Unit-VI Network Security and Public Key Infrastructure

6.1 Overview of Network Security

6.2 Digital Certificates and X.509 certificates, Certificate Life Cycle Management

6.3 PKI trust models, PKIX

6.4. Email Security: Pretty Good Privacy (PGP)

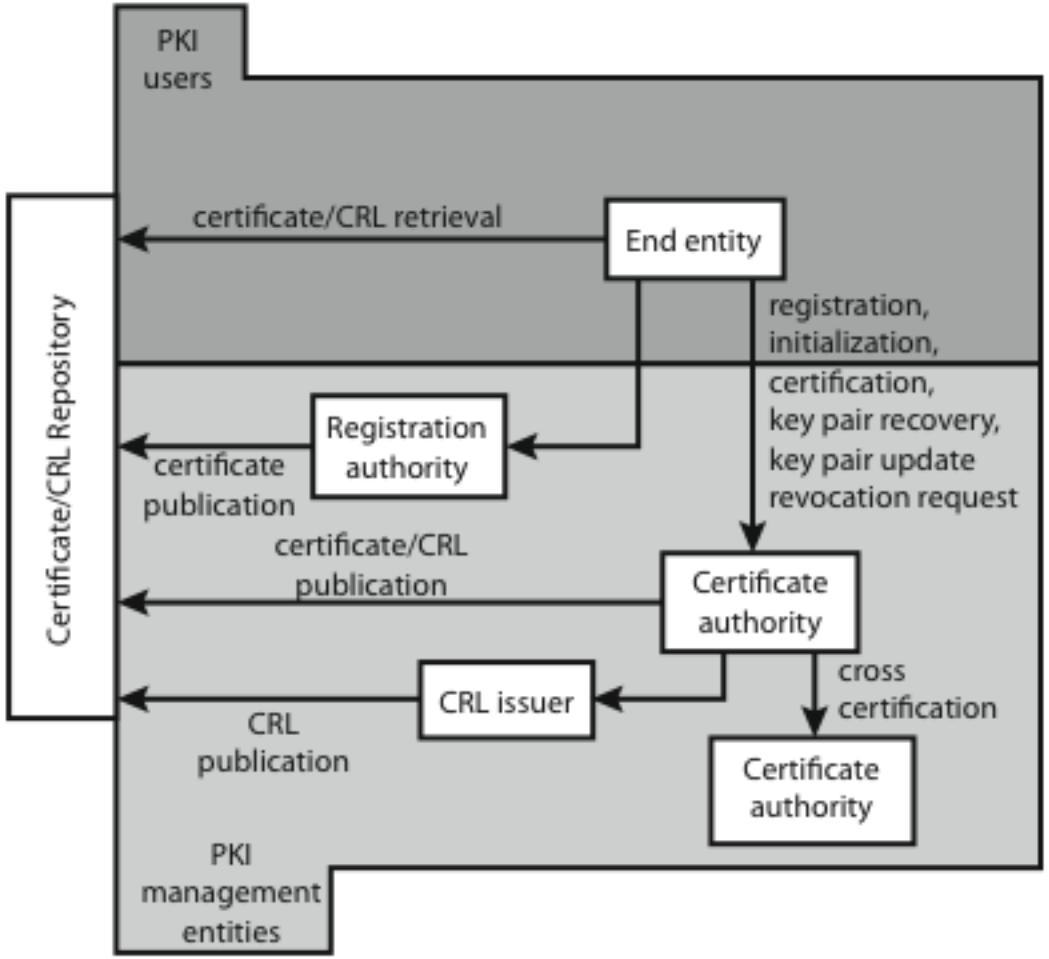
6.5. Secure Socket Layer (SSL) and Transport Layer Security (TLS)

6.6. IP Security (IPSec)

6.7. Firewalls and their types

PKI

- PKI is a set of standards, procedures, software, and people for implementing authentication using public key cryptography.
- PKI is used to request, install, configure, manage and revoke digital certificates.
- PKI offers authentication via digital certificates, and these digital certificates are signed and provided by **certificate authorities**.


