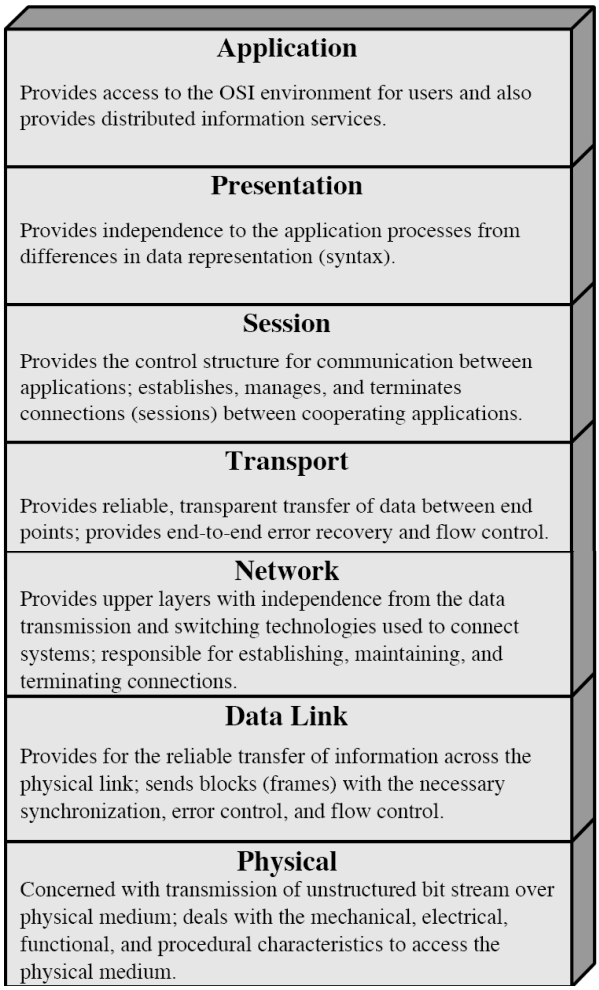
Chapter 8

Network Security

Networks and Cryptography

ISO/OSI model



Conceptually, each host has peer at each layer and peers communicate with peers at same layer (see books on network for detail)

Link and End-to-End Protocols

Let hosts C_0, …, C_n be such that C_i and C_{i+1} are directly connected, for $0 \leq i < n$. A communications protocol that has C_0 and C_n as its endpoints is called an **end-to-end protocol**. A communications protocol that has C_j and C_{j+1} as its endpoints is called a **link protocol**.

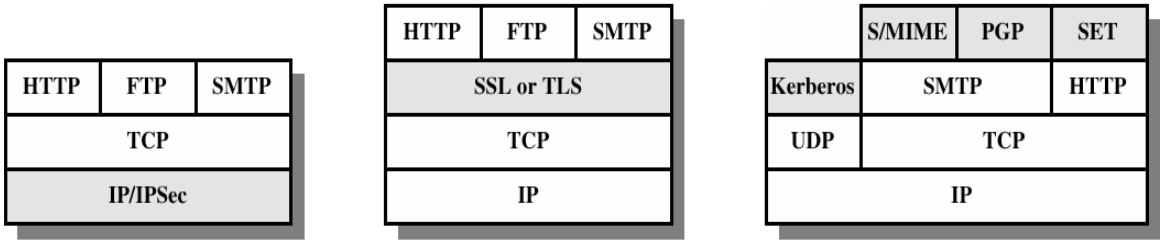
The difference between an end-to-end protocol and a link protocol is that the intermediate hosts play no part in an end-to-end protocol other than forwarding messages. Whereas, a link protocol describes how each pair of intermediate hosts processes each message.

Link encryption: Each host enciphers message and "next hop" host can read it i.e. intermediate hosts can read the message. For e.g. In PPP Encryption Control Protocol host gets message, deciphers it, figures out where to forward it, enciphers it in appropriate key and forwards it. Here each host shares key with neighbor and can be set on per-host or per-host-pair basis. Link encryption can protect headers of packets and it is possible to hide source and destination but, source can be deduced from traffic flows.

End-to-end encryption: Host enciphers message so host at other end of communication can read it i.e. message cannot be read at intermediate hosts for e.g. TELNET protocol where messages between client, server enciphered, and encipherment, decipherment occur only at these hosts. In this approach each host shares key with destination and can be set on per-host or per-host-pair basis. This approach cannot hide packet headers and attacker can read source, destination.

Security at Different Layers

The following figure shows the security at different layers



(a) Network Level (b) Transport Level (c) Application Level

Security at the Application Layer: E-Mail

a) 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. It's well featured and fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design. The actual operation of PGP is based on five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation.

