Plan of Talk

- **Transport Layer Security**
- **SSL**

Web Security Considerations

- The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets
- The following characteristics of Web usage suggest the need for tailored security tools:
  - Web servers are relatively easy to configure and manage
  - Web content is increasingly easy to develop
  - The underlying software is extraordinarily complex
    - May hide many potential security flaws
  - 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

	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•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	•Loss of information •Loss of privacy	Encryption, Web proxies
Denial of Service	•Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks	•Disruptive •Annoying •Prevent user from getting work done	Difficult to prevent
Authentication	•Impersonation of legitimate users •Data forgery	•Misrepresentation of user •Belief that false information is valid	Cryptographic techniques

Table 17.1 A Comparison of Threats on the Web

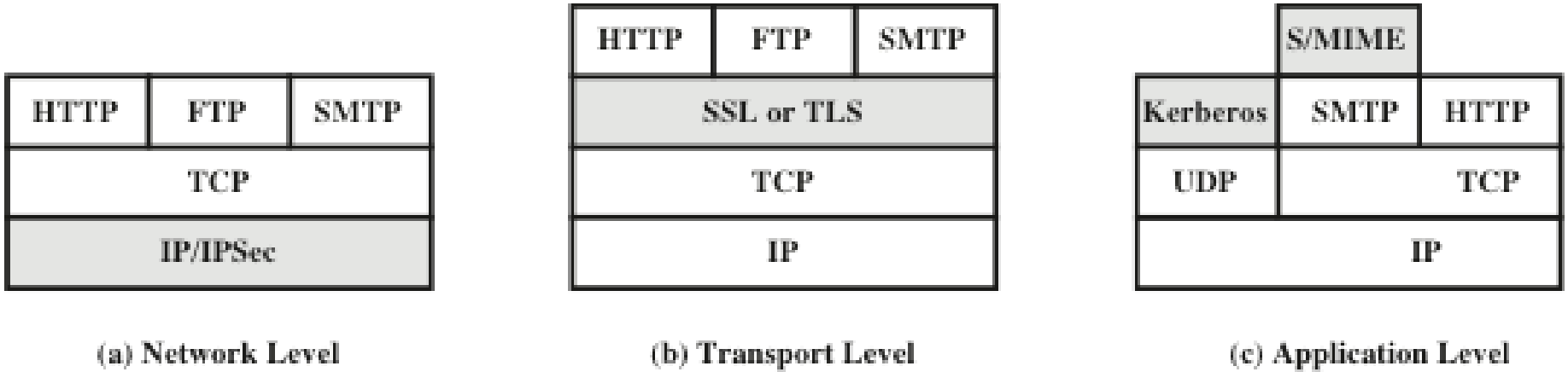


Figure 17.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Secure Sockets Layer (SSL)

- One of the most widely used security services
- 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

