ΕΘΝΙΚΟΝ & ΚΑΠΟΔΙΣΤΡΙΑΚΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟΝ ΑΘΗΝΩΝ
NATIONAL & KAPODISTRIAN UNIVERSITY OF ATHENS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών (Π.Μ.Σ.)

Ασφάλεια Δικτύων

Δρ. Κωνσταντίνος Παπαπαναγιώτου
conpap@di.uoa.gr

Κλάσεις Υπηρεσιών Ασφάλειας κατά OSI

Αυθεντικοποίηση

Έλεγχος Προσπέλασης / Πρόσβασης

Εμπιστευτικότητα

Ακεραιότητα

Μη αποποίηση

Υπηρεσία Αυθεντικοποίησης

Ομότιμων Οντοτήτων

Εξετάζει αν μία οντότητα που συμμετέχει σε μία επικοινωνία (σύνοδο ή συναλλαγή) είναι αυτή που ισχυρίζεται

Λαμβάνει χώρα κατά τη διάρκεια εγκατάστασης επικοινωνίας

Προέλευσης Δεδομένων

Εξετάζει αν η πηγή προέλευσης δεδομένων (π.χ., μηνύματος) είναι αυτή που ισχυρίζεται

Λαμβάνει χώρα κατά τη διάρκεια μεταφοράς των δεδομένων

Υπηρεσία Ελέγχου Πρόσβασης

Παρέχει προστασία χρήσης πόρων, αγαθών κοκ από μη εξουσιοδοτημένους χρήστες ή οντότητες

Συνεργασία με υπηρεσίες αυθεντικοποίησης

για να δοθεί πρόσβαση και δικαιώματα πρόσβασης σε πόρους ή αγαθά θα πρέπει να έχει προηγηθεί αυθεντικοποίηση οντότητας που αιτείται πρόσβασης

- *Υποκείμενο*, κάτι ο κάποιος στον οποίο ένα δικαίωμα πρόσβασης δίνεται ‘η απαγορεύεται (χρήστης, εφαρμογή, διεργασία, κλπ.).

- Αντικείμενο, κάτι για το οποίο δίνεται ή απαγορεύεται δικαίωμα πρόσβασης (π.χ. αρχείο, εκτυπωτής, εφαρμογή, κλπ.).

Κατηγορίες

Mandatory Access Control (MAC)
Discretionary Access Control (DAC)
Role Based Access Control (RBAC)

Υπηρεσία Εμπιστευτικότητας

Σύνδεσης

Σύνολο δεδομένων προς μετάδοση

Μη Εγκατεστημένης Σύνδεσης (connectionless)

Μεμονωμένων τμημάτων δεδομένων προς μετάδοση

Επιλεγμένων Πεδίων

Συγκεκριμένων πεδίων δεδομένων

Ροής Κίνησης

Από ανάλυση κυκλοφορίας

Υπηρεσία Ακεραιότητας

Σύνδεσης με αποκατάσταση

Σύνολο δεδομένων μίας σύνδεσης. Αποκατάσταση και ανάκτηση υπό περιπτώσεις

Σύνδεσης άνευ αποκατάστασης

Σύνολο δεδομένων μίας σύνδεσης. χωρίς αποκατάσταση

Μη Εγκατεστημένης Σύνδεσης (connectionless)

Μεμονωμένων τμημάτων δεδομένων προς μετάδοση

Επιλεγμένων Πεδίων

Συγκεκριμένων πεδίων δεδομένων

Μη - Αποποίηση

Non-Repudiation with proof of Origin

Παρέχει στον **Παραλήπτη** πιστοποίηση της αποστολής – προέλευσης των μηνυμάτων που λαμβάνει

Non-Repudiation with proof of Delivery

Παρέχει στον **Αποστολέα** πιστοποίηση της παράδοσης των μηνυμάτων που έστειλε

Υπηρεσίες Ασφάλειας κατά OSI

Επίπεδο	Υπηρεσία
Εφαρμογής	Αυθεντικοποίηση, Έλεγχος Προσπέλασης, Ακεραιότητα, Εμπιστευτικότητα Μη αποποίηση
Παρουσίασης	Εμπιστευτικότητα
Συνόδου	–
Μεταφοράς	Αυθεντικοποίηση, Έλεγχος Προσπέλασης, Ακεραιότητα, Εμπιστευτικότητα
Δικτύου	Αυθεντικοποίηση, Έλεγχος Προσπέλασης, Ακεραιότητα, Εμπιστευτικότητα
Ζεύξης Δεδομένων	Αυθεντικοποίηση, Έλεγχος Προσπέλασης, Ακεραιότητα, Εμπιστευτικότητα
Φυσικό	Εμπιστευτικότητα, Ακεραιότητα

Μηχανισμοί Ασφάλειας κατά OSI

1. *Κρυπτογραφία (Encipherment)*
2. *Ψηφιακές Υπογραφές (Digital Signatures)*
3. *Ελέγχου Πρόσβασης (Access Control)*
4. *Ακεραιότητας Δεδομένων (Data Integrity)*
5. *Ανταλλαγής Αυθεντικοποίησης (Authentication Exchange)*
6. *Εμβόλιμης Κίνησης (Traffic Padding)*
7. *Ελέγχου Δρομολόγησης (Routing Control)*
8. *Συμβολαιογραφίας (Notarization)*

Μηχανισμοί Ασφάλειας

1. *Κρυπτογραφία (Encipherment)*

Εμπιστευτικότητα

Συνεπικουρούν άλλους μηχανισμούς

2. *Ψηφιακές Υπογραφές (Digital Signatures)*

Επικύρωση ακεραιότητας,

αποτροπή αποποίησης αποστολής,

αυθεντικοποίηση

3. *Ελέγχου Πρόσβασης (Access Control)*

Έλεγχος προσπέλασης σε πόρους και αγαθά,

Εξουσιοδότηση

Χρήση μηχανισμών αυθεντικοποίησης

Μηχανισμοί Ασφάλειας (2)

