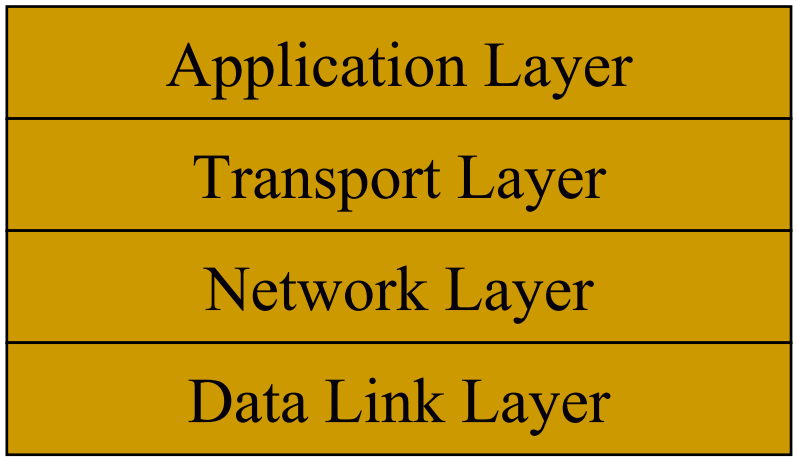
Ασφάλεια σε ένα Internet VPN

Γενικά

- Τα πρωτόκολλα TCP/IP δεν εμπεριέχουν μηχανισμούς κρυπτογράφησης, συνεπώς κάθε εφαρμογή πρέπει να περιέχει τους δικούς της μηχανισμούς κρυπτογράφησης.
- Κρυπτογραφικές τεχνικές μπορούν να υπάρξουν είτε στο επίπεδο εφαρμογών (π.χ. το πρωτόκολλο PGP (*Pretty Good Privacy)* για το e-mail ή τα SSL (*Secure Socket Layer*) και *Secure HTTP* για Web εφαρμογές) είτε στο επίπεδα ζεύξης δεδομένων ή δικτύου.
- Στα VPN η κρυπτογράφηση στο επίπεδο δικτύου είναι σημαντική.

Ασφάλεια: σε ποιο επίπεδο?



PGP, Kerberos, SSH, κ.ά.

Transport Layer Security (TLS)

IP Security

Hardware encryption

Κρυπτογραφικοί στόχοι

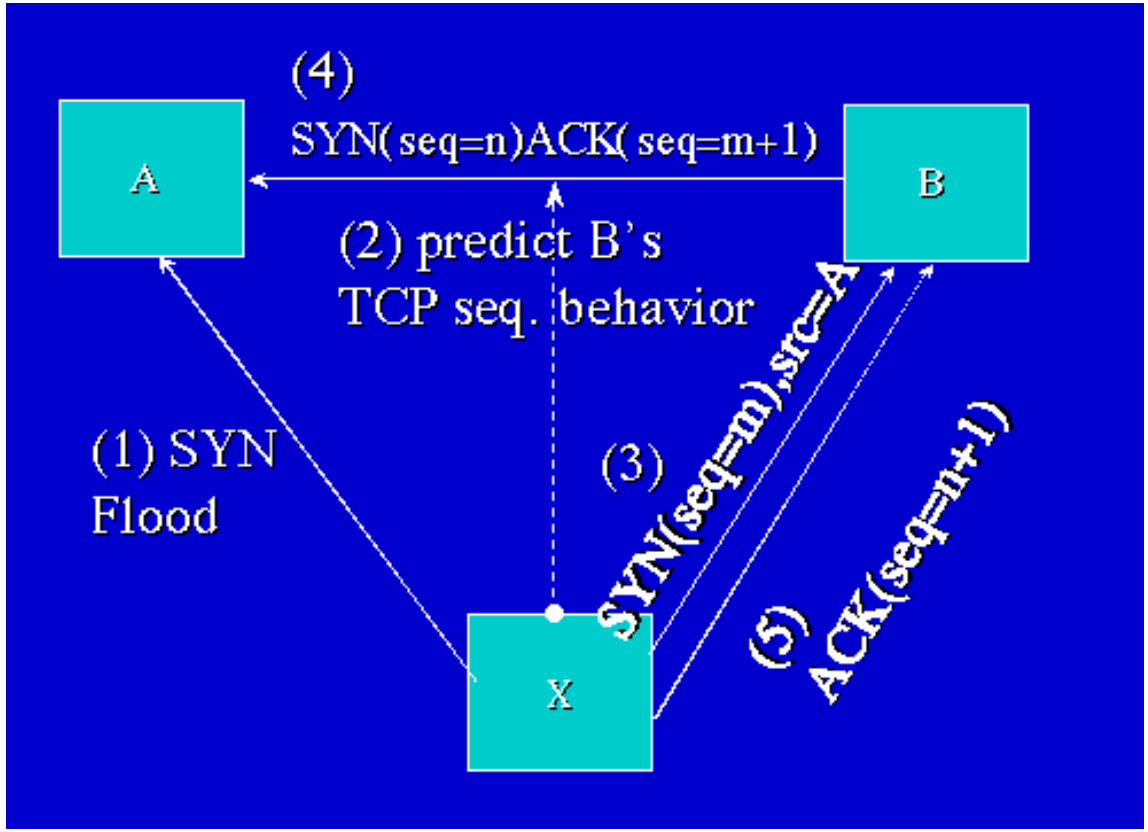
- Εμπιστευτικότητα
- Πιστοποίηση ταυτότητας αποστολέα
- Ακεραιότητα δεδομένων

