Cryptography and Network Security Chapter 16

Fifth Edition

by William Stallings

Chapter 16 – Transport-Level Security

Use your mentality

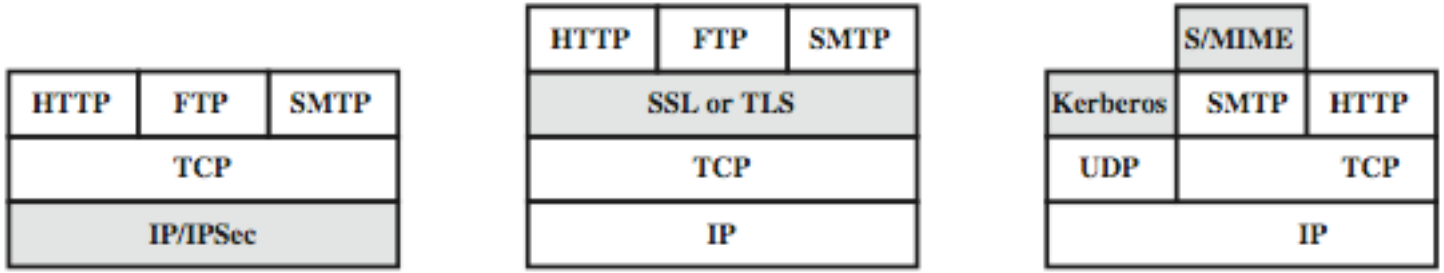
Wake up to reality

—From the song, "I've Got You under My Skin“ by Cole Porter

Web Security

- Το Web χρησιμοποιειται σημερα ευρυτατα απο κυβερνησεις, επιχειρησεις και ατομα.
- Ωστοσο το Internet και το Web ειναι τρωτα απο πλευρας ασφαλειας
- Υπαρχουν ποικιλες απειλες που αφορουν
  - Ακεραιοτητα (integrity)
  - Εμπιστευτικοτητα (confidentiality)
  - Αρνηση υπηρεσιας (denial of service)
  - Πιστοποιηση αυθεντικοτητας (authentication)
- Πρεπει να προστεθουν νεοι μηχανισμοι ασφαλειας

Προσεγγισεις στην ασφαλεια του Web Traffic



(a) Network Level

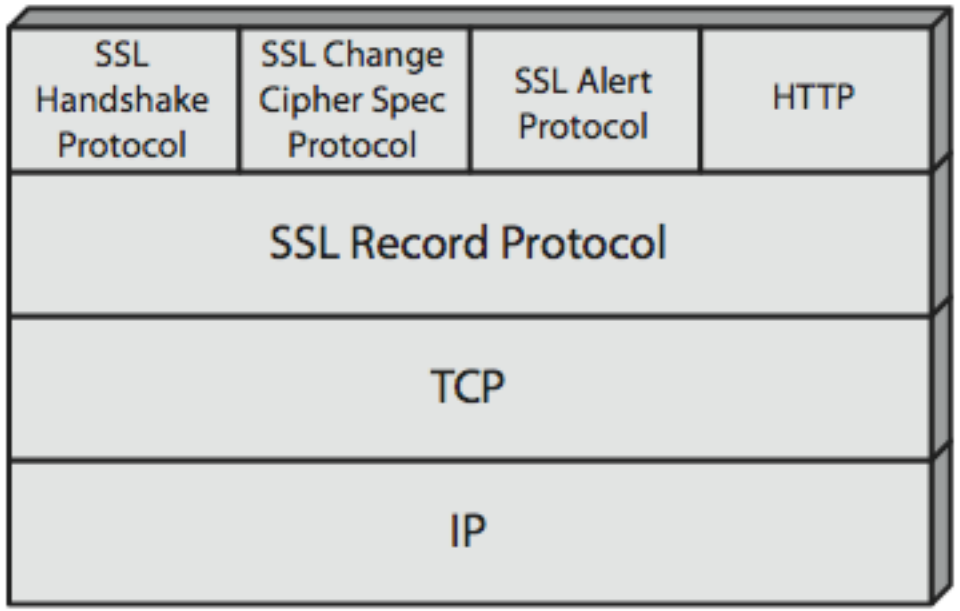
(b) Transport Level

(c) Application Level

SSL (Secure Socket Layer)

