

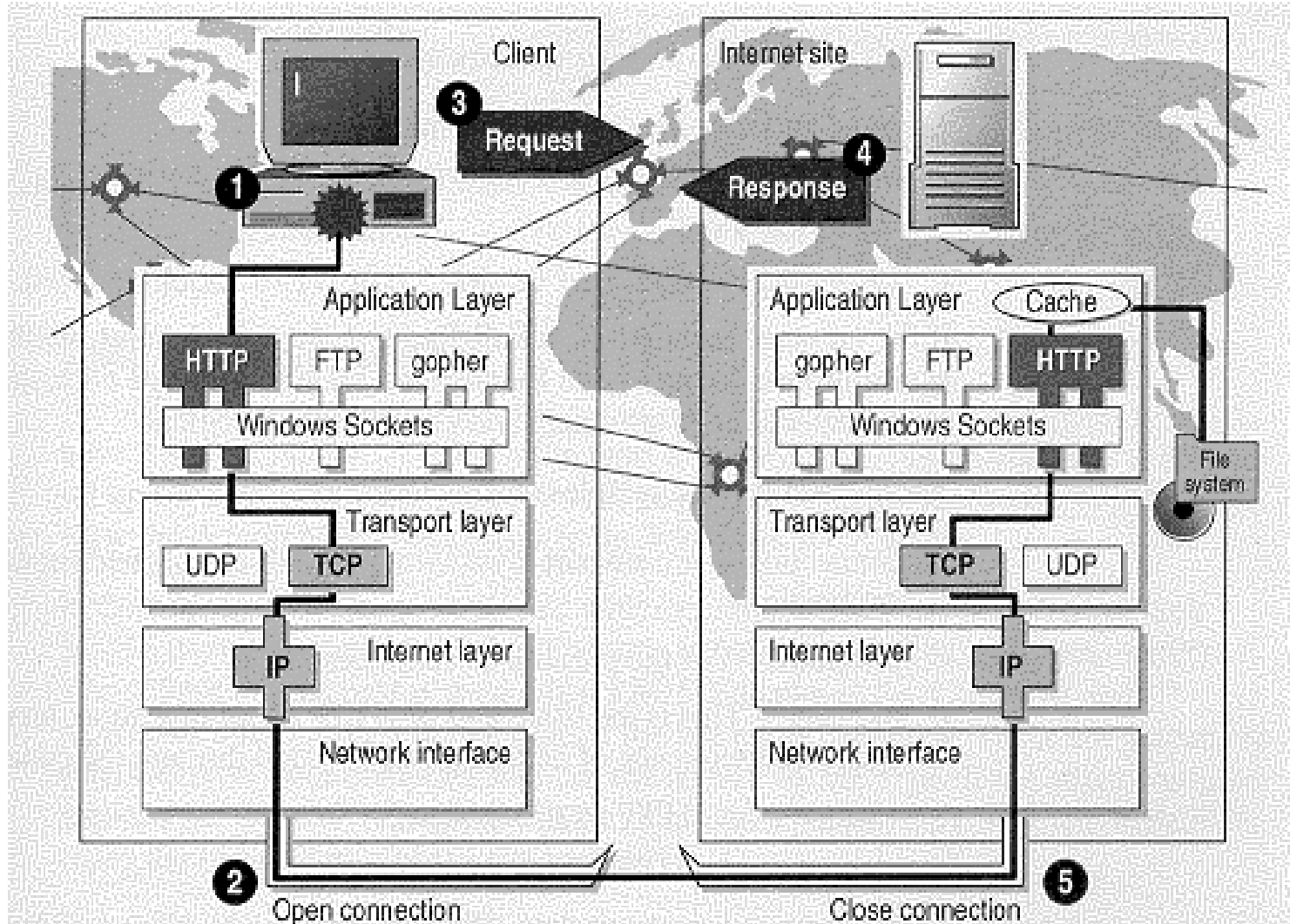
SSL - Secure Sockets Layer

The Internet Engineering Task Force (IETF) standard called Transport Layer Security (TLS) is based on SSL.

