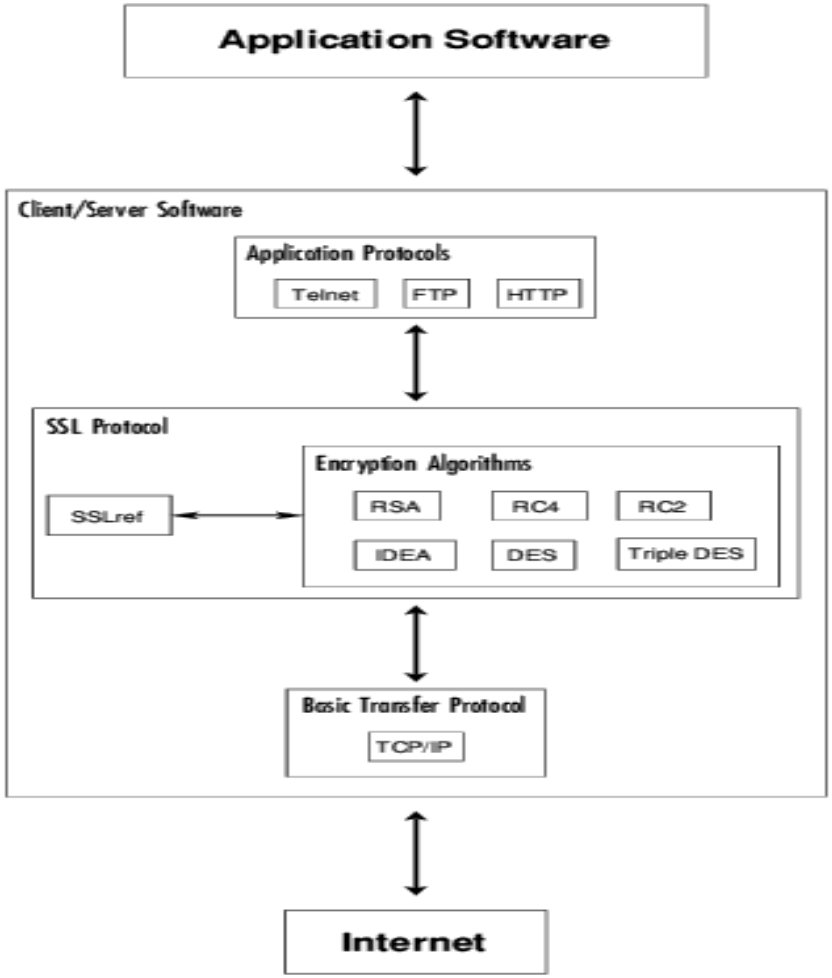
Εικονικά δίκτυα βασισμένα στο SSL

Εισαγωγή

- Το πρωτόκολλο SSL (Secure Socket Layer) αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών (π.χ. αριθμούς πιστωτικών καρτών)
- Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0).
- Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0).
- Αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία. Αυτή η νέα έκδοση του πρωτοκόλλου SSL τέθηκε επισήμως σε κυκλοφορία το Δεκέμβριο του 1995. Μετεξελίχτηκε στο TLS (Transport Layer Security)
- Βασικό χαρακτηριστικό: παρέχει TCP/IP ασφάλεια μεταξύ δύο συστημάτων, όπου το ένα δρα σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server).

Αρχιτεκτονική του SSL



•Πιστοποίηση ταυτότητας μέσω κρυπτογραφίας δημόσιου κλειδιού.