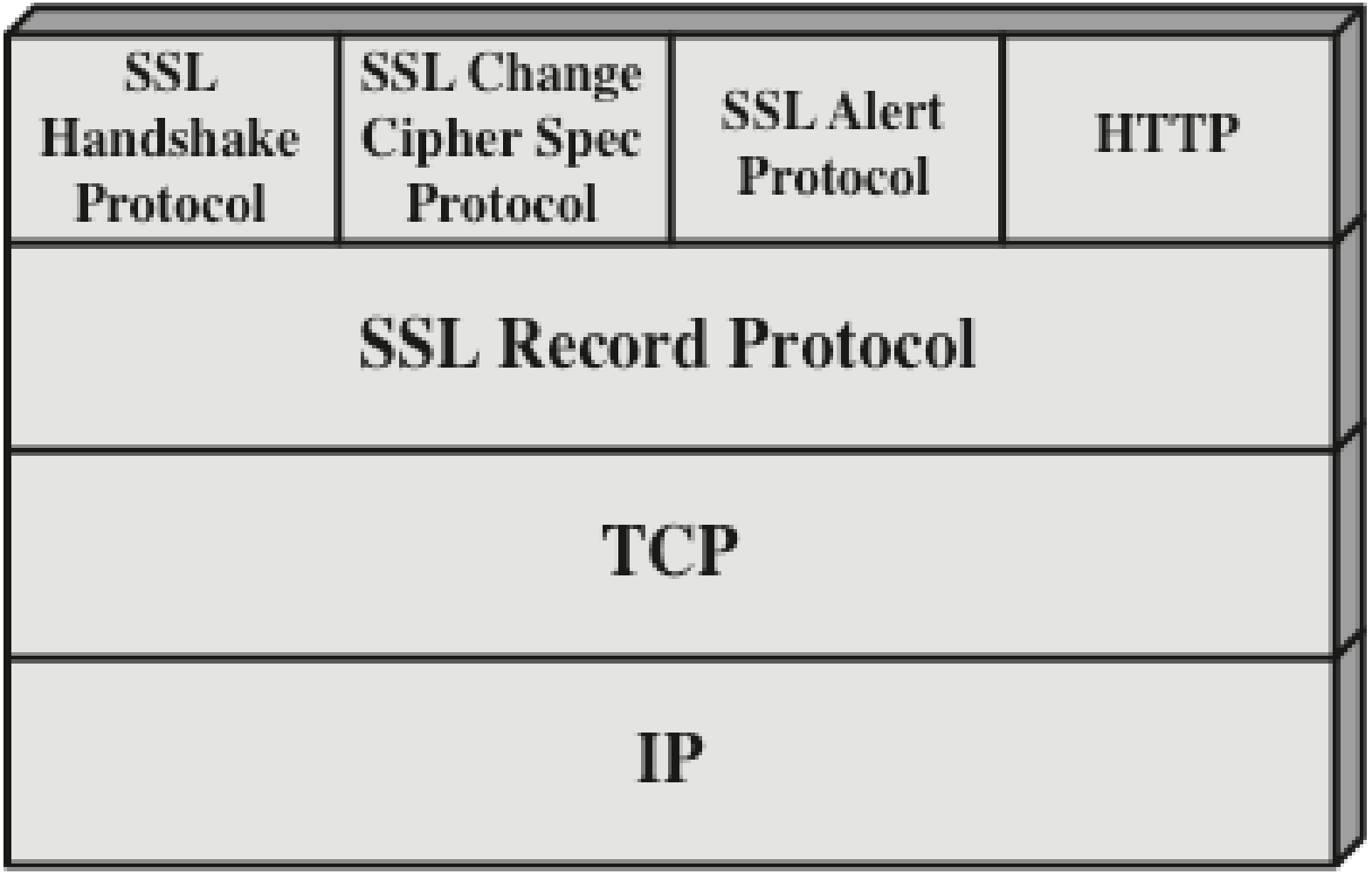


Figure 17.2 SSL Protocol Stack

SSL Architecture

- Two important SSL concepts are:

SSL connection

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

SSL session

- An association between a client and a server
- Created by the Handshake Protocol
- Define a set of cryptographic security parameters which can be shared among multiple connections
- Are used to avoid the expensive negotiation of new security parameters for each connection

A session state is defined by the following parameters:

Session identifier	Peer certificate	Compression method	Cipher spec	Master secret	Is resumable
An arbitrary byte sequence chosen by the server to identify an active or resumable session state	An X509.v3 certificate of the peer; this element of the state may be null	The algorithm used to compress data prior to encryption	Specifies the bulk data encryption algorithm and a hash algorithm used for MAC calculation; also defines cryptographic attributes such as the hash_size	48-byte secret shared between the client and the server	A flag indicating whether the session can be used to initiate new connections

A connection state is defined by the following parameters:

Server and client random
- Byte sequences that are chosen by the server and client for each connection

Server write MAC secret
- The secret key used in MAC operations on data sent by the server

Client write MAC secret
- The secret key used in MAC operations on data sent by the client

Server write key
- The secret encryption key for data encrypted by the server and decrypted by the client

Client write key
- The symmetric encryption key for data encrypted by the client and decrypted by the server