- Επιθέσεις σε IP πρωτόκολλα
  - Spoofing
  - Session hijacking
  - Sniffing
  - Man-in-the-middle-attack

Spoofing (Εξαπάτηση)

- Κάθε IP πακέτο περιέχει τις διευθύνσεις τόσο του αποστολέα όσο και του παραλήπτη. Με το spoofing ένας «εχθρός» μπορεί να χρησιμοποιήσει τη διεύθυνση κάποιου και να προσποιηθεί ότι είναι αυτός.
- Μόλις ο επιτιθέμενος Χ ανιχνεύσει μία επικοινωνία μεταξύ Α και Β:
  - Στέλνει στον Β μήνυμα, αλλά βάζοντας τη διεύθυνση του Α ως διεύθυνση αποστολέα
  - Ο Β απαντά στον Α με κάποιους αριθμούς, αναμένοντας ο Α να αποκριθεί σε αυτούς
  - Ο Χ στέλνει συνέχεια αλλεπάλληλα πακέτα στον Α ώστε να τον εμποδίσει να απαντήσει στις αιτήσεις του Β. Ταυτόχρονα, αν καταφέρει και βρει τους αριθμούς πακέτων που στέλνει ο Α (αυτό στην πράξη είναι αρκετά εύκολο να γίνει) τότε απαντά αυτός στον Β κι έτσι αποκαθίσταται μία σύνδεση μεταξύ Χ και Β. Ο Β πιστεύει ότι επικοινωνεί με τον Α.

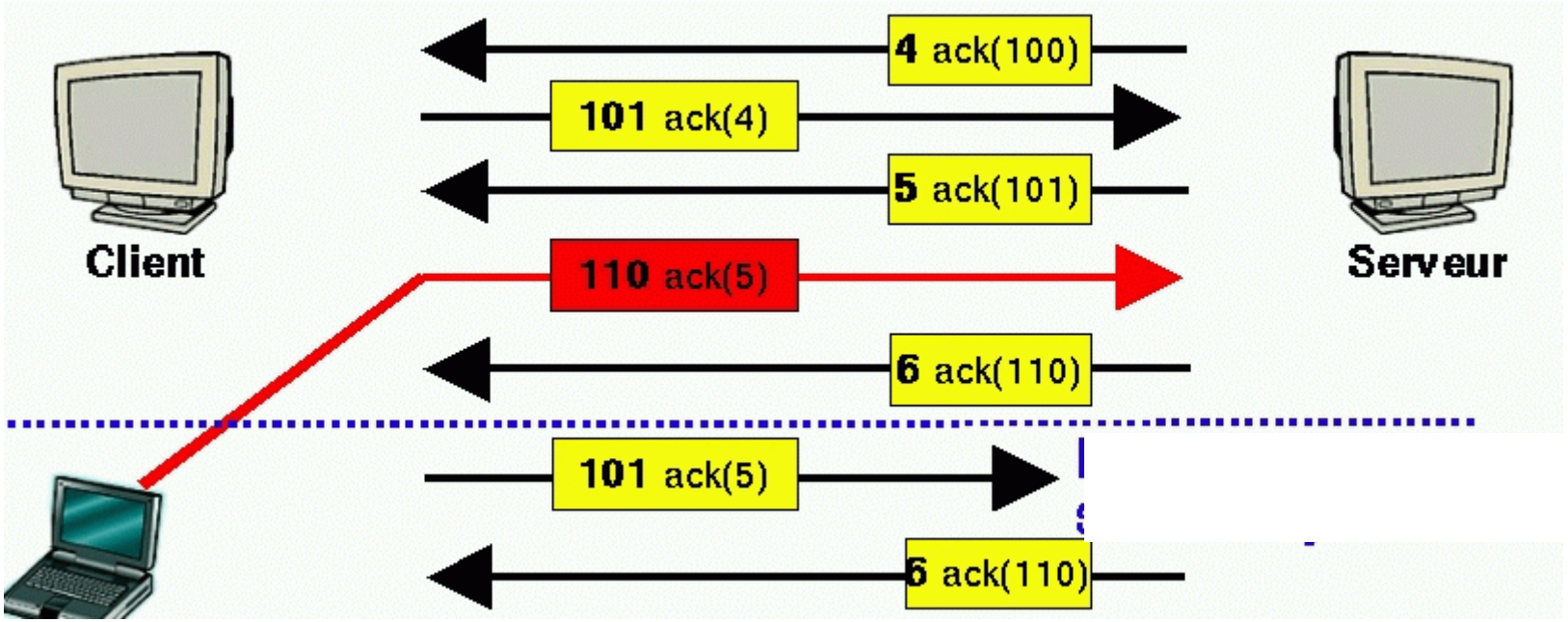
Spoofing (Σχηματική αναπαράσταση)