PKI
users
certificate/CRL retrieval
End entity
registration,
initialization,
certification,
key pair recovery,
key pair update
revocation request
Certificate/CRL Repository
Registration
authority
certificate
publication
certificate/CRL
publication
Certificate
authority
cross
certification
CRL issuer
CRL
publication
Certificate
authority
PKI
management
entities

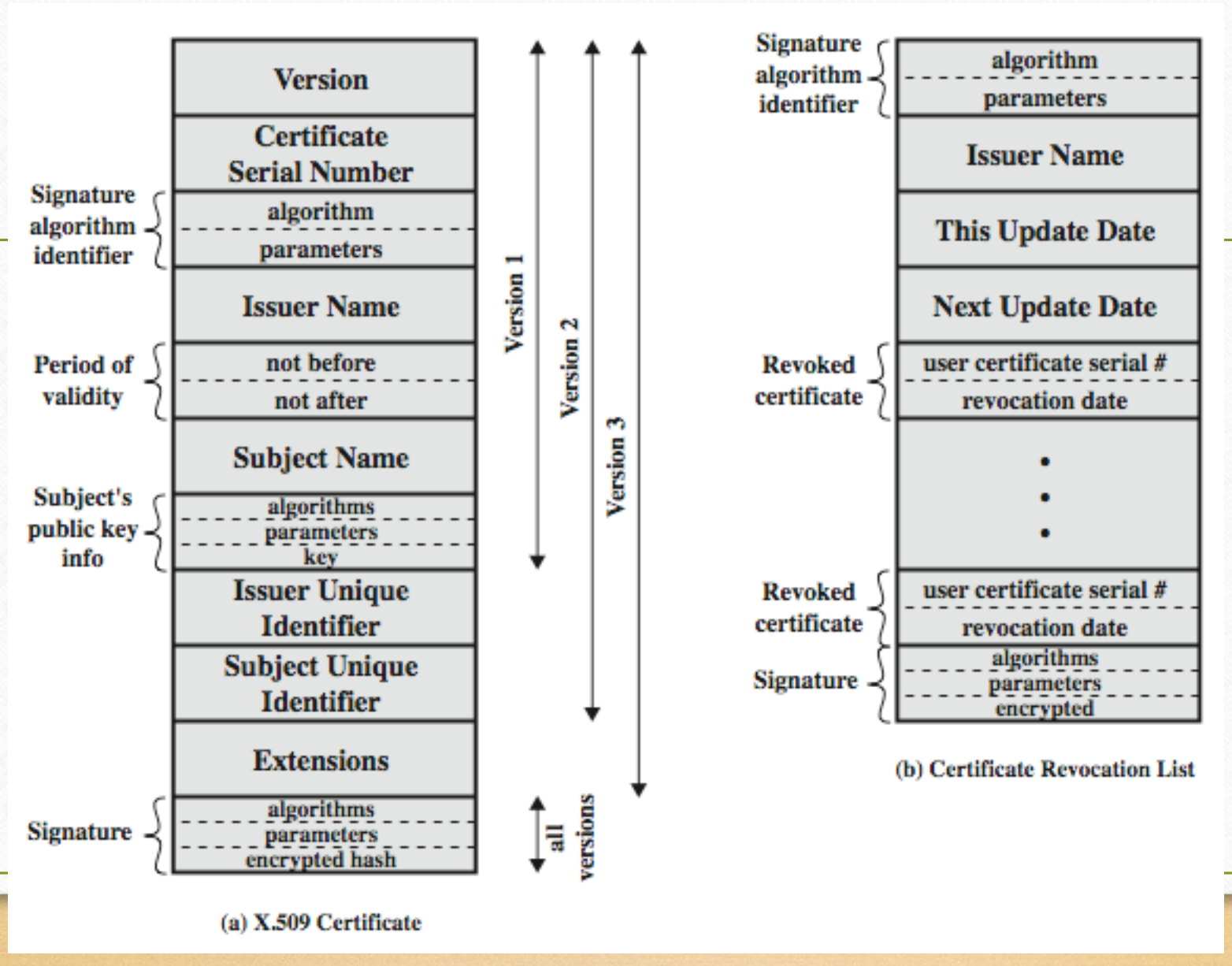
Functions

- functions:
  - registration
  - initialization
  - certification
  - key pair recovery
  - key pair update
  - revocation request
  - cross certification

