Module 6

WEB SECURITY CONSIDERATIONS

- The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets
- Web browsers are very easy to use, Web servers are relatively easy to configure and manage, and Web content is increasingly easy to develop, the underlying software is extraordinarily complex.
- A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex.
- Casual and untrained (in security matters) users are common clients for Web-based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Secure Socket Layer (SSL) and Transport Layer Security

- One of the most widely used security services
- With the protocol in place, an eavesdropper can only see the connection end points but cannot read or modify any of the actual data. Thus, it can protect user's personal data and ensure a safe transaction.
- A general purpose service implemented as a set of protocols that rely on TCP
  - Could be provided as part of the underlying protocol suite and therefore be transparent to applications
- Can be embedded in specific packages
- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.

SSL Protocol Stack

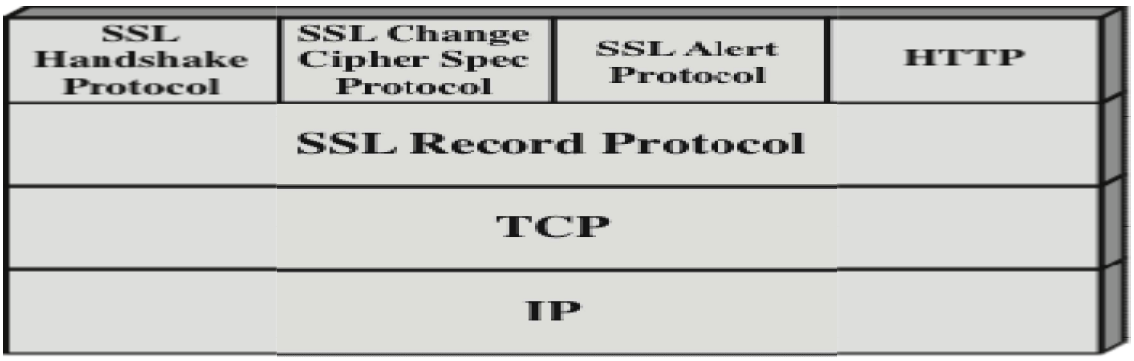


Figure 17.2 SSL Protocol Stack

- SSL is not a single protocol, but rather two layers of protocols
- The SSL Record Protocol provides basic security services to various higher layer protocols.
- The Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL.
- Three higher-layer protocols are defined as part of SSL:
    - The Handshake Protocol
    - The Change Cipher Spec Protocol
    - The Alert Protocol.
- These SSL-specific protocols are used in the management of SSL exchanges.

Two important SSL concepts

1. **SSL connection**

- A transport that provides a suitable type of service
- For SSL, such connections are peer-to-peer relationships
- Connections are transient (short time)
- Every connection is associated with one session

2. **SSL session**

    i. An association between a client and a server

    ii. Created by the Handshake Protocol

    iii. Define a set of cryptographic security parameters which can be shared among multiple connections

    iv. Are used to avoid the expensive negotiation of new security parameters for each connection.

Session State Parameters

1. **Session identifier**: An arbitrary byte sequence chosen by the server to identify an active or resumable session state
2. **Peer certificate**: An X509.v3 certificate of the peer; this element of the state may be null
3. **Compression method** : The algorithm used to compress data prior to encryption

4. **Cipher spec**: Specifies the bulk data encryption algorithm and a hash algorithm used for MAC calculation; also defines cryptographic attributes such as the hash_size
5. **Master secret**: 48-byte secret shared between the client and the server
6. **Is resumable** : A flag indicating whether the session can be used to initiate new connections

Connection State Parameters

1. **Server and client random**: Byte sequences that are chosen by the server and client for each connection
2. **Server write MAC secret**: The secret key used in MAC operations on data sent by the server
3. **Client write MAC secret**: The secret key used in MAC operations on data sent by the client
4. **Server write key**: The secret encryption key for data encrypted by the server and decrypted by the client
5. **Client write key**: The symmetric encryption key for data encrypted by the client and decrypted by the server
6. **Initialization vectors**: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key This field is first initialized by the SSL Handshake Protocol.The final ciphertext block from each record is preserved for use as the IV with the following 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 may not exceed $2^{64} – 1$

SSL RECORD PROTOCOL

- The SSL Record Protocol provides two services for SSL connections
- **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads
- **Message integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC)