4. *Ακεραιότητας Δεδομένων (Data Integrity)*

Αποτροπή τροποποίησης δεδομένων που μεταδίδονται

5. *Ανταλλαγής Αυθεντικοποίησης (Authentication Exchange)*

Επιβεβαίωση ταυτότητας οντοτήτων

Strong (κρυπτογραφία) vs Week (χωρίς κρυπτογραφία)

6. *Εμβόλιμης Κίνησης (Traffic Padding)*

Αποτροπή Ανάλυσης Κίνησης

7. *Ελέγχου Δρομολόγησης (Routing Control)*

Επιλογή συγκεκριμένης διαδρομής κατά τη μετάδοση της πληροφορίας

Ανίχνευση Εισβολέων

8. *Συμβολαιογραφίας (Notarization)*

Διασφαλίζουν ιδιότητες πληροφορίας, όπως προέλευση, προορισμός

Πρωτόκολλο

- Σύνολο κανόνων για ανταλλαγή μηνυμάτων μεταξύ 2 ή περισσότερων οντοτήτων σε ένα δίκτυο
  - Τυπικά: Κατανεμημένος αλγόριθμος.
- Σύμφωνα με το OSI: κανόνες που καθορίζουν την επικοινωνία μεταξύ ενός ζεύγους ομότιμων οντοτήτων.

Αυθεντικοποίηση

- Θέλουμε να σχεδιάσουμε ένα πρωτόκολλο αυθεντικοποίησης μετάξύ του Α και του Β.

  A ⟶ B: 'Hi B, I'm A'

- Είναι ασφαλές;

- Όχι – Οποιοσδήποτε μπορεί να προσποιηθεί τον Α.
- Χρειαζόμαστε κάτι ασφαλέστερο.
- Τα πρωτόκολλα αυθεντικοποίησης σχεδιάζονται βάση διαφόρων υποθέσεων:
  - Οι Α και Β μοιράζονται ένα κοινό μυστικό (π.χ. συνθηματικό, PIN, συμμετρικό κλειδί, βιομετρική πληροφορία, κλπ.).
  - Οι Α και Β έχουν ο καθένας το δημόσιο κλειδί του άλλου.

Ισχυρή Αυθεντικοποίηση

- Στην ισχυρή αυθεντικοποίηση μία οντότητα «αποδεικνύει» την ταυτότητά της στην άλλη επιδεικνύοντας τη γνώση ενός μυστικού που σχετίζεται με αυτή, χωρίς όμως να αποκαλύπτει το ίδιο το μυστικό.
- Γνωστή και ως: ‘challenge-response’ authentication.
- Συνήθως χρησιμοποιούνται μηχανισμοί κρυπτογράφησης:
  - Κρυπτογραφία (συμμετρική).
  - Ψηφιακές υπογραφές.

Παράδειγμα: Συνθηματικά

- Η Alice έχει ένα user ID και password που της επιτρέπει απομακρυσμένη πρόσβαση μέσω δικτύου σε έναν υπολογιστή Β.
  - Η Alice στέλνει το user ID και το password μέσω δικτύου
  - Ο Β χρησιμοποιεί το ID της Alice για να βρει την εγγραφή στο αρχείο συνθηματικών και να συγκρίνει το συνθηματικό της με την εγγραφή.
  - Εάν τα συνθηματικά είναι ίδια ο Β αυθεντικοποιεί την Alice.
- Αυθεντικοποίηση χρήστη βάση κάτι που ξέρει.
- Είναι ασφαλές το πρωτόκολλο;

Παράδειγμα: Συνθηματικά

- Το μυστικό είναι το συνθηματικό της Alice.
- Αποκαλύπτεται μέσα από το πρωτόκολλο άρα δεν είναι ασφαλές.
- Οποιοσδήποτε μπορεί να το υποκλέψει στο δίκτυο.
- Η προσέγγιση αυτή δεν είναι ασφαλής
  - Παρόλα αυτά χρησιμοποιείται ευρύτατα: π.χ. SNMPv1, ftp, telnet, webmail, …
- Μπορούμε να ενισχύσουμε την ασφάλεια στέλνοντας τη σύνοψη του password;
  - Ευάλωτο σε επιθέσεις λεξικού και επανάληψης (replay attacks).

Αυθεντικοποίηση χρήστη

- Στόχος: η αυθεντικοποίηση χρήστη στο σύστημα (ή και το αντίστροφο).
- Βασίζεται σε (ή σε συνδυασμό):
  - Κάτι που ξέρεις (password, PIN).
  - Κάτι που έχεις (smartcard, token,…)
  - Κάτι που είσαι (βιομετρικά χαρακτηριστικά)
- Περιορίζεται ανάλογα με το τι μπορεί να θυμάται ο χρήστης, να κουβαλάει μαζί του ή να είναι.
- Η αυθεντικοποίηση δεν αφορά πάντα χρήστες.

Αυθεντικοποίηση με Κρυπτογράφηση

- **Υποθέτουμε ότι** η Alice και ο Bob μοιράζονται ένα κοινό μυστικό (συμμετρικό) κλειδί K.
- **Στόχος:** Αυθεντικοποίηση της Alice.

- Η Alice στέλνει ένα εναρκτήριο μήνυμα.
- Ο Bob στέλνει στην Alice ένα μήνυμα *challenge* R, (τυχαία αλληλουχία από bit).
- Η Alice *απαντά με* $\{R \,||\, B\}_K$.
- Ο Bob ελέγχει αν αποκρυπτογραφώντας το μήνυμα λαμβάνει το R || B.
- Αν ναι η Alice έχει αυθεντικοποιηθεί.

