# UNIT-6

# Network Security and Public Key Infrastructure

## ⊛. Overview of Network Security:

Network Security is the process of taking preventive measures to protect the underlying networking infrastructure from unauthorized access, misuse, modification or destruction. Due to increase in internet-connected devices, the number of attackers are also increased. Attackers try to find and exploit vulnerabilities. There are many peoples who attempt to damage our internet-connected devices, or violate our privacy. So, ensuring network security has became important part in this modern networking world.

We can ensure network security by using strong and complex passwords. The passwords should not be simple, default and eaisly guessable ones. Access Control, Application Security, Firewalls, Virtual Private Network (VPN) etc. are some of the types of network security that helps to make our connection secure and safe to some extent.

## ⊛. Digital Certificates and X.509 certificates:

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity. The mostly used standard format for digital certificates is X.509.

X.509 certificate: X.509 is a standard defining the format of public key certificates. An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the hostname/domain or organization or individual contained within the certificate. The X.509 certificate is signed by a publicly trusted Certified Authority or self-signed. A typical X.509 standard digital certificate has following format:

| | |
|---|---|
| Version | Version of X.509 (mostly uses version 3). |
| Serial number | Unique number set by a CA. |
| Issuer | Name of the CA |
| Subject issued certificate | Name of a receiver of the certificate. |
| Validity period | Period in which certificate will valid. |
| Public key algorithm information of the subject of the certificate | Algorithm used to sign the certificate with digital signature. |
| Digital signature of the issuing authority | Digital signature of the certificate signed by CA. |
| Public Key | Public key of the subject |
| Extension | Optional Extensions (e.g, Key usage). |

## ⊛. Certificate Lifecycle Management:

Digital certificates ensure the secure transmission of sensitive information between client and server through identity authentication and data encryption. A large deployment of digital certificates and private keys must be managed. Managing multiple certificates with different expiry dates issued by different vendors challenges even the most sophisticated enterprise.

Many organizations use Managed Public Key Infrastructure (MPKI) initiative to reduce the strain. However, much of an MPKI initiative involves resource-intensive tasks.

## ⊛. PKI trust models, PKIX: → [Imp] describe purpose of PKI trust model? (2 to 3 marks)

The public key infrastructure is defined as the set of hardware, software, people, policies. and procedures needed to create, manage, store, distribute and revoke digital certificates based on asymmetric cryptography. The principal objective for developing a PKI is to enable secure, convenient, and efficient acquisition of public keys.

### PKIX (Public Key Infrastructure X.509):

PKIX model consists of following elements:

i) End Entity: A generic term term used to denote end users, devices or any other entity that can be identified in the subject field of a public key certificate.

ii) Certification Authority (CA): The issuer of certificates. It supports a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

iii) Registeration Authority (RA): An optional component that can assume a number of administrative functions from the CA.

iv) CRL issuer: An optional component that a CA can delegate to publish CRLs.

v) Repository: A generic term used to denote any method for storing certificates and CRLs so that they can be retrived by end entities.

### Functions of PKIX:

i) Registration: It is the process where an end entity makes itself known to a CA.

ii) Initialization: This deals with the basic problems, such as the methodology of verifying that the end-entity is taking to the right CA.

iii) Certification: In this step, the CA creates a digital certificates for the end-entity and returns it to end-entity.

iv) Key Generation: PKIX specifies that the end entity should be able to generate private and public key pair.

v) Key Update: This allows a smooth transmission from one expiring key pair to a fresh one, by the automatic renewal of digital certificates.

## ②. Email Security:

Encryption of emails and any other forms of communication is vital for the security, and privacy. PGP is one of the popular encryption and digital signature schemes in personal communication.

### Pretty Good Privacy (PGP):

PGP is an open-source, freely available software package for email security. It provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. The actual operation of PGP consists of 5 services which are as follows:

i) Authentication: PGP authentication is done through the use of digital signature. A hash code of message is created using SHA-1. The hash code is encrypted using DSS or RSA with the senders private key including message. The receiver uses RSA with the sender's public key to decrypt and recover the hash code. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

ii) Confidentiability: PGP provides confidentiability through the use of symmetric block encryption. A message is encrypted using CAST-128 or IDEA or 3 DES with one-time session key generated by the sender. The session key is encrypted using RSA with the recipient's public key and included with the message. The receiver uses RSA with its private key to decrypt and recover the session key. The session key is used to decrypt the message.

iii) Compression: PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for email transmission and for file storage. Message encryption is applied after compression to strengthen cryptographic security.

iv) Email Compatibility: The scheme used for e-mail compatibility is radix-64 conversion. To provide transparency for email application, an encrypted message may be converted to an ASCII string using radix 64-conversion. The use of radix 64 expands a message by 33%.

v) Segmentation: Email facilities often are restricted to a maximum length. To accommodate this, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing, including the radix-64 conversion.