- Ειναι υπηρεσία ασφαλειας του transport layer
- Αναπτυχθηκε αρχικα απο τη Netscape
- Η εκδοση 3 σχεδιαστηκε παιρνοντας υποψη την εμπειρια των προγενεστερων εκδοσεων
- Στη συνεχεια κατεστη Internet standard γνωστο ως TLS (Transport Layer Security)
- Χρησιμοποιει το TCP για να παρασχει μια αξιοπιστη υπηρεσια end-to-end (reliable end-to-end service)
- Το SSL εχει δυο επιπεδα πρωτοκολλων

SSL Architecture



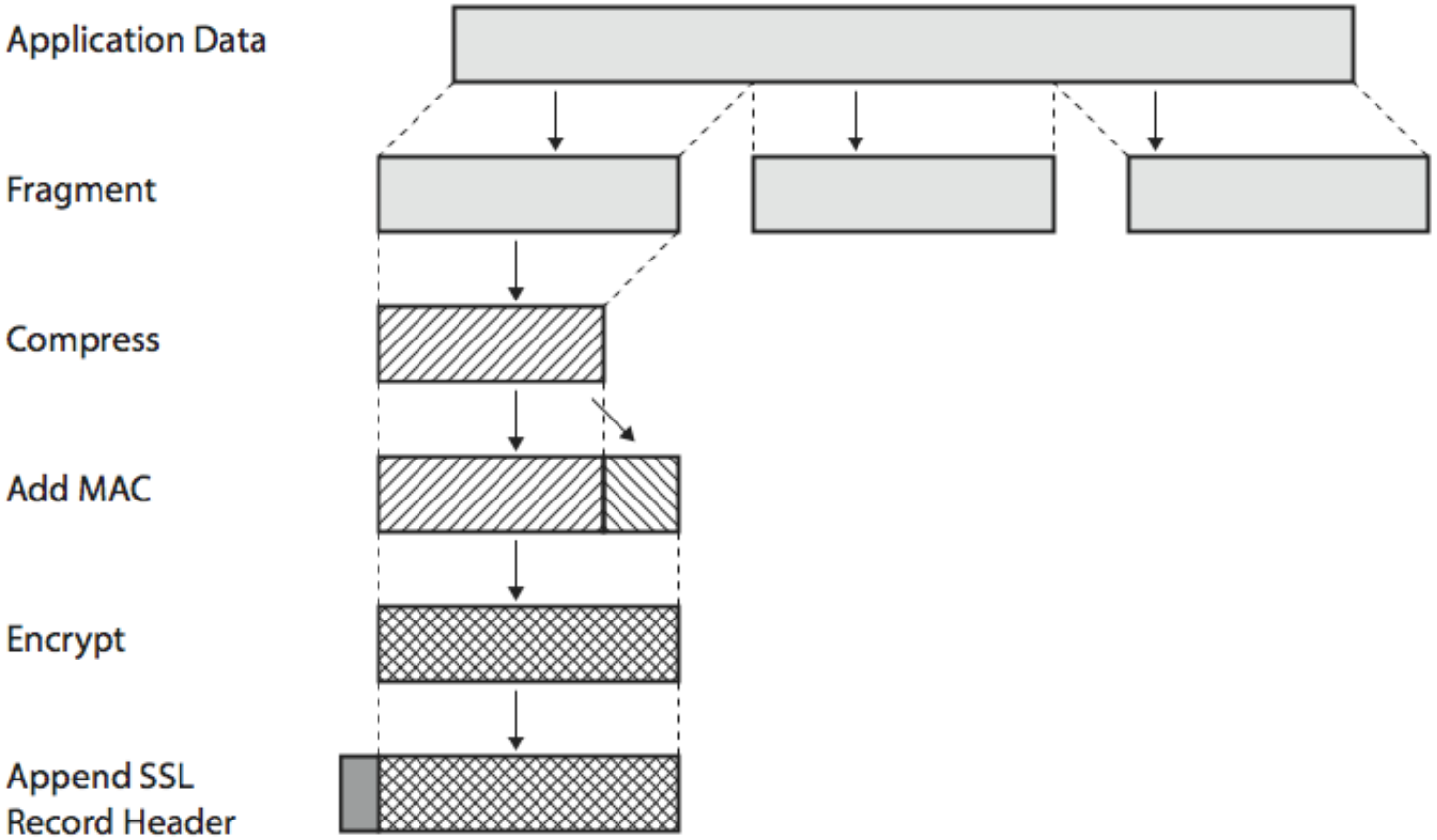
SSL Architecture

- **Συνδεση SSL (SSL connection)**
  - Μια προσωρινη συνδεση επικοινωνιας peer-to-peer
  - Σχετιζεται με μια Συνοδο SSL (SSL session)
- **Συνοδος SSL (SSL session)**
  - Ειναι ενας συνδεσμος μεταξυ client & server
  - Δημιουργειται απο το Πρωτοκολλο Χειραψιας (Handshake Protocol)
  - Οριζει ενα συνολο κρυπτογραφικων παραμετρων
  - Μπορει να τη μοιραζονται πολλες συνδεσεις SSL (SSL connections)

Υπηρεσιες του Πρωτοκολλου Εγγραφης SSL (SSL Record Protocol)

- **Εμπιστευτικοτητα (confidentiality)**
  - Χρησιμοποιει συμμετρικη κρυπτογραφηση με ενα κοινο κλειδι που οριζεται απο το Πρωτοκολλο Χειραψιας (Handshake Protocol)