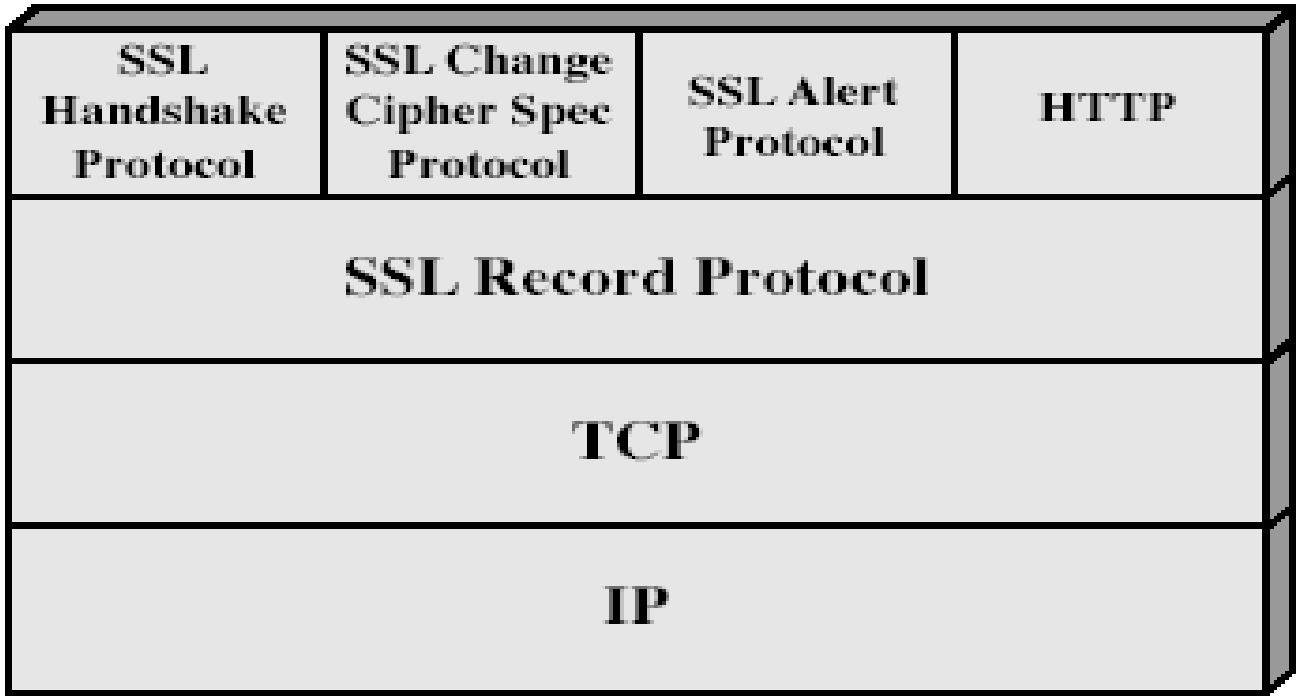
• Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων,

• Προστατεύεται η ακεραιότητα των δεδομένων, με χρήση MACs (πρωτόκολλα με συναρτήσεις κατακερματισμού για εξασφάλιση της ακεραιότητας των δεδομένων).

Γενικά χαρακτηριστικά

- Τα VPN βασισμένα σε SSL είναι πιο απλή λύση, σε σχέση με το IPSec, για απομακρυσμένη πρόσβαση.
- Υπάρχει όμως περιορισμένος αριθμός εφαρμογών για το SSL
  - HTTP, POP, IMAP, FTP, telnet
- Είναι δομημένο ώστε να δουλεύει μόνο πάνω σε TCP πακέτα
- Παρέχει υπηρεσίες ασφάλειας στο επίπεδο μεταφοράς
- Το SSL είναι ανεξάρτητο από το λειτουργικό σύστημα και επιτρέπει σε οποιονδήποτε κινητό χρήστη να συνδεθεί με ασφάλεια, ακόμα και από ένα μη ασφαλές άκρο.
- Τα SSL VPNs μπορούν να «περάσουν» πάνω από firewalls και να αντιμετωπίσουν θέματα NAT (Network Address Translation), ζητήματα τα οποία επιλύονται δύσκολα στην περίπτωση των IPSec VPNs.
- Έχει δύο στρώματα πρωτοκόλλων

Αρχιτεκτονική του SSL (στρωμάτωση των πρωτοκόλλων)



