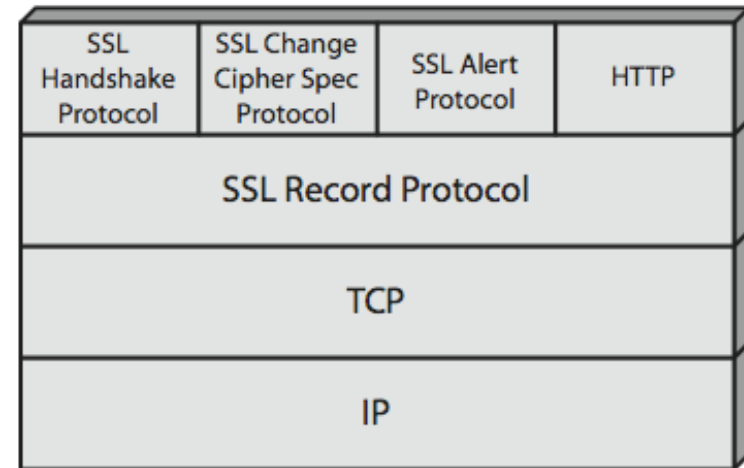


Internet Security Protocols and Standards

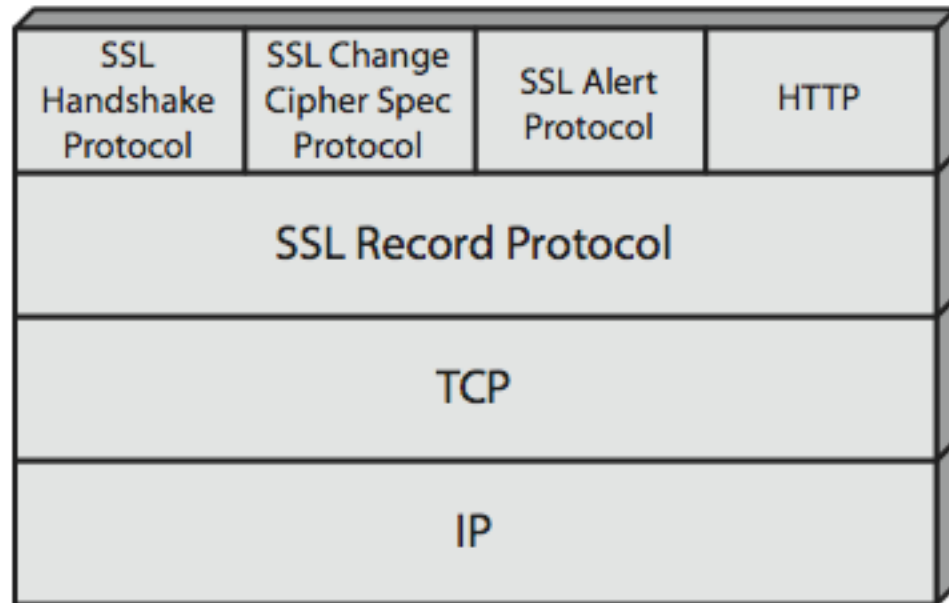


- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- IPv4 and IPv6 Security
- S/MIME (Secure/Multipurpose Internet Mail Extension)

Secure Sockets Layer (SSL)

- One of the most widely used security service is the SSL
- transport layer security service
 - originally developed by Netscape
 - version 3 designed with public input
- subsequently became Internet standard RFC2246: Transport Layer Security (TLS)
- use TCP to provide a reliable end-to-end service
- may be provided in underlying protocol suite (and is transparent to applications)
- or embedded in specific packages