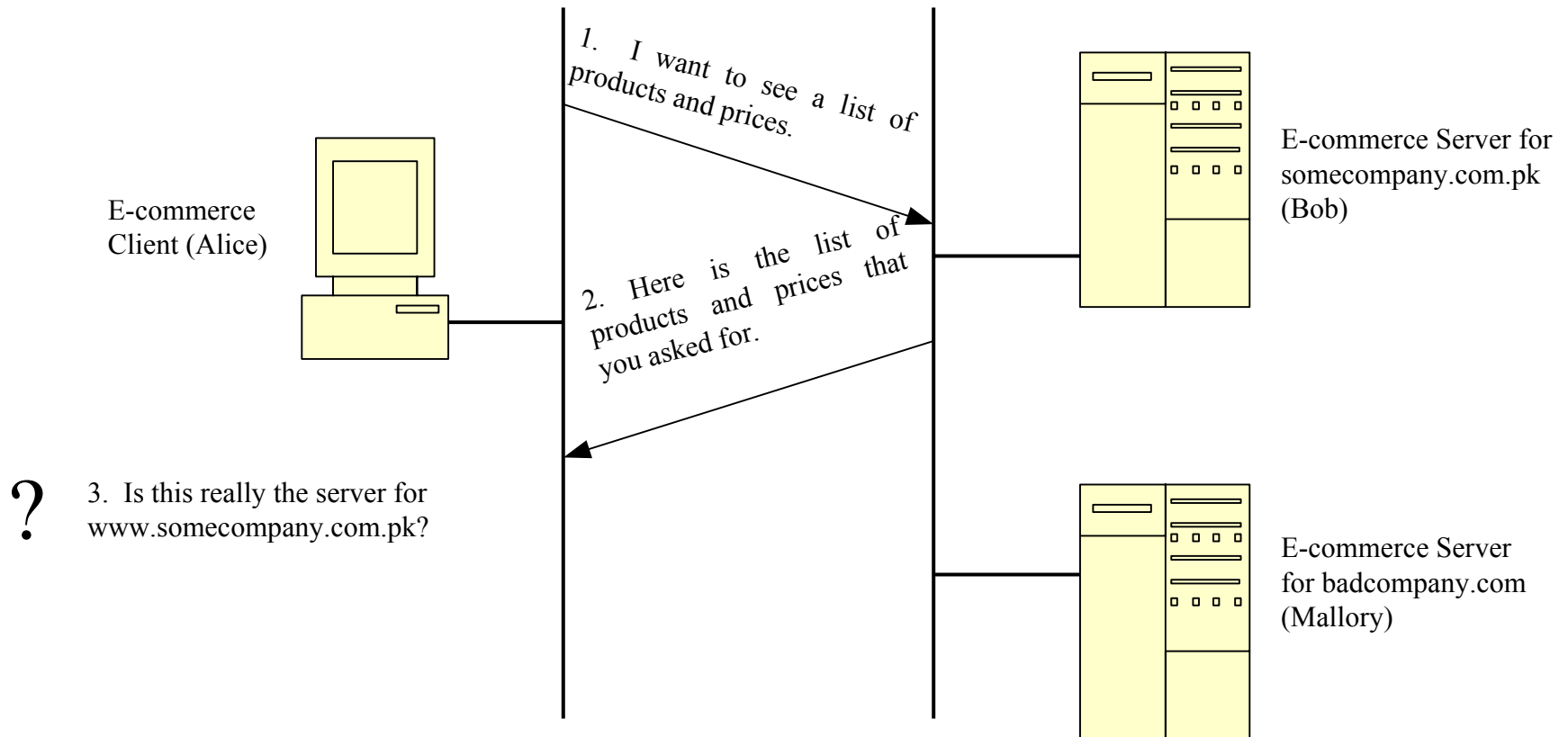
TCP/IP Protocol Suite

- The Transmission Control Protocol/Internet Protocol (TCP/IP) governs the transport and routing of data over the Internet.
- Other protocols, such as the HyperText Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), or Internet Messaging Access Protocol (IMAP), run "on top of" TCP/IP in the sense that they all use TCP/IP to support typical application tasks such as displaying web pages or running email servers.

