1. **Explain MIME, S/MIME in detail?**

MIME: Multipurpose Internet Mail Extension

-> MIME is a standard which is proposed by Bell Communication in 1991 in order to expand the limited capabilities of email (Email can send messages only in NVT 7-bits ascii format).

=> Email has simple structure.

-> In short, MIME is a supplementary protocol / or a add on which allows non-ascii data to be sent through email (via SMTP).

=> It allows users to exchange different kinds of data files on internet like audio, video, images, etc.

-> MIME is an extension to the internet email protocol

-> Email Messages with MIME formatting are typically transmitted with standard protocols like SMTP, POP (Post Office Protocol) and IMAP(Internet Message Access Protocol).

-> Although MIME was designed mainly for SMTP, its content types are also important in communication protocols.

Ex: In http protocol for WWW, servers insert a MIME header field at the beginning of any web transmission.

**MIME Header:**   
-> It is added to the original e-mail header section to define transformation. There are *five headers* that we add to the original header:

1. **MIME-Version –** Defines the version of the MIME protocol. It must have the parameter *Value 1.0*, which indicates that message is formatted using MIME.
2. **Content-Type –**Type of data used in the body of the message. They are of different types like text data (plain, HTML), audio content, or video content.
3. **Content-Type Encoding –** It defines the method used for encoding the message. Like 7-bit encoding, 8-bit encoding, etc.
4. **Content Id –** It is used for uniquely identifying the message.
5. **Content description –** It defines whether the body is actually an image, video, or audio.

Why MIME? (Limitations of SMTP Protocol)

-> SMTP has a very simple structure.

-> SMTP can only send the messages in NVT 7-bits ascii format.

-> It cannot be used for languages that don’t support 7-bits ascii format such as French, German, etc. So, in order to make SMTP more wide, we use MIME.

-> It cannot be used to send binary files or video or audio data.

**S/MIME: Secure Multipurpose Internet Mail Extension**

-> S/MIME is an upgrade version of MIME protocol.

-> provides security for commercial emails.

-> It is widely accepted method for sending digital signed and encrypted messages i.e, it allows us to digitally sign our email to verify ourselves as the legitimate sender.

-> S/MIME is based on asymmetric key encryption.

-> FUNCTION:

i) Authentication

ii) Message integrity

iii) Non-repudiation

iv) privacy

v) data security

So, In short S/MIME is a protocol used to encrypt emails and digitally sign them.

It provides two security services:

1. Digital signature (provides authentication and non-repudiation)
2. Message encryption (provides confidentiality and data-integrity)

2. How is PGP will protect Emails?

Pretty Good Privacy (PGP)

* widely used de facto secure email
* developed by Phil Zimmermann
* selected best available crypto algorithms to use
* integrated into a single program
* on Unix, PC, Macintosh and other systems
* originally free, now also have commercial versions available

PGP Operation – Authentication

1. sender creates message

2. use SHA-1 to generate 160-bit hash of message

3. signed hash with RSA using sender's private key, and is attached to message

4. receiver uses RSA with sender's public key to decrypt and recover hash code

5. receiver verifies received message using hash of it and compares with decrypted hash code.

PGP Operation – Confidentiality

1. sender generates message and 128-bit random number as session key for it

2. encrypt message using CAST-128 / IDEA / 3DES in CBC mode with session key

3. session key encrypted using RSA with recipient's public key, & attached to message.

4. receiver uses RSA with private key to decrypt and recover session key

5. session key is used to decrypt message.

PGP Operation – Confidentiality & Authentication

* can use both services on same message
* create signature & attach to message
* encrypt both message & signature
* attach RSA/ElGamal encrypted session key

PGP Operation – Compression

* by default PGP compresses message after signing but before encrypting
  + so can store uncompressed message & signature for later verification
  + & because compression is non deterministic
* uses ZIP compression algorithm

PGP Operation – Email Compatibility

* when using PGP will have binary data to send (encrypted message etc)
* however email was designed only for text
* hence PGP must encode raw binary data into printable ASCII characters
* uses radix-64 algorithm
  + maps 3 bytes to 4 printable chars
  + also appends a CRC
  + PGP also segments messages if too big

3. Email security?

* email is one of the most widely used and regarded network services
* currently message contents are not secure
  + may be inspected either in transit
  + or by suitably privileged users on destination system

Email Security Enhancements

* confidentiality
  + protection from disclosure
* authentication
  + of sender of message
* message integrity
  + protection from modification
* non-repudiation of origin
  + protection from denial by sender

Pretty Good Privacy (PGP)

* widely used de facto secure email
* developed by Phil Zimmermann
* selected best available crypto algorithms to use
* integrated into a single program
* on Unix, PC, Macintosh and other systems
* originally free, now also have commercial versions available

PGP Operation – Authentication

1. sender creates message

2. use SHA-1 to generate 160-bit hash of message

3. signed hash with RSA using sender's private key, and is attached to message

4. receiver uses RSA with sender's public key to decrypt and recover hash code

5. receiver verifies received message using hash of it and compares with decrypted hash code.