SSL Protocol Stack

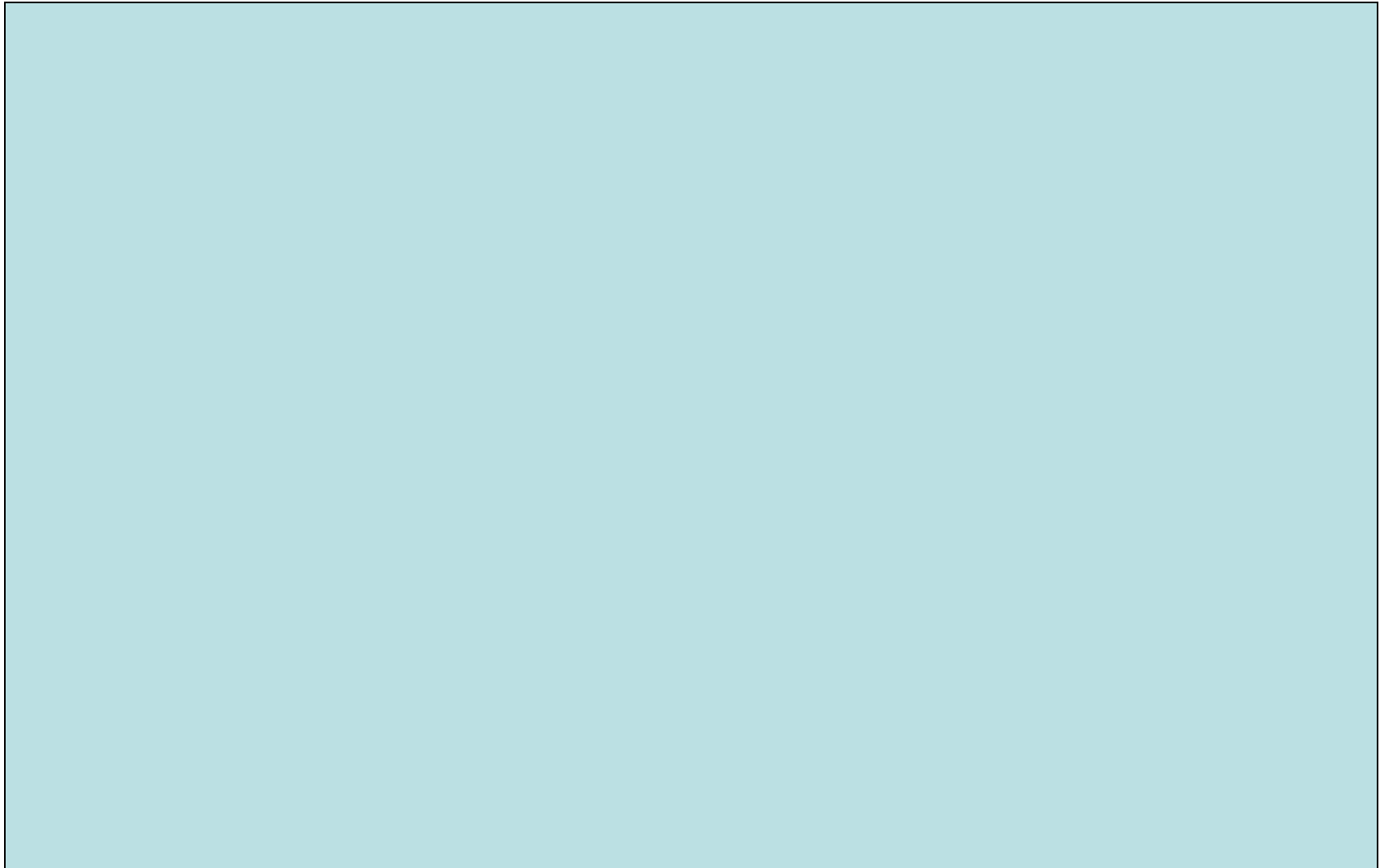


- **SSL session**
- **SSL connection**

SSL Record Protocol Services

- **Defines 2 services for SSL connections:**
- **message integrity**
 - defines a shared secret key that is used to form a message authentication code (MAC), which is similar to HMAC
- **confidentiality**
 - defines a shared secret key that is used for conventional encryption of SSL payloads.
 - the message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported as shown.
 - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128