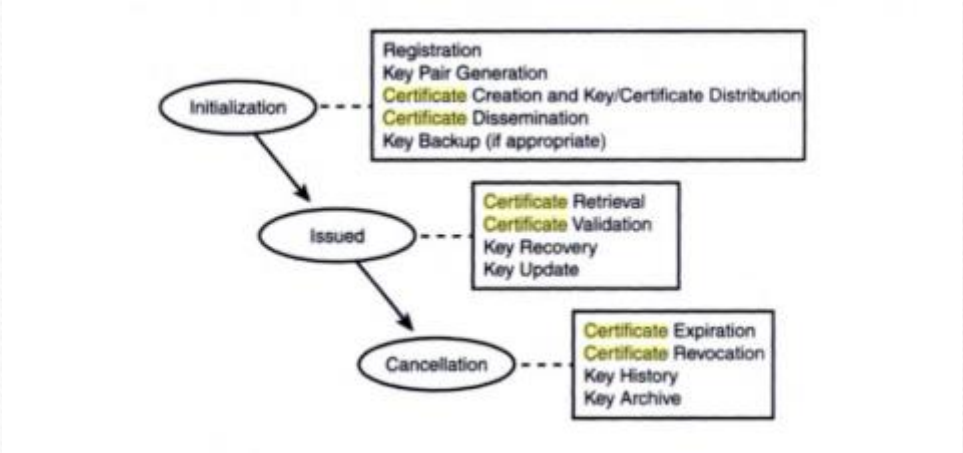
X.509 Authentication Service

- part of CCITT X.500 directory service standards
  - distributed servers maintaining user info database
- defines framework for authentication services
  - directory may store public-key certificates
  - with public key of user signed by certification authority
- also defines authentication protocols
- uses public-key crypto & digital signatures
  - algorithms not standardised, but RSA recommended
- X.509 certificates are widely used
  - have 3 versions