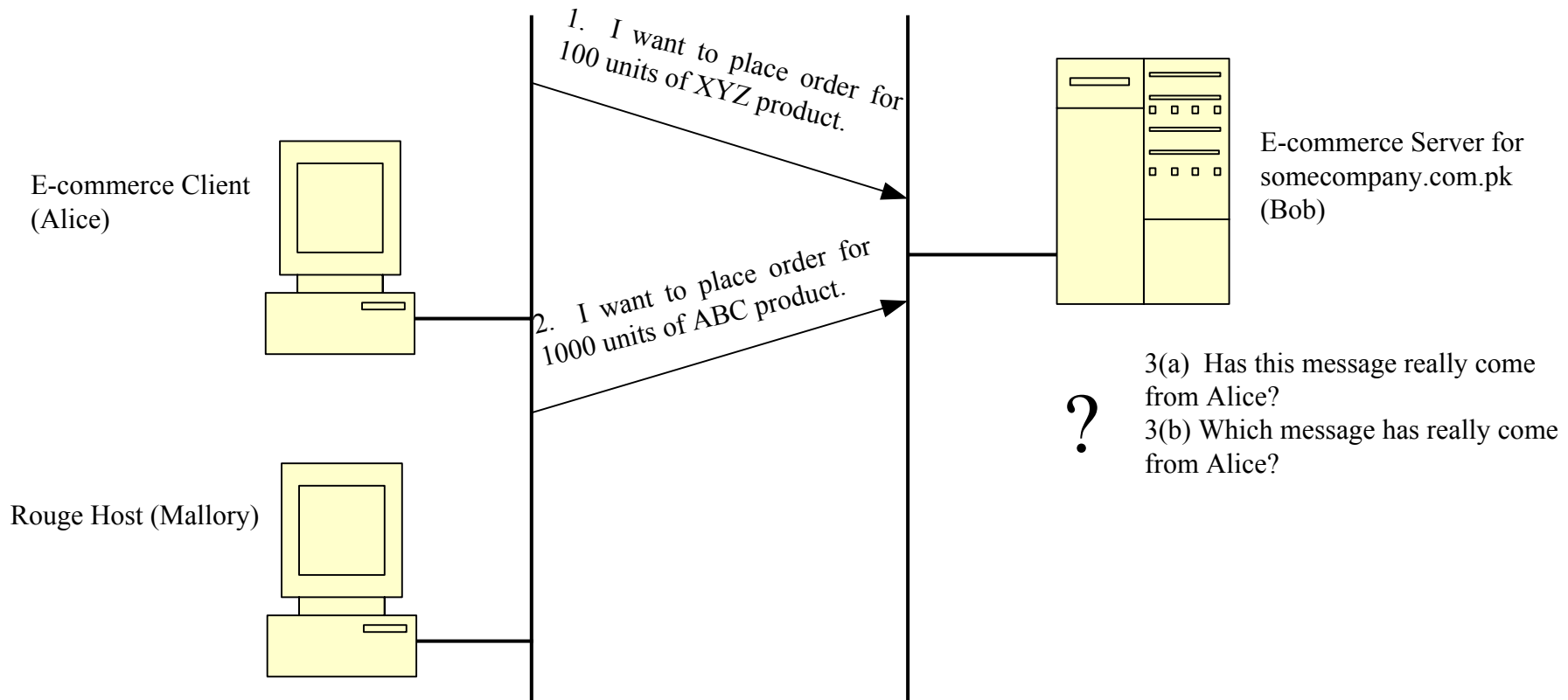
IP and Other Protocols



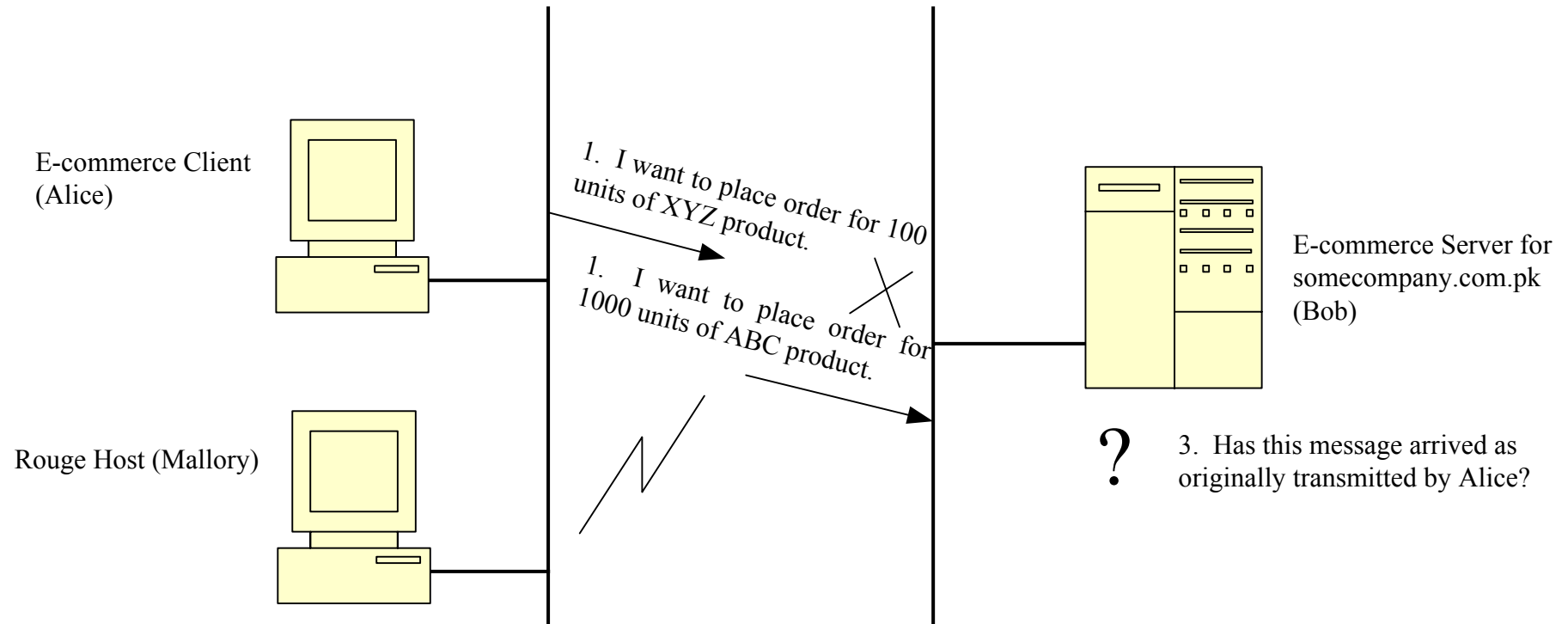
E-commerce Security Requirements - Authenticity



