacks at the Network layer include injecting the victim's network with a large amount of traffic that it cannot handle. Smurf and ICMP flood attacks are applied here.
- Denial of Service Attack at the **Data Link Layer** ensures that the data is effectively handed over to the physical layer. Attacks such us Collision, Unfairness and Exhaustion are based on attacking data frame detection, medium access control, multiplexing of data-streams and error control. There are well-known attacks at Data Link Layer.
- Jamming attacks are one of the most significant attacks in denial of service attacks on **physical layer.**

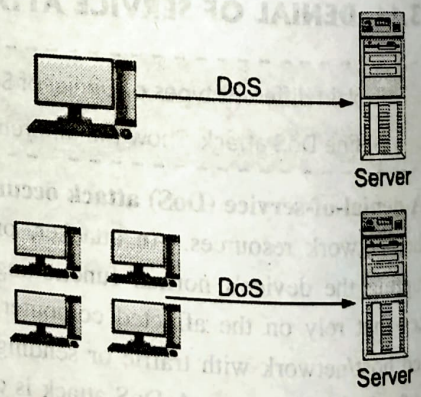
(2) Flood attacks

The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic and thus resulting in denial-of-service.

- **ICMP (Internet Control Message Protocol) flood :** This denial-of-service attack is based on crushing a target with ICMP (ping) packets. By flooding a target with more pings than it can respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack. This attack leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to intensify the traffic. This attack is also known as the **Smurf attack** or **Ping of death**.
- **SYN flood :** A three-way handshake method is used in TCP/IP network to create a connection between a local host/client and server. SYN flood attack occurs when an attacker sends a request to connect to the target server but never completes the handshake. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests for legitimate users. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

3.11.2 DoS and DDoS Attack

- An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. In a DoS attack, it's one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems at once.
- A DDoS attack occurs when multiple systems organize a synchronized DoS attack to a single target. DDoS attackers often leverage the use of a botnets. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software.
- Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.
- Since hosts are distributed, the attacker can leverage the greater volume of machine to execute a seriously disruptive attack. Also, the location of the attack is difficult to detect due to the random distribution of attacking systems. At the same time, the true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.



(1C3)Fig. 3.11.1: DoS attack and DDoS attack

3.11.3 DoS Attacks on Various Layers of OSI Model

The OSI model is a conceptual framework used to describe network connectivity in seven distinct layers. Let's discuss how DoS attacks can be mounted on every layer of OSI model.