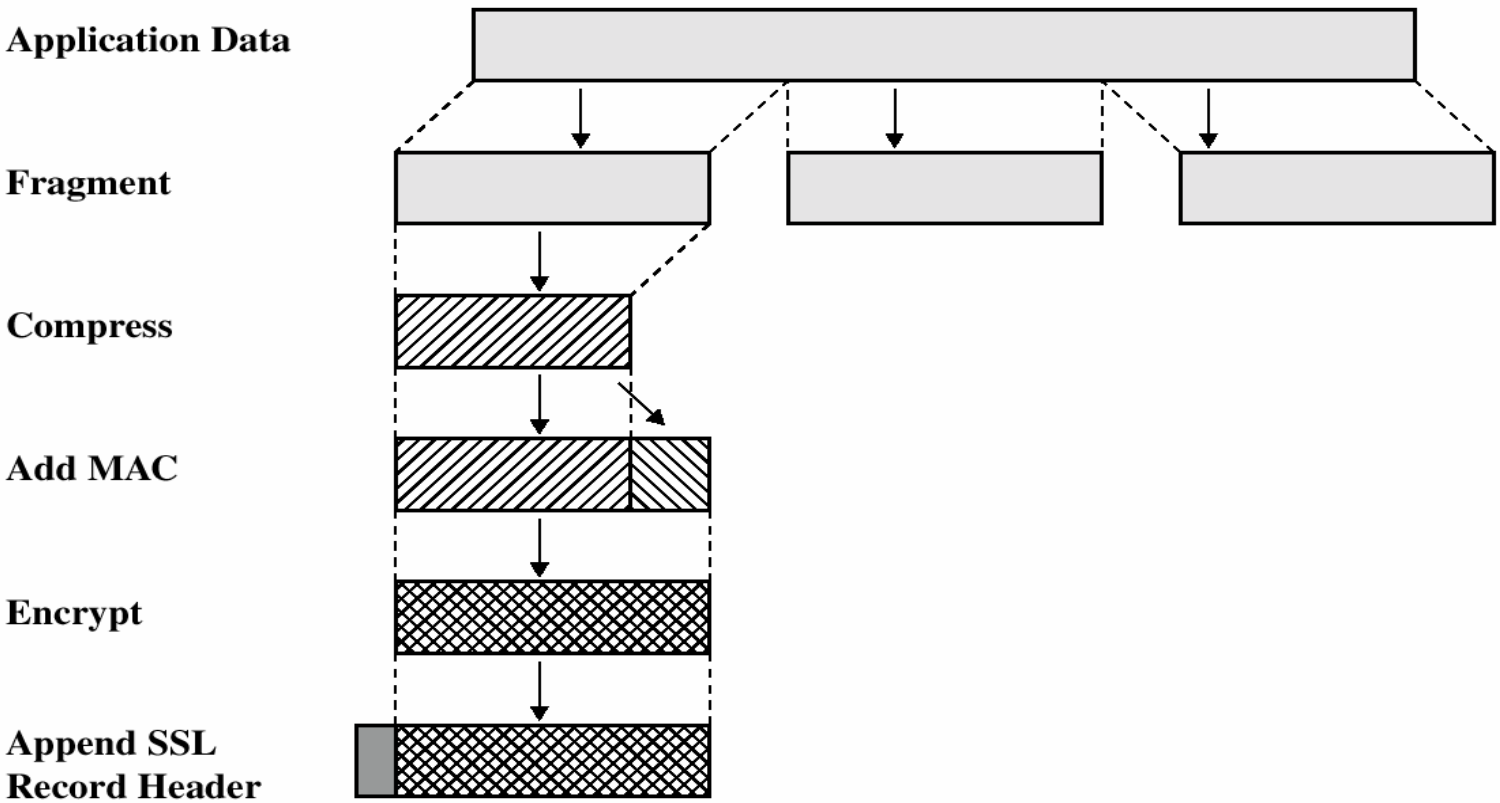
Λειτουργία του SSL

- **SSL σύνοδος (session)**
- Μεταξύ πελάτη και εξυπηρετητή
  - Δημιουργείται από το Handshake Protocol (πρωτόκολλο χειραψίας)
  - Ορίζει ένα σύνολο κρυπτογραφικών παραμέτρων
  - Σε μία σύνοδο μπορούν να υπάρχουν πολλές SSL συνδέσεις (connections)
- **SSL σύνδεση (connection)**
  - Μία διαφανής, peer-to-peer, σύνδεση, η οποία αντιστοιχίζεται σε μία SSL session

SSL record protocol

- **Εμπιστευτικότητα (confidentiality)**
  - Με χρήση συμμετρικής κρυπτογράφησης, με ένα διαμοιρασμένο κλειδί που ορίστηκε στο Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - Συνήθως το μήνυμα συμπιέζεται πριν την κρυπτογράφηση
- **Ακεραιότητα δεδομένων**
  - Χρήση MAC με ένα κοινό διαμοιρασμένο κλειδί
- **Προστασία από επιθέσεις τύπου επανεκπομπής μηνυμάτων**

