ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

Ενότητα #11: Ασφάλεια δικτύων

Καθηγητής Χρήστος Ι. Μπούρας

Τμήμα Μηχανικών Η/Υ & Πληροφορικής, Πανεπιστήμιο Πατρών

email: bouras@cti.gr, site: http://ru6.cti.gr/ru6/bouras

Σκοποί ενότητας

- Εξοικείωση με τα θέματα ασφάλειας δικτύων

Περιεχόμενα ενότητας

- Εισαγωγή
- Κρυπτογράφηση
- Secure Sockets Layer (SSL)
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Ασφάλεια σε επίπεδο δικτύου
- Τείχος προστασίας

Ασφάλεια δικτύων

Γενικά

- Αρχικά, τα δίκτυα υπολογιστών χρησιμοποιούνταν κυρίως από πανεπιστημιακούς ερευνητές, χωρίς κινδύνους για την ασφάλεια
- Σήμερα, χρησιμοποιούνται για τραπεζικές συναλλαγές, αγορές, υποβολή φορολογικών δηλώσεων και άλλου είδους προσωπικών στοιχείων
- Τα περισσότερα προβλήματα προκαλούνται σκόπιμα από κακόβουλα άτομα προκειμένου να ωφεληθούν, να προσελκύσουν την προσοχή, ή να βλάψουν κάποιον
- Διάφορες σημαντικές επιπτώσεις, που προκύπτουν είναι ο χαμένος χρόνος και κόπος για ανάνηψη, η απώλεια χρημάτων / αξιοπιστίας, νομικά προβλήματα κ.α.

Ασφάλεια

- Ορισμός: Με τον όρο ασφάλεια πληροφοριακών συστημάτων/δικτύων περιγράφεται το οργανωμένο πλαίσιο των αρχών, των πολιτικών και των διαδικασιών, καθώς και των σύγχρονων τεχνικών και μέτρων, που απαιτούνται για την προστασία των στοιχείων, που συνιστούν το πληροφοριακό σύστημα/δίκτυο, από κάθε είδους ενέργεια σκόπιμη ή τυχαία, που θεωρείται απειλή για το σύστημα, χωρίς να παρεμποδίζεται η απρόσκοπτη λειτουργία του και η ελεύθερη διακίνηση της πληροφορίας
- Βασικές αρχές της ασφάλειας είναι:
  - Εμπιστευτικότητα
  - Ακεραιότητα Δεδομένων
  - Διαθεσιμότητα

Είδη Επιθέσεων

- Εισβολή σε ένα δίκτυο (Intrusion)
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS)
- Υποκλοπή ευαίσθητων πληροφοριών

Intrusion

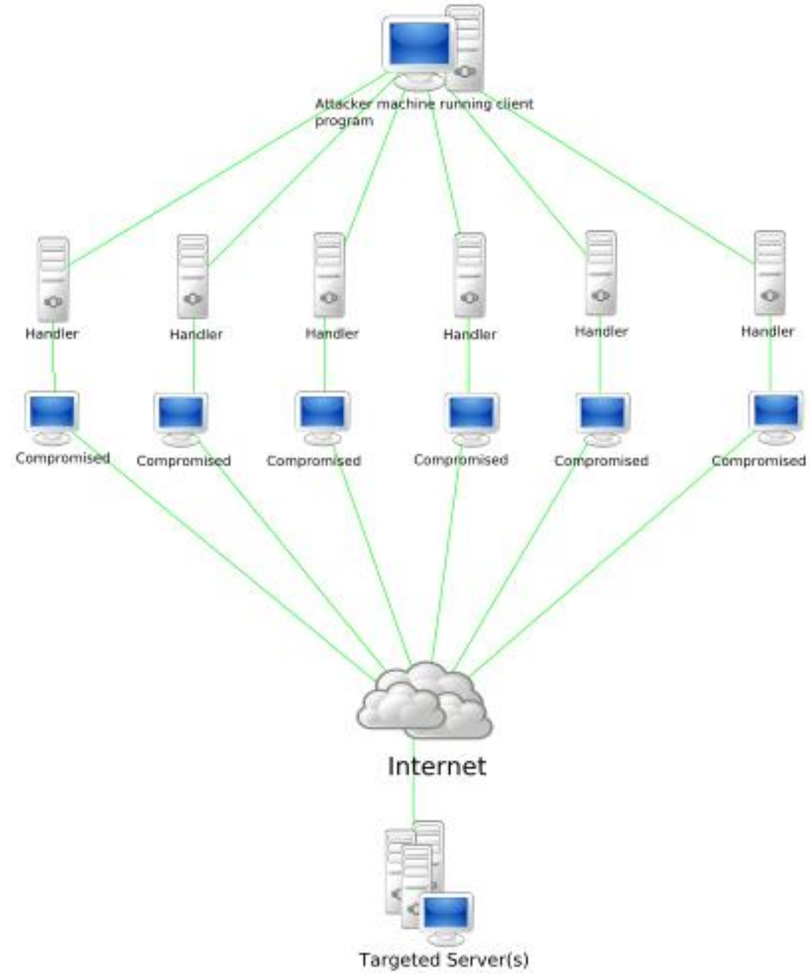
- Η εισβολή σε ένα δίκτυο (intrusion) είναι ο συνηθέστερος τρόπος επίθεσης
- Η εισβολή σε συστήματα έχει στόχο οι επιτιθέμενοι να αποκτήσουν τα δικαιώματα των νόμιμων χρηστών
- Για προστασία από τέτοιες επιθέσεις μπορεί να χρησιμοποιηθούν:
  - Τείχη Προστασίας (Firewalls)
  - Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems (IDS)
  - Συστήματα Ανίχνευσης και Πρόληψης Εισβολής (Intrusion Detection and Prevention Systems (IDPS))

Επιθέσεις άρνησης εξυπηρέτησης (Denial-of-service attack)