Session hijacking (Υποκλοπή συνδιάσκεψης)

- Ο επιτιθέμενος, αντί να επιχειρήσει από την αρχή τη δημιουργία σύνδεσης (όπως στο spoofing), προσπαθεί να αποκτήσει πρόσβαση σε μία υπάρχουσα.
- Αρχικά, παρακολουθεί μία συνδιάσκεψη προκειμένου να αναγνωρίσει την αρίθμηση στα πακέτα που ανταλλάσσονται.
- Στη συνέχεια στέλνει πακέτα στον Α προσποιούμενος ότι είναι ο Β, ενώ όπως και στο spoofing «φορτώνει» τον Α με πακέτα.

Session hijacking (σχηματική αναπαράσταση)

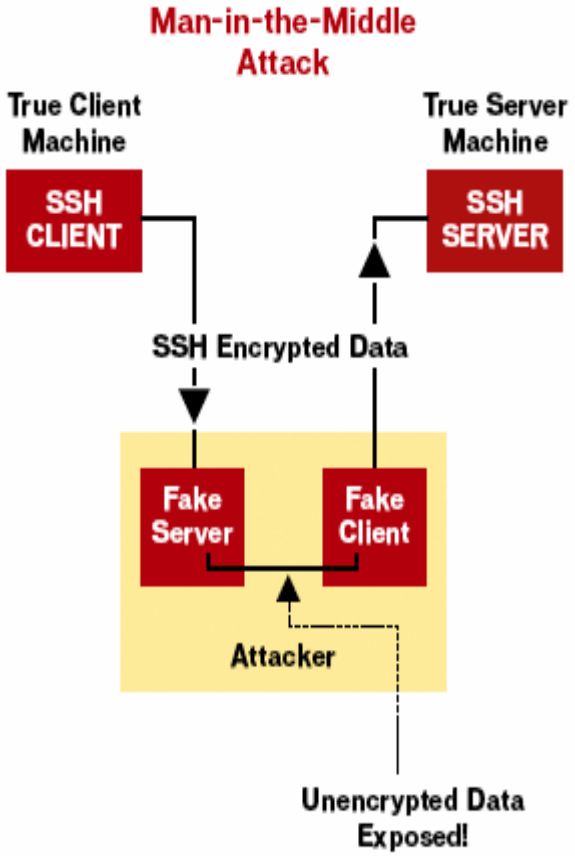


Sniffing

- Μπορούν να υπάρξουν συσκευές εφοδιασμένες με κατάλληλο software (sniffers) οι οποίες παρακολουθούν και καταγράφουν όλη την κίνηση του δικτύου. Αυτές δεν ανιχνεύονται εύκολα. Αν και είναι χρήσιμα εργαλεία για διαχειριστές, σε κακόβουλα χέρια γίνονται επικίνδυνες.
- Ελέγχοντας τις φυσικές συνδέσεις του δικτύου μπορούμε να αποκλείσουμε την ύπαρξη sniffer συσκευής.

Man-in-the-middle attack

- Σε μία επικοινωνία παρεμβάλλεται ένας τρίτος (για παράδειγμα, μπορεί να το κάνει αυτό αν ανακαλύψει το κλειδί κρυπτογράφησης, για το οποίο πρέπει να υπάρξει σωστός τρόπος ανταλλαγής του μεταξύ των συνδιαλεγομένων).