E-commerce Security Requirements - Authenticity

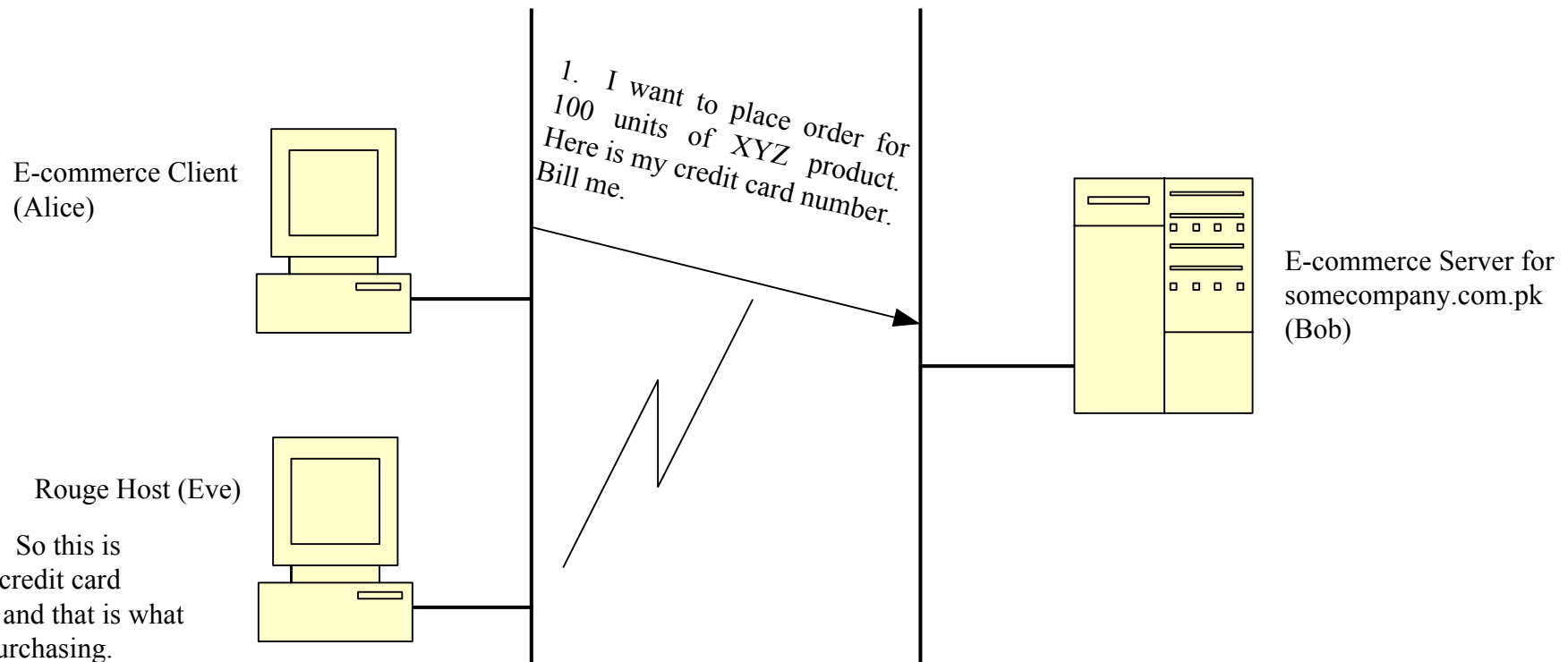


E-commerce Security Requirements - Integrity



E-commerce Security

Requirements - Confidentiality



TCP/IP Protocol Suite and Security

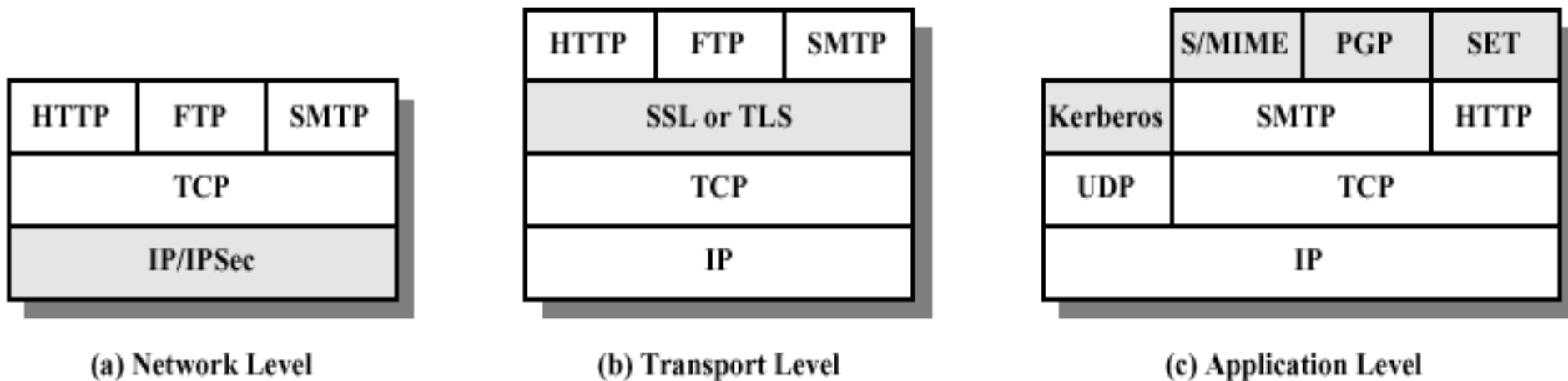
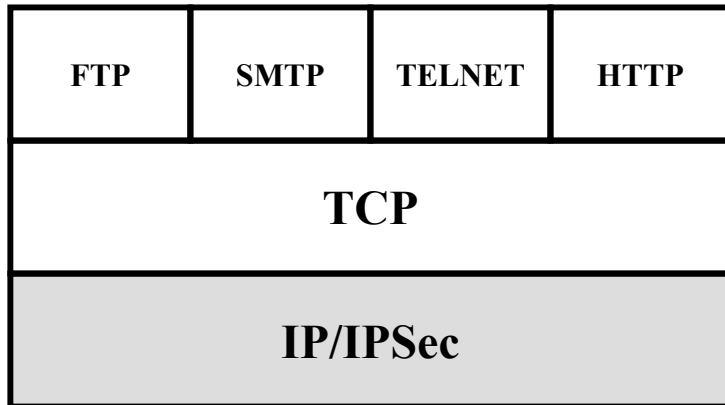
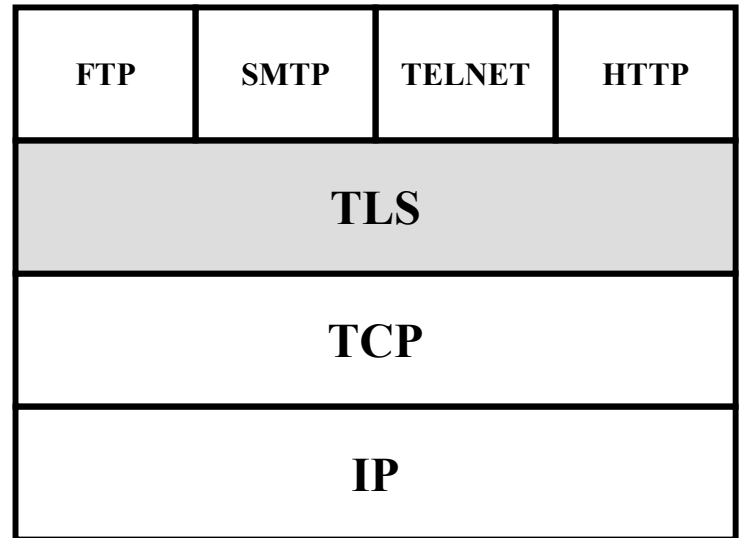