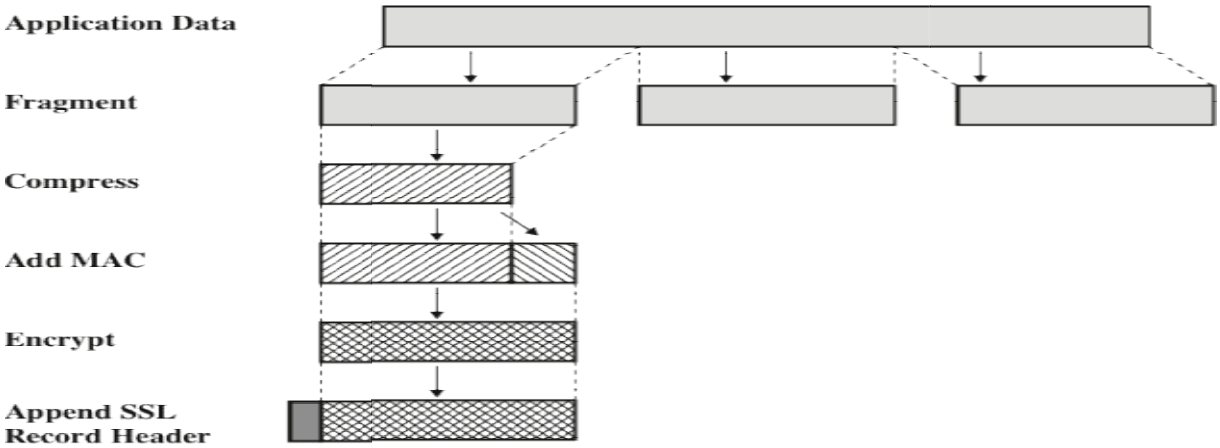


Figure 17.3 SSL Record Protocol Operation

- The Record Protocol takes an application message to be transmitted,
- fragments the data into manageable blocks, optionally compresses the data,
- applies a MAC, encrypts,adds a header, and transmits the resulting unit in a TCP segment.
- Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher- level users.
- The first step is fragmentation. Each upper-layer message is fragmented into blocks of
- 214 bytes (16384 bytes) or less. Next, compression is optionally applied.
- Compression must be lossless and may not increase the content length by more than 1024 bytes.
- The next step in processing is to compute a message authentication code over the compressed data. For this purpose, a shared secret key is used.
- Next, the compressed message plus the MAC are encrypted using symmetric encryption.
- The next step in processing is to compute a message authentication code over compressed data. For this a shared secret key is used.

SSL RECORD PROTOCOL Header Structure

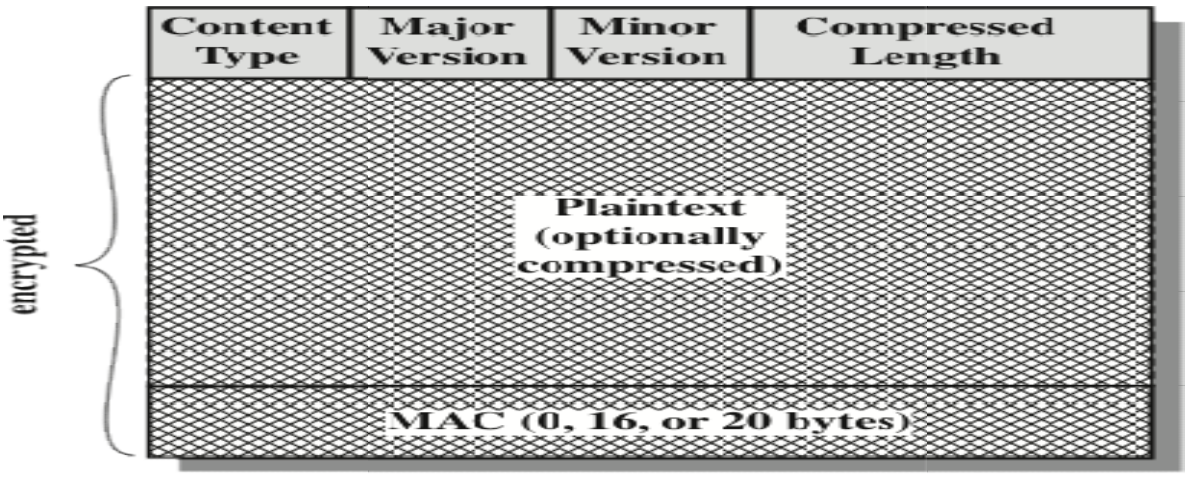
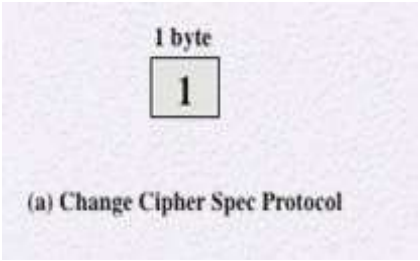


Figure 17.4 SSL Record Format

- The final step of SSL Record Protocol processing is to prepare a header consisting of the following fields:

    1. Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment.
    2. Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3.
    3. Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0.
    4. Compressed Length (16 bits): The length in bytes of the plaintext fragment (or compressed fragment if compression is used).

Change Cipher Spec Protocol



- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest.
- This protocol consists of a single message which consists of a single byte with the value 1.

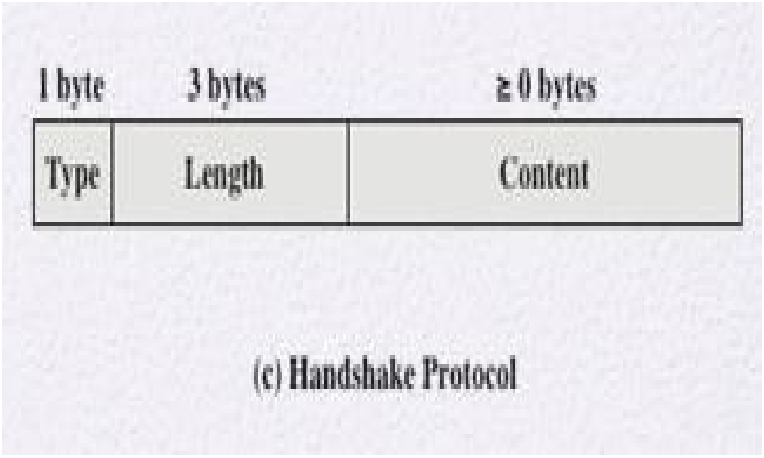
- The purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection

ALERT PROTOCOL

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- Each message in this protocol consists of two bytes
- The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
- If the level is fatal, SSL immediately terminates the connection.
- Other connections on the same session may continue, but no new connections on this session may be established.
- The second byte contains a code that indicates the specific alert.