Σχήματα πιστοποίησης ταυτότητας

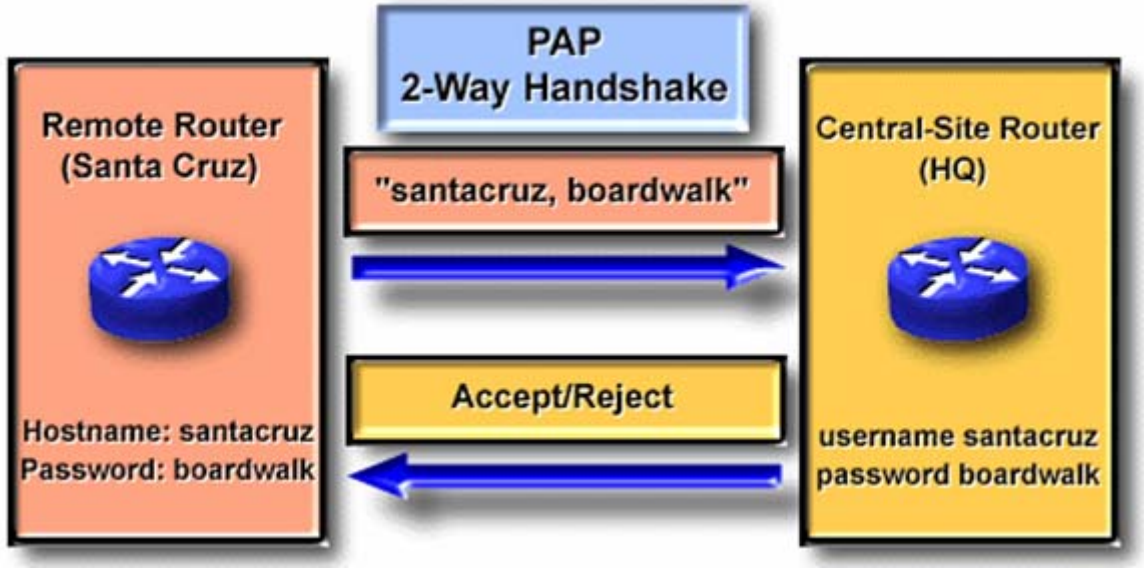
- Στα υπάρχοντα VPN η πιστοποίηση ταυτότητας γίνεται με κάποιον από τους ακόλουθους τρόπους
  - Παραδοσιακά password
  - One-time passwords
  - Συστήματα βασισμένα σε passwords (PAP, CHAP, TACACS (Cisco), RADIUS)
  - Συστήματα βασισμένα σε hardware (smart cards, PC cards)
  - Βιομετρικές τεχνικές (αναγνώριση φωνής, δακτυλικών αποτυπωμάτων κ.ο.κ.)

Passwords

- Παραδοσιακά Passwords: Πολύ ακατάλληλα. Σε πρωτόκολλα όπως telnet και ftp στέλνονται απευθείας μέσω του διαδικτύου – οποιοσδήποτε έχει πρόσβαση στο τι μεταδίδεται στο διαδίκτυο, τα διαβάζει.
- Passwords μίας χρήσης (one-time passwords): κάθε χρήστης έχει διαφορετικό password κάθε φορά που ξεκινά μια σύνδεση. Χαρακτηριστικό παράδειγμα το σύστημα S/Key. Κάθε χρήστης δίνει μία φράση, από την οποία το σύστημα γεννά διάφορα passwords, διαφορετικό κάθε φορά που ξεκινά νέα σύνδεση. Η φράση αυτή δεν «ταξιδεύει» στο Internet. Μειονέκτημά του ότι διαχειρίζεται δύσκολα δίκτυα με πολύ μεγάλο αριθμό χρηστών.

PAP (Password Authentication Protocol)

- Η σύνδεση αποκαθίσταται με δύο ενέργειες: ο αιτούμενος χρήστης δίνει το ID και το password, και ο καλούμενος εξετάζοντας μία βάση δεδομένων ελέγχει αν τα στοιχεία είναι σωστά. Αν ναι, στέλνει επιβεβαίωση και η σύνδεση αποκαθίσταται. Χρησιμοποιείται στο πρωτόκολλο PPP (Point-to-Point πρωτόκολλο).