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

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

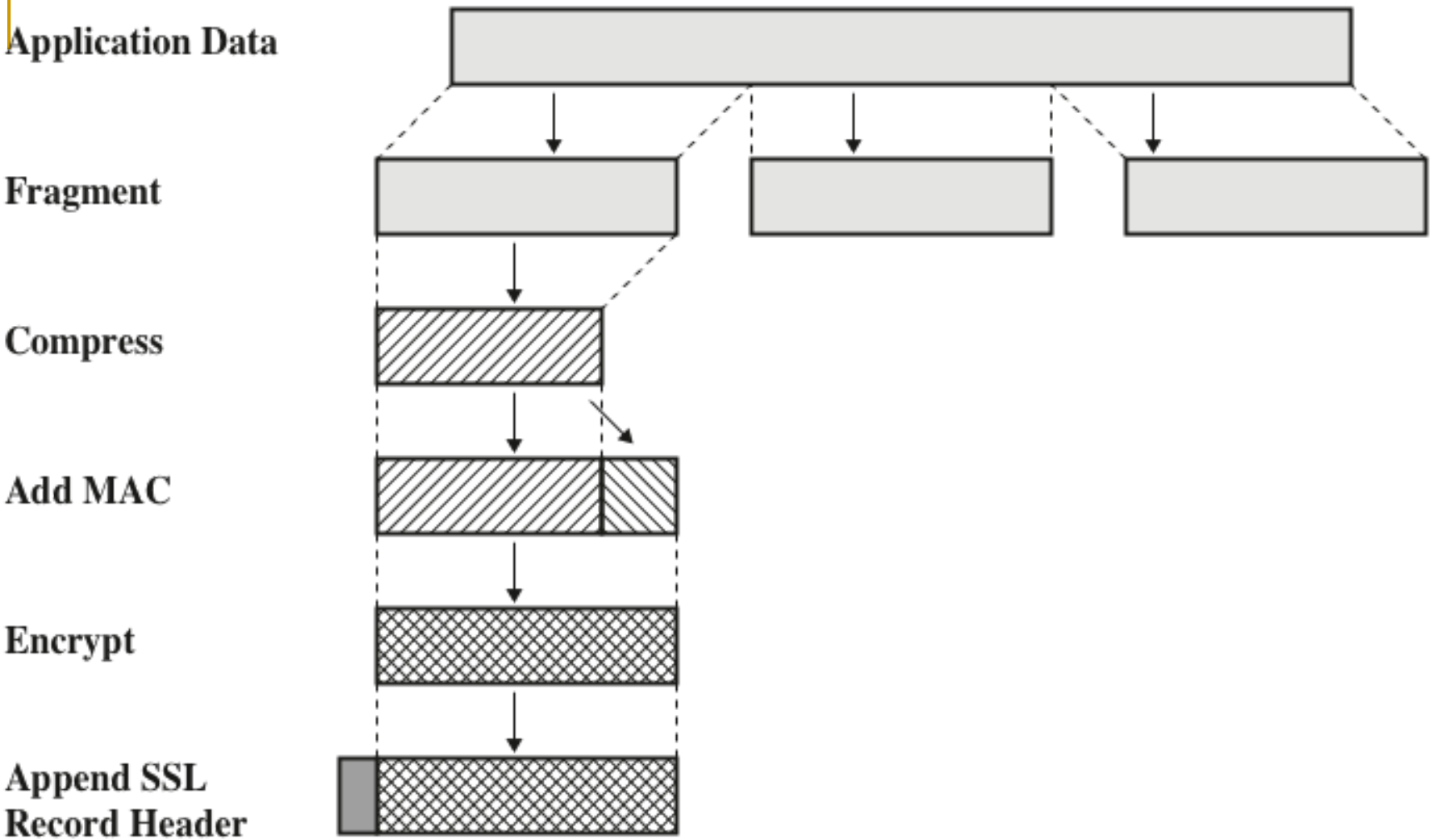


Figure 17.3 SSL Record Protocol Operation

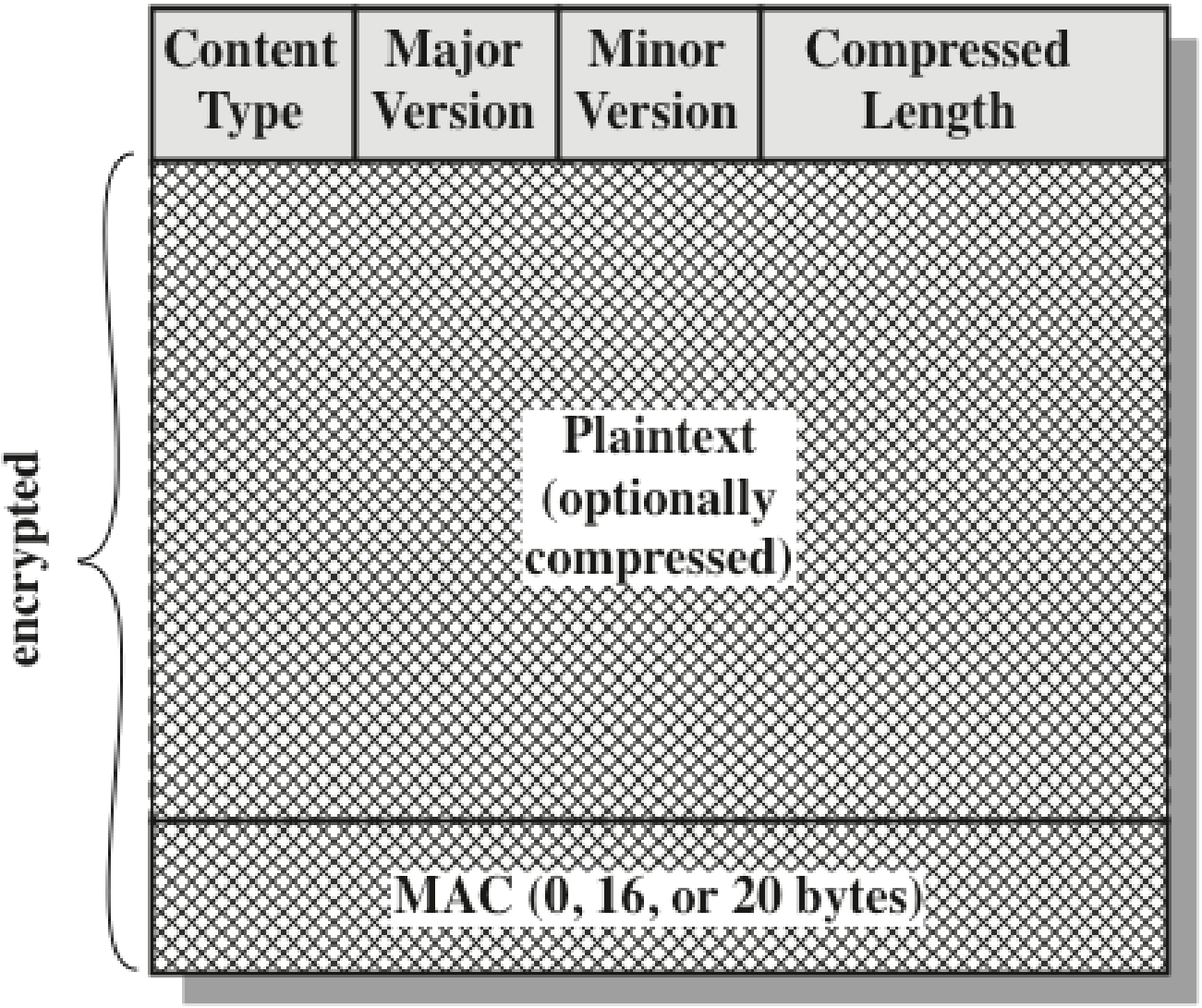
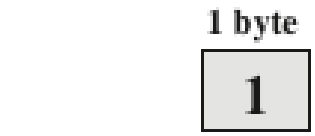
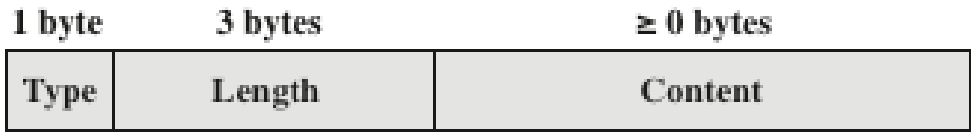


Figure 17.4 SSL Record Format



(a) Change Cipher Spec Protocol



(c) Handshake Protocol

(b) Alert Protocol

(d) Other Upper-Layer Protocol (e.g., HTTP)