- Denial-of-service attacks (DoS) ονομάζονται οι επιθέσεις εναντίον υπολογιστών / υπηρεσιών, που έχουν σκοπό να τους καταστήσουν ανίκανους να δεχτούν άλλες συνδέσεις και να μην μπορούν να εξυπηρετήσουν άλλους πελάτες
- Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης:
  - Επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί
  - Επίθεση μέσω αποστολής υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει πραγματικές αιτήσεις
- Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (Distributed Denial-of-Service attacks - DDoS) χρησιμοποιούν πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και θυτών

Παράδειγμα DDoS επίθεσης

Παράδειγμα DDoS επίθεσης



http://commons.wikimedia.org/wiki/File:Stachledraht_DDos_Attack.svg

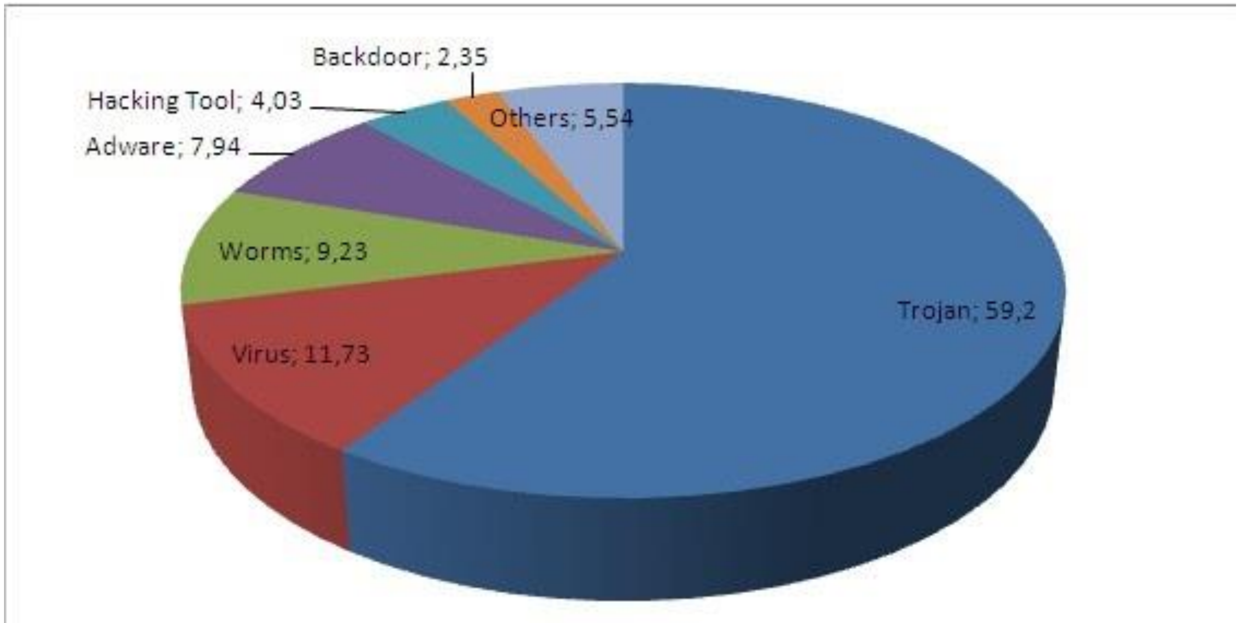
Υποκλοπή ευαίσθητων πληροφοριών

- Υπάρχουν επιθέσεις κατά τις οποίες ένας επιτιθέμενος αποκτά πρόσβαση σε ευαίσθητες πληροφορίες εξ΄ αποστάσεως, χωρίς την άμεση επαφή με το μηχάνημα
- Συνήθως, οι επιθέσεις αυτού του είδους εκμεταλλεύονται δικτυακές υπηρεσίες σχεδιασμένες για χρήση σε ασφαλή τοπικά δίκτυα και όχι στο Internet
- Ένα κατάλληλα ρυθμισμένο firewall συνήθως είναι ικανό να αποτρέψει τέτοιες επιθέσεις

Τεχνικές Επιθέσεων

- Επίθεση σε ιστοσελίδες
- Επίθεση στην υπηρεσία ονοματολογίας (Domain Name Servers -DNS)
- Επίθεση με Δούρειους Ίππους (Trojan Horses), “σκουλήκια” (worms), ιούς (viruses), ανιχνευτές (spies)
- Επίθεση στο ηλεκτρονικό ταχυδρομείο και στο πρωτόκολλό του (Simple Mail Transfer Protocol- SMTP)
- Επίθεση από υποκλοπή κωδικών πρόσβασης
- Sniffing
- Πλαστογράφηση(Spoofing) κ.α.

Αναλογία εμφάνισης επιθέσεων



source: http://press.pandasecurity.com/news/in-january-50-percent-of-computers-worldwide-were-infected-with-some-type-of-computer-threat/

Είδη επιθέσεων σε υπολογιστές και αναλογία εμφάνισής τους

Κρυπτογραφία

- Η κρυπτογραφία είναι η κυριότερη τεχνολογία ασφαλείας
- Ο όρος 'κρυπτογραφία' αναφέρεται σε ένα σύνολο τεχνικών, που χρησιμοποιούνται για να διασφαλίσουν ότι τα δεδομένα δε μπορούν να διαβαστούν από κάποιον που δεν είναι ο αποστολέας ή κανονικός παραλήπτης τους
- Το σύνολο δεδομένων μετατρέπεται από μία κατανοητή μορφή σε έναν «γρίφο»