Μειονεκτήματα του PAP

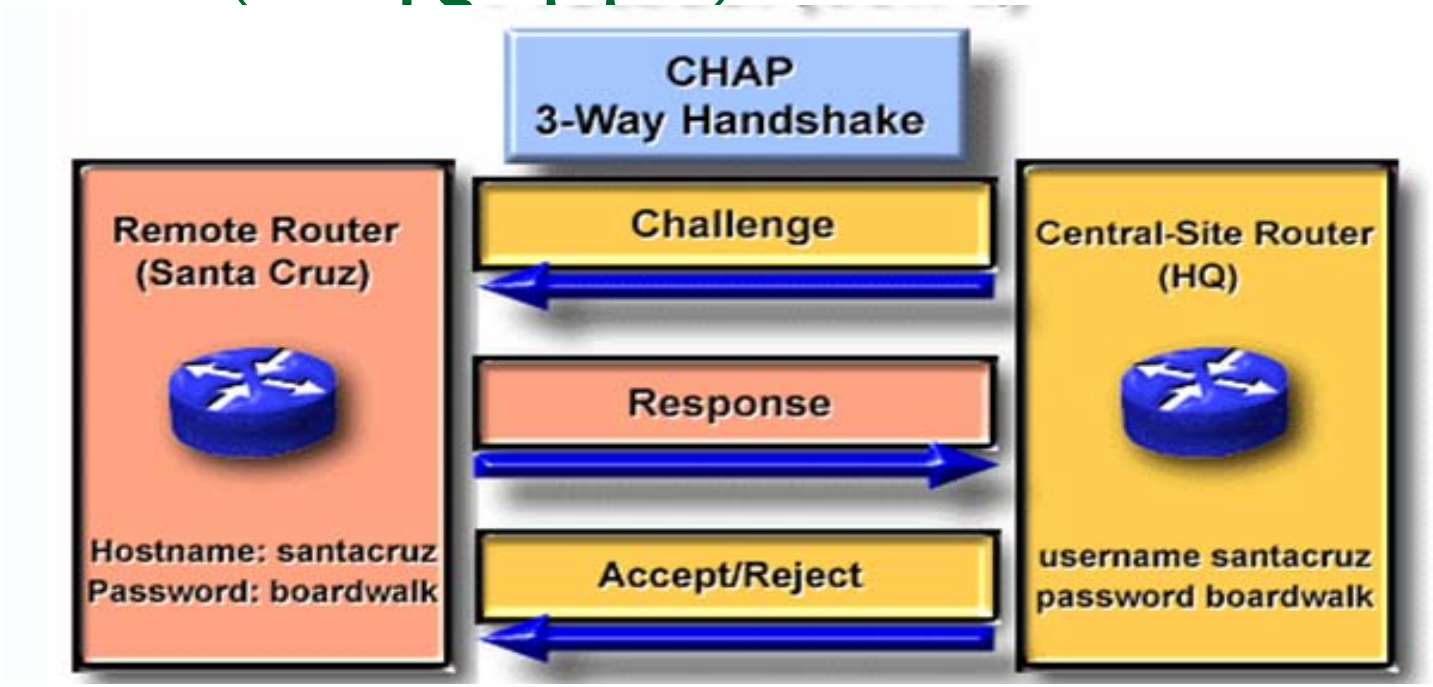
- Τα passwords μεταδίδονται «ελεύθερα» στο διαδίκτυο
- Κάποιος μπορεί να επιχειρεί δοκιμάζοντας με τυχαία passwords να επιτύχει πρόσβαση, μέχρις ότου το μαντέψει το password.
- Εναλλακτική επιλογή: CHAP

CHAP (Challenge Handshake Authentication Protocol)

Το CHAP χρησιμοποιείται:

- Για την έναρξη μίας επικοινωνίας
- Περιοδικά, κατά την διάρκεια που πραγματοποιείται η επικοινωνία, για επιβεβαίωση της ταυτότητας του συνδιαλεγομένου.
- Λειτουργία
  - Ο εξυπηρετητής στέλνει ένα μήνυμα-πρόκληση (challenge message).
  - Ο χρήστης απαντά με μία τιμή την οποία υπολογίζει, η οποία εξαρτάται από το password
  - Ο εξυπηρετητής έχει κάνει τον ίδιο υπολογισμό και αν οι δύο τιμές (η δική του και του χρήστη) ταυτίζονται, επιτρέπει πρόσβαση. Διαφορετικά, η σύνδεση τερματίζεται.

CHAP (διάγραμμα)