Το πρωτόκολλο

1. A ⟶ B: ‘Hi Bob, I’m Alice’
2. B ⟶ A: R (challenge)
3. A ⟶ B: $\{R \,||\, B\}_K$ (response)

Ασφάλεια του πρωτοκόλλου

1. Πώς μπορεί να είναι σίγουρος ο Bob ότι το μήνυμα 3 προήλθε όντως απ' την Alice;
2. Πώς μπορεί να είναι σίγουρος ο Bob ότι το μήνυμα 3 δεν είναι επανάληψη ενός προηγούμενου μηνύματος μεταξύ εκείνου και της Alice;

1. Μόνο η Alice (και ο Bob) γνωρίζουν το μυστικό κλειδί K.
2. Ο Bob διάλεξε το R τυχαία λίγο πριν στείλει το μήνυμα 2. Το R δεν θα πρέπει να έχει χρησιμοποιηθεί ξανά στο παρελθόν.

Ασφάλεια του πρωτοκόλλου

1. Γιατί ο Bob μπορεί να είναι σίγουρος ότι το μήνυμα 3 είναι για εκείνον;
2. Μπορεί ένας επιτιθέμενος να μαντέψει την τιμή του κλειδιού K παρατηρώντας μόνο την ανταλλαγή των μηνυμάτων;

1. Η Alice συμπεριλαμβάνει την ταυτότητα του Bob ‘B’ στο κρυπτογραφημένο μήνυμα.
2. Όχι αν ο αλγόριθμος κρυπτογράφησης είναι ισχυρός.

Ασφάλεια του πρωτοκόλλου

1. Έχει αυθεντικοποιηθεί η Alice στον Bob;
2. Έχει αυθεντικοποιηθεί ο Bob στην Alice;

1. Ναι.
2. Όχι. (Κάποιος μπορεί να παραστήσει τον Bob. Στόχος μας όμως κατά το σχεδιασμό ήταν η αυθεντικοποίηση της Alice και όχι του Bob.)

Επίθεση Επανάληψης (Replay Attack)

- Υποθέτουμε ότι ο Mallory θέλει να παραστήσει την Alice :

1. M(A)⟶B: ‘Hi Bob, I’m Alice’
2. B⟶M(A): R (challenge)
3. M(A)⟶B: ???

- Ο Mallory δεν μπορεί να κατασκευάσει τη σωστή απάντηση $\{R||B\}_K$ γιατί δεν γνωρίζει το κλειδί K και το R δεν έχει ξαναχρησιμοποιηθεί.
- Μπορεί ο Mallory να προβλέψει το R;

Επίθεση Επανάληψης (Replay Attack)

Ο Mallory αρχικά προσποιείται τον Bob στην Alice:

1. A → M(B): 'Hi Bob, I'm Alice'
2. M(B) → A: R **(Ο Μ προβλέπει ποιο R θα χρησιμοποιηθεί από τον Β)**
3. A → M(B): $\{R \,||\, B\}_K$

Ο Mallory κρατά το $\{R \,||\, B\}_K$ για να το χρησιμοποιήσει αργότερα:

1. M(A) → B: 'Hi Bob, I'm Alice'
2. B → M(A): R (Ο Μ προέβλεψε ότι αυτό το R θα χρησιμοποιούσε ο Β)
3. M(A) → B: $\{R \,||\, B\}_K$

Liveness - Freshness

- Η επίθεση επανάληψης αναδεικνύει την ανάγκη ύπαρξης μηχανισμών «επικαιροποίησης».
- **Liveness:** διασφάλιση ότι το μήνυμα έχει σταλεί σε αποδεκτά πρόσφατα χρονικά όρια**.**
- Επιτυγχάνεται μέσω του «*freshness*».
- **Freshness:** διασφάλιση ότι το μήνυμα δεν έχει χρησιμοποιηθεί στο παρελθόν και δημιουργήθηκε σε αποδεκτά πρόσφατο χρονικό όριο.
- Δύο βασικές μέθοδοι:
  - Nonce (**N**umber used **once**).
  - Time-stamps.

Nonces

- Nonce = number used once
- Κύριο χαρακτηριστικό: χρησιμοποιείται μία φορά, δεν πρέπει να έχει χρησιμοιποιηθεί ξανά στο παρελθόν.
  - Θεωρητικά μπορεί να είναι μετρητής.
- Θα πρέπει να μη μπορεί να προβλεφθεί το επόμενο nonce από κάποιον.
  - Δημιουργία R σαν μια μεγάλη τυχαία ακολουθία από bit.
- Προσοχή: το R δεν μπορεί να προβλεφθεί αλλά δεν είναι μυστικό.

Nonces

Θετικά:

- Πιο απλά στη διαχείριση από τα timestamps.

Αρνητικά:

- Απαιτούνται πιο πολλα μηνύματα σε σχέση με τα timestamps.
- Τυχαιότητα.
  - Δύσκολη η δημιουργία πραγματικά τυχαίων bit χωρίς ειδικό hardware.
  - Δύσκολη σε συσκευές με περιορισμένους πόρους.

Time-stamps

- Προσθήκη ημέρας/ώρας στο μήνυμα ώστε ο παραλήπτης να μπορεί να ελέγξει πόσο πρόσφατο είναι (αρκεί να προστατεύεται κρυπτογραφικά).
- A⟶B: ‘I’m Alice’, $\{T \,||\, B\}_K$
  - Ο Bob αποκρυπτογραφεί και ελέγχει αν το T είναι αρκετά πρόσφατο.