Handshake Protocol

- 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.
- The Handshake Protocol consists of a series of messages exchanged by client and server.



- Type(1 byte): indicates one of 10 messages (hello_request, client_hello etc)
- Length(3 bytes): The length of message in bytes
- Content(>-1 byte): Parameters related with the message

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

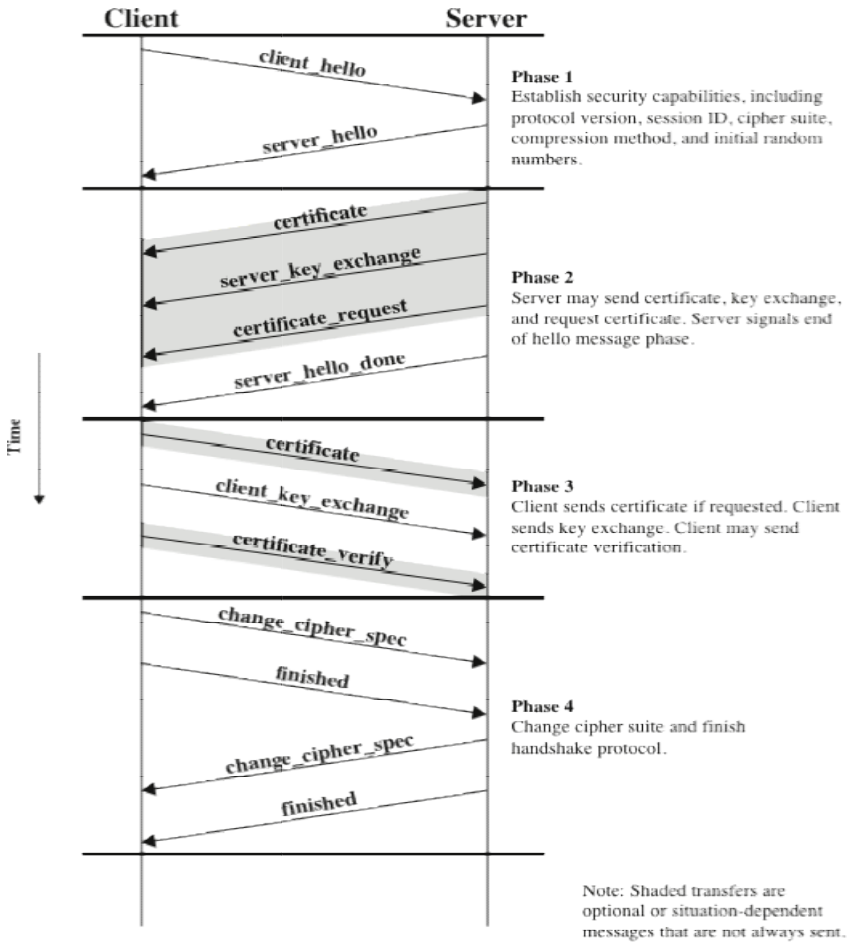


Figure 17.6 Handshake Protocol Action

TRANSPORT LAYER SECURITY

- Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
- A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.
- TLS can also be used to encrypt other communications such as email, messaging
  and voice over IP (VoIP).
- TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organization, and the first version of the protocol was published in 1999. The most recent version is TLS 1.3, which was published in 2018.

What is the difference between TLS and SSL?

- TLS evolved from a previous encryption protocol called Secure Sockets Layer (SSL), which was developed by Netscape.
- TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape.
- Because of this history, the terms TLS and SSL are sometimes used interchangeably.

What is the difference between TLS and HTTPS?

- HTTPS is an implementation of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services. Any website that uses HTTPS is therefore employing TLS encryption.

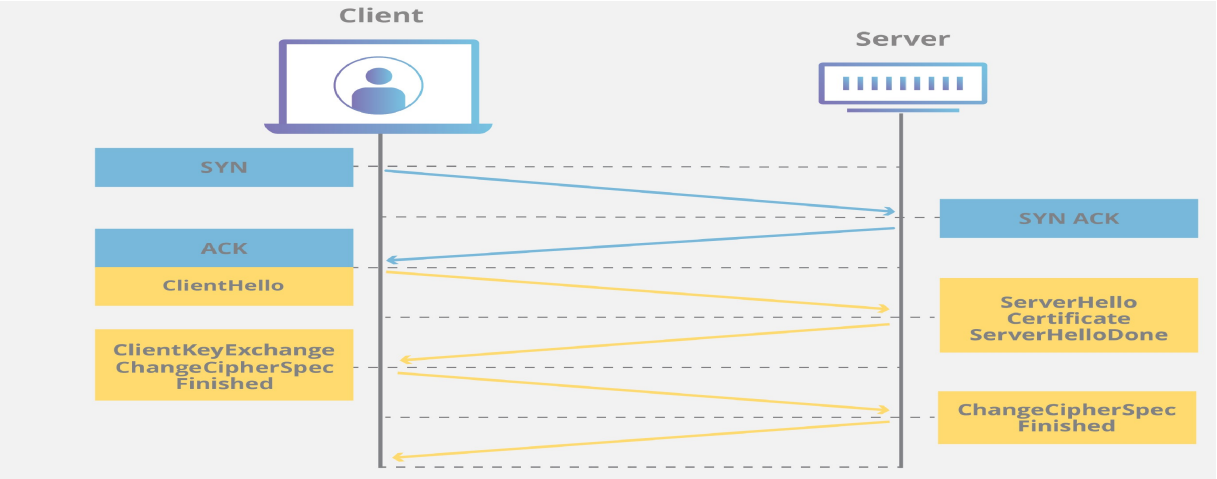
Why should businesses and web applications use the TLS protocol?

