Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

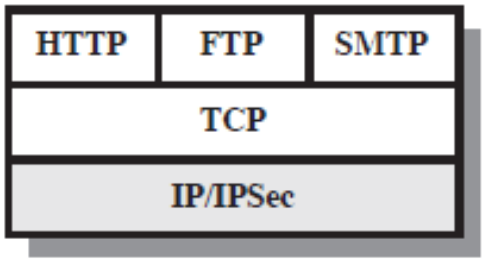
Διαχείριση και Ασφάλεια Δικτύων

Το Πρωτόκολλο SSL

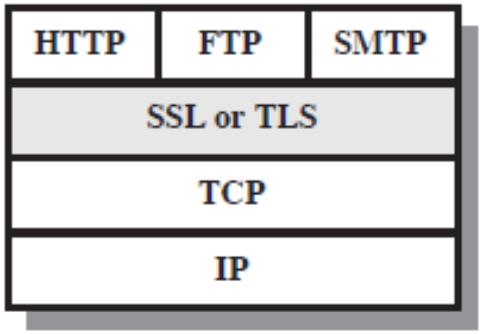
Δικτυακές απειλές

	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

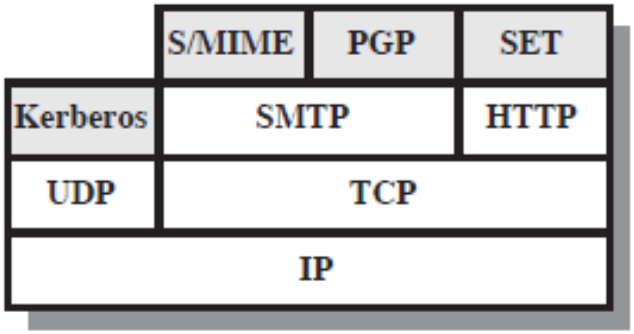
Προσεγγίσεις για την ασφάλεια δικτυακής κίνησης



