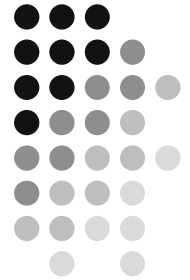
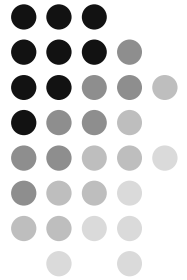
Transport-Level Security

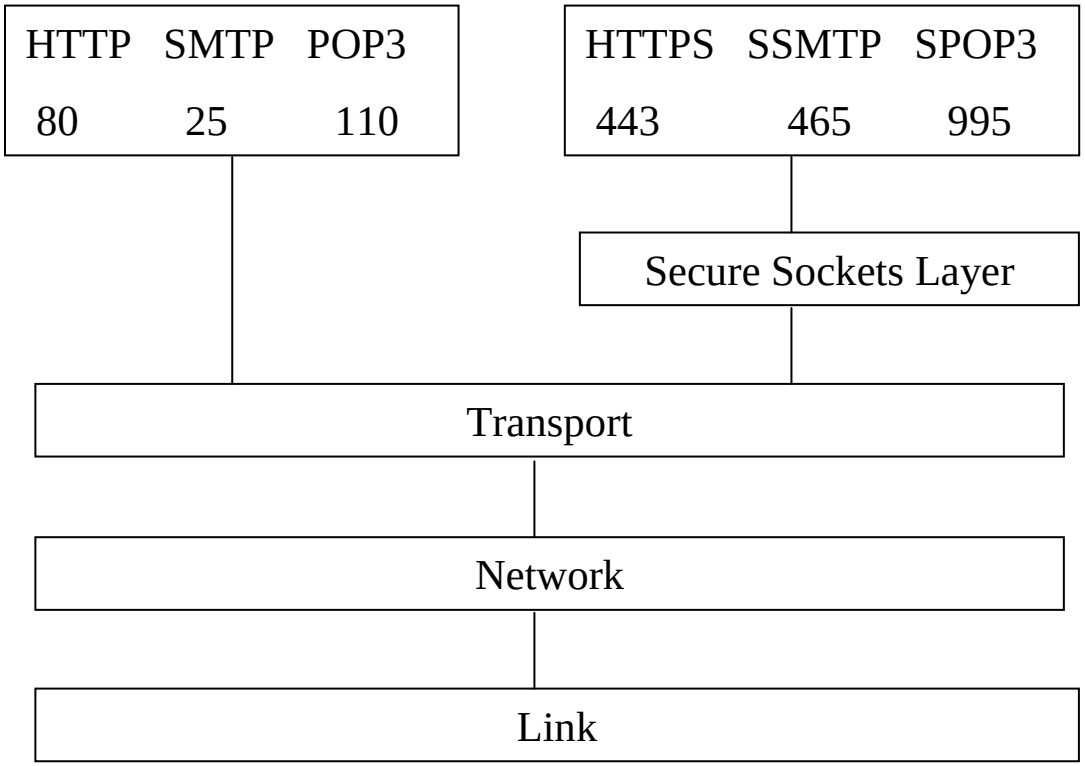


Web Security

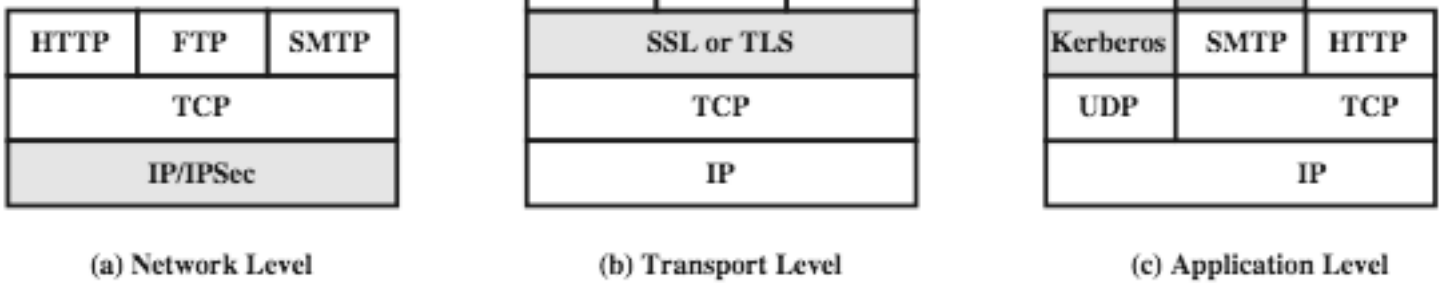


- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable
- have a variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