- TLS encryption can help protect web applications from data breaches and other attacks.
- Additionally, TLS-protected HTTPS is quickly becoming a standard practice for websites.
- For example, the Google Chrome browser is cracking down on non-HTTPS sites, and everyday Internet users are starting to become more wary of websites that do not feature the HTTPS padlock icon.

How does TLS work?

- For a website or application to use TLS, it must have a TLS certificate installed on its origin server
- A TLS certificate is issued by a certificate authority to the person or business that owns a domain.
- The certificate contains important information about who owns the domain, along with the server's public key, both of which are important for validating the server's identity.
- A TLS connection is initiated using a sequence known as the TLS handshake.
- When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the client device) and the web server.
- During the TLS handshake, the user's device and the web server:
- Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use

- Decide on which cipher suites they will use
- Authenticate the identity of the server using the server's TLS certificate
- Generate session keys for encrypting messages between them after the handshake is complete
- The TLS handshake establishes a cipher suite for each communication session.
- The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session.
- TLS is able to set the matching session keys over an unencrypted channel, thanks to public key cryptography.



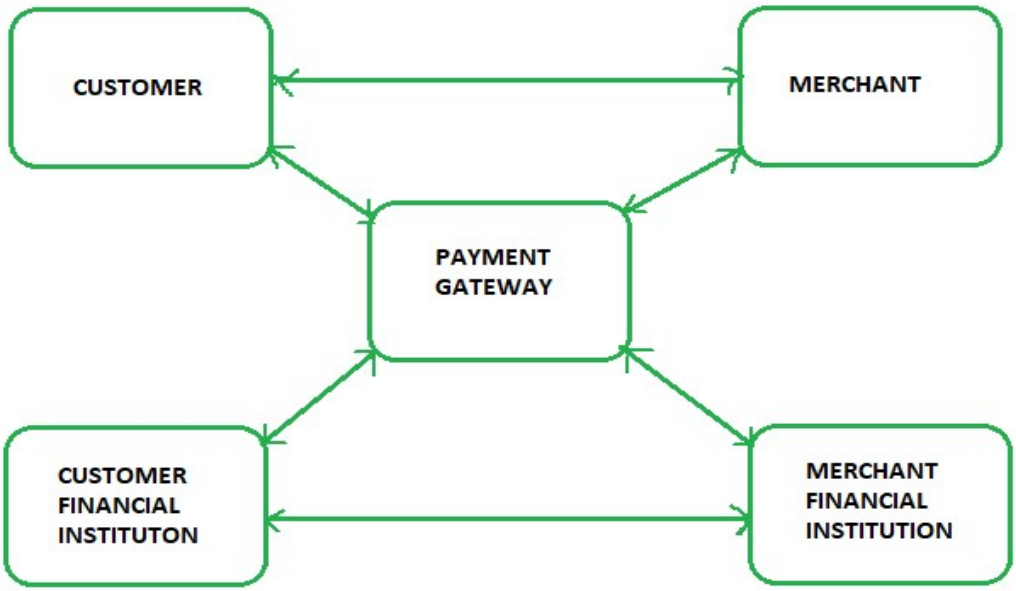
How does TLS affect web application performance?

- The latest versions of TLS hardly impact web application performance at all.
- Because of the complex process involved in setting up a TLS connection, some load time and computational power must be expended. The client and server must communicate back and forth several times before any data is transmitted, and that eats up precious milliseconds of load times for web applications, as well as some memory for both the client and the server.
- However, there are technologies in place that help to mitigate potential latency created by the TLS handshake.

SET

- Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards.
- SET is not some system that enables payment but it is a security protocol applied on those payments.

- It uses different encryption and hashing techniques to secure payments over internet done through credit cards.
- SET protocol restricts revealing of
    - Credit card details to merchants and
    - Order details to banks !!



Requirements in SET

- It has to provide mutual authentication i.e., cardholder authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Participants in SET

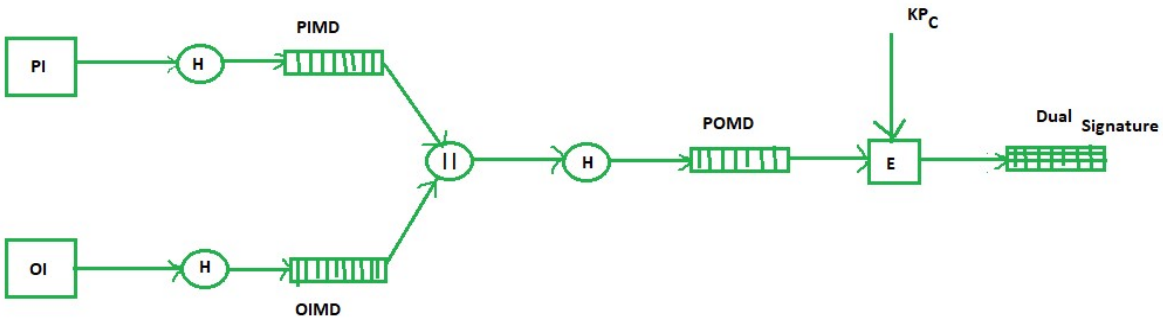
1. **Cardholder –** customer
2. **Issuer –** customer financial institution

3. **Merchant**
4. **Acquirer –** Merchant financial institution
5. **Certificate authority –** Authority which follows certain standards and issues certificates (like X.509V3) to all other participants.