X.509 Certificates



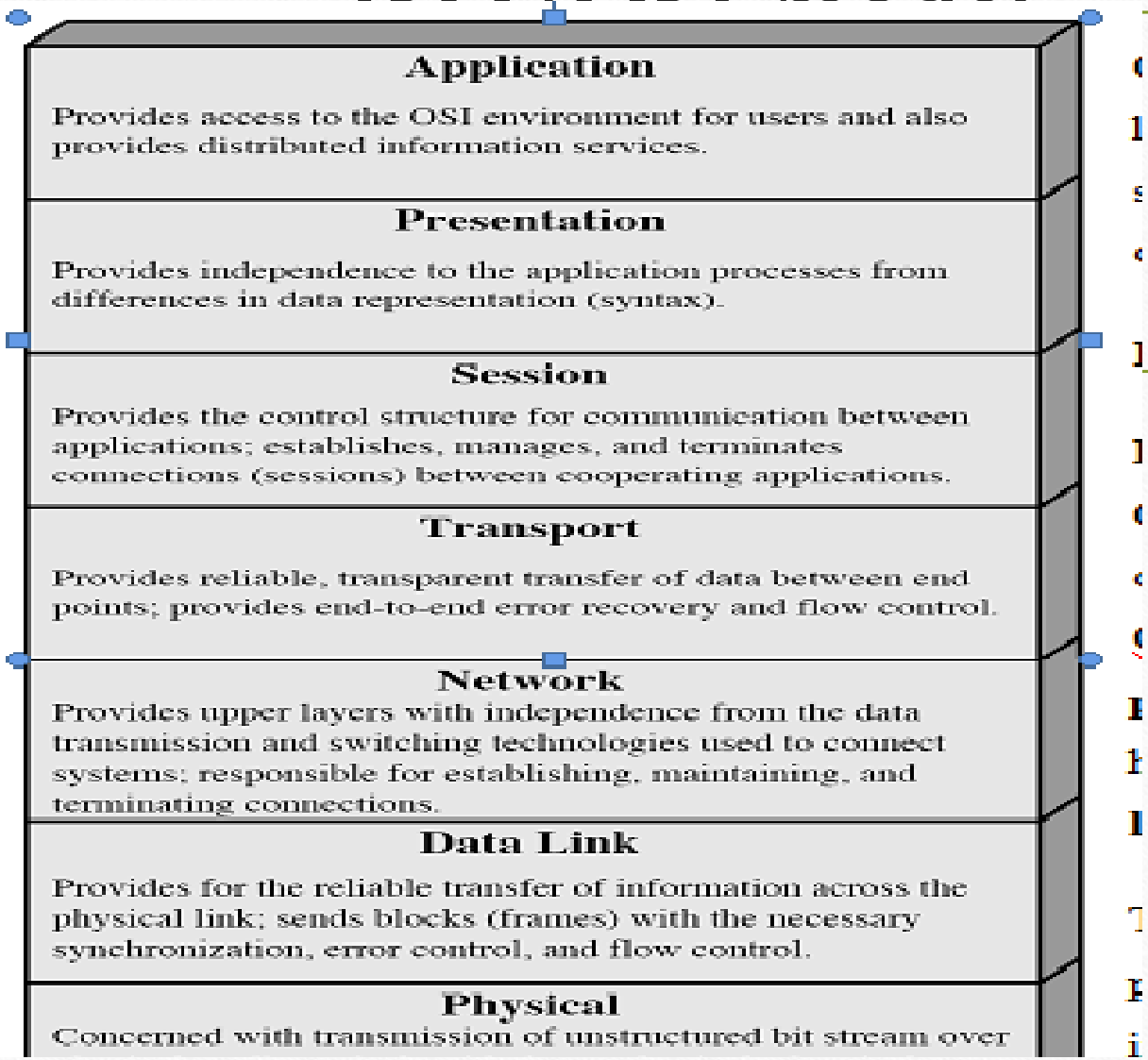
Certificate Life Cycle Management



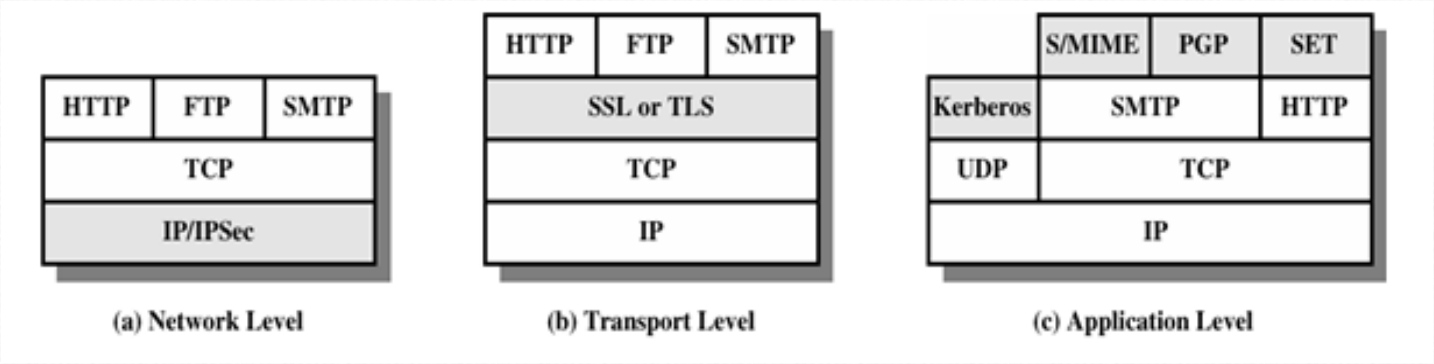
Network Security

- IP Security,
- Web Security,
- Secure Socket Layer (SSL),
- Transport Layer Security (TLS),
- Different versions of SNMPs, PGP.

ISO/OSI model



Security at Different Layers



Security at the Application Layer: E-Mail

- **Pretty Good Privacy (PGP):**

➢ PGP is a public key encryption package to protect e-mail and data files.

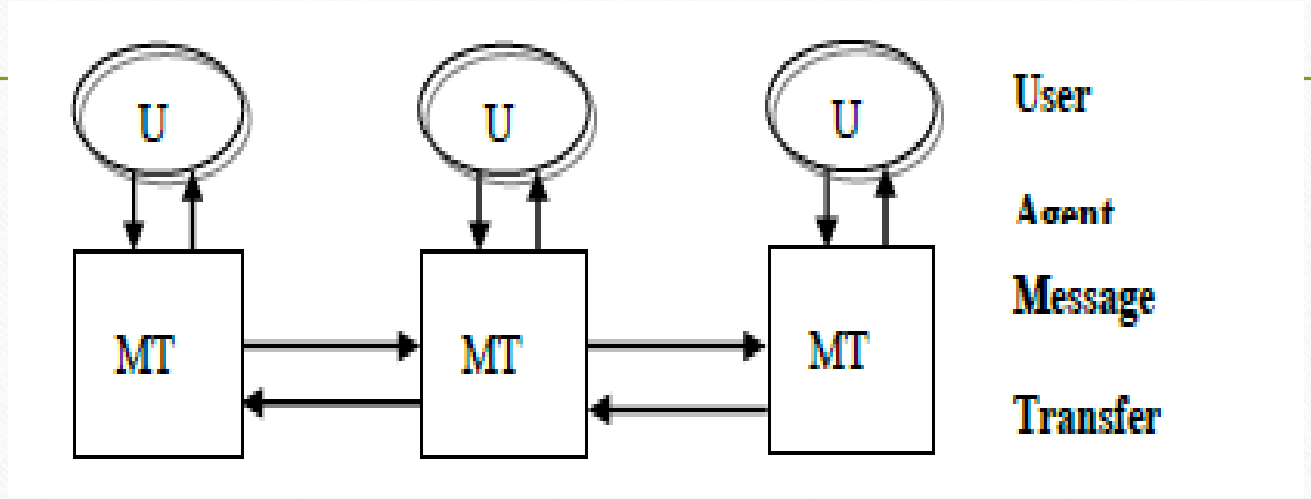
➢ It lets you communicate securely with people you've never met, with no secure channels needed for prior exchange of keys.