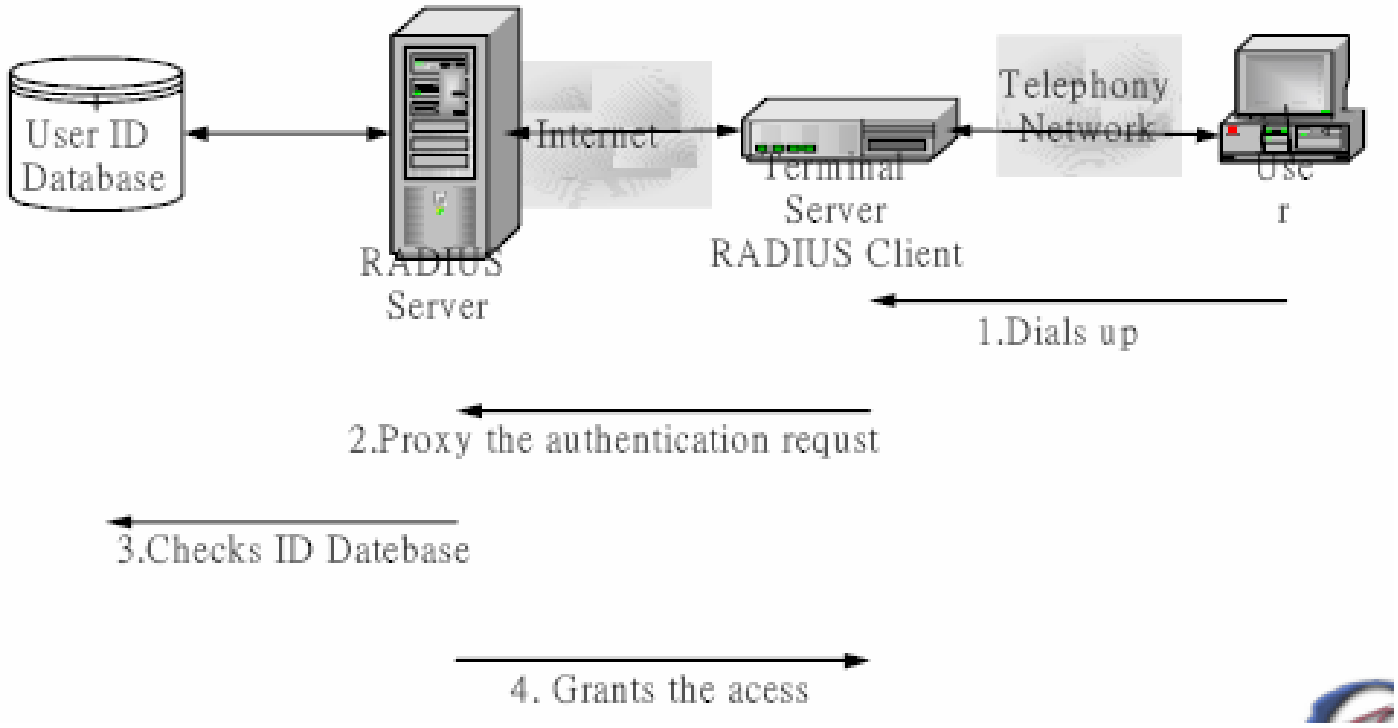


•Η ερώτηση-πρόκληση πρέπει να είναι τέτοια ώστε, κάποιος που βλέπει την ερώτηση και την απάντηση, να μην μπορεί να αποκτήσει καμία πληροφορία για το password!!!

•Μειονέκτημα: δύσκολα διαχειρίσιμο σε δίκτυα με πολύ μεγάλο αριθμό χρηστών

RADIUS (Remote Authentication Dial-In User Service)

- Μοντέλο πελάτη/εξυπηρετητή.

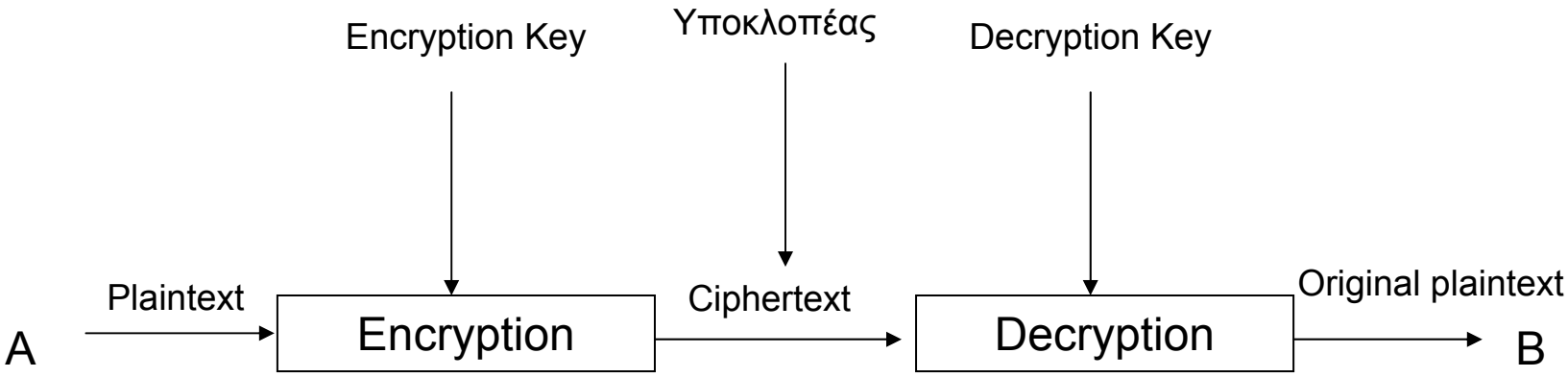


RADIUS (τρόπος λειτουργίας)

- Ο RADIUS client είναι στην ουσία ένας NAS (Network Access Server), ο οποίος δέχεται την αίτηση για επικοινωνία και προωθεί την αίτηση (password κτλ) στον server. Ο server ρωτά μία βάση δεδομένων και αντίστοιχα δέχεται ή απορρίπτει την αίτηση.
- Η επικοινωνία client-server γίνεται κρυπτογραφημένα.