Dual Signature

- The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers : Order Information (OI) for merchant Payment Information (PI) for bank

How to make **Dual Signature (DS)**?



PI stands for payment information

OI stands for order information

PIMD stands for Payment Information Message Digest

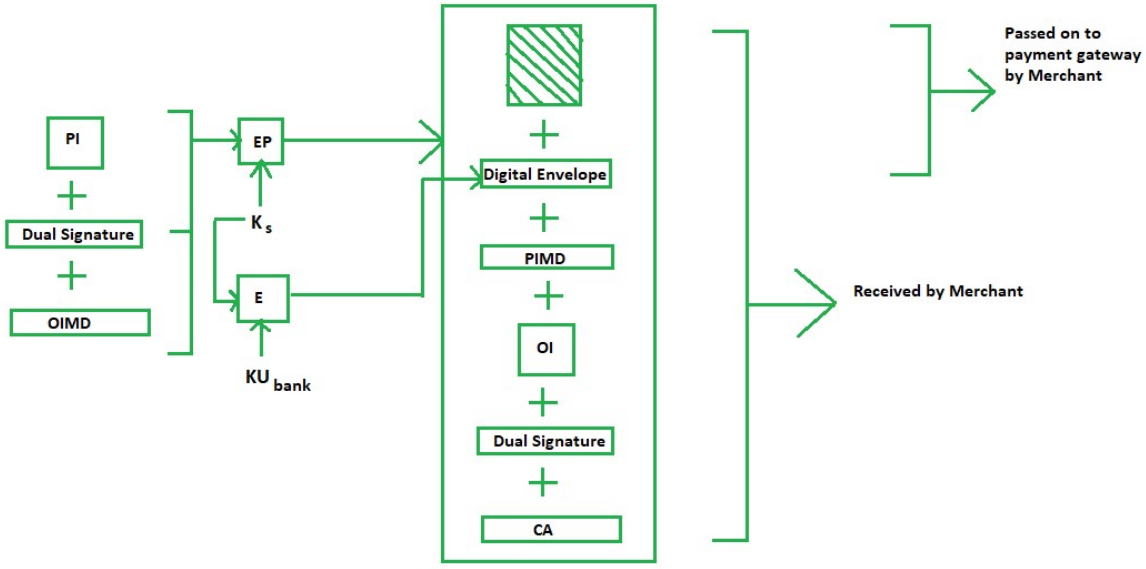
OIMD stands for Order Information Message Digest

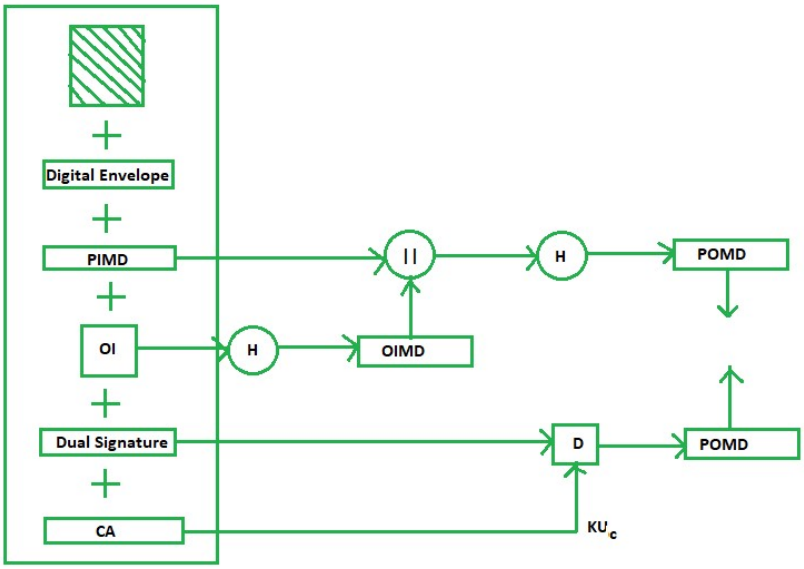
POMD stands for Payment Order Message Digest

Purchase Request Generation

- Before the Purchase Request exchange begins, the cardholder has completed browsing, selecting, and ordering
- The purchase request exchange consists of four messages:
- Initiate Request :brand of the credit card, ID, nonce
- Initiate Response : merchant's signature certificate, payment gateway's key exchange certificate
- Purchase Request

- Purchase Response : response block that acknowledges the order and references the corresponding transaction number
- The process of purchase request generation requires three inputs:
    - Payment Information (PI)
    - Dual Signature
    - Order Information Message Digest (OIMD)





PAYMENT PROCESS

- In two steps:
    - Payment authorization

- Payment capture

- Payment Authorization

- The merchant sends an authorization request message to the payment gateway consisting of the following:

1. Purchase-related information
    - » PI
    - » Dual signature calculated over the PI & OI and signed with customer's private key.
    - » The OI message digest (OIMD)
    - » The digital envelop
2. Authorization-related information
    - » An authorization block including:
        - A transaction ID
        - Signed with merchant's private key
        - Encrypted one-time session key
3. Certificates
    - » Cardholder's signature key certificate
    - » Merchant's signature key certificate
    - » Merchant's key exchange certificate