## ⊛. Secure Socket Layer (SSL) Protocol: [Imp]

It is a internet protocol for secure exchange of information between a web browser and a web server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack. SSL works in tems of connection and session between clients and servers.

SSL Architecture:

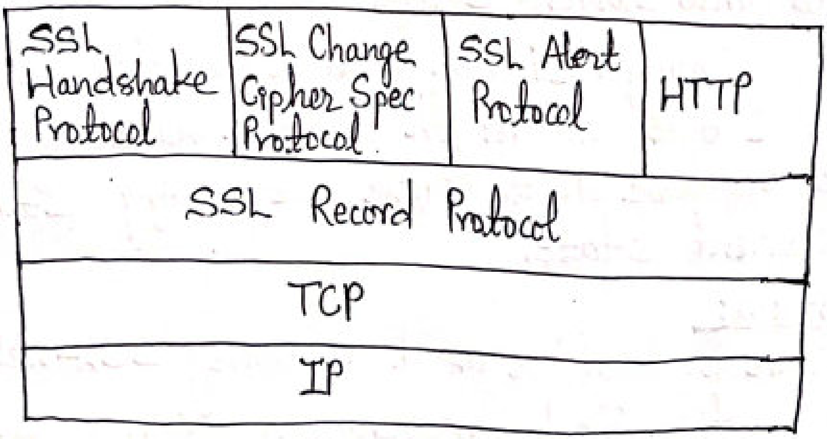


Fig: SSL Protocol Stack

## SSL Session:

→ A SSL session is an association between client and server.

→ Session is created by the SSL handshake protocol.

→ It defines a set of security parameters.

→ A session can consist of multiple connections.

→ It is useful to avoid expensive negotiations of security parameters for each connection.

## SSL Connection:

→ A connection is a transport that provides a suitable type of service.

→ For SSL, connections are peer-to-peer relationships.

→ The connections are temprory.

→ Every connection is associated with one session.

## SSL Record Protocol:

SSL Record Protocol provides two services for SSL connection:

i) Confidentiality: The handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

ii) Message Integrity: The handshake protocol also defines a shared secret key that is used to form a MAC.

## Change Cipher Spec Protocol:

This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in pending state. After handshake protocol the pending state is converted into current state.

Change-cipher protocol consists of single message which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.

## Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes. The first byte takes the value warning or fatal to convey the security of message. The second byte contains a code that indicates a specific alert.

## SSL Handshake Protocol:

Handshake protocol is used to establish a secure session between the client and the server. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The handshake protocol is used before any application data is transmitted. Handshake protocol uses four phases to complete its cycle:

i) Establish security capabilities.
ii) Server authentication and key exchange.
iii) Client authentication and key exchange.
iv) Change cipher Spec and Finish.

## ⊛. Transport Layer Security (TLS) Protocol:

The TLS protocol is the Internet Engineering Task Force (IETF) standard version of the SSL protocol. The TLS protocol allows client-server application to communicate across a network in a way designed to prevent eavesdropping and tampering. It ensures privacy between communicating applications and their use on the internet. Following are the additional features of TLS:

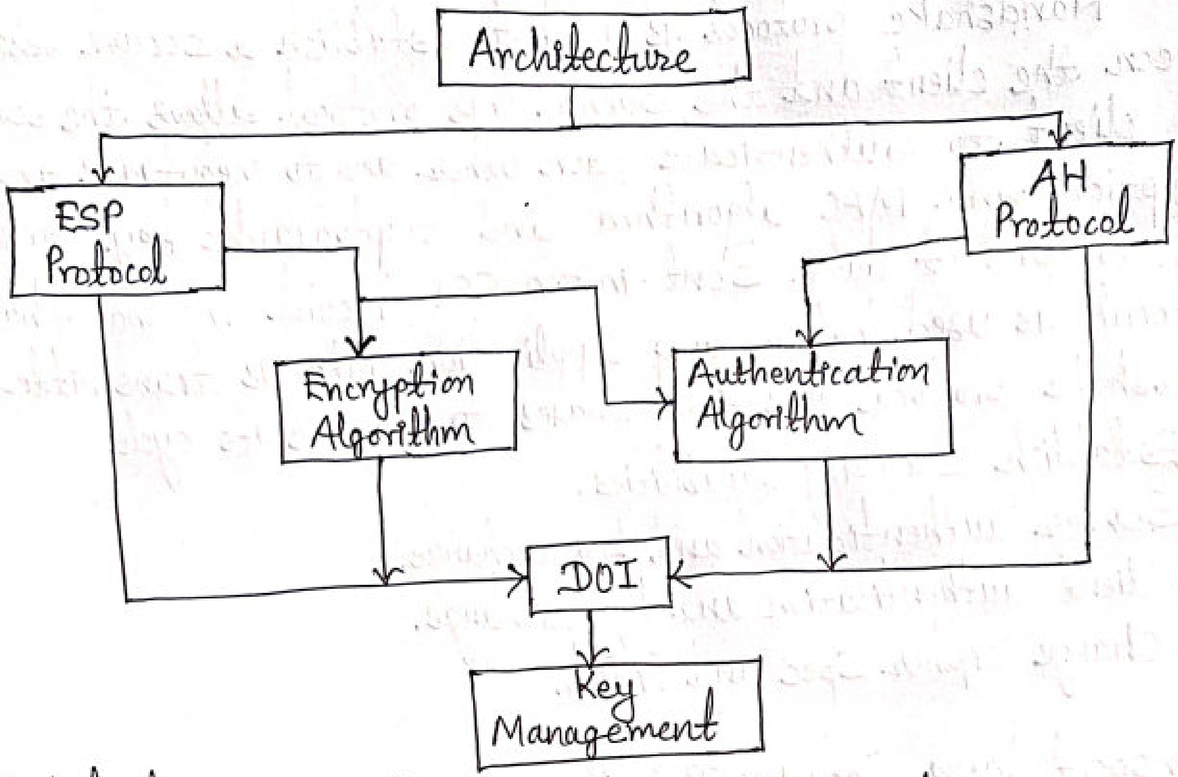
i) Interoperability: Ability to exchange TLS parameters by either party, with no need for one party to know the other's TLS implementation details.

ii) Expandability: To plan for future expansions and accommodation of new protocols.

## ⊛. IP Security (IPsec) Protocol:

Internet Protocol security (IPsec) is a set of security protocols and algorithms used to secure IP data at the network layer. IPsec provides data confidentiality, integrity, authentication of IP packets etc.

# IPSec Architecture:



Architecture: Covers the general concepts, security requirements, definitions, and mechanism defining IPSec technology.

Encapsulating Security Payload (EPS): Covers packet format and general issues related to the use of the ESP for packet encryption and optionally, authentication.

Authentication Header (AH): Covers the packet format and general issues related to the use of AH for packet authentication.

Encryption Algorithm: A set of documents that describe how various authentication algorithms are used for AH and for authentication option of ESP.

Domain of Interpretation (DOI): Contains the values needed for the other documents to relate to each other.

Key Management: Documents that describe key management schemes.

## IPsec Operation Modes:

IPSec has two operation modes:

i) **Transport Mode:** Only the payload or data of the orignal IP packet is protected in transport mode. The protected payload is then encapsulated by the IPsec headers and trailers while the original IP header remains intact and is not protected by IPsec.

ii) **Tunnel Mode:** The entire orignal IP packet is protected in tunnel mode. The packet is then encapsulated by the IPSec headers and trailers. Finally a new IP header is prefixed to the packet, Specifying the IPsec endpoints as the source and destination.

## ⊛. Firewalls: [Imp]

A firewall is a network security device, either hardware or software-based, which monitors all incomming and outgoing traffic and based on a defined set of security rules it accepts, drops or rejects that specific traffic.

Accept: allow the traffic
Reject: block the traffic but reply with an "unreachable error".
Drop: block the traffic with no reply.

### Characteristics:

- → It provides protection from various kinds of IP spoofing and routing attacks.
- → It provides a location for monitoring security-related errors.
- → A firewall is a convenient platform for several internet functions that are not security related such as NAT.
- → A firewall can serve as the platform for IPsec to implement virtual private networks.

## Types of Firewall:

1. **Packet filtering firewall:** Packet filtering firewalls are normally deployed on the routers which connect the internal network to internet. It can only be implemented on the network layer of OSI model. Packet filtering firewalls work on the basis of rules defined by Access Control Lists (ACL).

2. **Circuit Level Gateway Firewalls:** Circuit level gateways are deployed at the session layer of the OSI model. Circuit level gateway is comparatively inexpensive and provides anonymity to the private network. It's disadvantage is it does not filter individual packets.

3. **Application Level Gateway Firewalls:** Application level gateways work on the application layer of the OSI model. It provides protection for a specific application layer protocol. Proxy server is the best example of application level gateway firewalls.

4. **Stateful Inspection firewalls:** Stateful inspection firewall is a combination of all the firewalls Packet filtering, Circuit level gateway and Application level gateway. These firewalls can filter packets at network layer using ACL's.

5. **Next Generation Firewalls:** A next generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall. It allows or blocks traffic based on state, port and protocol.