PGP Operation – Confidentiality

1. sender generates message and 128-bit random number as session key for it

2. encrypt message using CAST-128 / IDEA / 3DES in CBC mode with session key

3. session key encrypted using RSA with recipient's public key, & attached to message.

4. receiver uses RSA with private key to decrypt and recover session key

5. session key is used to decrypt message.

**S/MIME: Secure Multipurpose Internet Mail Extension**

-> S/MIME is an upgrade version of MIME protocol.

-> provides security for commercial emails.

-> It is widely accepted method for sending digital signed and encrypted messages i.e, it allows us to digitally sign our email to verify ourselves as the legitimate sender.

-> S/MIME is based on asymmetric key encryption.

-> FUNCTION:

i) Authentication

ii) Message integrity

iii) Non-repudiation

iv) privacy

v) data security

4. Explain Trusted systems in detail

* Systems used to enhance the ability to defend against intruders and malicious programs.
* based on levels of security.

**Multilevel Security**

* When multiple categories or levels of data are defined, the requirement is referred to as multilevel security.
* Typically use Mandatory Access Control.
* Primary Security Goal: Confidentiality (ensures that information do not flow to those not cleared for that level).
* MLS means like whether the data is confidential or not so that it may helps the organization to encrypt them.
* Example of security levels
  + Top Secret
  + Secret
  + Confidential
  + Unclassified
  + In this case Top Secret > Secret > Confidential > Unclassified
* Access control: Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.
* Data access control is a technique used to regulate employees access to files in an organization.
* Data Access Control
  + General models of access control:
    - Access matrix
    - Access control list
    - Capability list
* A multilevel secure system must enforce:

No read up

No write down

Trojan Horse

* It is a type of malware (malicious software) designed to provide unauthorized, remote access to a user’s computer.
* Trojan horses do not have the ability to replicate themselves like viruses.
* With the help of Trojan, an user can get access to the Trojan horse infected computer and would be able to access the data.

Indications of Trojan Attack

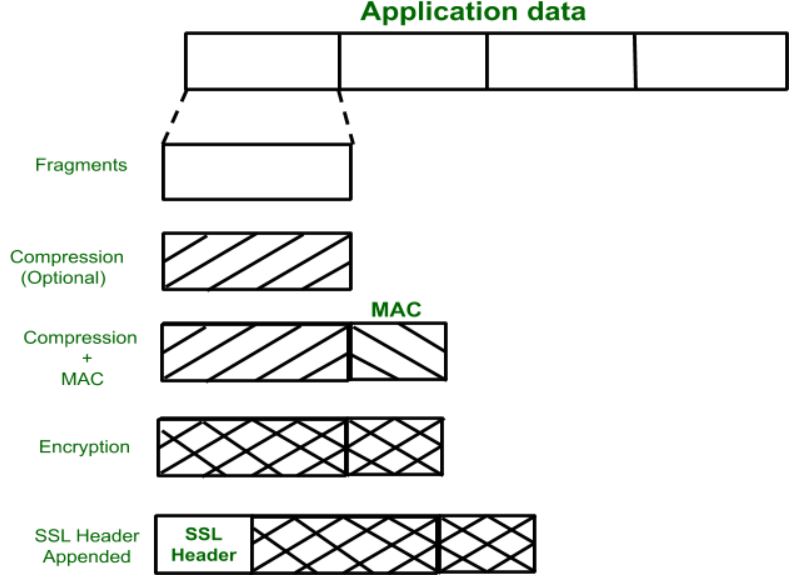
* Browser redirects to unknown pages.
* Anti virus is disabled.
* Strange pop ups or chat messages appear on the system.
* The computer shuts down automatically.
* Ctl+Alt+Del stops working.
* Printer prints documents automatically.

5. Explain SSL record protocol and handshake protocol in detail?

**SSL Record Protocol:**   
SSL Record provides two services to SSL connection.

* Confidentiality
* Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

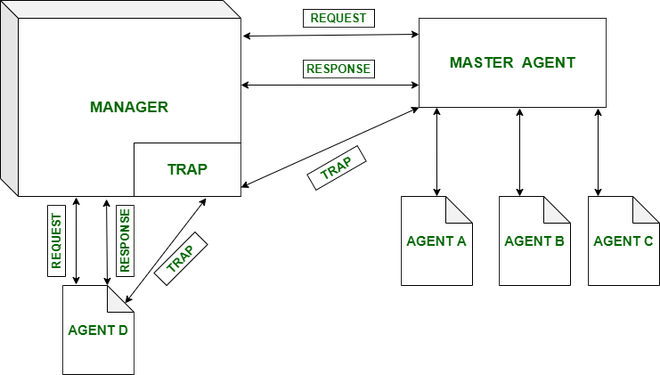


**Handshake Protocol:**   
Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

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

6. Explain SNMPV3 protocol in detail

SNMP stands for [**Standard Network Management Protocol**](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/). It is basically an Internet Standard Protocol which is used for monitoring and organizing information about the devices on IP network by sending and receiving requests. This protocol is used for organizing information from devices like switches, modems, routers, servers, printers etc.