Επίπεδο Δικτύου



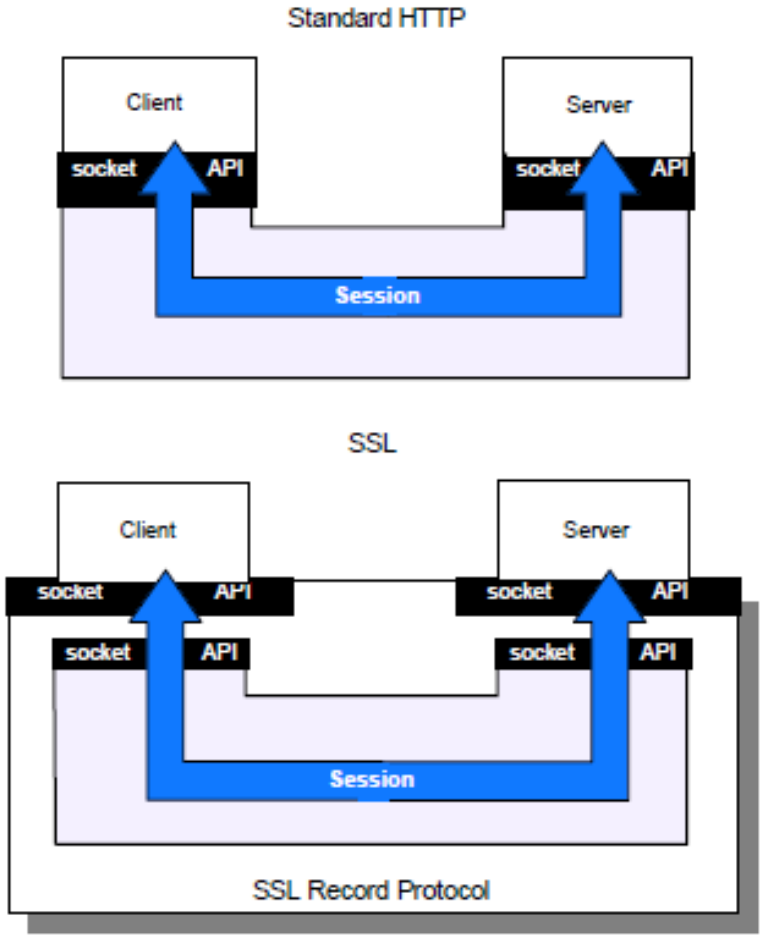
Επίπεδο Μεταφοράς



Επίπεδο Εφαρμογής

Το πρωτόκολλο SSL

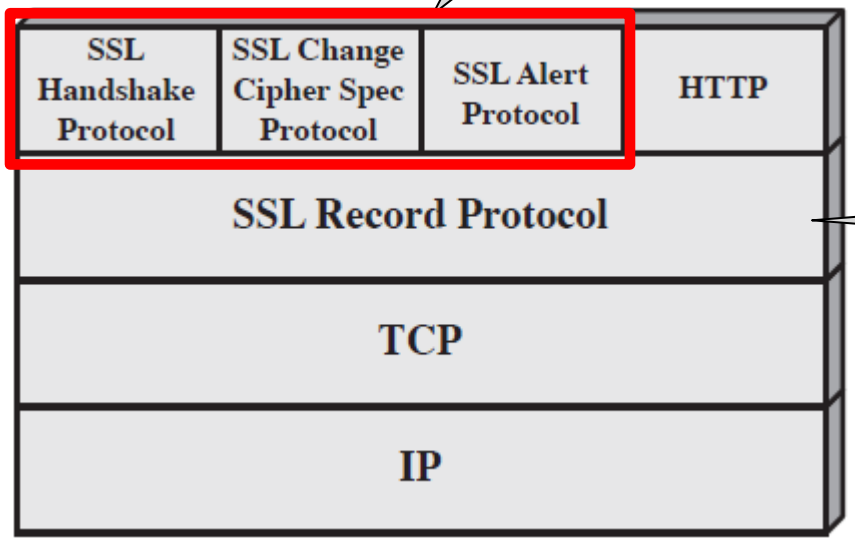
- Secure Socket Layer
- Υπηρεσία ασφάλειας του επιπέδου μεταφοράς
- Πρώτη ανάπτυξη από τη Netscape
- Τρίτη έκδοση (SSLv3): συλλογική εργασία που υποστηρίχτηκε από την IETF
- Transport Layer Security (TLS): η εξέλιξη του SSL, ως πρότυπο της IETF
- Γενική φιλοσοφία: χρήση του TCP για την παροχή αξιόπιστης υπηρεσίας από-άκρο-σε-άκρο
- Πρωτόκολλο δύο επιπέδων
  - Πρωτόκολλο Εγγραφής SSL
  - Πρωτόκολλα διαχείρισης (χειραψίας, αλλαγής προδιαγραφών κρυπτογράφησης, συναγερμών)



Αρχιτεκτονική SSL

Βασικές έννοιες:
- Σύνδεση (connection)
- Σύνοδος (session)