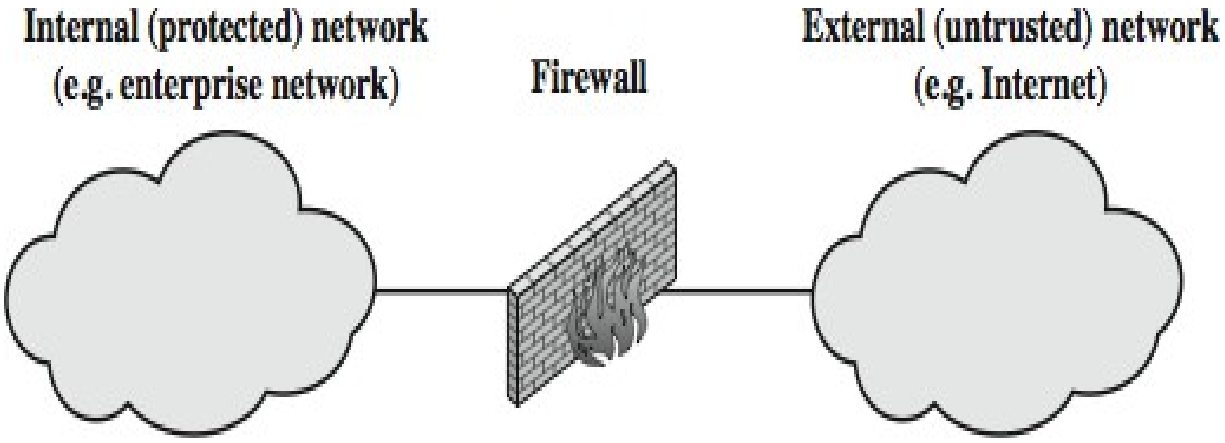
Payment Capture

- Consisting of a capture request and a capture response message
- Capture Request message,
    - the merchant generates, signs, and encrypts a capture request block, which includes the payment amount and the transaction ID.
- When the payment gateway receives the capture request message:
    - it decrypts and verifies the capture request block and
    - decrypts and verifies the capture token block.
- It then checks for consistency between the capture request and capture token.

- It then creates a clearing request that is sent to the issuer over the private payment network.
- This request causes funds to be transferred to the merchant's account.
- The gateway then notifies the merchant of payment in a **Capture Response message**.

FIREWALLS

- A firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter, forming a single choke point where security and audit can be imposed.



- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
    - provides a location for monitoring security-related events
    - is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs
    - A firewall can serve as the platform for IPSec to implement virtual private networks.
    - The firewall itself must be immune to penetration, since it will be a target of attack.

Techniques That Firewall Use To Control Access And Enforce Site's Security Policy

- **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound.
- **Direction control:** Determine the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service according to which user is attempting to access it.
- **Behaviour control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam.

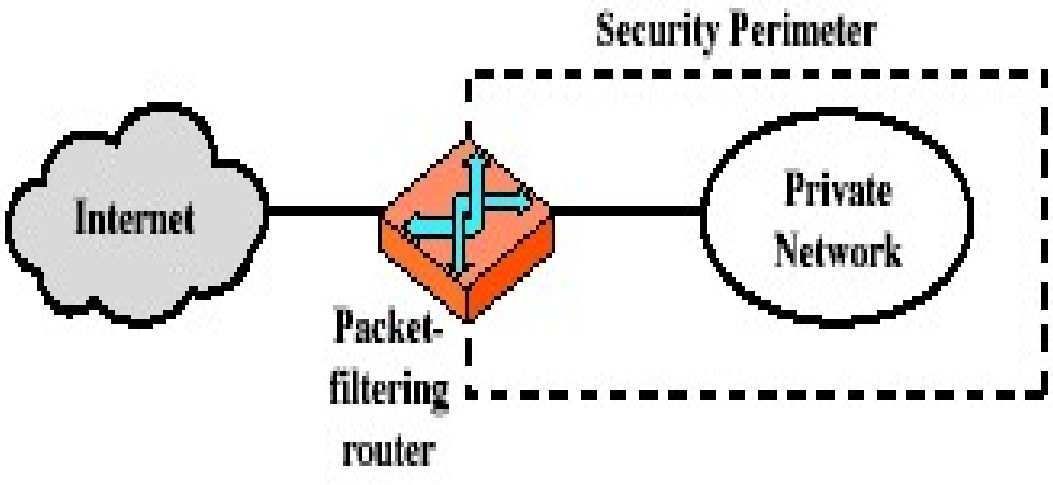
FIREWALL LIMITATIONS

- Cannot protect against attacks that bypass the firewall, eg PCs with dial-out capability to an ISP, or dial-in modem pool use
- Do not protect against internal threats, eg. disgruntled employee or one who cooperates with an attacker
- An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
- A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally

TYPES OF FIREWALLS

- PACKET FILTERS
- APPLICATION LEVEL GATEWAY
- Circuit-level gateway
- State ful inspection firewall

Firewalls – Packet Filters



(a) Packet-filtering router

- simplest of components

- 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

Allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.

The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts −

- **Selection criteria** − It is a used as a condition and pattern matching for decision making.
- **Action field** − This part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules.