SSL Record Protocol Operation



SSL Alert Protocol

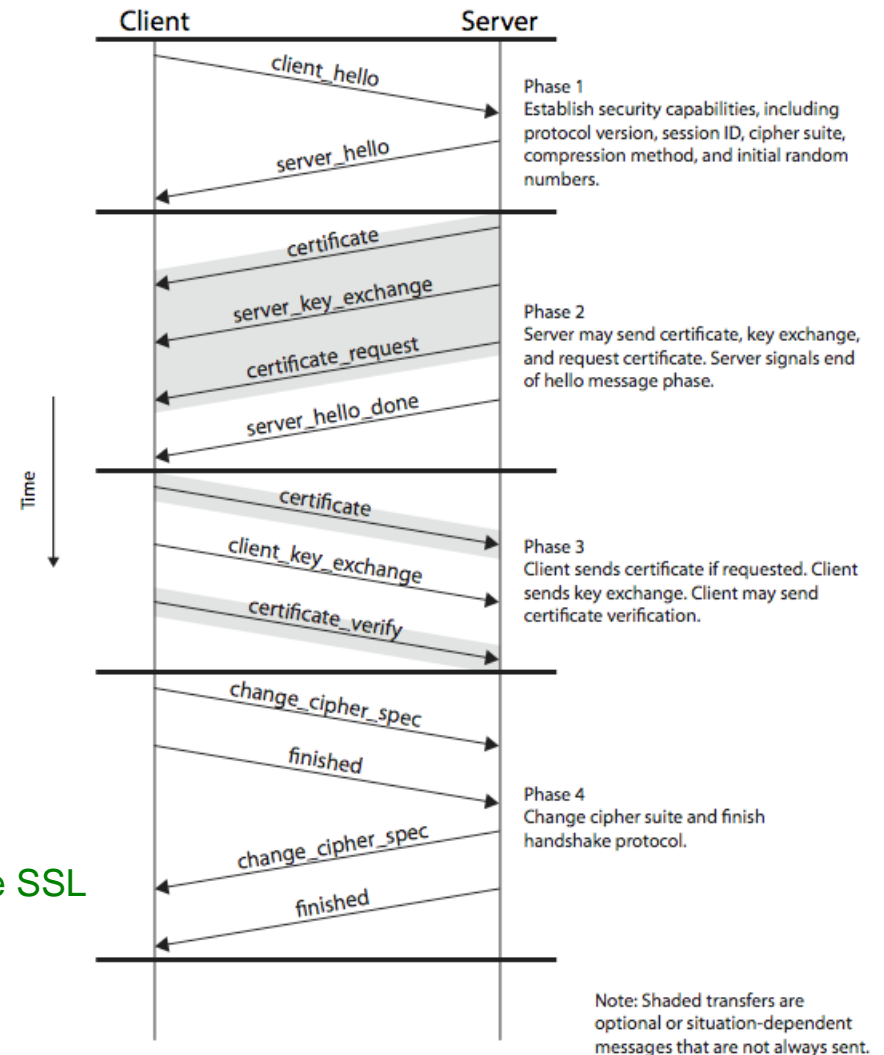
- conveys SSL-related alerts
- First byte indicates severity
 - Warning (1)
 - or fatal (2) – will terminate connection. Other connections on the same session may continue, but no new connections on this session may be established
- Second byte contains a code that indicates the specific alert
 - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
 - fatal: unexpected message, bad record MAC, decompression failure, handshake failure
- As with other applications that use SSL, alert messages are compressed and encrypted

SSL Handshake Protocol

- allows server & client to:
 - authenticate each other
 - to negotiate encryption & MAC algorithms
 - to negotiate cryptographic keys to be used

- comprises a series of messages in phases
 1. Establish Security Capabilities
 2. Server Authentication and Key Exchange
 3. Client Authentication and Key Exchange
 4. Finish

- SSL Change Cipher Spec Protocol
 - one of 3 SSL specific protocols which use the SSL Record protocol
 - a single message
 - causes pending state to become current



IP Security

- various application security mechanisms
 - eg. S/MIME, PGP,, SSL/HTTPS
- security concerns cross protocol layers
- hence would like security implemented by the network for all applications
- authentication & encryption security features included in next-generation IPv6
- also usable in existing IPv4

IP Headers

- IPv4

Version	Header Length	Type of service	Datagram Length (bytes)	
16-bit Identifier		Flags	13-bit fragmentation offset	
Time To Live	Upper-layer protocol	Header Checksum		
32-bit Source IP address				
32-bit Destination IP address				
Options (if any)				
Data				

32 bits

- IPv6

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
128-bit Source IP address				
128-bit Destination IP address				
Data				

32 bits

IPsec

- IP-level security encompasses three functional areas:
 - Authentication – this mechanism assures that a received packet was transmitted by the party identified as the source in the packet header, and that the packet has not been altered in transit
 - Confidentiality – this facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties
 - Key management – this facility is concerned with the secure exchange of keys.
- The key management IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet

IPsec Uses

The principal feature of IPsec that enables it to support varied applications is that it can encrypt and/or authenticate *all* traffic at the IP level. Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.



Benefits of IPsec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
 - original Internet RFC822 email was text only
 - MIME provided support for varying content types (text, images, video audio, application)
 - S/MIME adds security enhancements

- S/MIME provides the ability to sign and/ or encrypt email messages

- S/MIME support in many mail agents
 - eg MS Outlook, Firefox, Mac Mail etc

S/MIME Functions

- S/MIME content-types support new functions, including.:

Enveloped data: This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.

Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypt that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

Typical S/MIME Process