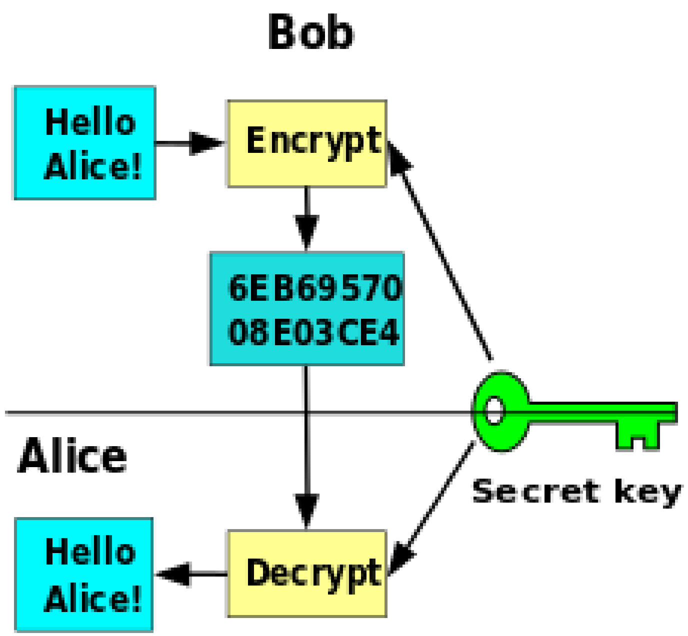
Πρώτες μέθοδοι κρυπτογράφησης

- Οι πρώτες μέθοδοι που χρησιμοποιούνταν ήταν:
  - Η αντικατάσταση
  - Ο μετασχηματισμός
- Στην πρώτη αντικαθίστανται διακριτά τμήματα του αρχικού κειμένου με άλλα, (π.χ. αλλάζοντας κάθε δυάδα γραμμάτων με κάποια άλλα) βάσει ενός κώδικα
- Στη δεύτερη, γίνονται σύνθετοι μετασχηματισμοί μεταξύ πολλών κομματιών του αρχικού κειμένου
- Παράδειγμα αντικατάστασης: η συσκευή Enigma, που χρησιμοποιήθηκε από τους Γερμανούς κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου

Μοντέρνα κρυπτογραφία

- Βασίζεται σε εξαιρετικά πολύπλοκους αλγορίθμους για τη μετατροπή ενός κειμένου σε κρυπτογραφημένο, διαδικασία γνωστή ως κρυπτογράφηση
- Οι αλγόριθμοι αλλάζουν τη λειτουργία τους βάσει ενός κλειδιού (ένα σύνολο χαρακτήρων, που αλλάζουν τον τρόπο της μετατροπής του κειμένου)
  - Απλό παράδειγμα: Η αντικατάσταση κάθε χαρακτήρα με τον ASCII χαρακτήρα, που βρίσκεται n θέσεις μπροστά στον πίνακα των ASCII, με το κλειδί να είναι το n.
- Αποκρυπτογράφηση: Ο παραλήπτης χρησιμοποιεί τον αλγόριθμο και το κλειδί για να ανακτήσει το αρχικό μήνυμα

Κρυπτογράφηση και αποκρυπτογράφηση



Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

(πηγή: https://en.wikipedia.org/wiki/Cryptography#/media/File:Symmetric_key_encryption.svg)

Κρυπτογραφία συμμετρικού κλειδιού

- Ο αποστολέας ενός μηνύματος κρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν αλγόριθμο, που βασίζεται σε κλειδί
- Το κρυπτογραφημένο μήνυμα στέλνεται μέσω του (ανασφαλούς) δικτύου
- Το κλειδί μεταφέρεται με κάποιον ασφαλή τρόπο στον παραλήπτη
- Ο παραλήπτης λαμβάνει το κλειδί και αποκρυπτογραφεί το μήνυμα
- Πλεονέκτημα: πολύ αποδοτική όσον αφορά τους πόρους
- Μειονέκτημα: το κλειδί πρέπει να μεταφερθεί μέσω ενός ασφαλούς μέσου

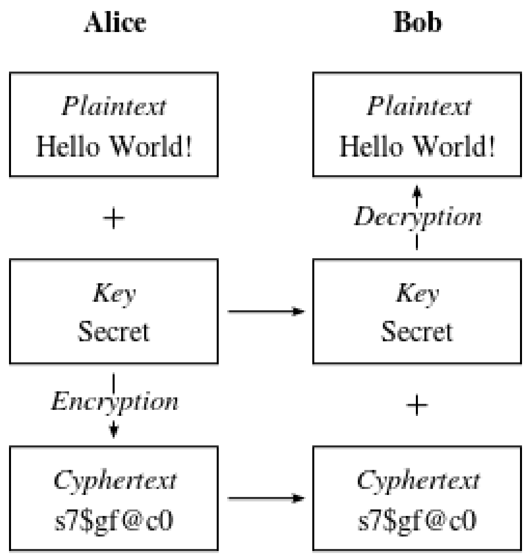
Αλγόριθμοι συμμετρικού κλειδιού

- Γνωστοί αλγόριθμοι συμμετρικού κλειδιού, που ακόμη χρησιμοποιούνται:
  - Data Encryption Standard (DES)
  - Τριπλός DES αλγόριθμος
  - Blowfish και ο διάδοχός του Twofish
  - International Data Encryption Algorithm (IDEA)
  - Rivest Cipher 4 (RC4)

Τρόποι επίθεσης σε αλγορίθμους συμμετρικού κλειδιού

- Δοκιμή όλων των δυνατών κλειδιών
- Επίθεση γνωστού κειμένου
- Επίθεση επιλεγμένου κειμένου
- Διαφορική επίθεση κρυπτανάλυσης
- Διαφορική επίθεση λαθών

Κρυπτογραφία συμμετρικού κλειδιού



http://en.wikipedia.org/wiki/Cryptography#mediaviewer/File:Symmetric-key_cryptography.svg

Κρυπτογραφία συμμετρικού κλειδιού, όπου το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση

Κρυπτογραφία δημοσίου κλειδιού (1/2)