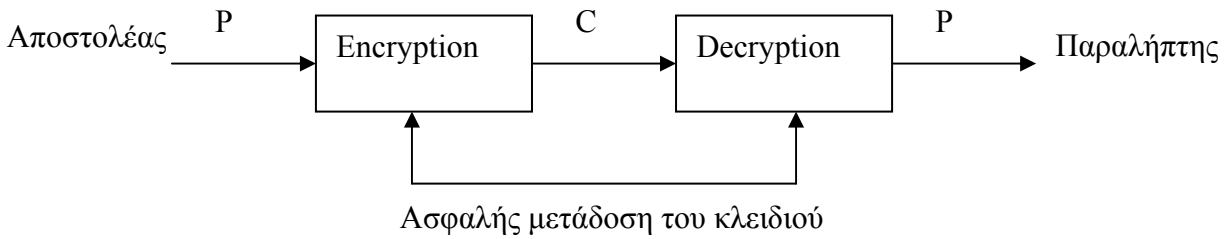
Αρχές Κρυπτογραφίας

- Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδιά (keys).



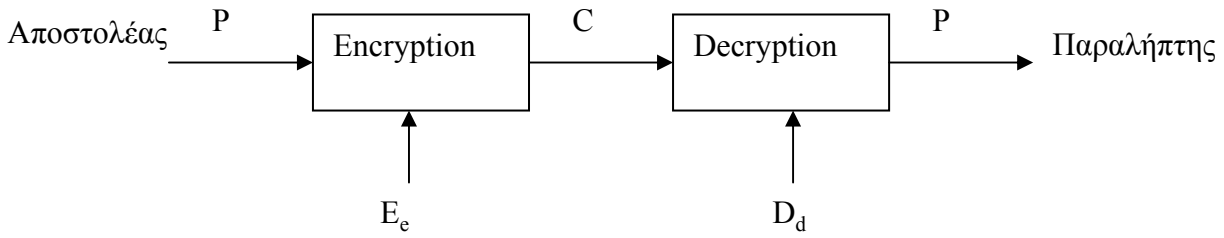
Όταν το κλειδί κρυπτογράφησης είναι ίδιο με το κλειδί αποκρυπτογράφησης, τότε το σύστημα λέγεται συμμετρικού κλειδιού. Διαφορετικά λέγεται ασύμμετρου ή δημοσίου κλειδιού.

Συμμετρικά κρυπτοσυστήματα



- Ο αποστολέας και ο παραλήπτης πρέπει από την αρχή να συμφωνήσουν στη χρήση ενός κοινού κλειδιού, το οποίο μόνο αυτοί γνωρίζουν.
- Ένα «ασφαλές κανάλι επικοινωνίας» πρέπει να υπάρχει για την επικοινωνία τους προκειμένου να ενημερώσει ο ένας τον άλλον για τον κλειδί.

Κρυπτοσυστήματα Δημοσίου κλειδιού

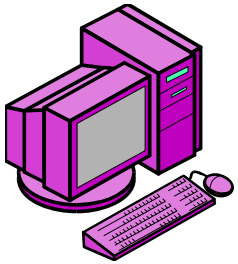


- Προτάθηκαν το 1976
- Κάθε συμμετέχων στο σύστημα κατέχει ένα ζευγάρι κλειδιών e και d, που το ένα αντιστρέφει το άλλο: Dd(Ee(m))=m
- Ένα από τα δύο κλειδιά μπορεί να είναι γνωστό, με την προϋπόθεση ότι η γνώση αυτή δεν οδηγεί σε προσδιορισμό του άλλου κλειδιού. Το e μπορεί να είναι δημόσιο (γνωστό), αλλά το d κρατείται μυστικό.
- Η ανταλλαγή κλειδιών μεταξύ αποστολέα και παραλήπτη αντικαθίσταται από την ύπαρξη ενός διαφανούς καταλόγου, στον οποίο όλοι έχουν πρόσβαση, και περιέχει τα κλειδιά e όλων των συμμετοχόντων.