Time-stamps

Θετικά:

- Χρειάζεται μόνο ένα μήνυμα αντί τριών.
- Δεν απαιτείται τυχαιότητα. Οι περισσότερες συσκευές διαθέτουν ρολόι.

Αρνητικά:

- Απαιτούνται συγχρονισμένα (με ασφάλεια) ρολόγια για την αποφυγή επιθέσεων επανάληψης
- Ούτως ή άλλως απαιτείται «παράθυρο» αποδοχής (λόγω καθυστέρησης στο δίκτυο).
- Απαιτείται αποθήκευση πρόσφατων μηνυμάτων για την αποφυγή επιθέσεων επανάληψης
  - Ο Mallory υποκλέπτει το μήνυμα αυθεντικοποίησης $\{T \,||\, B\}_K$ από την Alice και το αναπαράγει μέσα στο παράθυρο αποδοχής του B.

‘Λογικά’ Time-stamps

- Εναλλακτικά του ρολογιού: Η Alice και ο Bob χρησιμοποιούν ένα ζεύγος μετρητών N_{AB} and N_{BA}.
- Κάθε φορά που η Α στέλνει ένα μήνυμα τον Β συμπεριλαμβάνει την τιμή του $N_{AB,}$ και τον αυξάνει. Ομοίως και ο Β.
- Ο Β δέχεται μηνύματα από την Α μόνο αν η τιμή του $N_{AB,}$ είναι μεγαλύτερη από την τελευταία που έλαβε.
- Χρησιμοποιείται στο UMTS και στο SNMPv3.

‘Λογικά’ Time-stamps

Θετικά:

- Δεν χρειάζεται να δημιουργηθούν τυχαίες αλληλουχίες bit ή να συγχρονίζονται ρολόγια..

Αρνητικά:

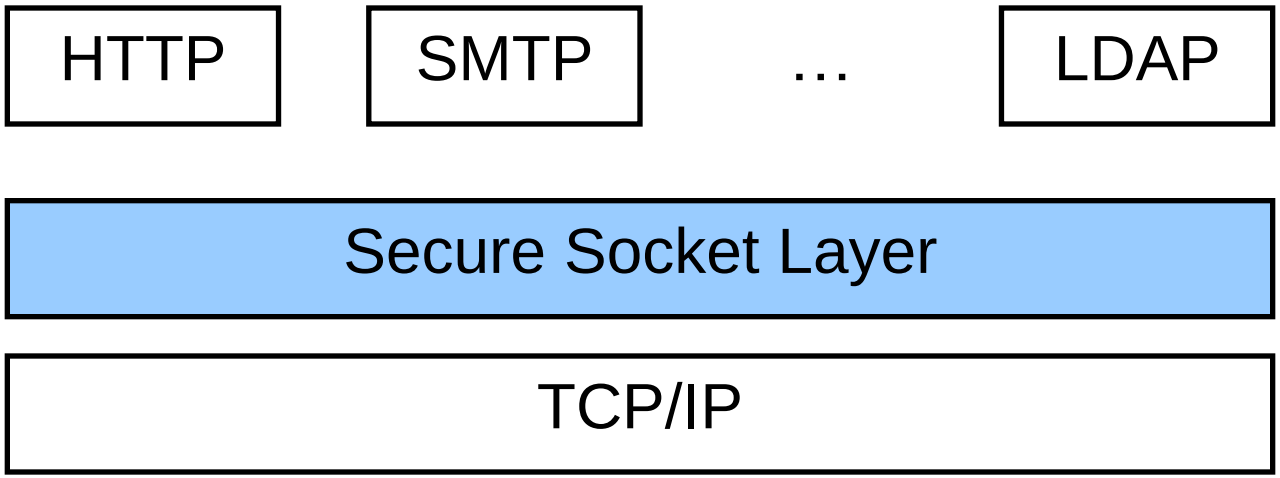
- Χρειάζεται ένα ζεύγος μετρητών για κάθε ζεύγος οντοτήτων που επικοινωνούν.
- Οι αριθμοί πρέπει να μένουν κρυφοί για να μην είναι προβλέψιμοι.

SSL/TLS

- SSL = Secure Sockets Layer
  - v1: δεν εκδόθηκε
  - v2: χρήσιμη αλλά με λάθη
  - v3
- TLS = Transport Layer Security
  - TLS 1.0 = SSL 3.0 με μικρές διορθώσεις
  - RFC 2246
  - http://www.openssl.org
- Χρησιμοποιείται ευρύτατα στους φυλλομετρητές για εφαρμογές ηλεκτρονικού εμπορίου

