Web security

Σαράντης Πασκαλής <paskalis@di.uoa.gr>
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Είδη απειλών

- Προβλήματα στον web server
- Προβλήματα στον web client
- Υποκλοπή δεδομένων που μεταφέρονται ανάμεσα σε client και server

Προβλήματα στον web server

- Ανεύρεση και απόκτηση εμπιστευτικών δεδομένων
- Εκτέλεση εντολών στον υπολογιστή του server → μεταβολή του συστήματος
- Απόκτηση πληροφορίας για το μηχάνημα του server → χρήση για τη διάβρωση του συστήματος
- Επίθεση άρνησης υπηρεσίας →το μηχάνημα καθίσταται άχρηστο

Προβλήματα στον web client

- «Ενεργό» περιεχόμενο που μπορεί να προκαλέσει:
  - κατάρρευση του browser
  - ζημιά στο σύστημα του χρήστη
  - απώλεια ιδιωτικότητας (privacy)
  - απλή ενόχληση
- Κακή χρήση προσωπικών πληροφοριών που παρέχει ο χρήστης εσκεμμένα ή όχι

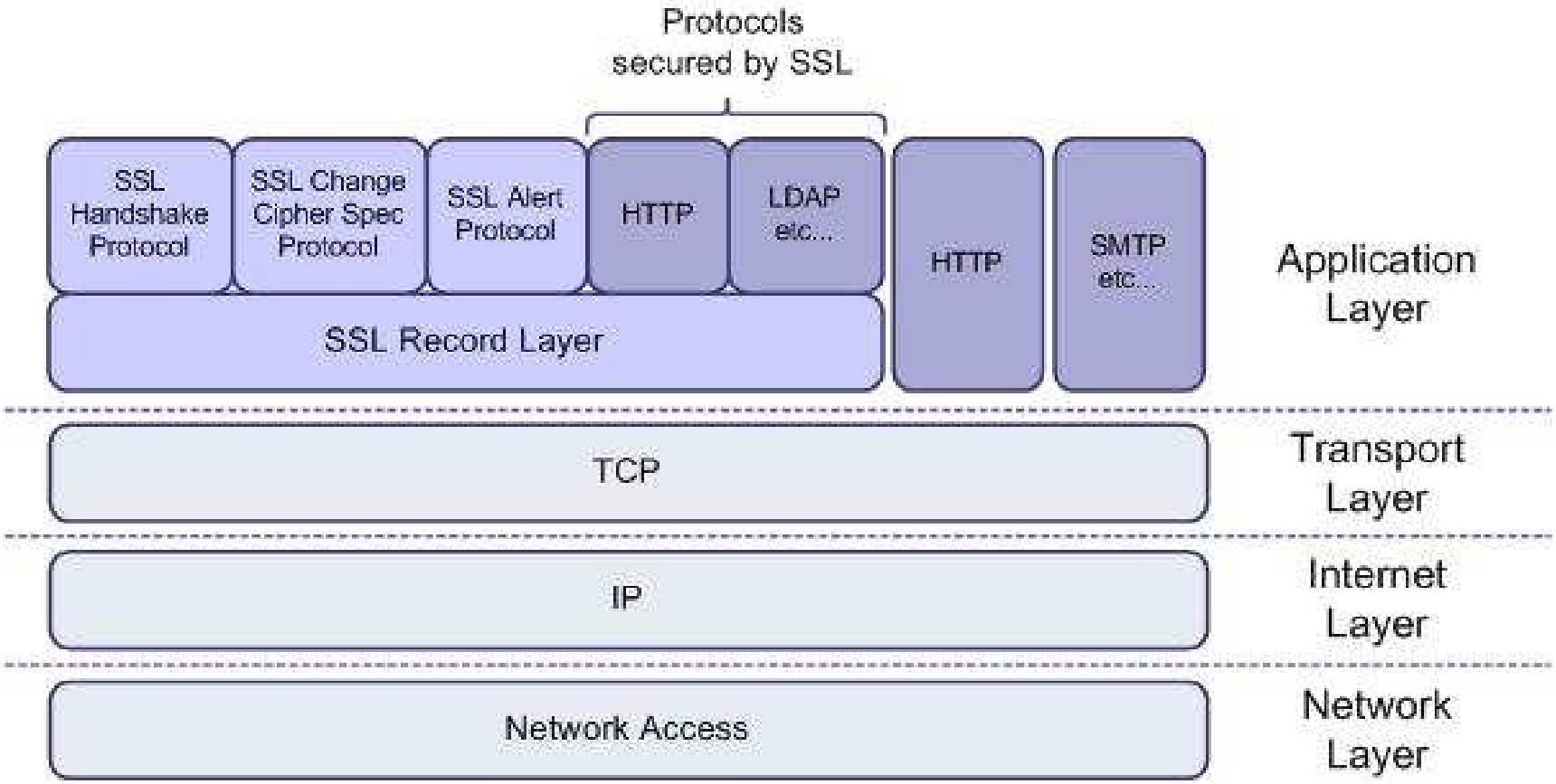
Υποκλοπή δεδομένων

- Ο υποκλοπέας μπορεί να βρίσκεται:
  - Στο δίκτυο στο μέρος του client
  - Στο δίκτυο στο μέρος του server (και στο intranet)
  - Στον πάροχο Internet του client
  - Στον πάροχο Internet του server
  - Στον ιεραρχικά ανώτερο πάροχο Internet μέσα από τους δρομολογητές του οποίου διοχετεύεται η κίνηση

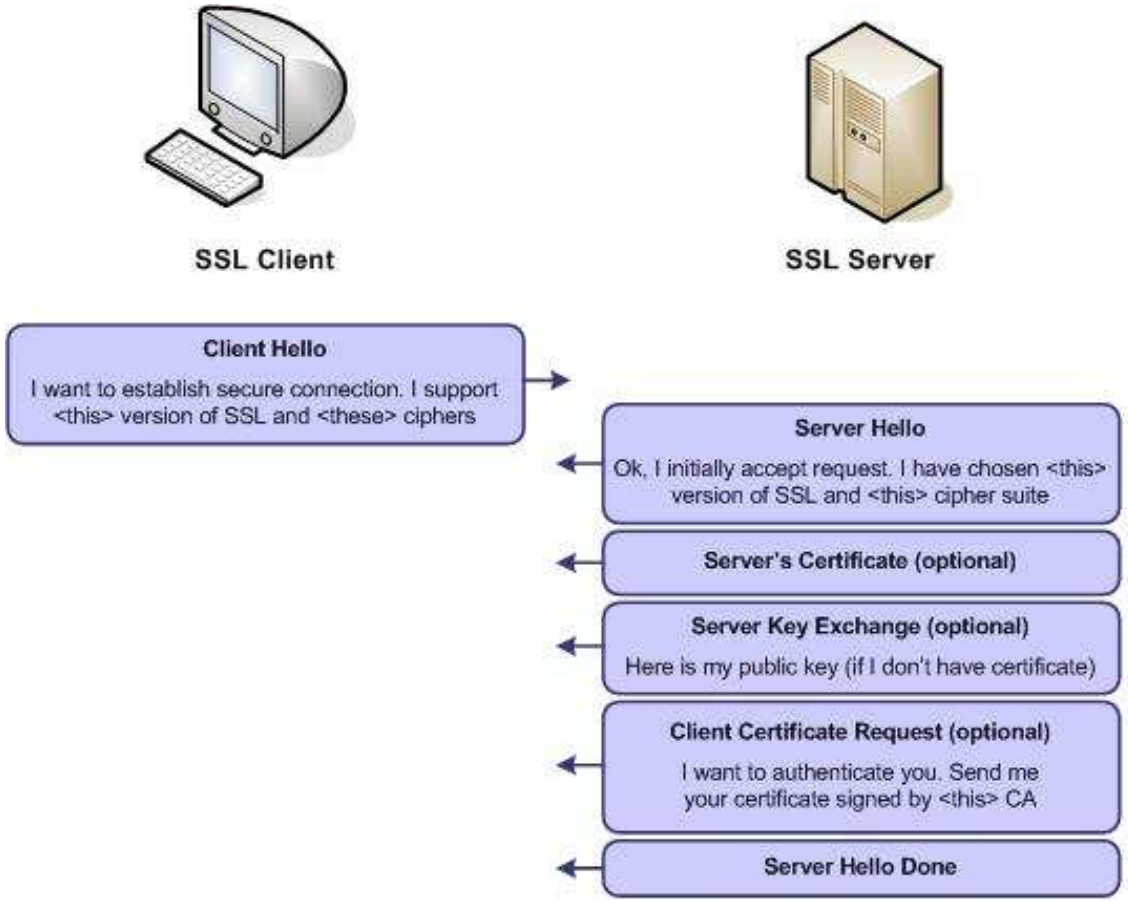
Κρυπτογράφηση επικοινωνίας

- Χρήση πρωτοκόλλου SSL – Secure Sockets Layer (παλαιό όνομα) ή TLS – Transport Layer Security (νέο όνομα)
  - Διαπραγμάτευση αλγορίθμων και κλειδιών κρυπτογράφησης
  - Εγκατάσταση κρυπτογραφημένου τούνελ
  - Προαιρετική πιστοποίηση των μερών που επικοινωνούν μέσω πιστοποιητικών (certificates)

SSL στη στοίβα



Λειτουργία SSL 1/2



Λειτουργία SSL 2/2