➢ The actual operation of PGP is based on five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation.

- PGP provides authentication via a digital signature scheme.
- PGP provides confidentiality by encrypting messages before transmission
- PGP compresses the message after applying the signature and before encryption. The idea is to save space.
- PGP encrypts a message together with the signature (if not sent separately) resulting into a stream of arbitrary 8-bit octets. But since many e-mail systems permit only use of blocks consisting of ASCII text, PGP accommodates this by converting the raw 8-bit binary streams into streams of printable ASCII characters using a radix-64 conversion scheme. On receipt, the block is converted back from radix-64 format to binary.
- To accommodate e-mail size restrictions, PGP automatically segments email messages that are too long. However, the segmentation is done just before transmitting it.

Privacy Enchanced Mail (PEM):

- The figure below shows a typical network mail service. The U (user agent) interacts directly with the sender. When the message is composed, the U hands it to the MT (message transport, or transfer, agent). The MT transfers the message to its destination host, or to another MT, which in turn transfers the message further. At the destination host, the MT invokes a user agent to deliver the message.


U
U
U
MT
MT
MT
User
Agent
Message
Transfer

- An attacker can read electronic mail at any of the computers on which MTs handling the message reside, as well as on the network itself.
- Four types of attacks (violation of confidentiality, authentication, message integrity, and nonrepudiation) make electronic mail nonsecure. So IETF with the goal of e-mail privacy develop electronic mail protocols that would provide the following services.

1. Confidentiality, by making the message unreadable except to the sender and recipient(s)

2. Origin authentication, by identifying the sender precisely

3. Data integrity, by ensuring that any changes in the message are easy to detect

4. Nonrepudiation of origin (if possible)

The protocols were named Privacy-Enhanced Electronic Mail (or PEM).

PEM vs. PGP

- Use of different ciphers: PGP uses IDEA cipher but PEM uses DES in CBC mode.
- Use of certificate models: PGP uses general “web of trust” but PEM uses hierarchical certification structure

Security at the Transport Layer

- **Secured Socket Layer (SSL)**
  - The Secure Socket Layer (SSL) is a standard developed by Netscape Corporation to provide security in WWW browsers and servers.
  - The current version, SSLv3, is the basis for an Internet standard protocol under development.
  - The newer protocol, the Transport Layer Security (TLS) protocol, is compatible with SSLv3 and has only minor changes. It has not yet been adopted formally.

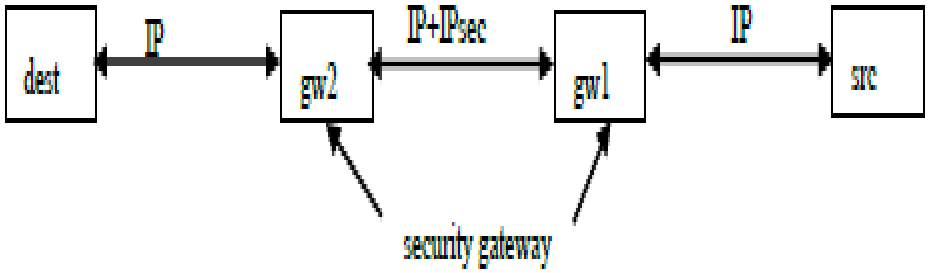
SSL GOALS

- **Cryptography security:** One of the SSL protocol's primary goals is to establish a secure connection between two parties. A symmetric Encryption is used after an initial handshake to define a secret key.
- **Reliability:** The connection is reliable. Message transport includes a message integrity check using a keyed MAC computed using secure hash functions.
- **Interoperability:** Different applications should be able to successfully exchange cryptographic parameters without knowledge of one another's code.
- **Extensibility:** Provide a framework that allows new public-key and bulk encryption methods to be incorporated as necessary. This will also achieve the goal of avoiding the need to implement an entire new security library.
- **Relative efficiency:** Cryptographic operations tend to be highly CPU intensive. For this reason the SSL protocol has some options (such as caching and compression), which allow a reduction in the number of connections that need to be established from scratch and a reduction in network activity.