Τρόπος λειτουργίας του SSL record protocol



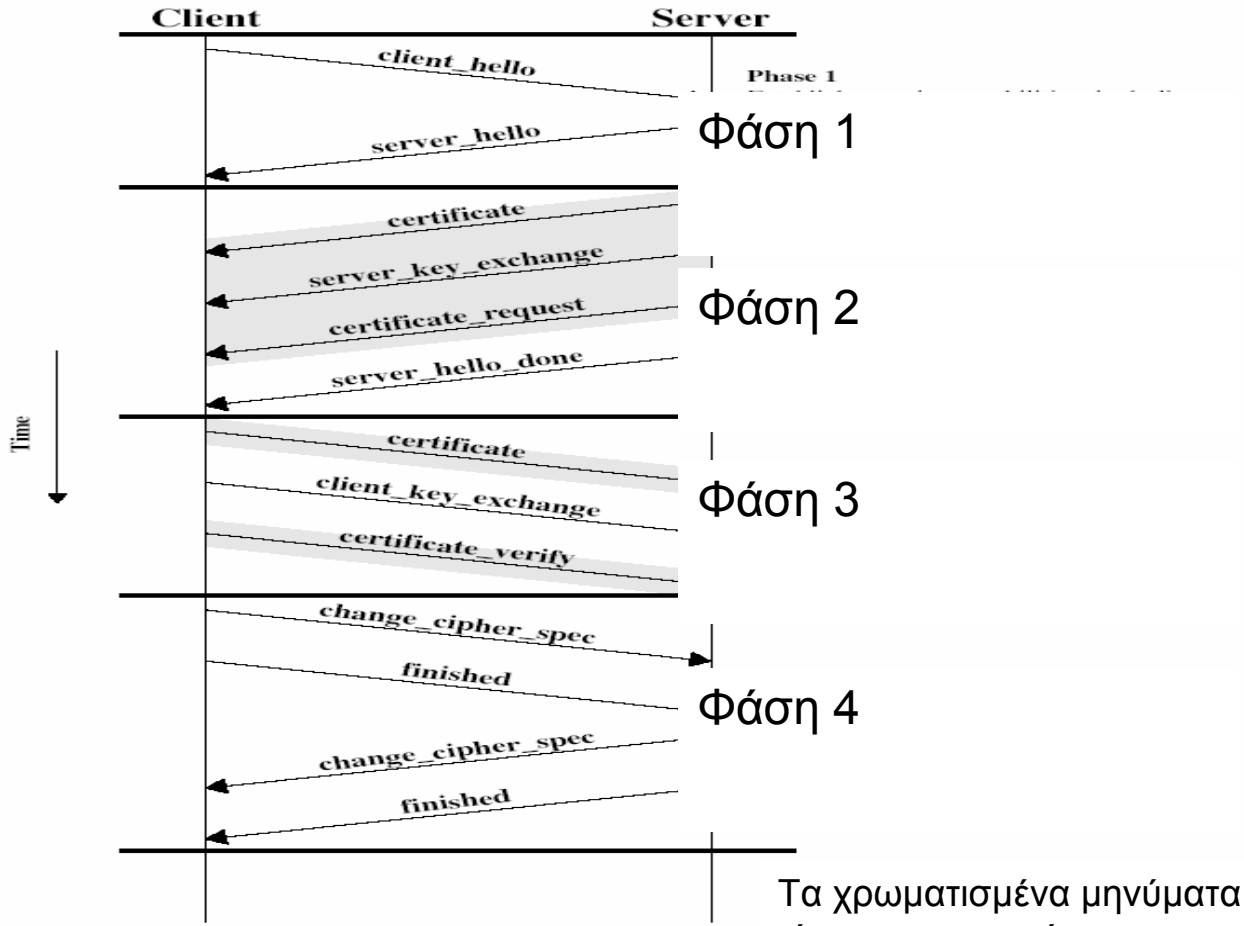
Κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στο SSL

Block Cipher		**Stream Cipher**	
Αλγόριθμος	**Μέγεθος κλειδιού**	**Αλγόριθμος**	**Μέγεθος κλειδιού**
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

SSL handshake protocol

- Πραγματοποιεί μεταξύ client και server:
  - Πιστοποίηση ταυτότητας
  - Διαπραγμάτευση αλγορίθμων κρυπτογράφησης και αλγορίθμων MAC
  - Διαπραγμάτευση των κλειδιών (παραγωγή ενός κύριου (master) κλειδιού, από το οποίο παράγονται κάποια υποκλειδιά που θα χρησιμοποιηθούν).