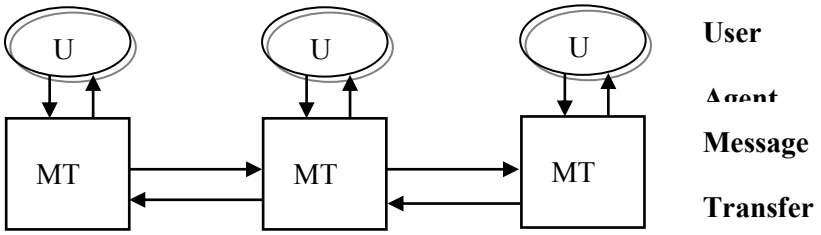
- PGP provides authentication via a digital signature scheme.
- PGP provides confidentiality by encrypting messages before transmission
- PGP compresses the message after applying the signature and before encryption. The

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 after all the housekeeping is done on the message, just before transmitting it. So the session key and signature appear only once at the beginning of the first segment transmitted. At receipt, the receiving PGP strips off all e-mail headers and reassembles the original mail.

b) 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.



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. An attacker could also modify the message without the recipient detecting the change. Because authentication mechanisms are minimal and easily evaded, a sender could forge a letter from another and inject it into the message handling system at any MT, from which it would be forwarded to the destination. Finally, a sender could deny having sent a letter, and the recipient could not prove otherwise to a disinterested party. These 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

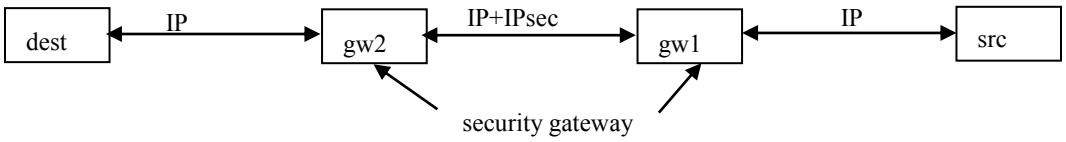
- **Use of different ciphers:** PGP uses IDEA cipher but PEM uses DES in CBC mode.
- **Use of certificate models:** PGP uses general "web of trust" but PEM uses hierarchical certification structure
- **Handling end of line:** PGP remaps end of line if message tagged "text", but leaves them alone if message tagged "binary" whereas PEM always remaps end of line.

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.



Security at the Transport Layer

Secured Socket Layer (SSL)

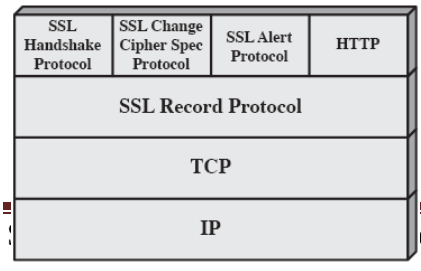
The Secure Socket Layer (SSL) is a standard developed by Netscape Corporation to provide security in WWW browsers and servers. The current version, SSLv3, is the basis for an Internet standard protocol under development. The newer protocol, the Transport Layer Security (TLS) protocol, is compatible with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

SSL Main Goals

1. **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.
2. **Reliability:** The connection is reliable. Message transport includes a message integrity check using a keyed MAC computed using secure hash functions.
3. **Interoperability:** Different applications should be able to successfully exchange cryptographic parameters without knowledge of one another's code.
4. **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.
5. **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.

SSL Architecture

SSL, a set of protocols, uses TCP to provide reliable end to end service. SSLv3 consists of two layers (see figure below) 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. Two peers may have many sessions active at the same time, but this is not common.

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.

A connection describes how data is sent to, and received from, the peer. Each party keeps information related to a connection. Each peer has its own parameters. The information associated with the connection includes the following.

1. **Server and client random:** Random data for server and client for each connection.
2. **Server write MAC secret:** Key for MAC operations on data written by the server.
3. **Client write MAC secret:** Key for MAC operations on data written by the client.
4. **Server write key:** Cipher key for encryption by the server and decryption by client.
5. **Client write key:** Cipher key for encryption by the client and decryption by server.
6. **Initialization vectors (IV):** When a block cipher in CBC mode is used, IV is maintained for each key. This field is first initialized by the SSL handshake protocol then final ciphertext block from each record is preserved for use with the next record.
7. **Sequence numbers:** Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a **change cipher spec** message, the appropriate sequence number is set to zero. Sequence numbers are of type uint64 and may not exceed 2^{64}-1.

The SSL Handshake Protocol

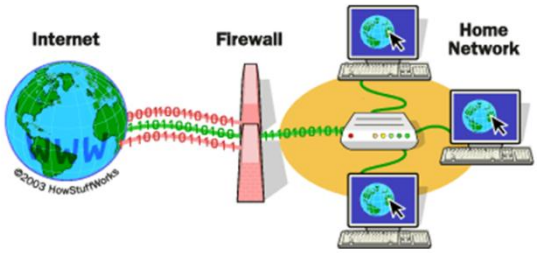
This protocol, also called the key-exchange protocol, is responsible for establishing a secure session between two parties. The SSL handshake protocol can be divided to several important stages:

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.

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. A firewall system is usually located at a higher level gateway, such as a site's connection to the Internet, however firewall systems can be located at lower-level gateways to provide protection for some smaller collection of hosts or subnets. 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.
- They can provide more robust authentication than standard applications might be able to do.