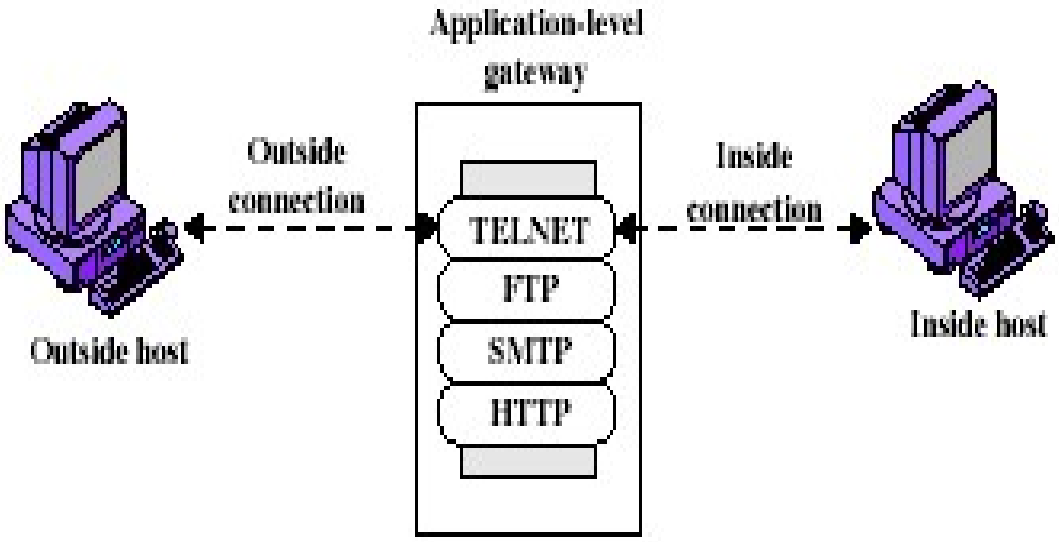
As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets.

Attacks on Packet Filters

- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- source routing attacks
  - attacker sets a route other than default
  - block source routed packets

- tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check

Firewalls - Application Level Gateway (or Proxy)



(b) Application-level gateway

- use an application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported
- An application-level gateway acts as a relay node for the application-level traffic. They intercept incoming and outgoing packets, run proxies that copy and forward information across the gateway, and function as a ***proxy server***, preventing any direct

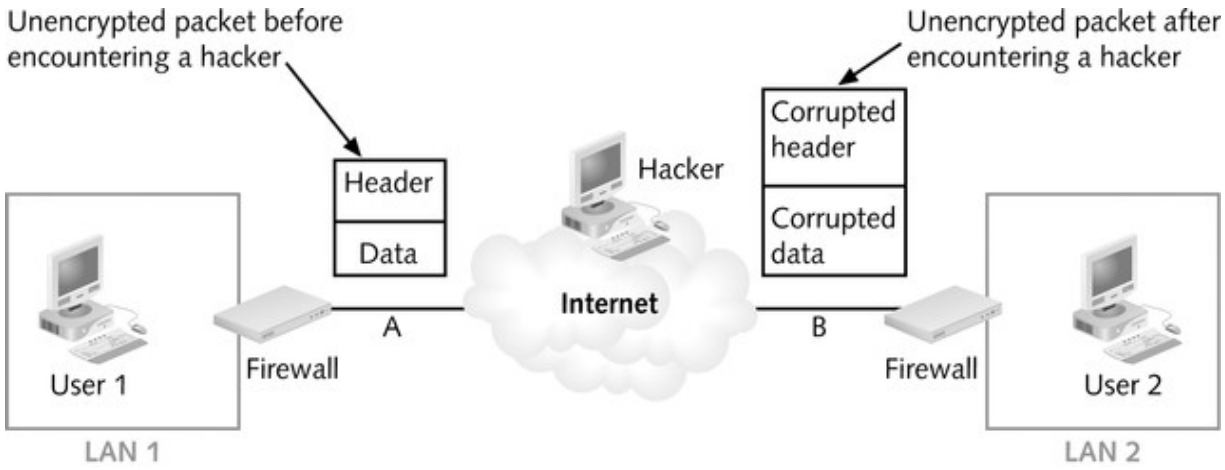
connection between a trusted server or client and an untrusted host.

- The proxies are application specific. They can filter packets at the application layer of the OSI model.
- An application-specific proxy accepts packets generated by only specified application for which they are designed to copy, forward, and filter. For example, only a Telnet proxy can copy, forward, and filter Telnet traffic.
- If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services that have no proxies configured. For example, if a gateway runs FTP and Telnet proxies, only packets generated by these services can pass through the firewall. All other services are blocked.