- Χρησιμοποιεί δυο κλειδιά: ένα δημόσιο και ένα ιδιωτικό
- Το δημόσιο διανέμεται και μπορεί να το έχει στην κατοχή του οποιοσδήποτε σε αντίθεση με το ιδιωτικό
- Τα κλειδιά δημιουργούνται σε ζεύγη και με μέθοδο που καθιστά ανέφικτο να βρεθεί το ένα κλειδί από το άλλο
- Κείμενο, που κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί μόνο από το άλλο κλειδί του ζεύγους και αντίστροφα
- Προτάθηκε ώστε να μην υπάρχει η ανάγκη μετάδοσης του κλειδιού, όπως συμβαίνει στην κρυπτογραφία συμμετρικού κλειδιού

Κρυπτογραφία δημοσίου κλειδιού (2/2)

- Ο παραλήπτης ενός μηνύματος χρησιμοποιεί τα κλειδιά με τον ακόλουθο τρόπο:
  - Δημοσιοποιεί το δημόσιο κλειδί του (π.χ. σε ένα site)
  - Ο επίδοξος αποστολέας χρησιμοποιεί το δημόσιο κλειδί για να κάνει την κρυπτογράφηση
  - Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται από τον παραλήπτη χρησιμοποιώντας το ιδιωτικό κλειδί
- Δεν χρειάζεται ο παραλήπτης να δημοσιοποιήσει το κλειδί

Τεχνολογίες της κρυπτογραφίας δημοσίου κλειδιού (1/2)

- Οι έξυπνες κάρτες αποτελούν έναν από τους πιο ασφαλείς τρόπους για να διασφαλιστεί η προστασία ενός ιδιωτικού κλειδιού
  - Έχουν μέγεθος πιστωτικής κάρτας και περιέχουν και το ιδιωτικό και το δημόσιο κλειδί
  - Πρέπει να συνδεθούν στον υπολογιστή προκειμένου να εκτελεστεί η κρυπτογράφηση
  - Όποιος θέλει να αποκτήσει το ιδιωτικό κλειδί πρέπει να κλέψει την κάρτα
- Ανταλλαγή κλειδιού Diffie-Hellman. Τεχνική για την ανταλλαγή ενός συμμετρικού κλειδιού χρησιμοποιώντας δημόσιο κλειδί

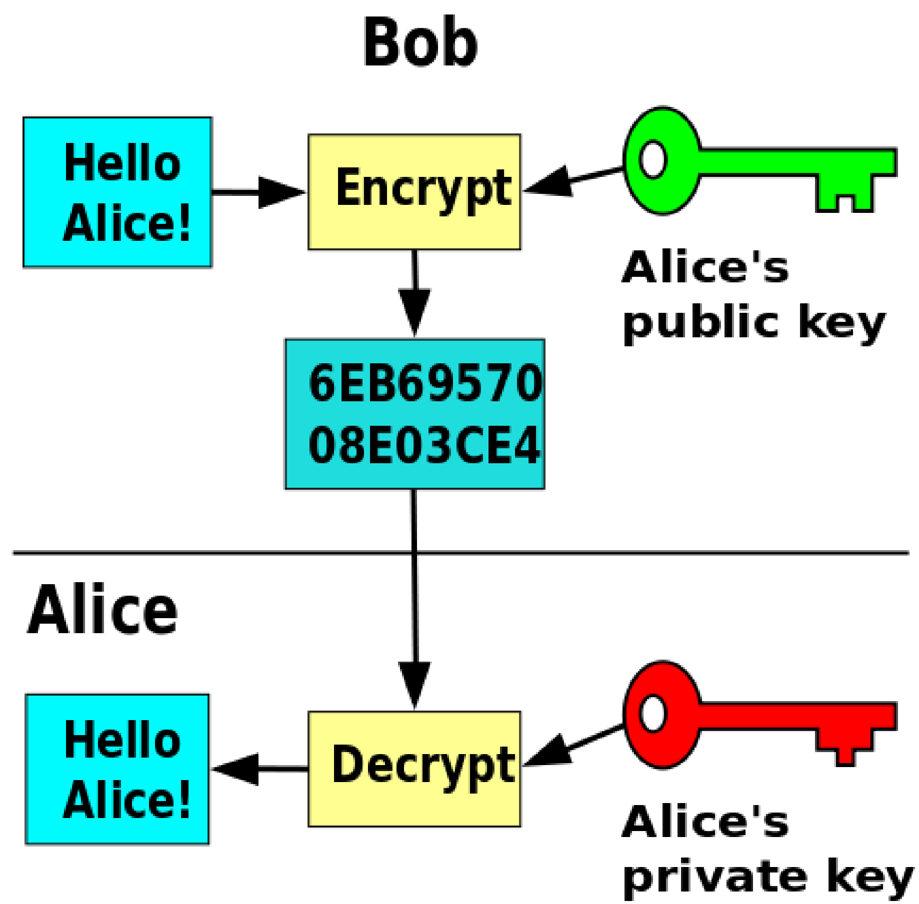
Τεχνολογίες της κρυπτογραφίας δημοσίου κλειδιού (2/2)

- Rivest-Shamir-Adleman (RSA): Είναι το πιο γνωστό σύστημα κρυπτογράφησης δημοσίου κλειδιού
  – Χρησιμοποιείται για την αποστολή μέσω μη ασφαλούς γραμμής και για τη δημιουργία ψηφιακών υπογραφών (σειρές χαρακτήρων, που πιστοποιούν την ταυτότητα του αποστολέα)
- El Gamel system: Σύστημα δημοσίου κλειδιού, που βασίζεται στην τεχνική Diffie-Hellman
- Digital Signature Standard (DSS). Μπορεί να χρησιμοποιηθεί για ψηφιακές υπογραφές, και αν τροποποιηθεί, για κανονική μεταφορά δεδομένων