  - Κρυπτογραφικοι αλγοριθμοι που χρησιμοποιουνται: AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - Το μηνυμα συμπιεζεται πριν κρυπτογραφηθει
- **Ακεραιοτητα Μηνυματος (message integrity)**
  - Χρησιμοποιειται ενα πρωτοκολλο MAC (message authenticaion code) με ενα κοινο μυστικο κλειδι
  - Παρομοιο με το HMAC αλλα με διαφορετικο padding

Λειτουργια του SSL Record Protocol



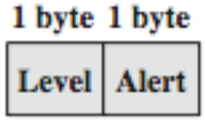
SSL Change Cipher Spec Protocol

- Ειναι ενα απο τα τρια SSL-specific πρωτοκολλα που χρησιμοποιουν το SSL Record protocol
- Ειναι το πιο απλο πρωτοκολλο και αποτελειται απο ενα μονο μηνυμα του ενος byte
- Κανει την κατασταση pending, να γινει current
- Δηλαδη επικαιροποιει (update) τον κρυπτογραφικο αλγοριθμο που χρησιμοποιειται

(a) Change Cipher Spec Protocol

SSL Alert Protocol

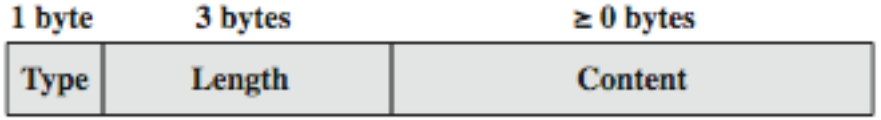
- μεταφερει προειδοποιησεις (alerts) σχετικους με το SSL στην ομολογη οντοτητα (peer entity)
- σοβαροτητα
  - warning ή fatal
- Συγκεκριμενη προειδοποιηση
  - **fatal:** unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - **warning:** close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- Ειναι συμπιεσμενο και κρυπτογραφημενο, οπως ολα τα δεδομενα του SSL