Πρωτόκολλο SSL/TLS

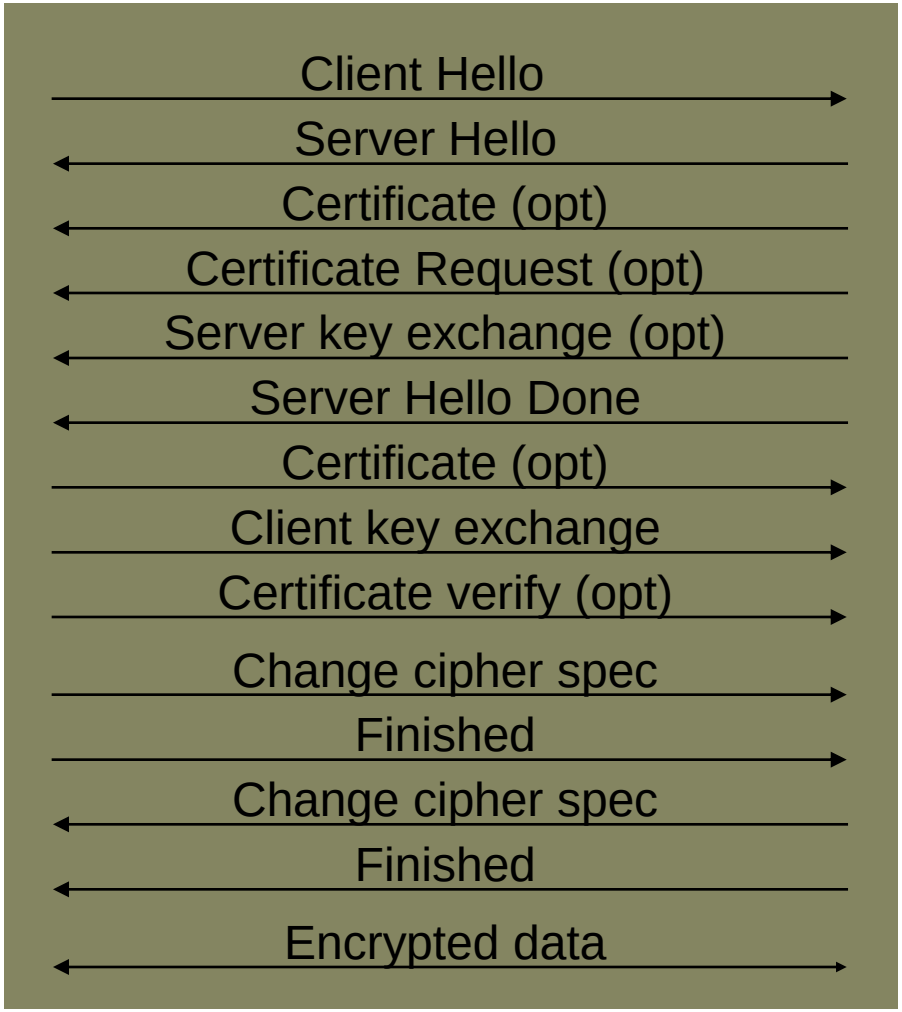
- Το πρωτόκολλο SSL παρεμβάλλεται μεταξύ του TCP/IP και του επιπέδου εφαρμογής προκειμένου να:
  - πιστοποιεί τον εξυπηρέτη στον εξυπηρετούμενο
  - πιστοποιεί τον εξυπηρετούμενο στον εξυπηρέτη
  - κρυπτογραφεί την επικοινωνία



Ανατομία του πρωτοκόλλου SSL

- Δύο επί μέρους πρωτόκολλα
  - χειραψία SSL
  - ανταλλαγή δεδομένων SSL
- Στόχοι χειραψίας
  - Να πιστοποιηθεί ο εξυπηρετητής στον εξυπηρετούμενο
  - Συμφωνία πάνω στους αλγόριθμους κρυπτογραφίας που θα χρησιμοποιηθούν για την επικοινωνία
  - Προαιρετικά, πιστοποίηση εξυπηρετούμενου στον εξυπηρετητή
  - Δημιουργία «διαμοιραζόμενων μυστικών» μέσω τεχνικών κρυπτογραφίας δημόσιου κλειδιού για την κρυπτογράφηση της επικοινωνίας
  - Εγκαθίδρυση του κρυπτογραφημένου διαύλου επικοινωνίας

Χειραψία πρωτοκόλλου SSL



Βήματα Χειραψίας SSL (1)

- *Client Hello* – αποστέλλονται στον εξυπηρέτη:
  - αριθμός έκδοσης SSL του εξυπηρετούμενου
  - λίστα υποστηριζόμενων αλγόριθμων κρυπτογράφησης και αντιστοίχων μεγεθών κλειδιών
  - ταυτότητα της συνόδου κ.τ.λ.
- *Server Hello – αποστέλλονται στον εξυπηρετούμενο*
  - αριθμός έκδοσης SSL του εξυπηρέτη
  - ο πιο κατάλληλος αλγόριθμος κρυπτογράφησης
  - το επιλεγμένο μήκος κλειδιών

Βήματα Χειραψίας SSL (2)

- *Certificate* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρέτη)
  - ο εξυπηρέτης αποστέλλει το πιστοποιητικό του στον εξυπηρετούμενο. Το πιστοποιητικό περιέχει το δημόσιο κλειδί του εξυπηρέτη. Ο εξυπηρετούμενος διακριβώνει την ταυτότητα του εξυπηρέτη.
- *Certificate request* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρετούμενου)
  - *ο εξυπηρέτης αποστέλλει ένα μήνυμα με το οποίο ζητά το πιστοποιητικό του εξυπηρετούμενου.*

Βήματα Χειραψίας SSL (3)

- *Server key exchange* - (προαιρετικό, αν το πιστοποιητικό του εξυπηρέτη δεν είναι επαρκές για την ανταλλαγή κλειδιών που θα ακολουθήσει)
- *Server Hello Done*
  - Ο εξυπηρέτης υποδεικνύει ότι έχει τελειώσει την προκαταρκτική φάση εγκαθίδρυσης της συνόδου
- *Certificate* (προαιρετικό, αν ο εξυπηρέτης έχει αποστείλει μήνυμα certificate request)
  - ο εξυπηρετούμενος αποστέλλει το πιστοποιητικό του, ο εξυπηρέτης το επαληθεύει

Βήματα Χειραψίας SSL (4)

- *Client key exchange*
  - ο εξυπηρετούμενος δημιουργεί το προκαταρκτικό μυστικό (premaster secret) για τη συγκεκριμένη σύνοδο, το κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρέτη και το αποστέλλει σ' αυτόν.
- *Certificate verify* (προαιρετικό, αν ο εξυπηρέτης έχει ζητήσει το πιστοποιητικό του εξυπηρετούμενου)
  - το μήνυμα αυτό επιτρέπει στον εξυπηρέτη να ολοκληρώσει τη διαδικασία επαλήθευσης του πιστοποιητικού