Παράδειγμα κρυπτογραφίας δημοσίου κλειδιού

Κρυπτογραφία (ασύμμετρου) δημόσιου κλειδιού:

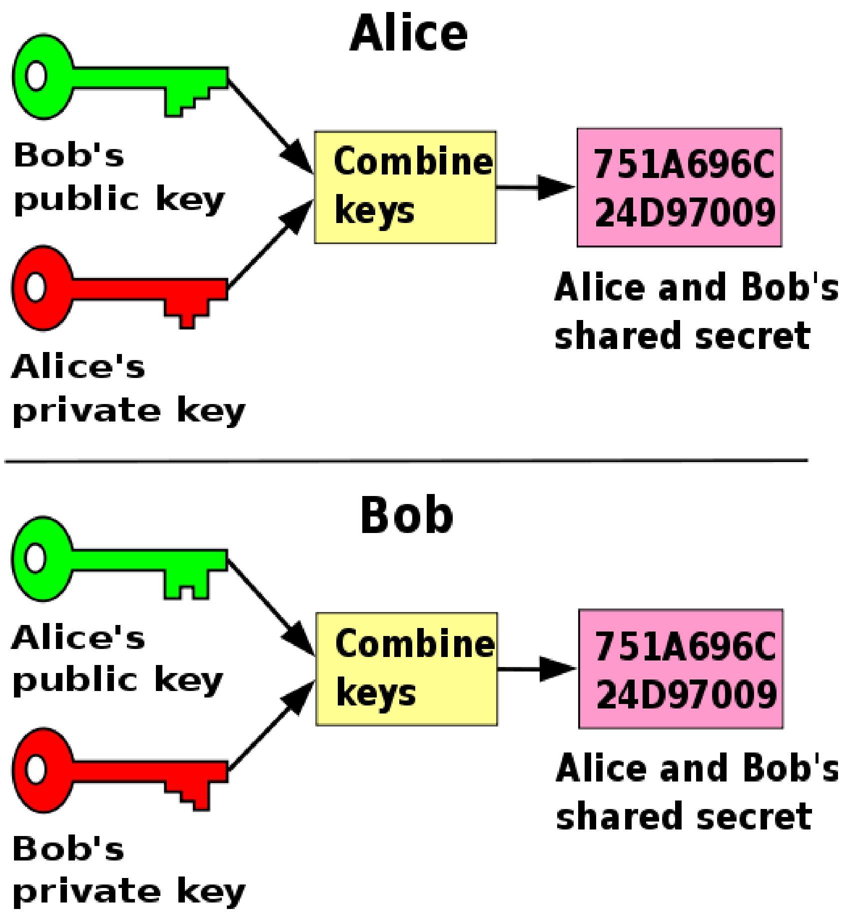
Ο οποιοσδήποτε μπορεί να κρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί, αλλά μόνο ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει (πηγή: http://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg)



Ανταλλαγή κλειδιού Diffie-Hellman

Ανταλλαγή κλειδιού Diffie-Hellman.

Κάθε πλευρά δημιουργεί ένα ζεύγος δημόσιου / ιδιωτικού κλειδιού και διανέμει το δημόσιο κλειδί. Μετά την απόκτηση ενός αυθεντικού αντιγράφου του δημόσιου κλειδιού της άλλης πλευράς, οι δύο πλευρές μπορούν να υπολογίσουν ένα κοινό μυστικό offline (shared secret)
(πηγή:http://commons.wikimedia.org/wiki/File:Public_key_encryption.svg)



Επιθέσεις σε συστήματα δημοσίου κλειδιού

- Δυο είδη επιθέσεων υπάρχουν σε συστήματα δημοσίου κλειδιού:
  - Η πρώτη είναι επίθεση με δεδομένα (factoring attack) και βασίζεται στην ανάλυση
  - Η δεύτερη είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται

Secure Sockets Layer (SSL)

- Το Secure Sockets Layer (SSL) είναι μια από τις πιο δημοφιλείς τεχνολογίες - ίσως η πιο δημοφιλής, που βασίζεται στην κρυπτογραφία
- Αναπτύχθηκε αρχικά από τη Netscape Corporation για τον φυλλομετρητή Netscape Navigator
- Λειτουργεί σαν ένα επίπεδο, που υπάρχει ανάμεσα σε πρωτόκολλα, όπως το HTTP και το FTP και υποκείμενα πρωτόκολλα, που υπάρχουν στο TCP/IP