Διαχείριση συναλλαγών SSL

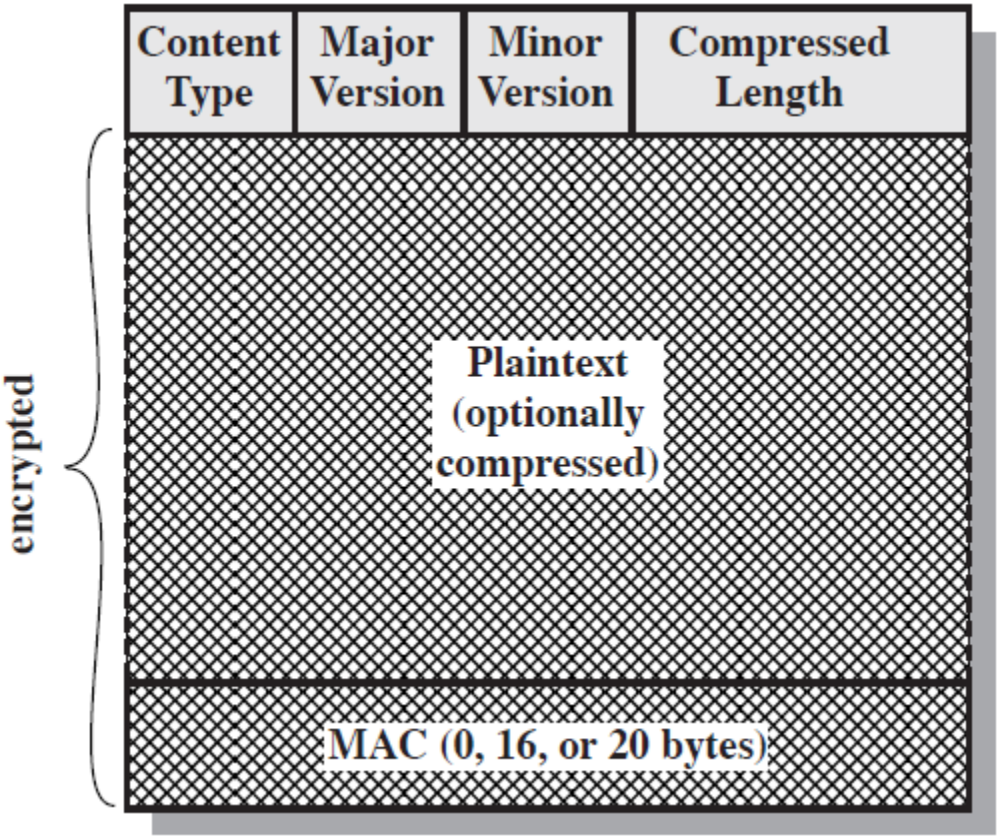


Βασικές υπηρεσίες ασφάλειας

Λειτουργία Πρωτοκόλλου Εγγραφής SSL

- Εμπιστευτικότητα
  - Μέσω συμμετρικής κρυπτογράφησης
  - Οι παράμετροι ορίζονται από τη διαδικασία "χειραψίας"
- Ακεραιότητα
  - Μέσω πρωτοκόλλου MAC

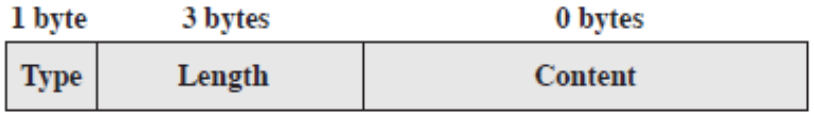
Μορφή εγγραφής SSL



Πρωτόκολλο Χειραψίας SSL

- SSL Handshake Protocol
- Ακολουθεί το πρότυπο client – server
- Επιτρέπει σε client και server:
  - Να πιστοποιήσουν την ταυτότητά τους αμοιβαία
  - Να διαπραγματευτούν τις παραμέτρους που θα χρησιμοποιήσουν
    - Κρυπτογραφικά κλειδιά
    - Κρυπτογραφικούς αλγορίθμους
    - Αλγορίθμους MAC
- Συνίσταται στην ανταλλαγή σειράς μηνυμάτων μεταξύ client και server, που χωρίζονται σε τέσσερις φάσεις:
  - Εγκατάσταση δυνατοτήτων ασφάλειας
  - Πιστοποίηση server και ανταλλαγή κλειδιών
  - Πιστοποίηση client και ανταλλαγή κλειδιών
  - Φάση τερματισμού

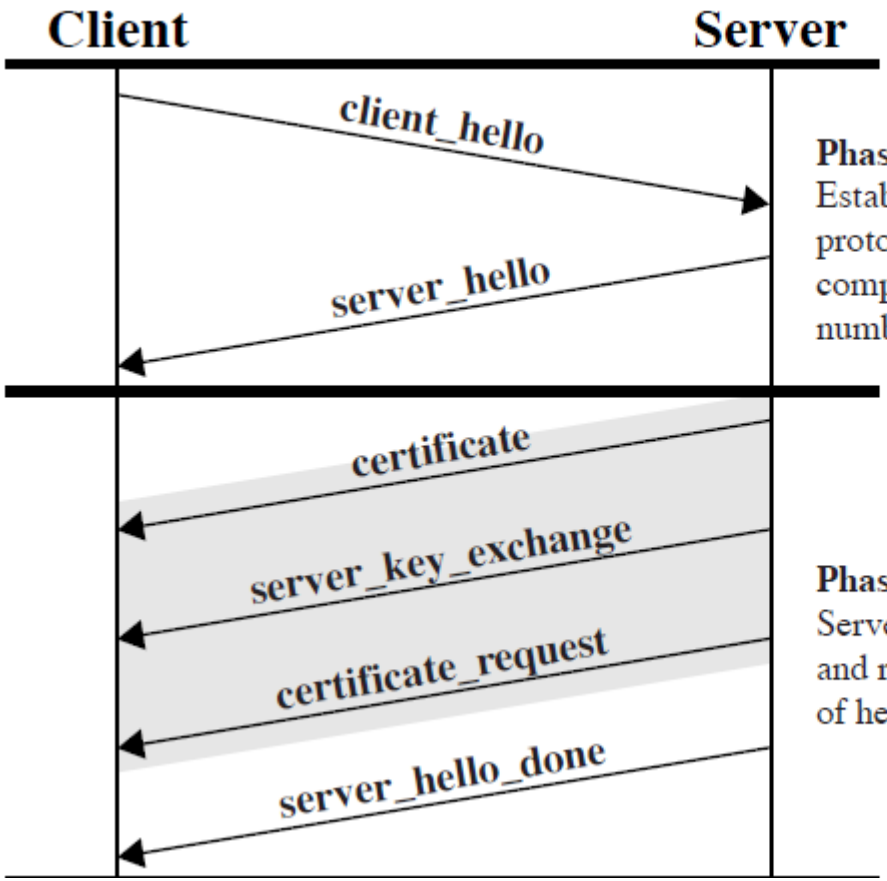
Μορφή μηνυμάτων:



Τύποι μηνυμάτων Πρωτοκόλλου Χειραψίας SSL

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

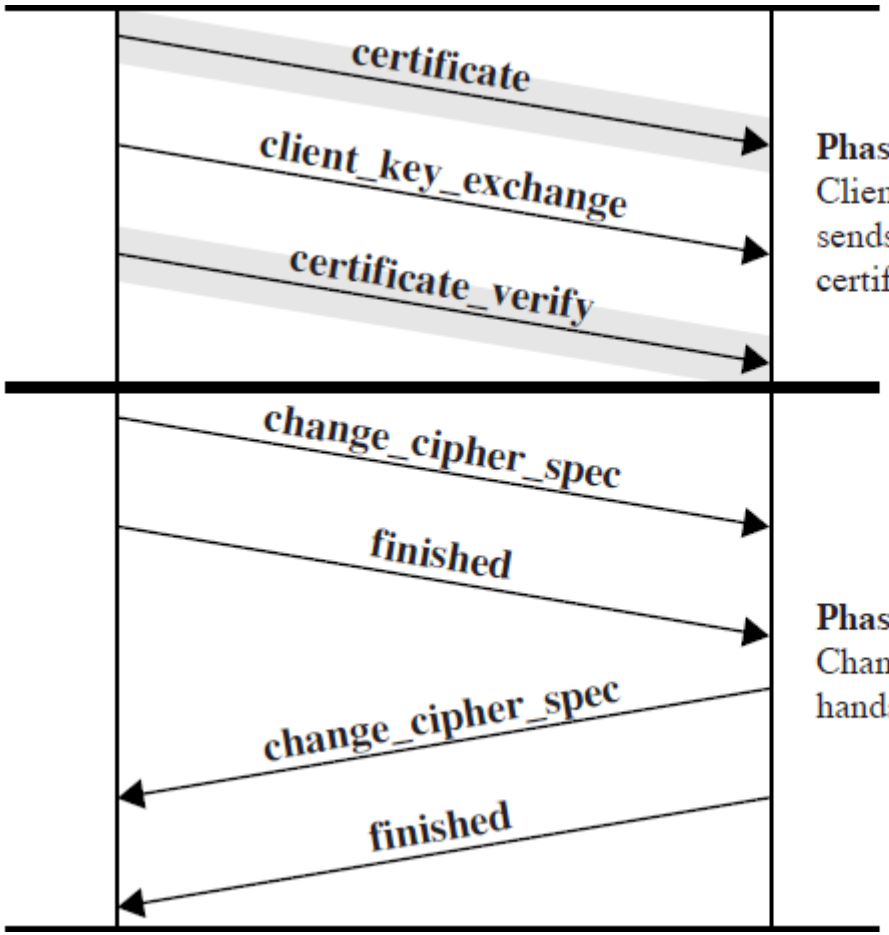
Μηχανισμός Πρωτοκόλλου Χειραψίας SSL



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.

Μηχανισμός Πρωτοκόλλου Χειραψίας SSL



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.

Πρωτόκολλο "Συναγερμού" SSL

- Μεταφορά συναγερμών (alerts) στην ομότιμη οντότητα
- Δύο είδη πληροφορίας
  - Τύπος μηνύματος
    - Προειδοποίηση (warning)
    - Καταστροφή (fatal)
  - Συγκεκριμενοποίηση μηνύματος
    - Προειδοποίηση:
      no_certificate, bad_certificate, unsupported_certificate, certificate_revoked, certificate_expired, certificate_unknown, close_notify
    - Καταστροφή:
      unexpected_message, bad_record_mac, decompression_failure, handshake_failure, illegal_parameter