Table of Contents

17.1 Web Security Considerations

Web Security Threats

- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable
- have a variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

17.2 Secure Sockets Layer

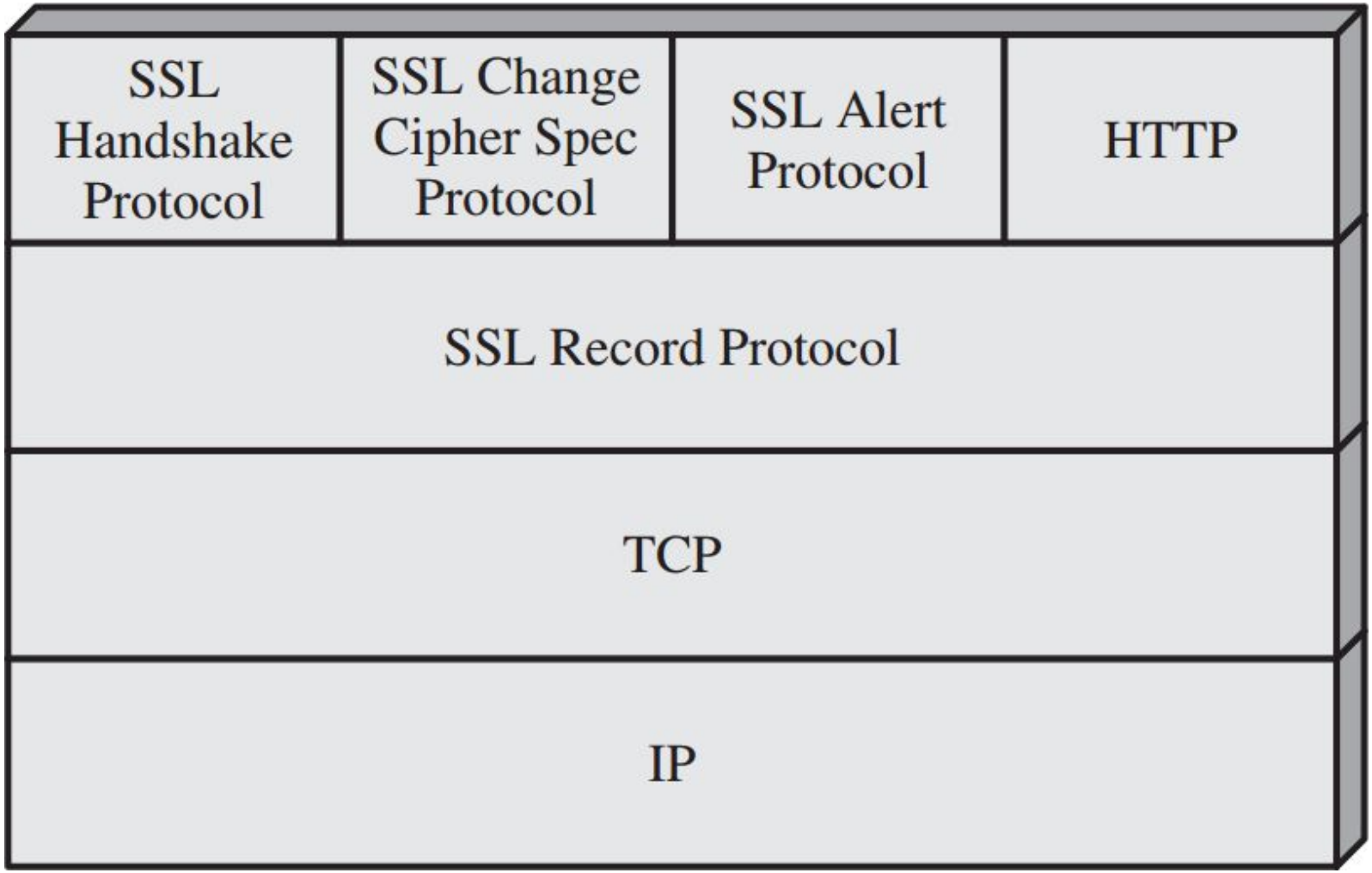
Secure Sockets Layer

- transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS

  (Transport Layer Security)

- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols

SSL Architecture



SSL Protocol Stack

SSL Architecture

Two important SSL concepts are the SSL session and the SSL

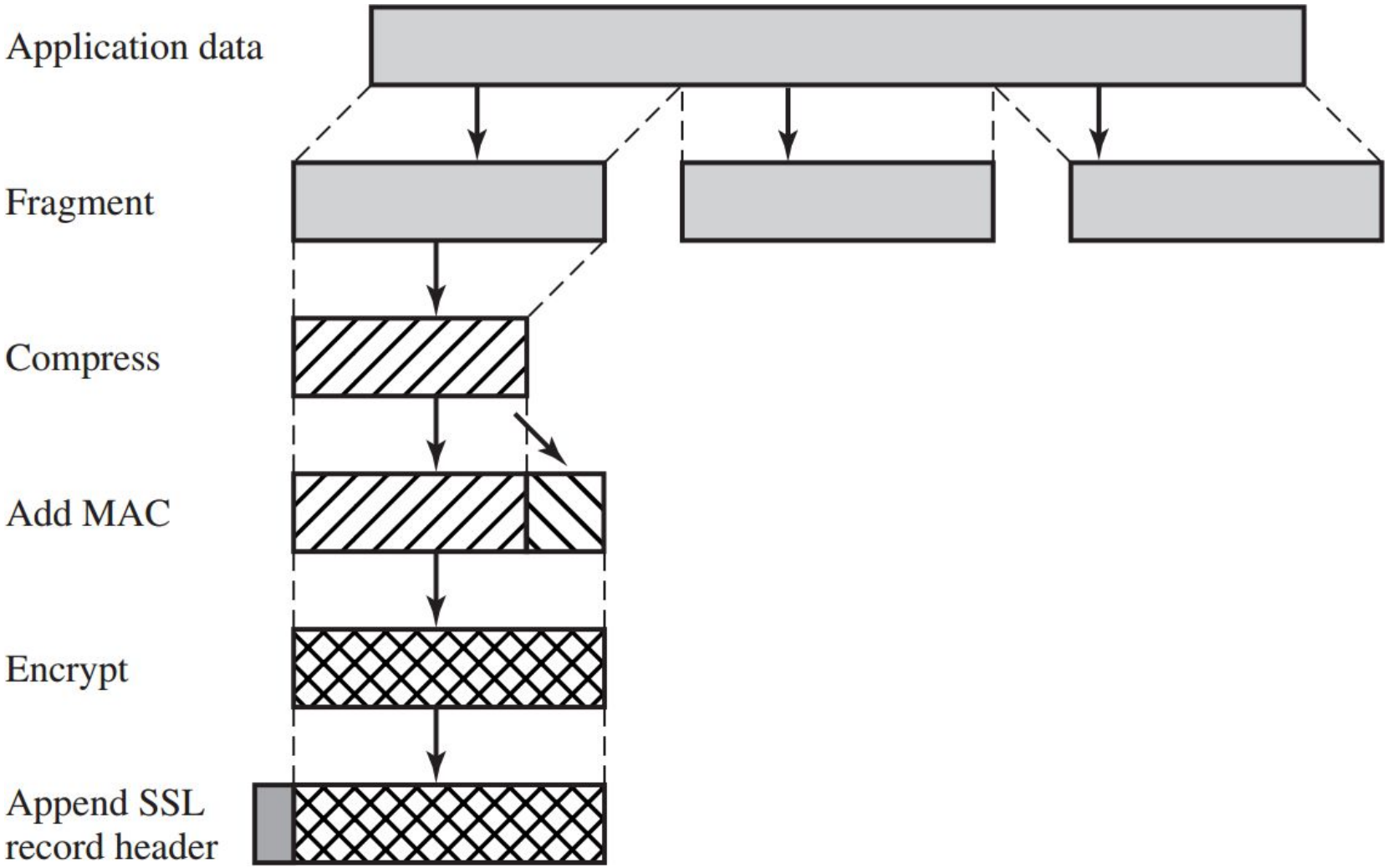
connection:

- SSL connection
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session
- SSL session
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections

SSL Record Protocol Services

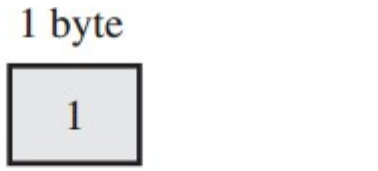
- Message Integrity
  - using a MAC with shared secret key
  - similar to HMAC but with different padding
- Confidentiality
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption

SSL Record Protocol Operation



SSL Change Cipher Spec Protocol

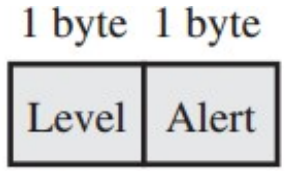
- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use



(a) Change Cipher Spec Protocol

SSL Alert Protocol

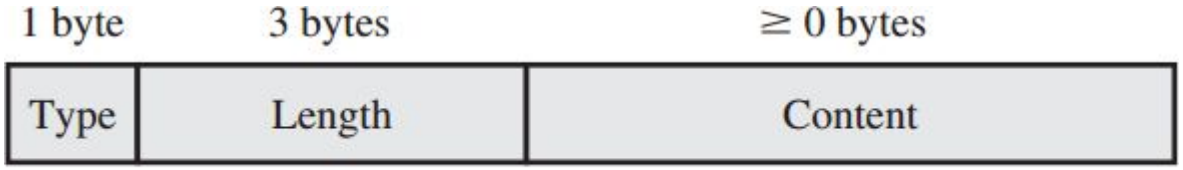
- Conveys SSL-related alerts to peer entity
- Severity
  - warning or fatal
- Specific alert
  - fatal: unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data