Security at the Network Layer

IPSec (Internet Protocol Security)

- IPSec is a suite of authentication and encryption protocols developed by the Internet Engineering Task Force (IETF) and designed to address the inherent lack of security for IP-based networks.
- It is a collection of protocols and mechanisms that provide **confidentiality, authentication, message integrity, and replay detection at the IP layer.** In the data transmission IPsec protect all messages sent along a path. If the IPsec mechanisms reside on an intermediate host (for example, a firewall or gateway), that host is called a security gateway.

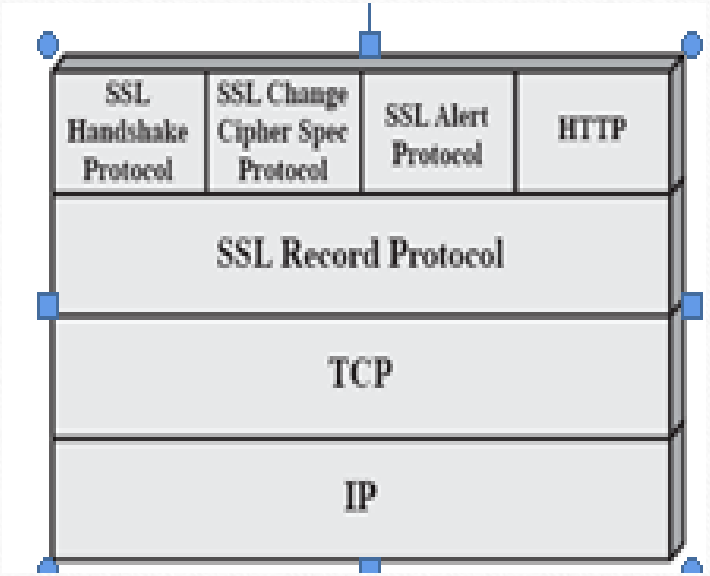

dest
IP
gw2
IP+IPsec
gw1
IP
src
security gateway

Security at the Transport Layer

Secured Socket Layer (SSL)

- The Secure Socket Layer (SSL) is a standard developed by Netscape Corporation to provide security in WWW browsers and servers. The current version, SSLv3, is the basis for an Internet standard protocol under development. The newer protocol, the Transport Layer Security (TLS) protocol, is compatible with SSLv3 and has only minor changes.

SSL ARCHITECTURE



- SSL, a set of protocols, uses TCP to provide reliable end to end service.
- SSLv3 consists of two layers (see figure) supported by numerous cryptographic mechanisms.
- The lower layer called SSL Record Protocol provides the basic security services to various higher level protocols, particularly HTTP.
- There are three higher level protocols that are defined as parts of SSL namely SSL Handshake Protocol, the Change Cipher Spec Protocol, and Alert Protocol.

- SSL works in terms of **connections** and **sessions** between clients and servers.
- An SSL **session** is an association between two peers.
- An SSL **connection** is the set of mechanisms used to transport data in an SSL session. A single session may have many connections.

Each party keeps information related to a session with each peer. The data associated with a session includes the following information.

1. **Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.**
2. **Peer certificate: X509.v3 certificate of the peer. This may be null.**
3. **Compression method: The algorithm used to compress data prior to encryption.**
4. **Cipher spec: Specifies the bulk data encryption algorithm (null, DES, etc.) and a MAC algorithm (MD5 or SHA). It also defines attributes such as the hash_size.**
5. **Master secret: 48-byte secret shared between the client and server.**
6. **Is resumable: Defines whether the session can be used to initiate new connections.**

The SSL Handshake Protocol

- This protocol, also called the key-exchange protocol, is responsible for establishing a secure session between two parties. The SSL handshake protocol can be divided to several important stages:

1. Authenticate the server to the client.
2. Negotiation of common cryptographic algorithms, that both server and client support.
3. Authenticate the client to the server (optional).
4. Using public-key encryption to exchange cryptography parameters (shared secrets).
5. Establish an encrypted SSL connection.