Βήματα Χειραψίας SSL (5)

- *Change cipher spec*
  - Ο εξυπηρετούμενος είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
  - Ο εξυπηρετούμενος τελείωσε το δικό του τμήμα της χειραψίας
- *Change cipher spec*
  - Ο εξυπηρέτης είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
  - Ο εξυπηρέτης έχει τελειώσει το δικό του τμήμα της χειραψίας

Ανταλλαγή δεδομένων στο SSL

- Με συμμετρικό αλγόριθμο κρυπτογραφίας
- Το κλειδί παράγεται με βάση το *προκαταρκτικό μυστικό*
- Ο αλγόριθμος παραγωγής εξαρτάται από τον συμμετρικό αλγόριθμο κρυπτογραφίας που θα χρησιμοποιηθεί και το μήκος των κλειδιών

SessionKey = genKey(premasterSecret, cipher, keyLen)

IPSec

- Προσφέρει ασφάλεια στο επίπεδο δικτύου
  - Δεν απαιτεί αλλαγές σε εφαρμογές
  - Οι χρήστες δεν χρειάζεται να γνωρίζουν τίποτα
- Αρχικός ορισμός: IETF RFCs 4301-4309 (2005)
  - Επανεκδόσεις των RFCs 2401–2412 (1998)
  - Επόμενα RFCs προσδιορίζουν νέες μετατροπές (νέοι αλγόριθμοι κρυπτογράφησης κλπ.)

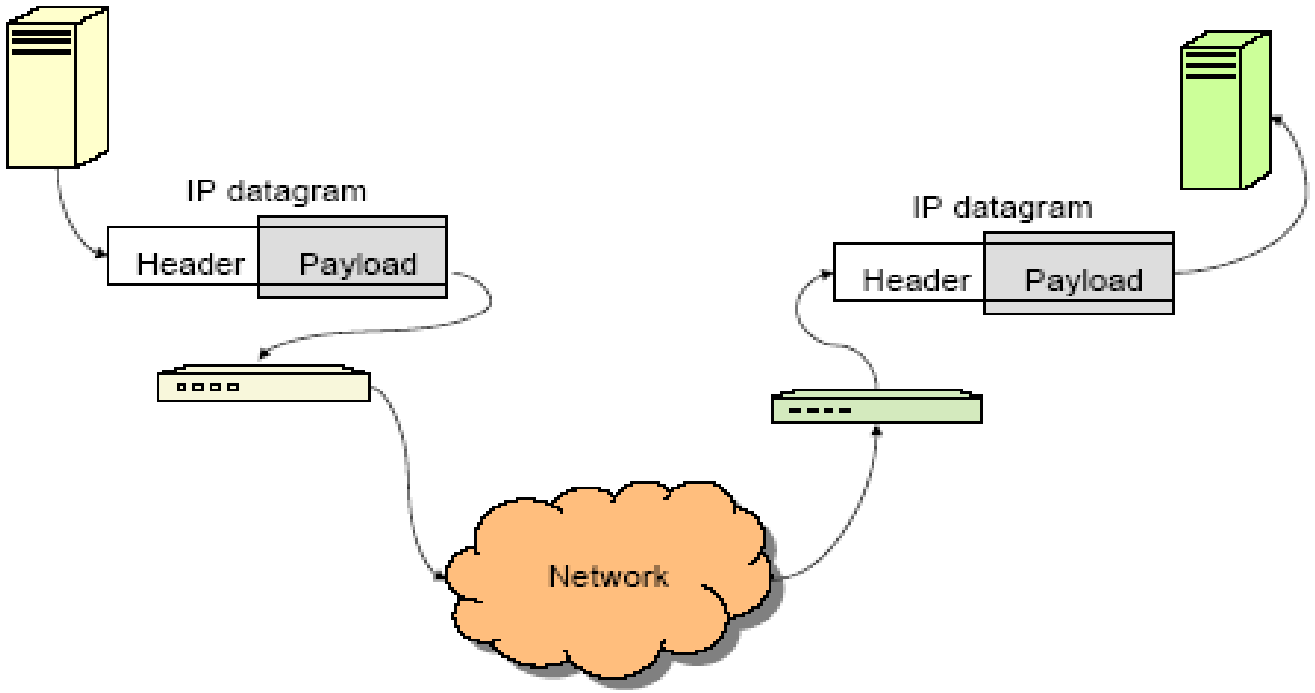
Βασικά Χαρακτηριστικά

- Δύο βασικοί τρόποι λειτουργίας
  - Από άκρο σε άκρο (transport mode)
  - Από δίκτυο σε δίκτυο (tunnel mode)
- Προσφέρει υπηρεσίες αυθεντικοποίησης και/ή εμπιστευτικότητας δεδομένων
  - Πρωτόκολλα AH και ESP
- Προσφέρει διάφορες μεθόδους εγκαθίδρυσης κλειδιών
  - IKE
  - ISAKMP
  - IKEv2 (RFC 4306, 2005)

Transport Mode

- Προστασία πρωτοκόλλων υψηλών επιπέδων δικτύωσης
- Καλύπτει IP datagrams και ορισμένα πεδία επικεφαλίδας
  - πακέτα TCP, UDP, ICMP, κλπ.
- Host-to-host (end-to-end)
  - Η επεξεργασία λαμβάνει χώρα στα άκρα του ασφαλούς καναλιού
  - Οι κόμβοι στα άκρα πρέπει να γνωρίζουν πώς να εφαρμόζουν το IPSec