(b) Alert Protocol

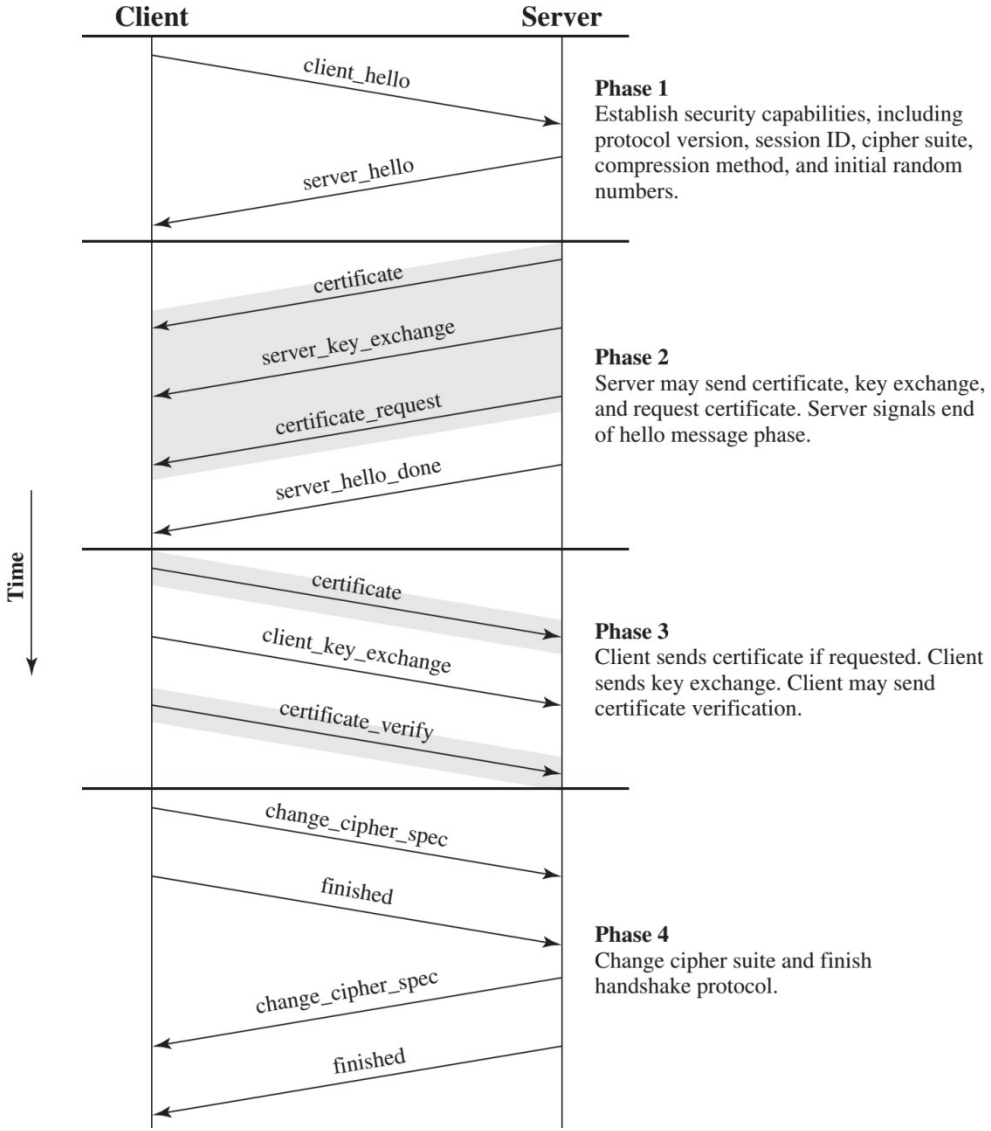
SSL Handshake Protocol

- 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



(c) Handshake Protocol

SSL Handshake Protocol



17.3 Transport Layer Security

TLS (Transport Layer Security)

- IETF standard RFC 2246 similar to SSLv3
- with minor differences
  - in record format version number
  - uses HMAC for MAC
  - a pseudo-random function expands secrets
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate types & negotiations
  - changes in crypto computations & padding

17.4 HTTPS

HTTPS

- HTTPS (HTTP over SSL)
  - combination of HTTP & SSL/TLS to secure communications between browser & server

    documented in RFC2818

    no fundamental change using either SSL or TLS
- use https:// URL rather than http://
  - and port 443 rather than 80
- encrypts
  - URL, document contents, form data, cookies, HTTP headers

HTTPS

- Connection Initiation
  - TLS handshake then HTTP request(s)
- Connection Closure
  - have “Connection: close” in HTTP record
  - TLS level exchange close_notify alerts
  - can then close TCP connection
  - must handle TCP close before alert exchange sent

    or completed

Thanks!