Figure 14.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack



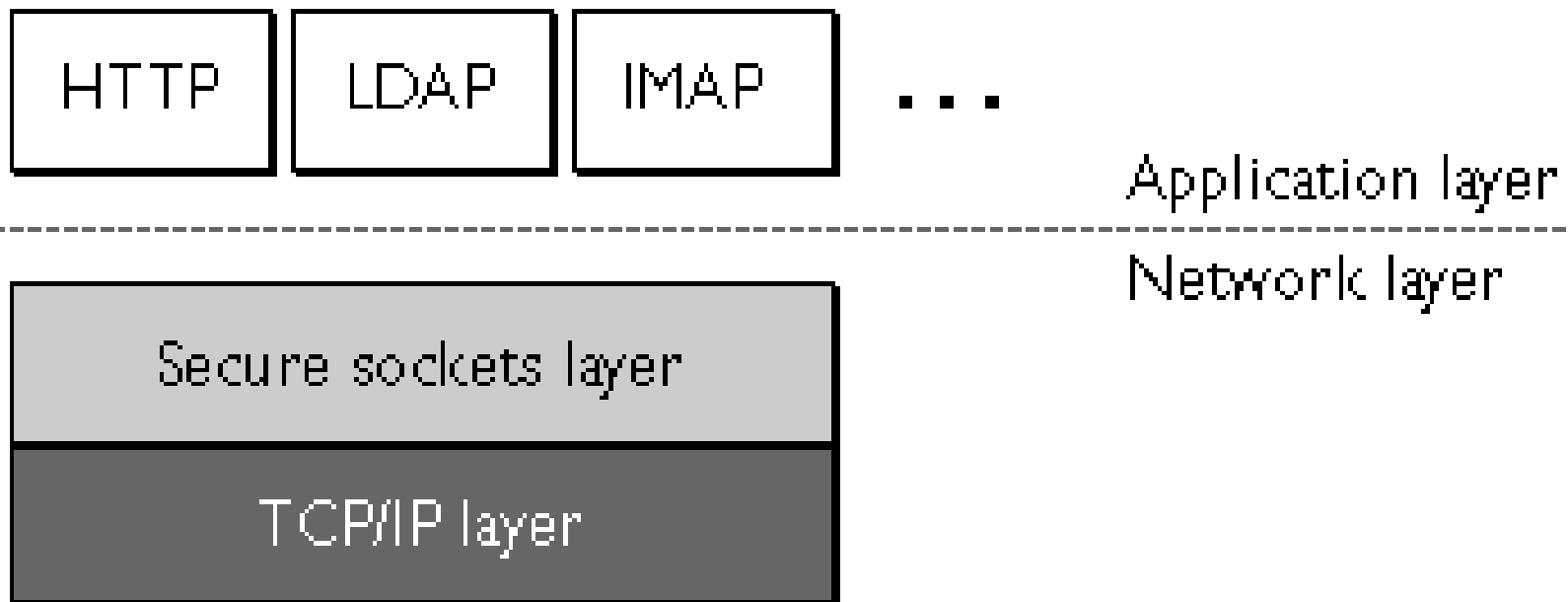
IPSec is located at the
Network Level



TLS is located above the
Transport Level

TCP/IP Protocol Suite and Security

The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.