(b) Alert Protocol

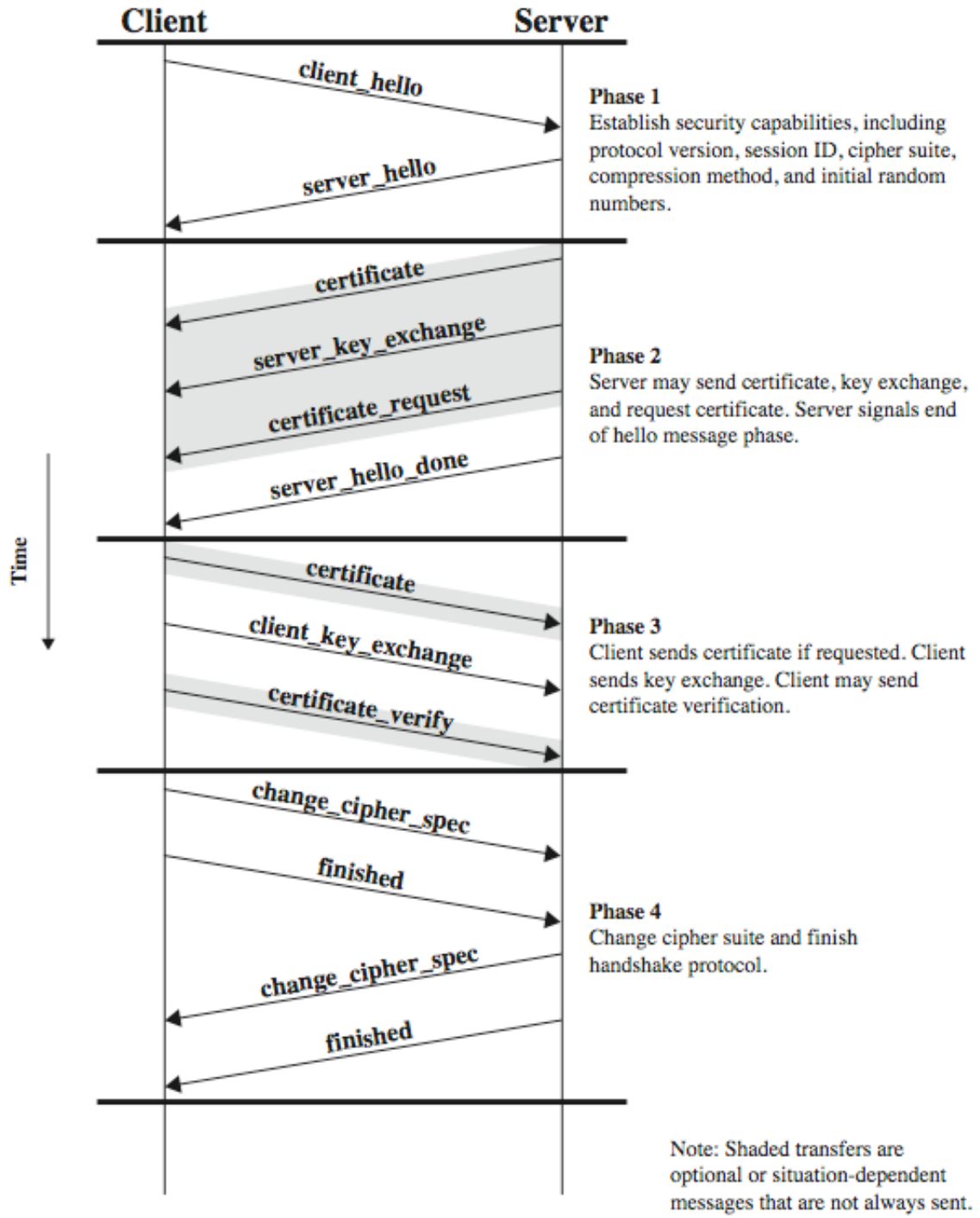
SSL Handshake Protocol

- Επιτρεπει σε server και client να:
  - Πιστοποιησουν ο ενας την αυθεντικοτητα του αλλου
  - Να διαπραγματευτουν για το ποιοι αλγοριθμοι κρυπτογραφησης και MAC θα χρησιμοποιηθουν
  - Διαπραγματευονται για τα κρυπτογραφικα κλειδια που θα χρησιμοποιηθουν
- Αποτελουνται απο ακολουθιες μηνυματων χωρισμενες σε φασεις
  1. Εγκατασταση δυνατοτητων ασφαλειας
  2. Πιστοποιηση αυθεντικοτητας του Server και ανταλλαγη κλειδιου
  3. Πιστοποιηση αυθεντικοτητας του Client και ανταλλαγη κλειδιου
  4. Τερματισμος



(c) Handshake Protocol

SSL Handshake Protocol



Κρυπτογραφικοι Υπολογισμοι (Cryptographic Computations)