Figure 17.5 SSL Record Protocol Payload

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

Table 17.2 SSL Handshake Protocol Message Types

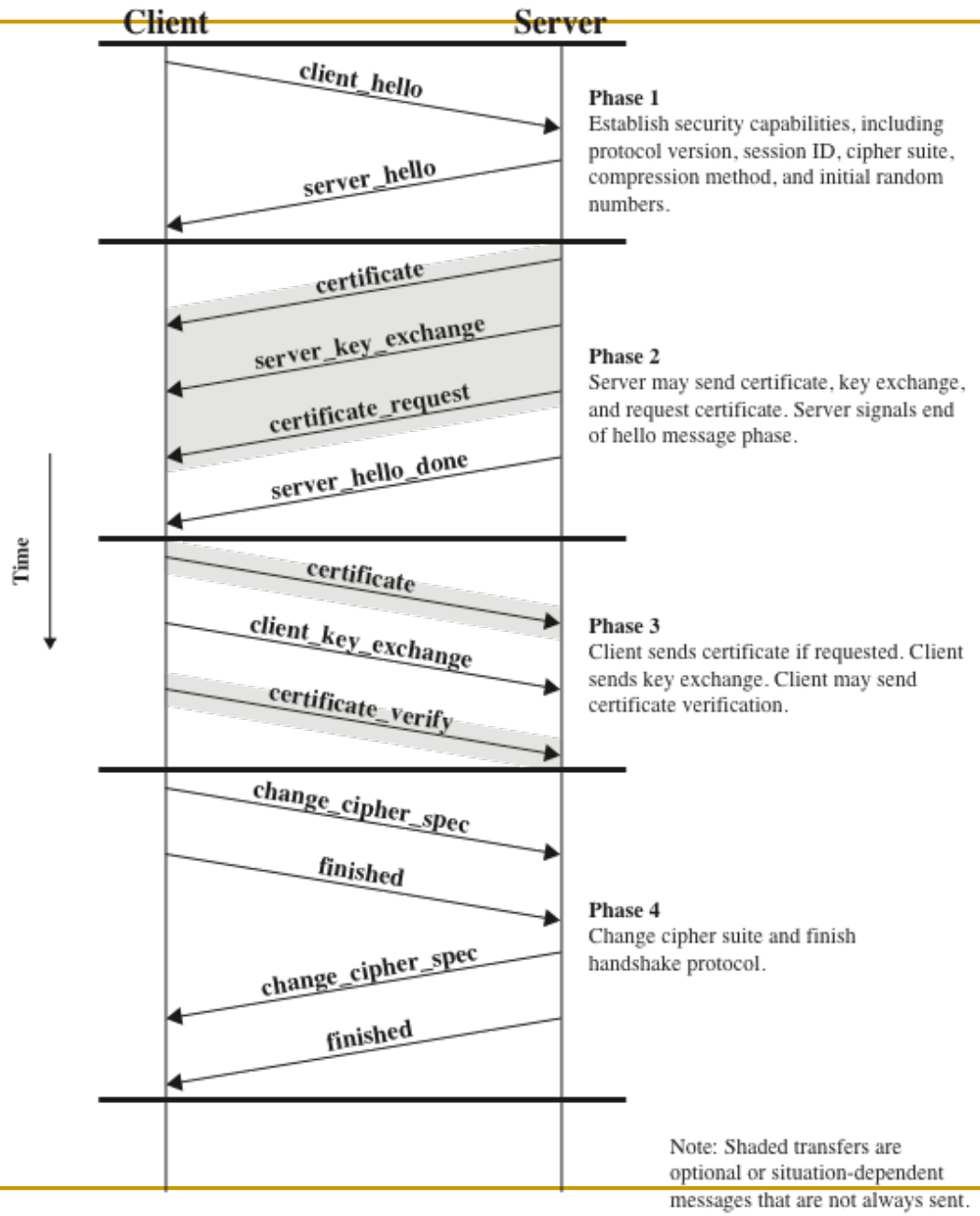


Figure 17.6 Handshake Protocol Action

Cryptographic Computations

- Two further items are of interest:
  - The creation of a shared master secret by means of the key exchange
    - The shared master secret is a one-time 48-byte value generated for this session by means of secure key exchange
  - The generation of cryptographic parameters from the master secret
    - CipherSpecs require a client write MAC secret, a server write MAC secret, a client write key, a server write key, a client write IV, and a server write IV which are generated from the master secret in that order
      - These parameters are generated from the master secret by hashing the master secret into a sequence of secure bytes of sufficient length for all needed parameters

Summary

- Web Security Considerations
- SSL
  - Other topics in the book (Not examinable)
    - Transport Layer Security
    - HTTPS
    - SSH