Τρόπος λειτουργίας συστημάτων δημοσίου κλειδιού

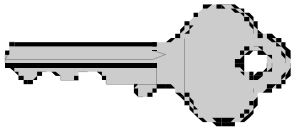
- Όταν ένα πρόσωπο A θέλει να στείλει ένα μήνυμα m σε ένα πρόσωπο B, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη B χρησιμοποιείται για τη δημιουργία του κρυπτογράμματος $E_e(m)$. Αφού το E_e είναι πλήρως διαθέσιμο σε κάποιον δημόσιο κατάλογο στον οποίο έχουν όλοι πρόσβαση, ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα με προορισμό τον B. Ωστόσο, μόνο ο B, ο οποίος έχει πρόσβαση στο ιδιωτικό του κλειδί αποκρυπτογράφησης D_d μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό $D_d(E_e(m))$.
- Στο IPSec: συμμετρική κρυπτογράφηση, όπου όμως η ανταλλαγή κλειδιού γίνεται με κρυπτογραφία δημοσίου κλειδιού.

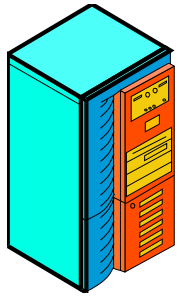
Διανομή κλειδιού με χρήση αλγορίθμου Δημοσίου κλειδιού



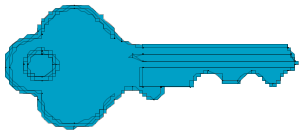
Αποστολέας Α

1. Δημιουργία συμμετρικού κλεδιού



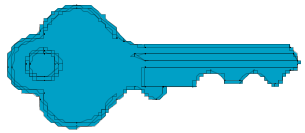


Παραλήπτης Β

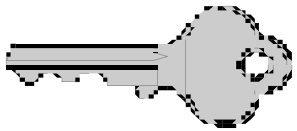


2. Κρυπτογράφηση Του κλειδιού με το Δημόσιο Κλειδί του Β

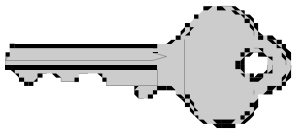
3. Αποστολή του συμμετρικού κλειδιού (κρυπτογραφημένου)



4. Αποκρυπτογράφηση του συμμετρικού κλειδιού, με χρήση του Ιδιωτικού κλειδιού του Β

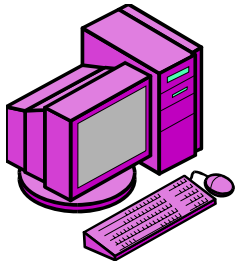


5. Χρήση του συμμετρικού κλειδιού για κρυπτογράφηση του μηνύματος

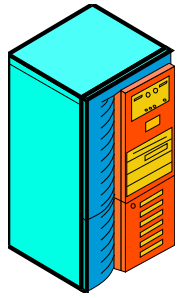


Παράδειγμα – Diffie-Hellman μέθοδος

1. Συμφωνία για το Diffie-Hellman ζευγάρι p (πρώτος αριθμός) και g (γεννήτορας mod p)



A

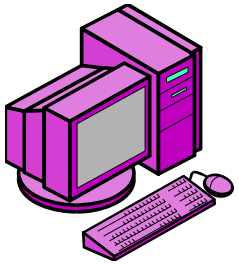


B

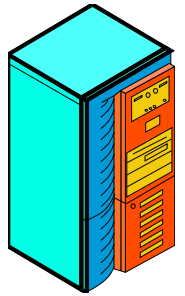
2. Δημιουργία τυχαίου αριθμού x

2. Δημιουργία τυχαίου αριθμού y

Diffie-Hellman μέθοδος (II)



A



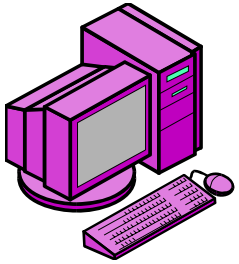
B

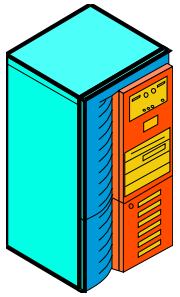
3.
Υπολογισμός
$x' = g^x \bmod p$

4.
Ανταλλαγή x', y'
χωρίς ασφάλεια

3.
Υπολογισμός
$y' = g^y \bmod p$

Diffie-Hellman μέθοδος (III)





A

5.
Υπολογισμός κλειδιού=
$y'^{x} \bmod p$
$=g\hat{}^{xy} \bmod p$

B

5.
Υπολογισμός κλειδιού=
$x'^{y} \bmod p$
$=g^{xy} \bmod p$

6. Κρυπτογράφηση με το παραπάνω συμμετρικό κλειδί που υπολογίστηκε