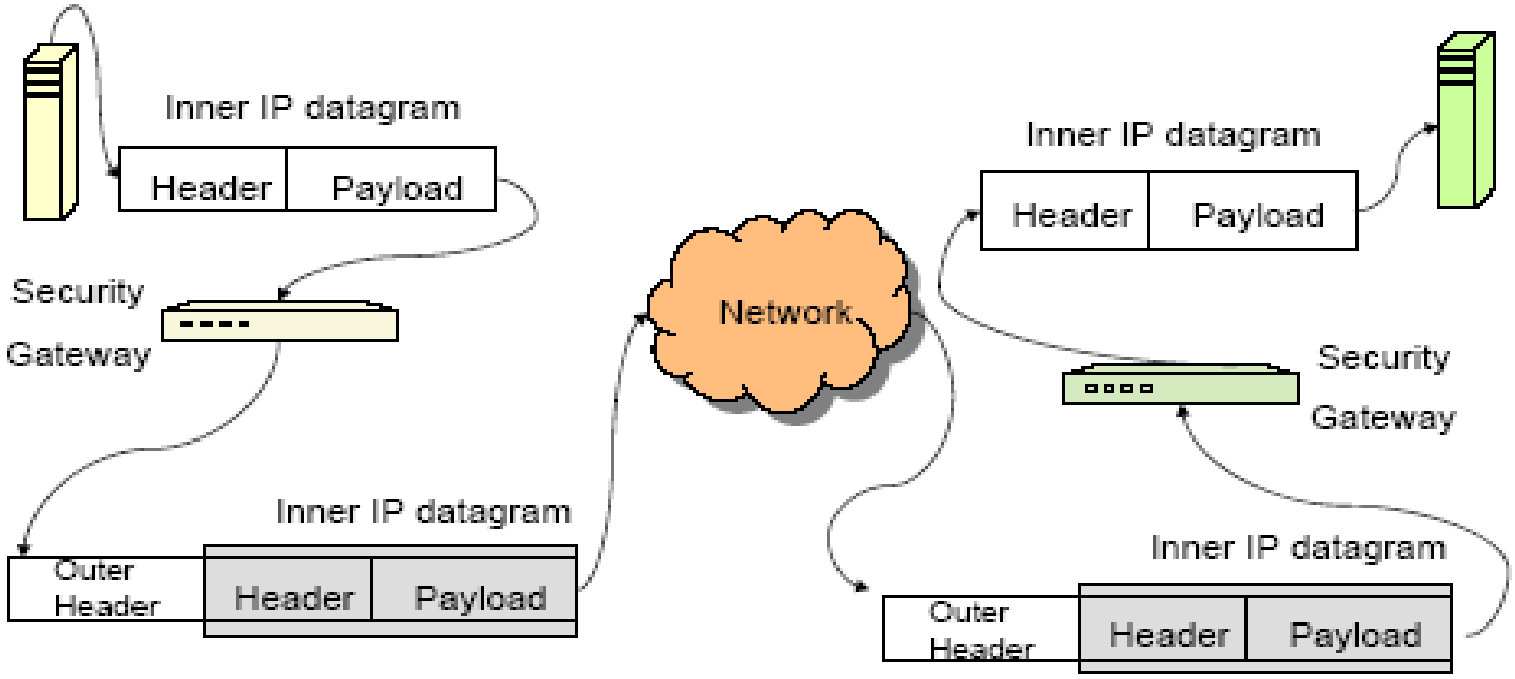
Transport Mode (2)



Tunnel Mode

- Προστατεύεται ολόκληρο το IP datagram
- Ολόκληρο το datagram μαζί με κάποια πεδία ασφάλειας χρησιμοποιούνται σα νέο φορτίο του «εξωτερικού» datagram
- Ουσιαστικά το αρχικό, «εσωτερικό» datagram ενθυλακώνεται μέσα στο «εξωτερικό»
- Όλη η επεξεργασία λαμβάνει χώρα σε security gateways για λογαριασμό των τελικών κόμβων
  - Π.χ. firewalls, routers, κλπ. που υποστηρίζουν IPSec
  - Gateway-to-gateway ασφάλεια
  - Οι τελικοί κόμβοι δε χρειάζονται να γνωρίζουν τίποτα περί IPSec
- Οι ενδιάμεσοι κόμβοι δε μπορούν να δουν το εσωτερικό datagram.
  - Ακόμα και οι διευθύνσεις αποστολέα και παραλήπτη αποκρύπτονται.

Tunnel Mode (2)



Πρωτόκολλο AH

- AH = Authentication Header (RFC 4302)
- Προσφέρει
  - αυθεντικοποίηση προέλευσης δεδομένων
  - ακεραιότητα δεδομένων
- Αυθεντικοποιεί όλα τα δεδομένα και ένα μεγάλο μέρος της επικεφαλίδας
- Αποτρέπει την αλλαγή των διευθύνσεων IP
  - Η διεύθυνση του αποστολέα αυθεντικοποιείται
- Αποτρέπει επανάληψη παλαιότερων πακέτων
  - Χρησιμοποιεί sequence numbers
  - Προστατεύει την ακεραιότητά τους
  - Οι παραλήπτες ελέγχουν τα sequence numbers των εισερχόμενων πακέτων
  - Απορρίπτουν επαναλήψεις και πακέτα που είναι πολύ παλιά
- Χρησιμοποιεί MAC και συμμετρικά κλειδιά μεταξύ τελικών κόμβων

Πρωτόκολλο ESP

- ESP = Encapsulating Security Payload (RFC 4303)
- Προσφέρει
  - Εμπιστευτικότητα
    - Προστασία των δεδομένων (payload) στο Transport Mode και του εσωτερικού datagram στο Tunnel Mode
    - Ο sequence number δεν κρυπτογραφείται
  - Αυθεντικότητα/ακεραιότητα
    - Προστασία των δεδομένων (payload) στο Transport Mode και του εσωτερικού datagram στο Tunnel Mode
    - Τα δεδομένα επικεφαλίδας δεν προστατεύονται
- Περιορισμένη υπηρεσία εμπιστευτικότητας κατά τη ροή δεδομένων σε Tunnel Mode
- Χρησιμοποιεί συμμετρική κρυπτογραφία και MAC, βασιζόμενο σε μυστικά κλειδιά που μοιράζονται οι τελικοί κόμβοι