- Δημιουργια master secret
  - Εχει μεγεθος 48 bytes και ειναι μιας χρησης.
  - Παραγεται χρησιμοποιωντας ασφαλη ανταλλαγη κλειδιου (RSA / Diffie-Hellman)
- Δημιουργια κρυπτογραφικων παραμετρων
  - 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
  - Δημιουργουνται με hashing του master secret

TLS (Transport Layer Security)

- IETF standard RFC 2246, παρομοιο με το SSLv3
- Με μικρες διαφορες
  - Στον αριθμο version του record format
  - Χρησιμοποιει HMAC για MAC
  - Μια ψευδοτυχαια συναρτηση επεκτεινει τα μυστικα (secrets)
    - Βασιζεται στο HMAC και χρησιμοποιει SHA-1 ή MD5
  - Εχει προσθετους alert codes
  - Υπαρχουν αλλαγες στους υποστηριζομενους κρυπτογραφικους αλγοριθμους
  - Αλλαγες στους τυπους πιστοποιητικων και στη διαπραγματευση
  - Αλλαγες στους κρυπτογραφικους υπολογισμους και στο padding

HTTPS

- HTTPS (HTTP over SSL)
  - συνδιασμος HTTP και SSL/TLS για ασφαλεις επικοινωνιες μεταξυ browser & server
    - Παρουσιαζεται στο RFC2818
    - Δεν εχει ουσιαστικη διαφορα οταν χρησιμοποιειται το SSL ή το TLS
- «https:// URL» αντι για «http://URL»
  - Και port 443 αντι για port 80
- Κρυπτογραφει
  - URL, περιεχομενα του document, δεδομενα απο φορμες, cookies, επικεφαλιδες HTTP