A Comparison of Threats on the Web

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none">•Modification of user data•Trojan horse browser•Modification of memory•Modification of message traffic in transit	<ul style="list-style-type: none">•Loss of information•Compromise of machine•Vulnerability to all other threats	Cryptographic checksums
Confidentiality	<ul style="list-style-type: none">•Eavesdropping on the Net•Theft of info from server•Theft of data from client•Info about network configuration•Info about which client talks to server	<ul style="list-style-type: none">•Loss of information•Loss of privacy	Encryption, web proxies
Denial of Service	<ul style="list-style-type: none">•Killing of user threads•Flooding machine with bogus requests•Filling up disk or memory•Isolating machine by DNS attacks	<ul style="list-style-type: none">•Disruptive•Annoying•Prevent user from getting work done	Difficult to prevent
Authentication	<ul style="list-style-type: none">•Impersonation of legitimate users•Data forgery	<ul style="list-style-type: none">•Misrepresentation of user•Belief that false information is valid	Cryptographic techniques

Services Provided by SSL

- SSL encrypts data so that no one who intercepts is able to read it.
- SSL can assure a client that they are dealing with the real server they intended to connect to.
- SSL can prevent any unauthorized clients from connecting to the server.
- SSL prevents anyone from meddling with data going to or coming from the server.

Services Provided by SSL

- These capabilities address fundamental concerns about communication over the Internet and other TCP/IP networks:
- SSL server authentication
- SSL client authentication
- An encrypted SSL connection

SSL Server Authentication

- SSL server authentication allows a user to confirm a server's identity.
- SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.
- This confirmation might be important if the user, for example, is sending a credit card number over the network and wants to check the receiving server's identity.

SSL Client Authentication

- SSL client authentication allows a server to confirm a user's identity.
- Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs.
- This confirmation might be important if the server, for example, is a bank sending confidential financial information to a customer and wants to check the recipient's identity.

An encrypted SSL connection

- An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality.
- Confidentiality is important for both parties to any private transaction.
- In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering--that is, for automatically determining whether the data has been altered in transit.