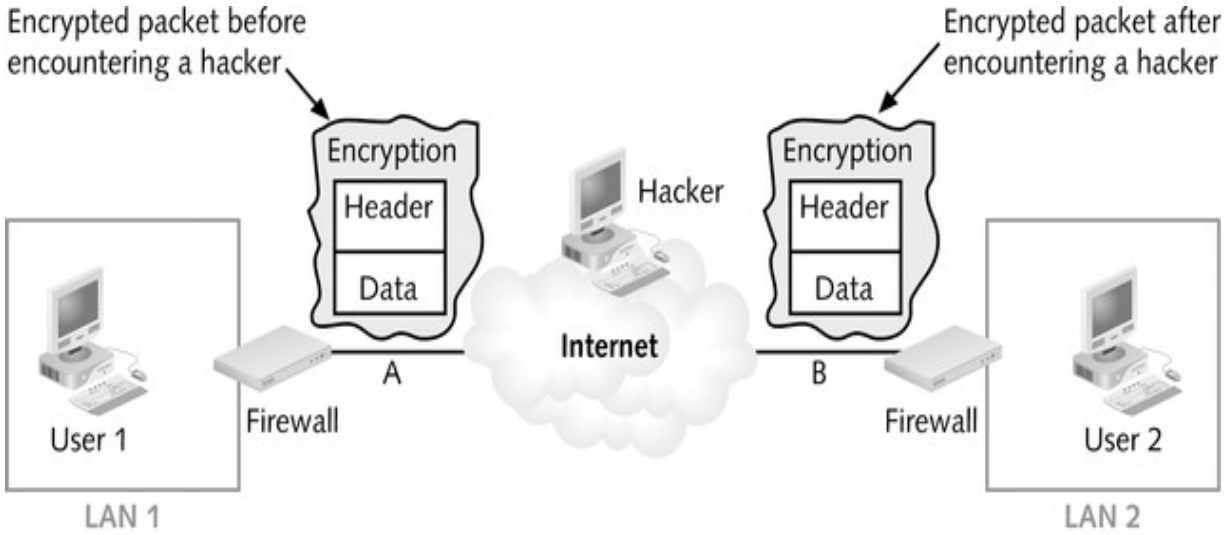
Encrypted Tunnels

- Firewalls and Encryption
  - Hackers take advantage of a lack of encryption
  - Encryption:
    - » Preserves data integrity
    - » Increases confidentiality
    - » Is relied upon by user authentication
    - » Plays a fundamental role in enabling VPNs

Hacker and an Unencrypted Packet



Hacker and an Encrypted Packet



– **The Cost of Encryption**

  » CPU resources and time

  » Encrypted packets may need to be padded to uniform length to ensure that some algorithms work effectively

  » Can result in slowdowns

  » Monitoring can burden system administrator

– **Preserving Data Integrity**

  » Even encrypted sessions can go wrong as a result of man-in- the-middle attacks

  » Encryption canperform non-repudiation using a digital signature.

– **Maintaining Confidentiality**

  » Encryption conceals information to render it unreadable to all but intended recipients

– **Authenticating Network Clients**

  » Firewalls need to trust that the person's claimed identity is genuine

  » Firewalls that handle encryption can be used to identify individuals who have "digital ID cards" that include encrypted codes

  » Digital signatures

» Public keys

» Private keys

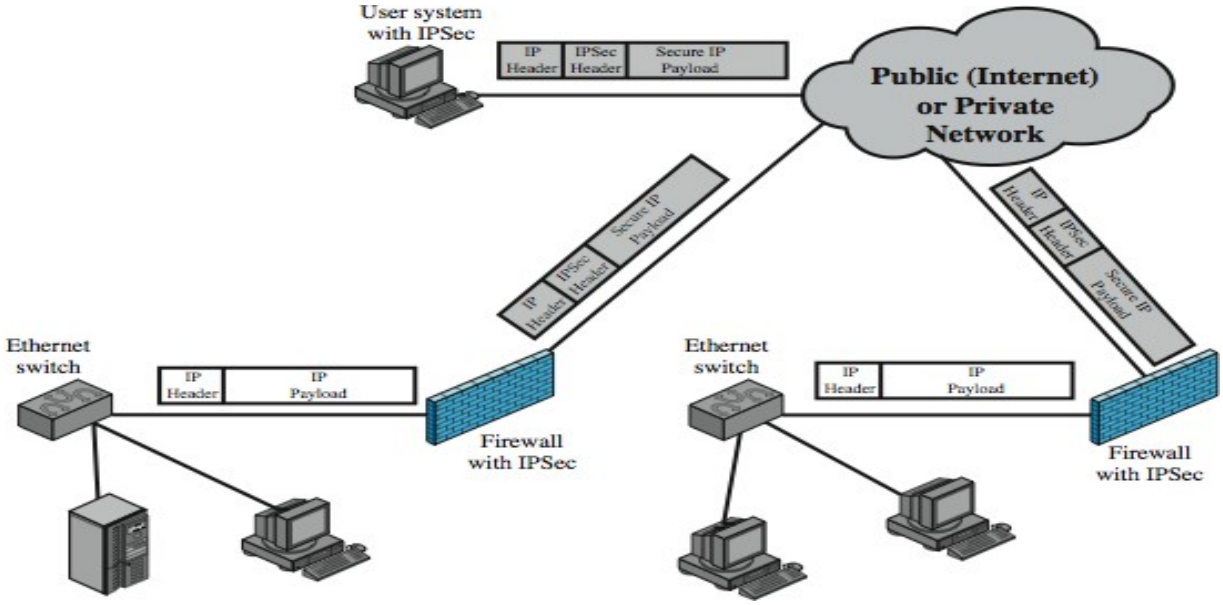
– **Enabling Virtual Private Networks (VPNs)**

– As an integral part of VPNs, encryption:

– Enables the firewall to determine whether the user who wants to connect to the VPN is actually authorized to do so

– Encodes the data payload to maintain privacy

Virtual Private Networks



- The virtual private network (VPN) offers an attractive solution to network managers.
- The VPN consists of a set of computers that is interconnected by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.
- At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs).
- The Internet or some other public network can be used to interconnect sites, providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider.
- That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.

- If IPSec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted.
- In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses. IPSec could be implemented in the boundary router, outside the firewall.
- However, this device is likely to be less secure than the firewall and thus less desirable as an IPSec platform.