Security Associations

- Το IPSec παρέχει ποικίλες επιλογές για τη χρήση αλγορίθμων κρυπτογράφησης και αυθεντικοποίησης
  - Δύο οντότητες που θέλουν να επικοινωνήσουν πρέπει να συμφωνήσουν εκ των προτέρων στο είδος της ασφάλειας
- Η Security Association (SA) είναι συμφωνία μεταξύ δύο άκρων για μεθόδους και αλγορίθμους ασφαλείας που επιθυμούν να χρησιμοποιήσουν κατά τη σύνοδο:
  - mode λειτουργίας (transport, tunnel)
  - αλγόριθμοι κρυπτογράφησης
  - αλγόριθμοι αυθεντικοποίησης
  - κλειδιά, διάρκεια ισχύος κλειδιών κτλ .
- SADB (Security Associations Database)
  - Κάθε IPSec end-point διατηρεί μία βάση δεδομένων που αποθηκεύονται τα ενεργά SAs
- Αποφασίζονται κατά περίπτωση ή όπως προτάσσει το IKE

Διαχείριση Κλειδιών

- Το IPSec απαιτεί μεγάλο αριθμό συμμετρικών κλειδιών
  - Ένα για κάθε SA
  - Δυνητικά, διαφορετικά SAs για κάθε συνδυασμό:

    {ESP,AH} x {tunnel,transport} x {αποστολέας, παραλήπτης} x {πρωτόκολλο} x {πόρτα}
- Από πού προέρχονται SAs και κλειδιά;
  - Ανάθεση «με το χέρι»
    - Ικανοποιητική λύση για μικρό αριθμό κόμβων μόνο
  - IKE: Internet Key Exchange, RFC 2409 (v1), RFC 4306 (v2).
    - Βασίζεται στα πρωτόκολλα Oakley και SKEME και στο πλαίσιο του ISAKMP
  - IKEv2
    - Προορίζεται να αντιμετωπίσει τα προβλήματα και την πολυπλοκότητα του IKEv1, αλλά…

OAKLEY/ISAKMP

- OAKLEY
  - πρωτόκολλο ανταλλαγής κλειδιών
  - Βασισμένο σε Diffie-Hellman (DH)
    - Παρέχει πρόσθετη ασφάλεια σε σχέση με το απλό DH
  - Είναι γενικό, δεν απαιτεί ειδικά formats
- ISAKMP
  - Παρέχει ένα πρωτόκολλο για διαχείριση κλειδιών και διαπραγμάτευση παραμέτρων / αλγορίθμων
    - Εγκαθίδρυση, μετατροπή, διαγραφή SAs.
    - Ορίζει διαδικασίες και format πακέτων

IKE: Στόχοι

- Αυθεντικοποίηση των οντοτήτων που συμμετέχουν
- Εγκαθίδρυση ενός νέου, κοινού μυστικού
  - Χρησιμοποιείται για να παραχθούν τα υπόλοιπα κλειδιά
  - Για την εμπιστευτικότητα και την ακεραιότητα του καναλιού διαχείρισης του IKE
  - Για γενική χρήση στα SAs
- Μικρή αντοχή σε επιθέσεις τύπου Denial-of-Service
- Ασφαλή διαπραγμάτευση παραμέτρων και αλγορίθμων
  - Μέθοδος αυθεντικοποίησης, μέθοδος ανταλλαγής κλειδιών, αλγόριθμοι κρυπτογράφησης, MAC, σύνοψης, κλπ.

IKE: 1η Φάση

- **1η Φάση**:
  - Διαπραγμάτευση ενός ειδικού SA, του IKE SA, καθώς και πληροφοριών σχετικά με κλειδιά
    - Το IKE SA προσδιορίζει αλγόριθμους κρυπτογράφησης και MAC που θα χρησιμοποιηθούν για την ανάπτυξη ενός ασφαλούς καναλιού στη 2η φάση.
    - Επίσης, προσδιορίζει μέθοδο αυθεντικοποίησης και παραμέτρους Diffie-Hellman που θα χρησιμοποιηθούν στην 1η φάση
  - Σύνολο αλγορίθμων και δεδομένων που ονομάζονται σουίτα προστασίας
  - Το IKE SA ισχύει αμφίδρομα και περιέχει διαφορετικές πληροφορίες από τα υπόλοιπα, «κανονικά» SAs

IKE: 2η Φάση

- **2η Φάση:** Διαπραγμάτευση SAs για γενική χρήση
  - Χρησιμοποιεί ένα ασφαλές κανάλι για να διαπραγματευτεί περαιτέρω τα SAs
  - Οι αλγόριθμοι γι' αυτό το κανάλι έχουν ορισθεί από το IKE SA στην 1η φάση
  - Τα κλειδιά προέρχονται από την ανταλλαγή Diffie-Hellman στην πρώτη φάση.
  - Η 2η φάση μπορεί επίσης να χρησιμοποιηθεί για ασφαλή μεταφορά μηνυμάτων διαχείρισης και λαθών
  - Σε κάθε εκτέλεση της πρώτης φάσης μπορεί να αντιστοιχούν πολλές εκτελέσεις της 2ης φάσης. Πολλά SAs μπορούν να διαπραγματευτούν σε κάθε εκτέλεση
  - Το αποτέλεσμα είναι γρήγορη και φθηνή εγκαθίδρυση SAs