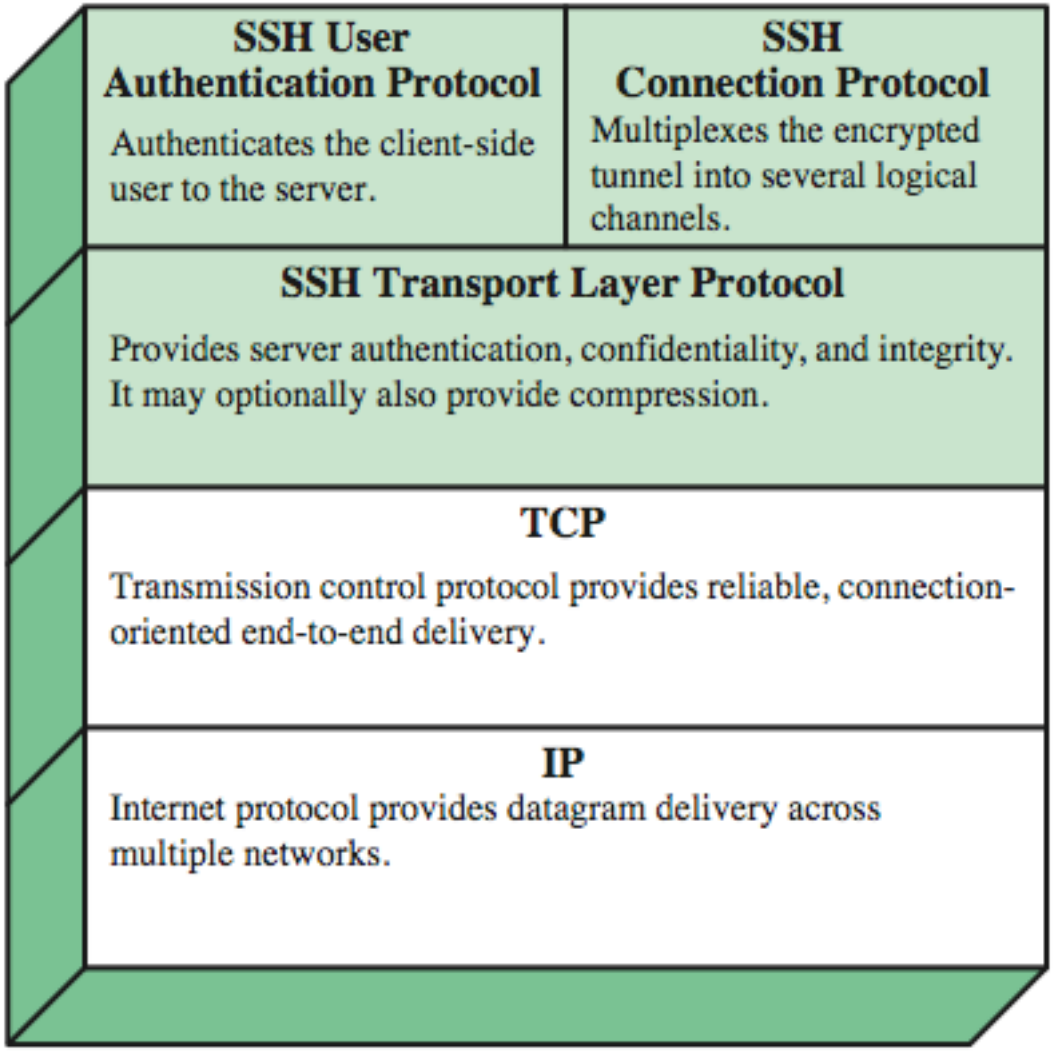
Χρηση του HTTPS

- **Ξεκινημα συνδεσης**
  - TLS handshake και στη συνεχεια HTTP request(s)
- **Κλεισιμο συνδεσης**
  - εχει “Connection: close” στο HTTP record
  - TLS level exchange close_notify alerts
  - Τοτε μπορει να κλεισει τη συνδεση TCP
  - Πρεπει να μπορει να χειριστει ενδεχομενο (απο λαθος) κλεισιμο του TCP πριν σταλει ή ολοκληρωθει το alert exchange

Secure Shell (SSH)

- Πρωτοκολλο για ασφαλεις δικτυακες επικοινωνιες
  - Σχεδιασμενο ωστε να ειναι απλο και φθηνο
- Το SSH1 παρειχε ασφαλες remote logon
  - Αντικαθιστα το TELNET και αλλα μη ασφαλή σχηματα
  - Επισης, εχει πιο γενικη ικανοτητα client/server
- Το SSH2 διορθωνει εναν αριθμο σφαλματων ασφαλειας
- Παρουσιαζεται στα RFCs 4250 εως 4254
- SSH clients & servers ειναι ευρεως διαθεσιμοι
- Ειναι οτι πρεπει για remote login/ X tunnels

SSH Protocol Stack



SSH Transport Layer Protocol

- Η πιστοποιηση αυθεντικοτητας του server πραγματοποιειται στο transport layer, και βασιζεται στο ζευγος κλειδιων server/host
  - Η πιστοποιηση αυθεντικοτητας του server απαιτει οι clients να γνωριζουν εκ των προτερων τα κλειδια του host

- Ανταλλαγη πακετων
  - Αποκατασταση συνδεσης TCP
  - Και στη συνεχεια μπορουν να ανταλλαγουν δεδομενα
    - Ανταλλαγη identification string, διαπραγματευση αλγοριθμου, ανταλλαγη κλειδιου, τελος ανταλλαγης κλειδιου, αιτηση υπηρεσιας
  - Χρησιμοποιει συγκεκριμενο format πακετου