Λειτουργίες που έχουν ενσωματωθεί στο SSL

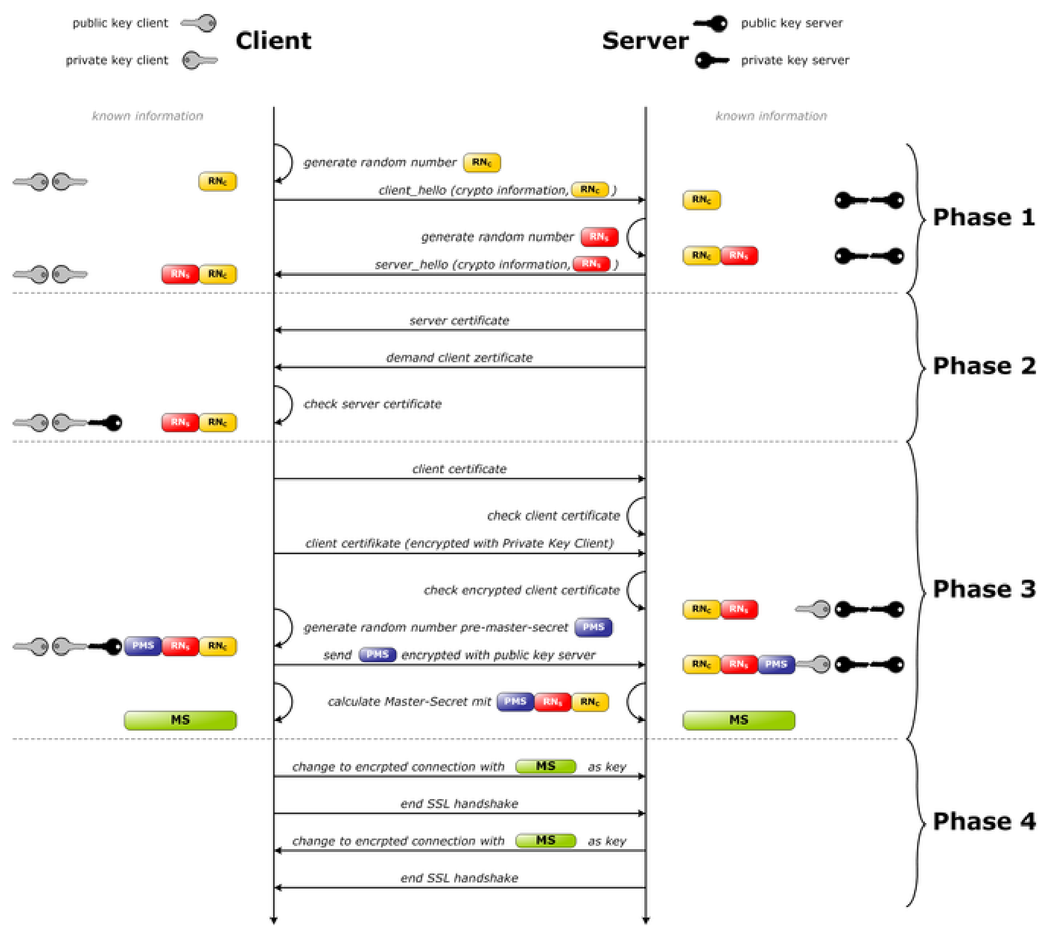
- Αυθεντικοποίηση διακομιστή SSL. Επιτρέπει σε ένα πελάτη να πιστοποιήσει την ταυτότητα ενός διακομιστή
  - Με κρυπτογραφία δημοσίου κλειδιού πιστοποιεί την ψηφιακή υπογραφή ενός διακομιστή και βεβαιώνει ότι αυτό εκδόθηκε από έγκυρη αρχή πιστοποίησης
- Αυθεντικοποίηση πελάτη SSL. Με παρόμοιο τρόπο με τον οποίο πιστοποιούνται οι διακομιστές, πιστοποιούνται και οι πελάτες
- Κρυπτογραφία SSL. Το SSL χρησιμοποιεί μια ποικιλία τεχνικών συμμετρικής κρυπτογραφίας για να την αποστολή και λήψη δεδομένων

Υποπρωτόκολλα του SSL

- Πρωτόκολλο Εγγραφής SSL (Record protocol): Χρησιμοποιείται για τη μετάδοση μεγάλων όγκων δεδομένων
- Πρωτόκολλο Χειραψίας SSL (Handshake): Χρησιμοποιείται για να εγκαταστήσει τους κωδικούς και τους αλγορίθμους που θα χρησιμοποιηθούν για τη μεταφορά δεδομένων

Σχηματική αναπαράσταση χειραψίας

Σχηματική αναπαράσταση χειραψίας SSL με αμφίδρομη πιστοποίηση



http://commons.wikimedia.org/wiki/File:Ssl_handshake_with_two_way_authentication_with_certificates.png

Τεχνολογίες που περιλαμβάνονται στο SSL

- Το πρωτόκολλο SSL υποστηρίζει αρκετούς κώδικες και κρυπτογραφικούς αλγόριθμους
- Εξαρτώνται από την έκδοση του SSL, την πολιτική ασφαλείας των δυο πλευρών και τους περιορισμούς που θέτει η αμερικάνικη κυβέρνηση
- Στις τεχνολογίες περιλαμβάνονται οι αλγόριθμοι:
  - DES
  - DSA
  - Key Extraction Algorithm (KEA)
  - RSA
  - Και πολλοί άλλοι, όπως οι: MD5, SHA-1, SKIPJACK, Triple DES

Η διαδικασία μεταφοράς (1/3)

- Η διαδικασία μεταφοράς δεδομένων ανάμεσα σε ένα πελάτη, (π.χ. browser), και ένα διακομιστή με τη χρήση SSL περιλαμβάνει τα εξής βήματα:
  – Το πρώτο βήμα περιλαμβάνει τη χρήση του πρωτοκόλλου χειραψίας SSL
  – Ο πελάτης στέλνει στον διακομιστή κάποια δεδομένα, όπως την έκδοση του SSL, τις ρυθμίσεις κρυπτογράφησης κ.α.
  – Ο διακομιστής απαντά και στέλνει και το ψηφιακό του πιστοποιητικό

Η διαδικασία μεταφοράς (2/3)

– Αν η ανταλλαγή δεδομένων απαιτεί από τον πελάτη να δώσει το δικό του ψηφιακό πιστοποιητικό, τότε συμβαίνει στο σημείο αυτό
– Ο πελάτης πιστοποιεί τον διακομιστή και αν υπάρχει πρόβλημα ο χρήστης ειδοποιείται
– Χρησιμοποιώντας τα δεδομένα που προέκυψαν από την χειραψία, ο πελάτης δημιουργεί δεδομένα γνωστά ως premaster secret
– Ο διακομιστής πιστοποιεί τον πελάτη (Συνήθως δεν χρειάζεται)

Η διαδικασία μεταφοράς (3/3)

– Οι δυο πλευρές φτιάχνουν δεδομένα που λέγονται master secret που δημιουργείται εν μέρει από το premaster secret

– Από το master secret, ο πελάτης και ο διακομιστής δημιουργούν ένα ζευγάρι κλειδιών

– Το ένα δημιουργείται για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων από τον πελάτη στον διακομιστή ενώ το άλλο από τον διακομιστή στον πελάτη