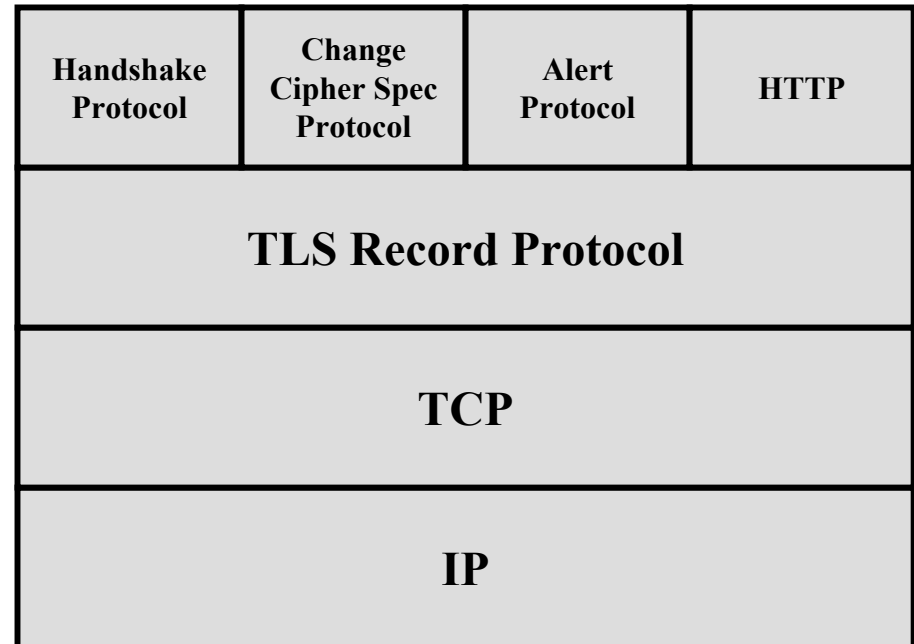
SSL Movie



Video Clip

SSL Sub-protocols

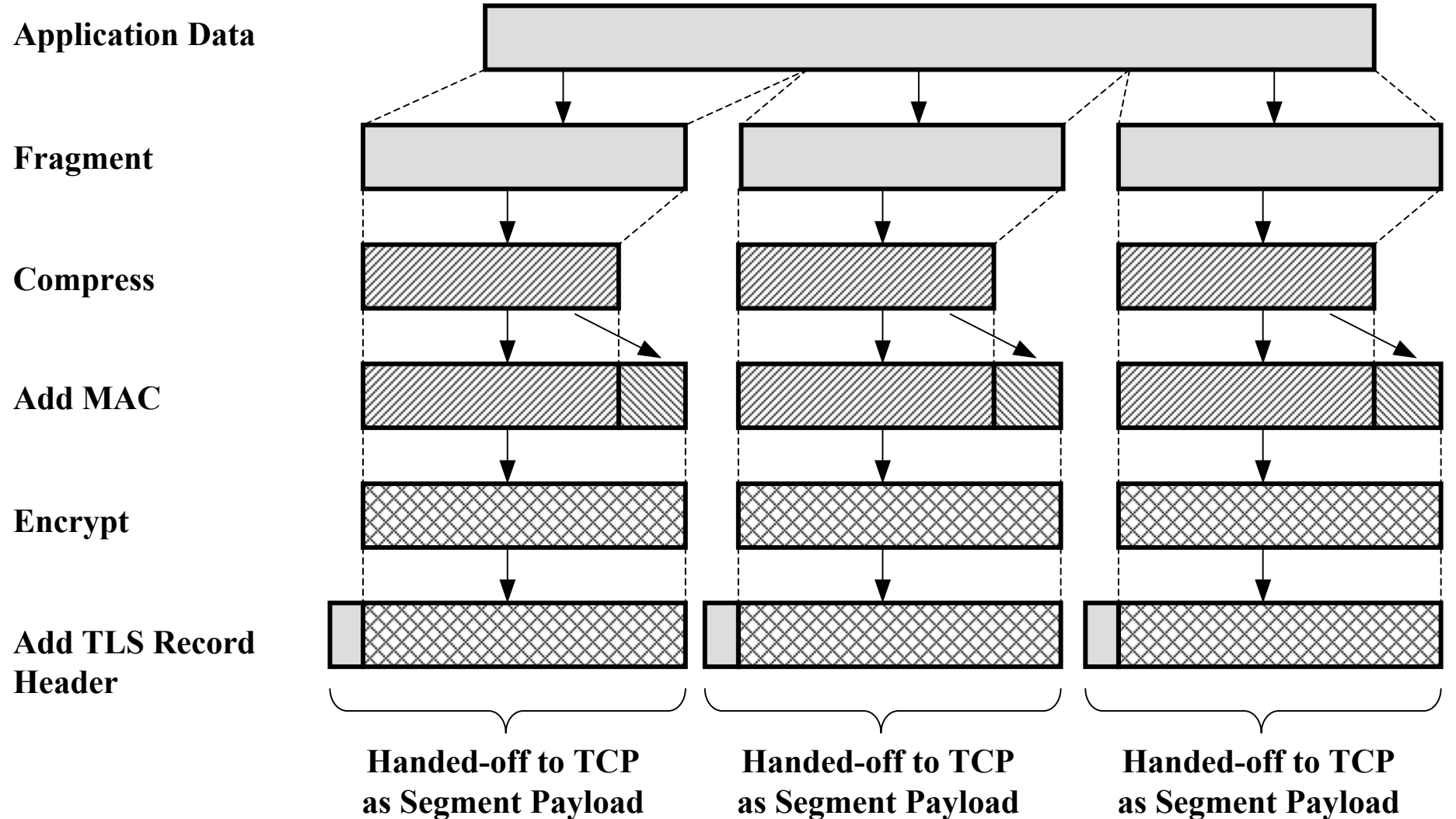
- The SSL protocol includes two major sub-protocols:
- the SSL record protocol
- The SSL Control Protocols
 - ⊗ the SSL handshake protocol
 - ⊗ Change Cipher Spec Protocol
 - ⊗ Alert Protocol



The SSL Record Protocol

- The SSL record protocol defines the format used to transmit data
- The SSL record protocols 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)

SSL Record Protocol Operation



SSL Record Format

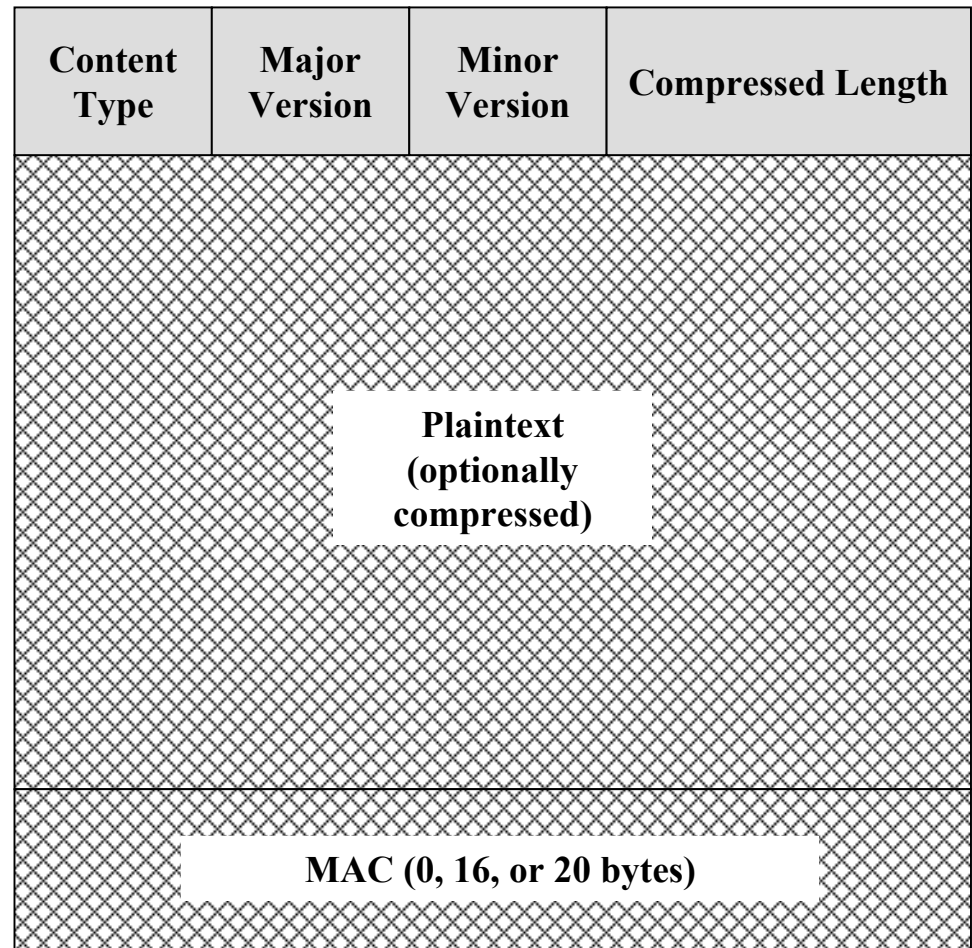
Content Type (8 bits):
The higher-layer protocol used to process the enclosed fragment.