SSH User Authentication Protocol

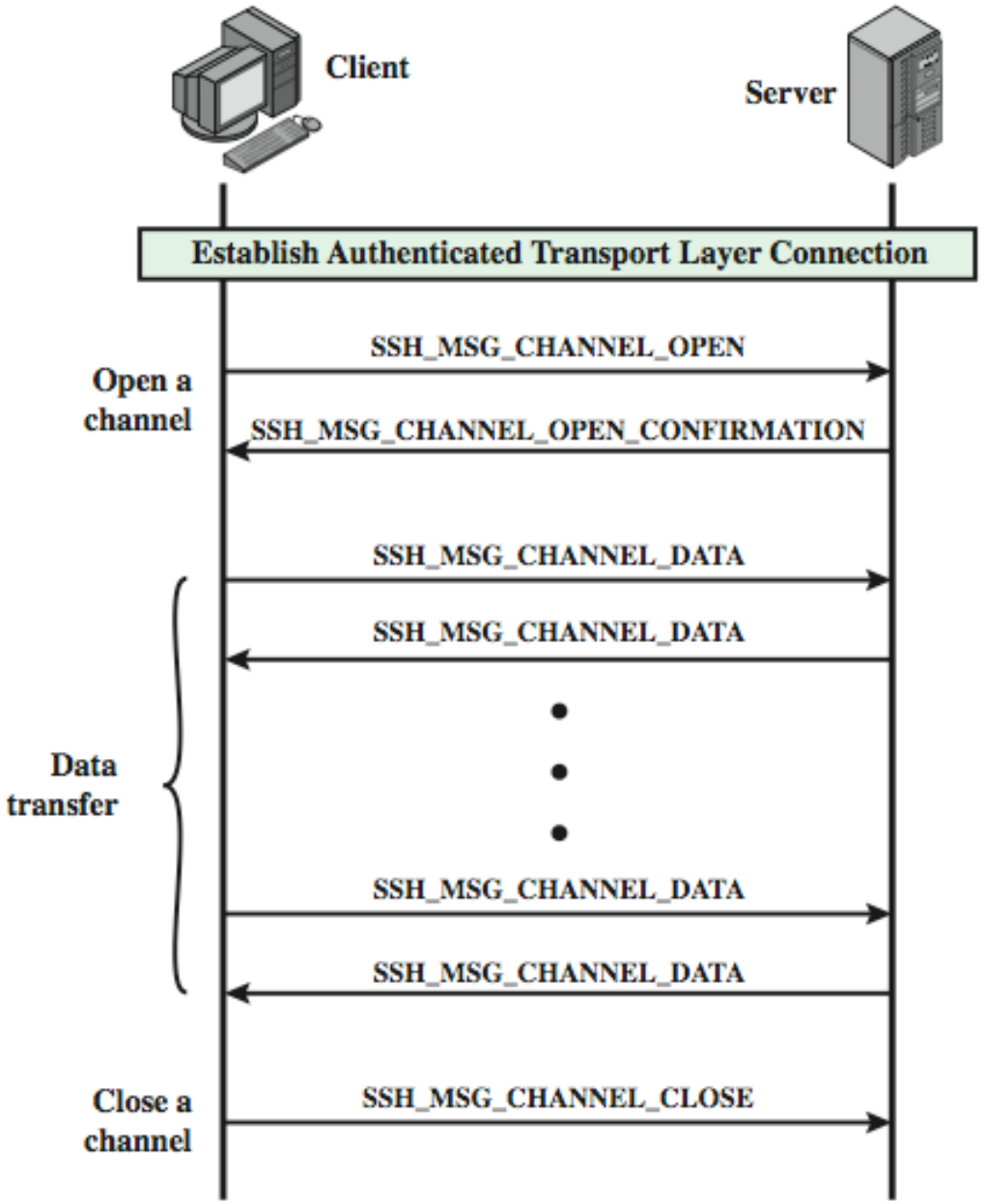
- Πιστοποιει τη αυθεντικοτητα του client στον server
- Υπαρχουν τρεις τυποι μηνυματων:
  - SSH_MSG_USERAUTH_REQUEST
  - SSH_MSG_USERAUTH_FAILURE
  - SSH_MSG_USERAUTH_SUCCESS
- Χρησιμοποιουνται οι ακολουθες μεθοδοι πιστιποιησης αυθεντικοτητας

  public-key, password, host-based

SSH Connection Protocol

- Τρεχει στο SSH Transport Layer Protocol
- Προϋποθετει ασφαλη συνδεση πιστοποιησης αυθεντικοτητας
- Χρησιμοποιειται για πολλαπλα λογικα καναλια
  - Οι επικοινωνιες SSH χρησιμοποιουν ξεχωριστα καναλια
  - Η καθε πλευρα μπορει να τα ανοιξει με ενα μοναδικο αριθμο id
  - Υπαρχει ελεγχος ροης
  - Υπαρχουν τρια σταδια:
    - Ανοιγμα ενος καναλιου, μεταφορα δεδομενων, κλεισιμο καναλιου
  - Τεσσερις τυποι:
    - session, x11, forwarded-tcpip, direct-tcpip.