Where SSL Fits



Web Traffic Security Approaches

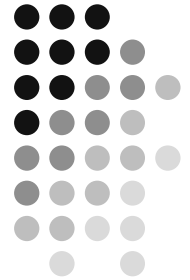


(a) Network Level

(b) Transport Level

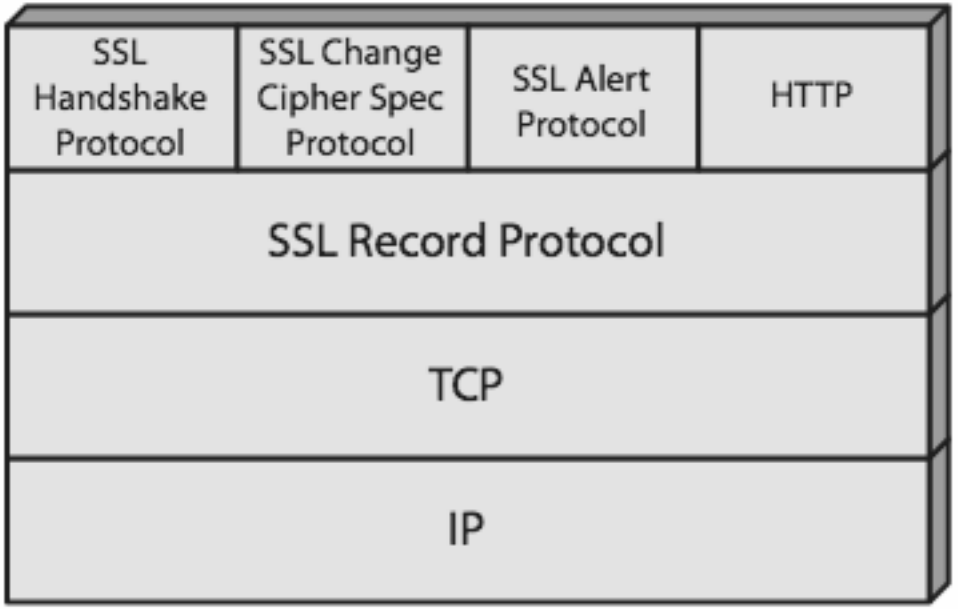
(c) Application Level

SSL (Secure Socket Layer)

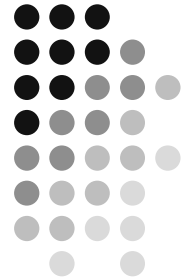


- transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS (Transport Layer Security)
- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols

SSL Architecture

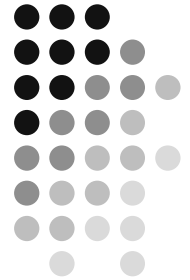


SSL Architecture



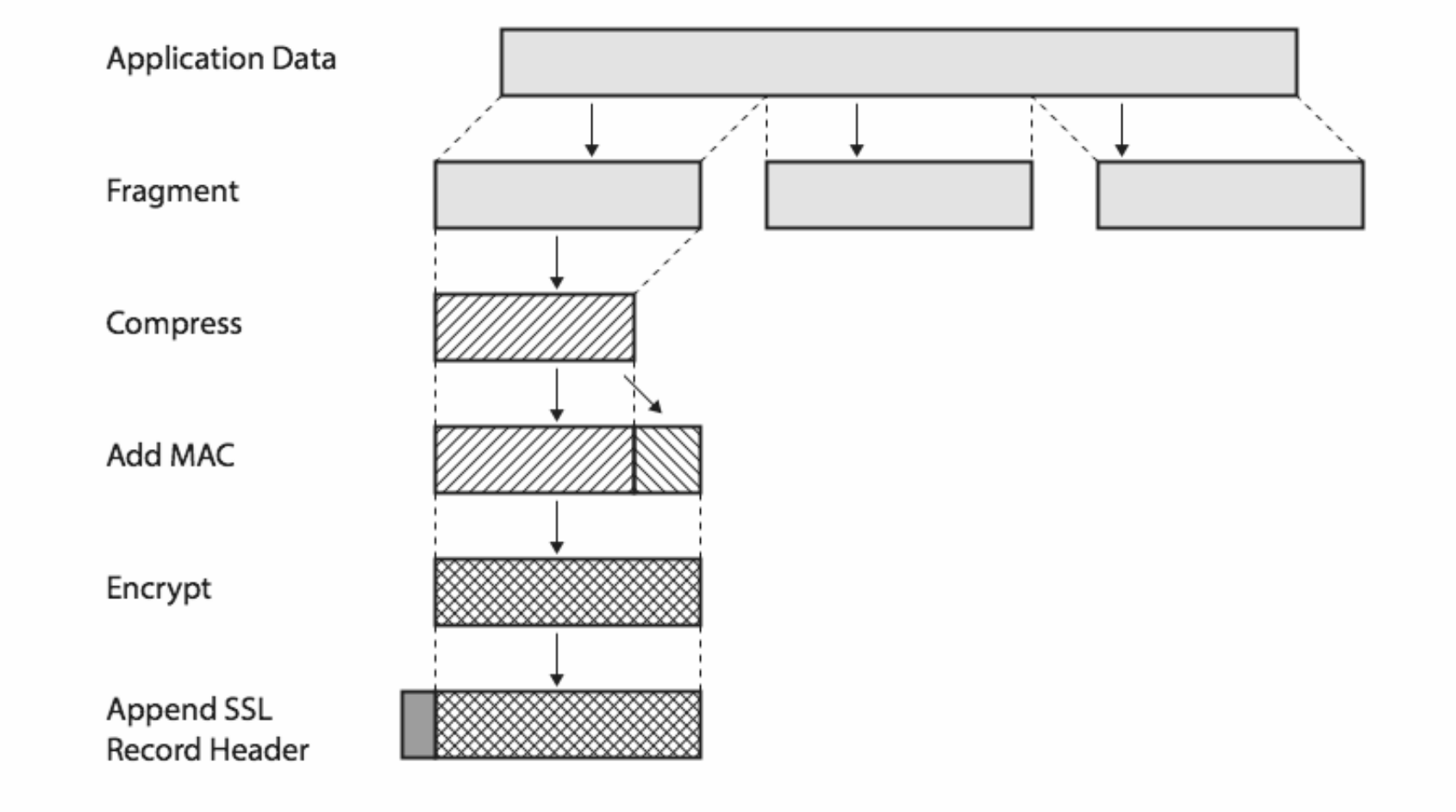
- **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session
- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections

SSL Record Protocol Services

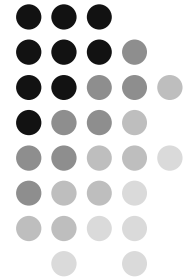


- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption
- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC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

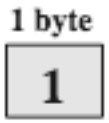
SSL Record Protocol Operation



SSL Change Cipher Spec Protocol



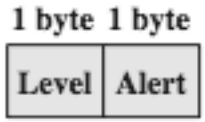
- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use



(a) Change Cipher Spec Protocol

SSL Alert Protocol

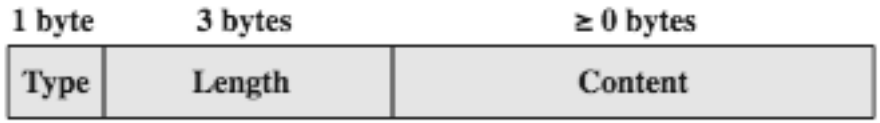
- conveys SSL-related alerts to peer entity
- severity
  - warning or fatal
- specific alert
  - fatal: unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked,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