Major Version (8 bits):
Indicates the major version of SSL in use.
E.g. 3

Minor Version (8 bits):
e.g. 0

Compressed length (16 bits): The length in bytes of the plain text fragment. The maximum value is $2^{14} + 2048$

Encrypted



SSL Record Protocol Payload

1 byte



(a) Change
Cipher Spec
Protocol

1 byte

3 bytes

3 bytes



(c) Handshake
Protocol

1 byte

1 byte



(b) Alert Protocol

Up to $2^{14} + 2048$ bytes



(d) Other Upper Layer Protocol as TLS
Payload

The SSL Handshake protocol

- The SSL handshake protocol involves using the SSL record protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection. This exchange of messages is designed to facilitate the following actions:
 - ⊗ Authenticate the server to the client.
 - ⊗ Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
 - ⊗ Optionally authenticate the client to the server.
 - ⊗ Use public-key encryption techniques to generate shared secrets.
 - ⊗ Establish an encrypted SSL connection.

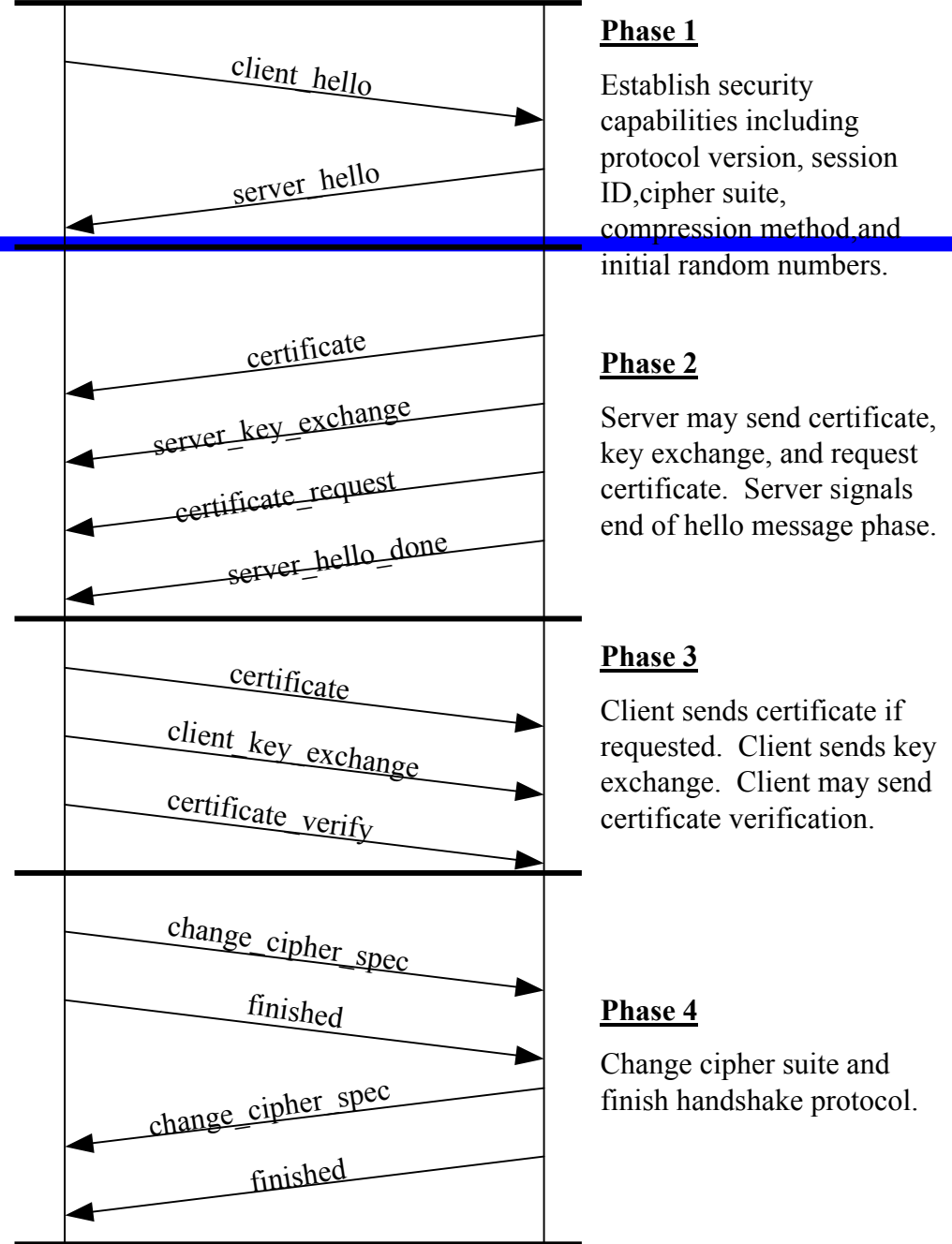
SSL Handshake Protocol Message Types

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

Client

Server

Time
↓



Phase 1

Establish security capabilities including protocol version, session ID, cipher suite, compression method and initial random numbers.

Phase 2

Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3

Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4

Change cipher suite and finish handshake protocol.

Read the TLS Paper