SSH Connection Protocol Exchange



Προωθηση Θυρας (Port Forwarding)

- Μετατρεπει τη μη ασφαλη συνδεση TCP σε μια ασφαλη συνδεση SSH
  - Το SSH Transport Layer Protocol αποκαθιστα μια συνδεση TCP μεταξυ του SSH client και του server
  - Το traffic του client ανακατευθυνεται στο τοπικο SSH, ταξιδευει μεσω tunnel, και τελικα το μαρυνο SSH παραδιδεται στον server
- Υποστηριζονται δυο ειδη προωθησης θυρας
  - Τοπικη προωθηση (local forwarding)
  - Μακρυνη προωθηση (remote forwarding)

Τοπικη Προωθηση (local forwarding)

- Ανακατευθυνει συγκεκριμενο application layer traffic απο μια μη ασφαλη συνδεση TCP σε ενα ασφαλες SSH tunnel.
- **Παραδειγμα**

Εστω οτι εχουμε εναν e-mail client στο PC μας και τον χρησιμοποιουμε για να διαβαζουμε τα mail μας μεσω POP3 στο port 110. Μπορουμε να καταστησουμε ασφαλες αυτο το traffic με τον εξης τροπο:

1. Ο SSH **client** αποκαθιστα μια συνδεση με τον remote server.
2. Επιλεγει ενα μη χρησιμοποιουμενο port (π.χ. 9999) και ρυθμιζει το SSH να δεχεται traffic απο αυτο το port που προοριζεται για το port 110 του server.
3. Ο SSH client λεει στον SSH server να δημιουργησει μια συνδεση με τον προορισμο (στην περιπτωση μας, το port 110 του mail server).
4. Ο client παιρνει οσα bit στελνονται στο port 9999 και τα στελνει στον server μεσα στην κρυπτογραφημενη συνοδο SSH. Ο server αποκρυπτογραφει τα εισερχομενα bits και στελνει το plaintext στο port 110.
5. Στην αλλη κατευθυνση, ο SSH server παιρνει καθε bit που λαμβανεται στο port 110, και το στελνει μεσα στο SSH session πισω στον client, ο οποιος τα αποκρυπτογραφει και τα στελνει στην διεργασια που ειναι συνδεμενη στο port 9999.

Μακρυνη Προωθηση (remote forwarding)

- Ο SSH client του χρηστη ενεργει για λογαριασμο του server. Ο client λαμβανει το traffic με ενα συγκεκριμενο αριθμο port προορισμου, τοποθετει το traffic στο σωστο port και το στελνει στον προορισμο που επιλεγει ο χρηστης.
- **Παραδειγμα**

  Εστω οτι θελουμε απο το σπιτι μας να προσπελασουμε εναν server στη δουλεια, ο οποιος επειδη βρισκεται πισω απο firewall δεν θα αποδεχτει αιτημα SSH απο τον υπολογιστη του σπιτιου μας. Ωστοσο, απο τη δουλεια μπορει να εγκατασταθει ενα SSH tunnel με χρηση remote forwarding, ως εξης:

1. Απο τον υπολογιστη της δουλειας, εγκαθισταται μια συνδεση SSH με τον υπολογιστη του σπιτιου. Το firewall θα το επιτρεψει, αφου προκειται για μια προστατευμενη εξερχομενη συνδεση.
2. Πρεπει να ρυθμιστει ο SSH server, ετσι ωστε να ακουει σε ενα τοπικο port (π.χ. στο 22) και να λαμβανει δεδομενα που κατευθυνονται στο μακρυνο port (εστω 2222).
3. Τωρα, μπορουμε να παμε στο σπιτι μας και να ρυθμισουμε το SSH να δεχεται traffic στο port 2222.
4. Τωρα, μπορουμε να εγκαταστησουμε ενα SSH tunnel που μπορει να χρησιμοποιηθει για remote logon στον server της δουλειας.

Συνοψη

- Εξετασαμε:
  - Την αναγκη για ασφαλεια στο web
  - Τα πρωτοκολλα ασφαλειας του transport layer SSL/TLS
  - Το HTTPS
  - Το SSH