**Special Features about SNMPv3 :**

* v3 is the latest version of SNMP which involves great management services with enhanced security.
* The SNMPv3 architecture makes the use of User-based Security Model (USM) for security of the messages & the View-based Access Control Model (VACM) for accessing the control over the services.
* SNMP v3 security models supports authentication and encrypting.
* SNMPv3 supports Engine ID Identifier, which uniquely identifies each SNMP identity. The Engine ID is used to generate a unique key for authenticating messages.
* v3 provides secure access to the devices that send traps by authenticating users & encrypting data packets which are sent across the network.
* It also introduces the ability to configure and modify the SNMP agent using SET for the MIB objects. These commands enable deletion, modification, configuration and addition of these entries remotely.
* USM – For facilitating remote configuration and management of the security module.
* VACM – For facilitating remote configuration & management for accessing the controlling module.

**SNMPv3 Architecture :**

The architecture of the v3 consists of –

* Data definition language,
* Definition of MIB
* Protocol definition
* Security and administration.

**Mechanism of version 3 :**

* 16-byte key between sender & receiver
* Triple Data Encryption Standard
* Advanced Encryption Standard
* Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode
* MD5 message digest algorithm

7. How IDS will helpful to secure different systems?

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

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

1. **Network Intrusion Detection System (NIDS)**
2. **Host Intrusion Detection System (HIDS)**
3. **Protocol-based Intrusion Detection System (PIDS)**
4. **Application Protocol-based Intrusion Detection System**
5. **Hybrid Intrusion Detection System**

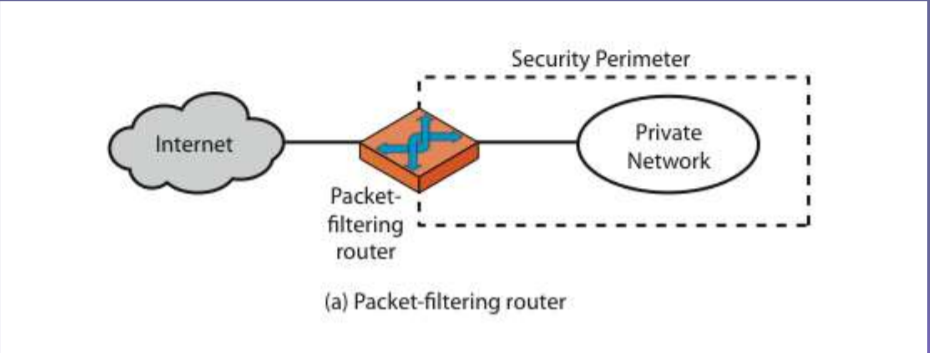
**Detection Method of IDS:**

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.
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.

8. Explain different types of Fire Walls in detail with configuration

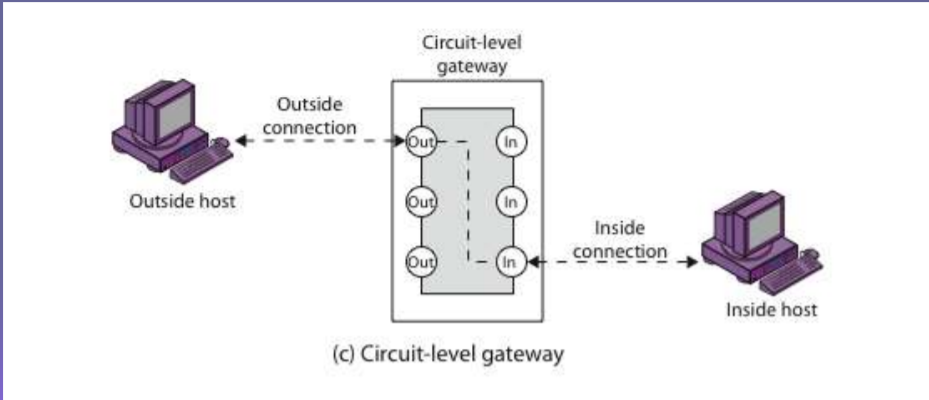
Firewalls – Packet Filters

* simplest, fastest firewall component
* foundation of any firewall system
* examine each IP packet (no context) and permit or deny according to rules
* hence restrict access to services (ports)
* possible default policies
  + that not expressly permitted is prohibited
  + that not expressly prohibited is permitted



Firewalls - Circuit Level Gateway

* relays two TCP connections
* imposes security by limiting which such connections are allowed
* once created usually relays traffic without examining contents
* typically used when trust internal users by allowing general outbound connections
* SOCKS is commonly used



Firewalls - Application Level Gateway (or Proxy)

* have application specific gateway / proxy
* has full access to protocol λ user requests service from proxy
* proxy validates request as legal λ then actions request and returns result to user
* can log / audit traffic at application level ¬ need separate proxies for each service
* some services naturally support proxying
* others are more problematic