Ανταλλαγή μηνυμάτων στο SSL Handshake Protocol



Τα χρωματισμένα μηνύματα είναι προαιρετικά

SSL handshake protocol

Φάση 1

C➔S:

- Ενημέρωση για το ποιους αλγόριθμους μπορεί να υποστηρίξει
- Αίτηση για αυθεντικοποίηση του εξυπηρετητή S

S➔ C:

- Επιβεβαίωση των αλγορίθμων
- Απόδοση ενός τυχαίου μοναδικού αριθμού στη σύνδεση (connection id)

SSL handshake protocol

Φάση 2

S➔ C: Server certificate

- Ο server αποδεικνύει την ταυτότητα του με την αποστολή του ψηφιακού του πιστοποιητικού (το οποίο φέρει την υπογραφή μίας διαπιστευμένης αρχής).
- Προαιρετικά, μπορεί να ζητήσει πιστοποίηση ταυτότητας από τον client.

SSL handshake protocol

Φάση 3

C➔S:

- Πιστοποίηση ταυτότητας (αν του έχει ζητηθεί)
- Από κοινού απόφαση των κρυπτογραφικών αλγορίθμων που θα χρησιμοποιηθούν, καθώς και του συμμετρικού κλειδιού που θα χρησιμοποιηθεί, βάση της ακόλουθης διαδικασίας:
  - Ο client παράγει έναν τυχαίο αριθμό τον οποίο στέλνει στο server, κρυπτογραφημένο με το δημόσιο κλειδί του server (που έχει αποκτηθεί από το πιστοποιητικό του server).
  - β) Ο server απαντά με περισσότερα τυχαία δεδομένα (κρυπτογραφημένα με το δημόσιο κλειδί του client, αν είναι διαθέσιμο. Αλλιώς, στέλνει τα δεδομένα μη κρυπτογραφημένα - cleartext).
  - γ) Τα κλειδιά κρυπτογράφησης παράγονται από όλα αυτά τα τυχαία δεδομένα, με τη χρήση των συναρτήσεων κατακερματισμού.

SSL handshake protocol

Φάση 4:

Επιβεβαίωση της διαδικασίας ανταλλαγής κλειδιού – λήξη της διαδικασίας Handshake.

Αντοχή του SSL σε επιθέσεις

- Ευαίσθητο στην ανάλυση κίνησης (οι IP διευθύνσεις είναι μη κρυπτογραφημένες).
- Dictionary attack – Brute Force attack
  - Ανθεκτικό, λόγω του μεγάλου μήκους του κλειδιού
- Replay Attack
  - Ανθεκτικό, λόγω του μοναδικού αριθμού id (μεγέθους 128 bit) που χαρακτηρίζει την κάθε σύνοδο.
- Man-in-the-Middle Attack
  - Ανθεκτικό, λόγω της πιστοποίησης ταυτότητας στην οποία υποβάλλεται ο server.

VPN: SSL ή IPSEC?

	SSL	**IPSEC**
Εφαρμογές	Ο,τιδήποτε σχετικό με web, ανταλλαγή αρχείων ή email	Όλες όσες βασίζονται σε IP
Κρυπτογράφηση	Ισχυρή (128 bits)	Ισχυρή (128 bits, 168 bits)
Πιστοποίηση ταυτότητας	Ψηφιακά πιστοποιητικά	Ψηφιακά πιστοποιητικά
Κόστος	Χαμηλό	Υψηλό
Πολυπλοκότητα υλοποίησης	Χαμηλή	Υψηλή

Γενικά το SSL συνιστάται για συγκεκριμένες εφαρμογές, οι οποίες είναι απομακρυσμένης πρόσβασης (πελάτης-προς-δίκτυο και όχι δίκτυο-προς-δίκτυο). Δεν είναι κατάλληλο για μετάδοση φωνής