The SSL Change Cipher Spec Protocol

- It is used in the last stage of the SSL Handshake protocol to let the parties know to move from the pending state to the current state i.e. the parties finishes using the key-exchange algorithm and moves on to use the encryption and MAC algorithms, which were defined in the Handshake protocol. This message has one byte with content of '1' and is encrypted and compressed under the current CipherSpec.

The SSL Alert Protocol

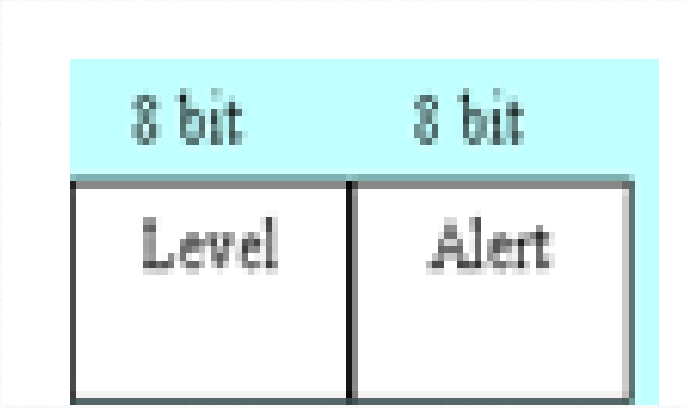
- It is responsible for informing errors that occur during connection.

- There are two levels of alerts:
  - a fatal alert or a warning alert.

    If alert is fatal the connection is terminated immediately. Other connections of the same session may continue, but this session ID will be marked as invalid so that no new connections can be established on this session.

Level: Indicates a fatal or warning alert

Alert: Indicates the specific alert



SSL Application Data Protocol

- This protocol simply passes data from the application layer to the SSL Record Protocol layer. The record protocol transports the data to the peer using the current compression and cipher algorithms

Transport Layer Security(TLS)

- TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL.
- There are two differences between the SSLv3 and TLS MAC schemes: the actual algorithm and the scope of the MAC calculation. TLS makes use of the HMAC algorithm defined as

$HMAC_K(M) = H[(K^+ \text{ XOR opad}) || H[(K^+ \text{ XOR ipad}) || M]]$

- SSLv3 uses the same algorithm, except that the padding bytes are concatenated with the secret key rather than being XORed with the secret key padded to the block length.

- The level of security should be about the same in both cases.

Firewalls

- Firewall is hardware device or software applications that act as filters between a company's private network and the internet. It protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service by enforcing an access control policy between two networks.
- The main purpose of a firewall system is to control access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated. A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet.

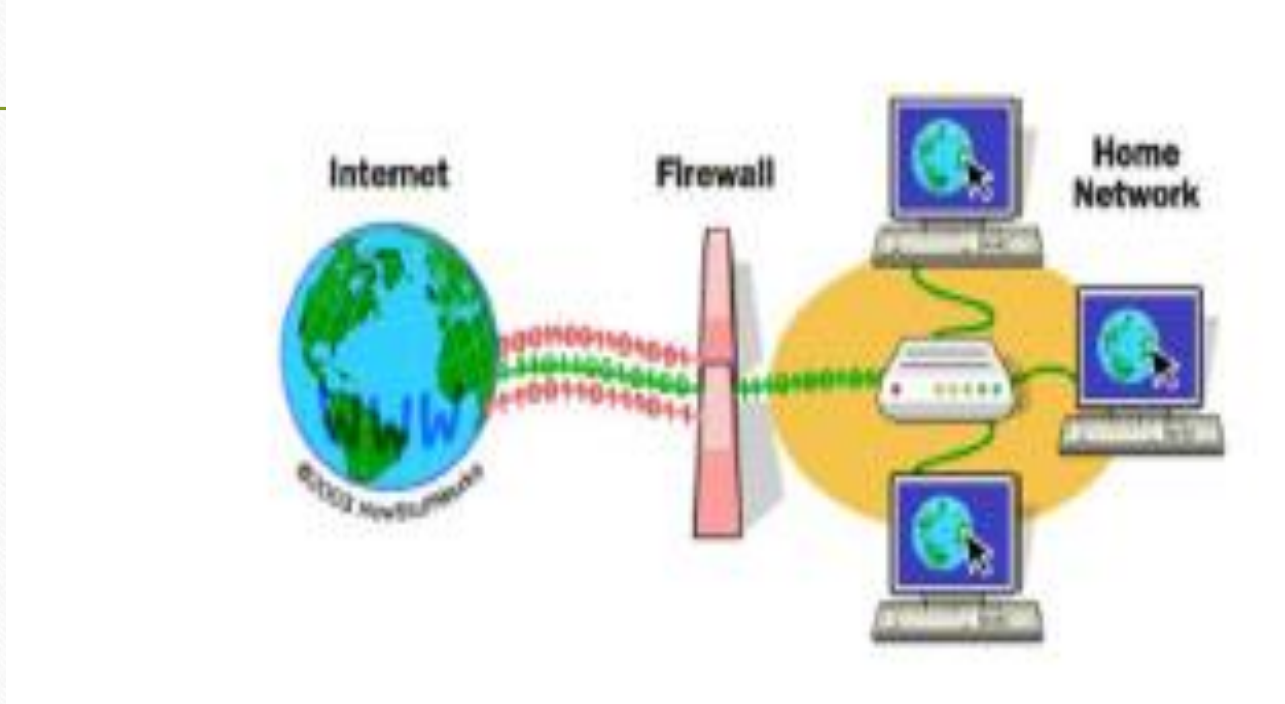
- The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. The earliest firewalls were simply routers.
- Firewalls provide several types of protection:

  - They can block unwanted traffic.

  - They can direct incoming traffic to more trustworthy internal systems. They hide vulnerable systems, which can't easily be secured from the Internet.

  - They can log traffic to and from the private network.

  - They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.


Internet
Firewall
Home
Network

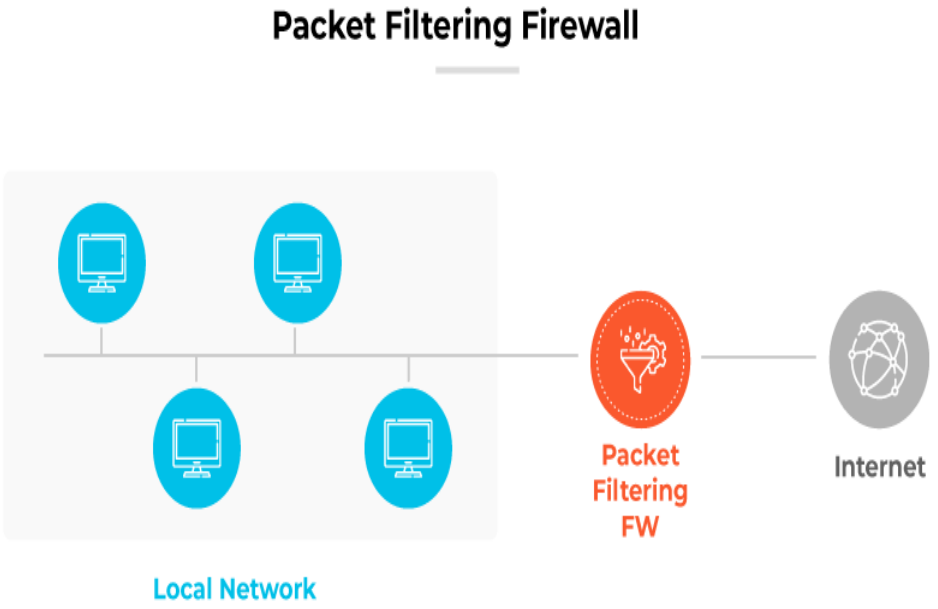
Types of firewalls yourself

- Firewalls, Firewall Characteristics,
- Types of Firewalls: Packet filtering firewall, Circuit-level gateway, Stateful inspection firewall, Proxy firewall, Next-generation firewall

Types

Packet Filtering

- A packet filtering firewall controls data flow to and from a network.
- Works at the network layer.
- These firewalls rely on pre-defined rules that evaluate specific attributes of the packets such as source IP, destination IP, ports, and protocols. If the attributes match the established rules, the packet is allowed to pass through. If not, the packet is blocked.



Types

A Circuit Level gateway

- A circuit-level gateway functions primarily at the session layer of the OSI model. Its role is to oversee and validate the handshaking process between packets, specifically for TCP and UDP connections. By examining the handshake process and the IP addresses associated with packets, this firewall identifies legitimate traffic and deters unauthorized access.