(b) Alert Protocol

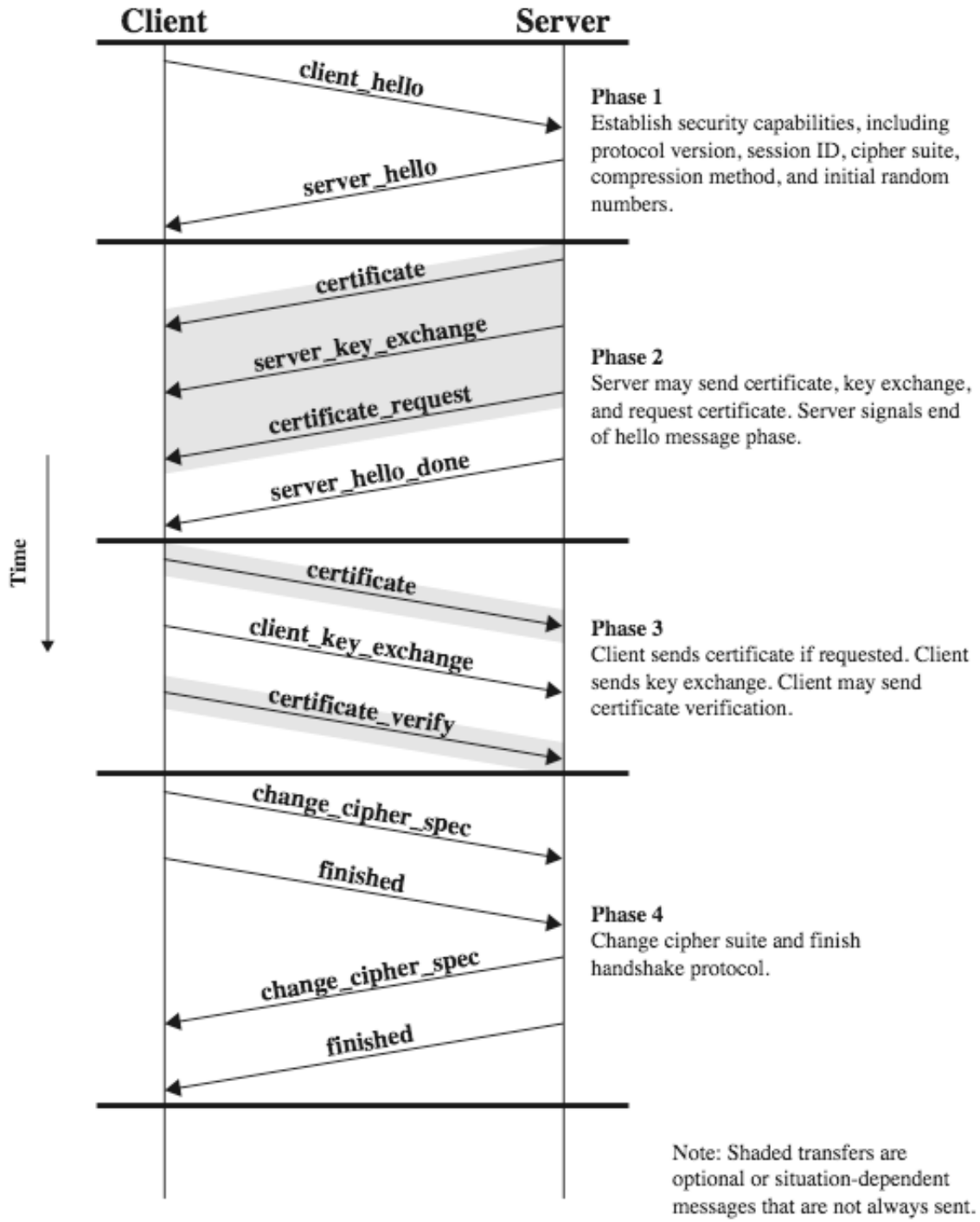
SSL Handshake Protocol

- 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

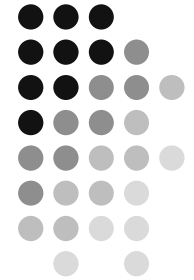


(c) Handshake Protocol

SSL Handshake Protocol

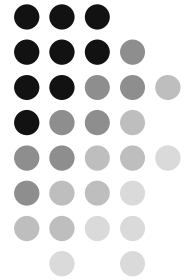


Cryptographic Computations



- master secret creation
  - a one-time 48-byte value
  - generated using secure key exchange (RSA / Diffie-Hellman) and then hashing info
- generation of cryptographic parameters
  - 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
  - generated by hashing master secret

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
    - based on HMAC using SHA-1 or MD5
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate types & negotiations
  - changes in crypto computations & padding

Summary

Discussed about

- SSL/TLS- overview
- SSL Architecture
- SSL Record Protocol Services
- SSL Change Cipher Spec Protocol
- SSL Alert Protocol
- Transport Layer Security

Test Your Understanding

- Which one of the following is not a higher –layer SSL protocol?
- a) Alert Protocol
- b) Handshake Protocol
- c) Alarm Protocol
- d) Change Cipher Spec Protocol
- Which one of the following is not a higher –layer SSL protocol?
  a) Alert Protocol
  b) Handshake Protocol
  c) Alarm Protocol
  d) Change Cipher Spec Protocol