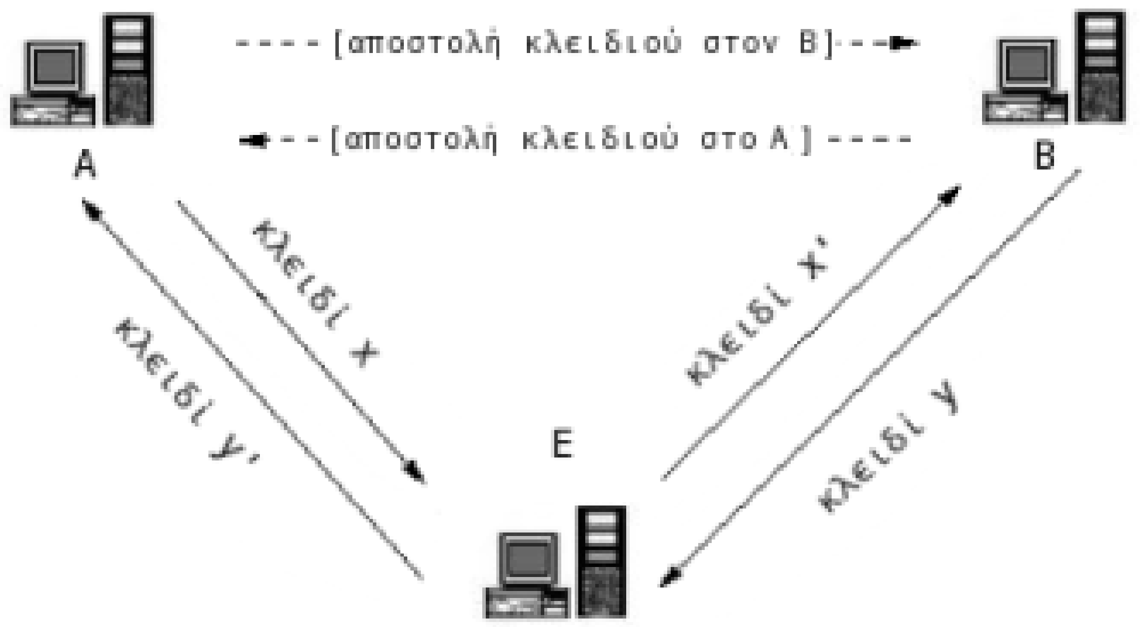
Τέλος διαδικασίας

- Η χειραψία είναι πλήρης και οι δυο πλευρές μπορούν να ξεκινήσουν να στέλνουν η μια στην άλλη κρυπτογραφημένα δεδομένα
- Χρησιμοποιούν έναν από τους αλγορίθμους που υπάρχουν στην έκδοση του SSL που χρησιμοποιείται
- Αφού έχει ολοκληρωθεί η επικοινωνία καταστρέφεται η σύνδεση

Επίθεση Man-In-the-Middle (1/2)

- Το SSL μπορεί να είναι ευάλωτο σε μια μορφή επίθεσης που αποκαλείται επίθεση Man-In-the-Middle
- Σε αυτήν παρεμβάλλεται ένας υπολογιστής ή πρόγραμμα μεταξύ του πελάτη και του διακομιστή
- Ο ενδιάμεσος υπολογιστής αρχίζει τη διαδικασία της χειραψίας με τον πελάτη και δημιουργεί ένα δικό του master secret και δυο κλειδιά
- Τα κλειδιά χρησιμοποιούνται για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν πληροφορίες, που θα έπρεπε να μεταφέρονται μεταξύ του πελάτη και του πραγματικού διακομιστή

Επίθεση Man-In-the-Middle (2/2)



Επίθεση Man-In-The-Middle όπου Α και Β οι νόμιμοι χρήστες και Ε ο επιτιθέμενος

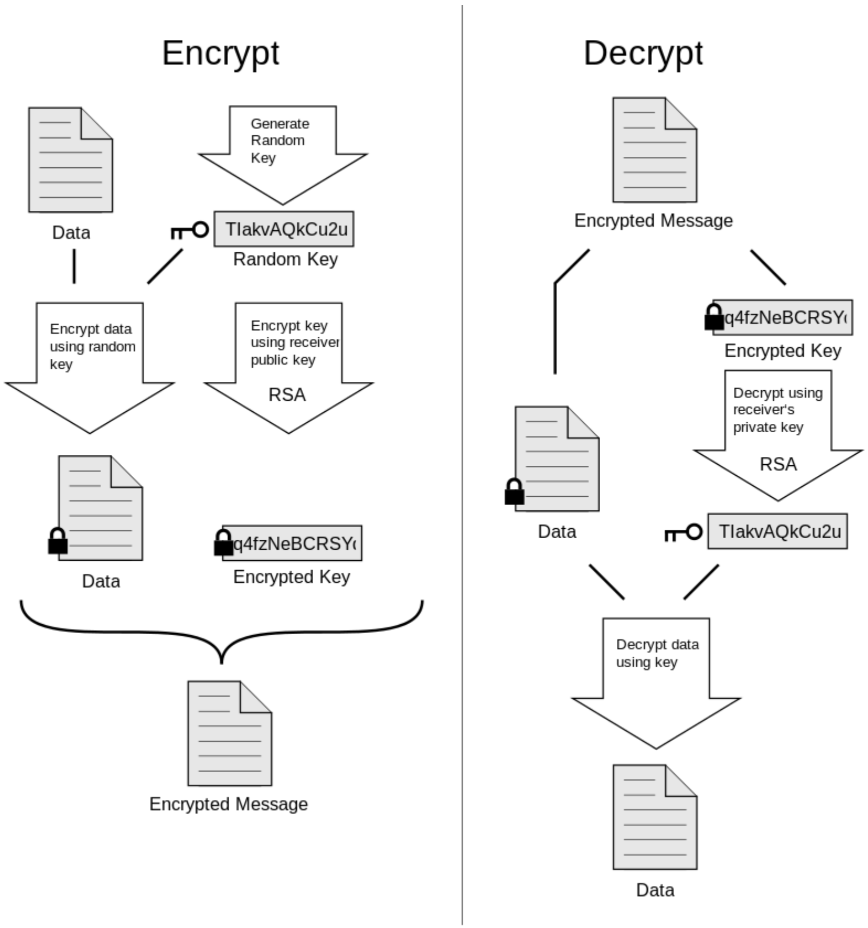
(πηγή: https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle#/media/File:Man-in-the-middle_attack.PNG)

Συστήματα ασφάλειας ηλεκτρονικού ταχυδρομείου

- Pretty Good Privacy (PGP):
  - Παρέχει προστασία απορρήτου, πιστοποίηση ταυτότητας, ψηφιακές υπογραφές και συμπίεση
  - Χρησιμοποιεί κρυπτογραφία IDEA και διαχείριση κλειδιών RSA
- Privacy-enhanced Electronic Mail (PEM):
  - Καλύπτει τους ίδιους τομείς με το PGP, αλλά δεν κατάφερε να διαδοθεί τόσο
- Secure/Multipurpose Internet Mail Extensions (S/MIME):
  - Παρέχει πιστοποίηση ταυτότητας, ακεραιότητα, μυστικότητα, και μη αποκήρυξη
  - Υποστηρίζει μεγάλη ποικιλία κρυπτογραφικών αλγορίθμων

Λειτουργία PGP

Λειτουργία PGP



source: http://commons.wikimedia.org/wiki/File:PGP_diagram.svg

IP security (IPsec)

- Η Internet Engineering Task Force (IETF) δημιούργησε το IP Security Working Group με στόχο να σχεδιάσει μια αρχιτεκτονική ασφαλείας και αντίστοιχα πρωτόκολλα
- Το αποτέλεσμα ονομάζεται ασφάλεια IP (IP security - IPsec)
- Κάποιοι χρήστες δεν επιθυμούν κρυπτογράφηση (επειδή είναι υπολογιστικά δαπανηρή)
- Αποφασίστηκε να απαιτείται πάντοτε η κρυπτογράφηση αλλά να επιτρέπεται η χρήση ενός κενού αλγόριθμου

Υπηρεσίες IPsec (1/2)

- Οι υπηρεσίες που μπορούν να θεωρηθούν μέρος του IPsec βασίζονται στην κρυπτογραφία συμμετρικού κλειδιού και περιλαμβάνουν:
  - Έλεγχο πρόσβασης:
    - Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί κωδικό. Διάφορα πρωτόκολλα ασφαλείας μπορούν να χρησιμοποιηθούν
  - Ακεραιότητα δεδομένων:
    - Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου
  - Πιστοποίηση του αποστολέα:
    - Γίνεται με χρήση των κατάλληλων αλγορίθμων ψηφιακών κλειδιών

Υπηρεσίες IPsec (2/2)

– Προστασία εναντίων επιθέσεων τύπου packet replay:
  - Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις, όπου ο επιτιθέμενος προσπαθεί να βλάψει την διαθεσιμότητα του συστήματος
– Κωδικοποίηση των δεδομένων:
  - Παρέχονται μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων
– Εξασφάλιση του απόρρητου της ροής των δεδομένων:
  - Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων

IPsec πρωτόκολλα

- Το IPsec χρησιμοποιεί τα ακόλουθα πρωτόκολλα:
  – Authentication Headers (AH): παρέχει ακεραιότητα και πιστοποίηση για IP datagrams και προστασία από replay attacks
  – Encapsulating Security Payloads (ESP): παρέχει εμπιστευτικότητα, πιστοποίηση, ακεραιότητα, υπηρεσία anti-replay
  – Security Associations (SA): περιλαμβάνει το πακέτο των αλγορίθμων και των δεδομένων που παρέχουν τις απαραίτητες παραμέτρους για τις λειτουργίες των AH και ESP

Δομή Authentication Headers

<table>
<tr><th colspan="34">Authentication Header format</th></tr>
<tr><td>Offsets</td><td>Octet$_{16}$</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet$_{16}$</td><td>Bit$_{10}$</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>0</td><td>0</td><td colspan="8">Next Header</td><td colspan="8">Payload Len</td><td colspan="16">Reserved</td></tr>
<tr><td>4</td><td>32</td><td colspan="32">Security Parameters Index (SPI)</td></tr>
<tr><td>8</td><td>64</td><td colspan="32">Sequence Number</td></tr>
<tr><td>C</td><td>96</td><td colspan="32" rowspan="2">Integrity Check Value (ICV)
...</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>

Δομή Authentication Headers

(πηγή: http://en.wikipedia.org/wiki/IPsec)

Δομή Encapsulating Security Payloads

<table>
<tr><th colspan="34">*Encapsulating Security Payload* format</th></tr>
<tr><th>*Offsets*</th><th>Octet$_{16}$</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet$_{16}$</th><th>Bit$_{10}$</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="32">*Security Parameters Index (SPI)*</td></tr>
<tr><td>4</td><td>32</td><td colspan="32">*Sequence Number*</td></tr>
<tr><td>8</td><td>64</td><td colspan="32" rowspan="2">*Payload data*</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>...</td><td>...</td><td colspan="8"></td><td colspan="24" rowspan="2">*Padding (0-255 octets)*</td></tr>
<tr><td>...</td><td>...</td><td colspan="8"></td></tr>
<tr><td>...</td><td>...</td><td colspan="16"></td><td colspan="8">*Pad Length*</td><td colspan="8">*Next Header*</td></tr>
<tr><td>...</td><td>...</td><td colspan="32" rowspan="2">*Integrity Check Value (ICV)*
...</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>

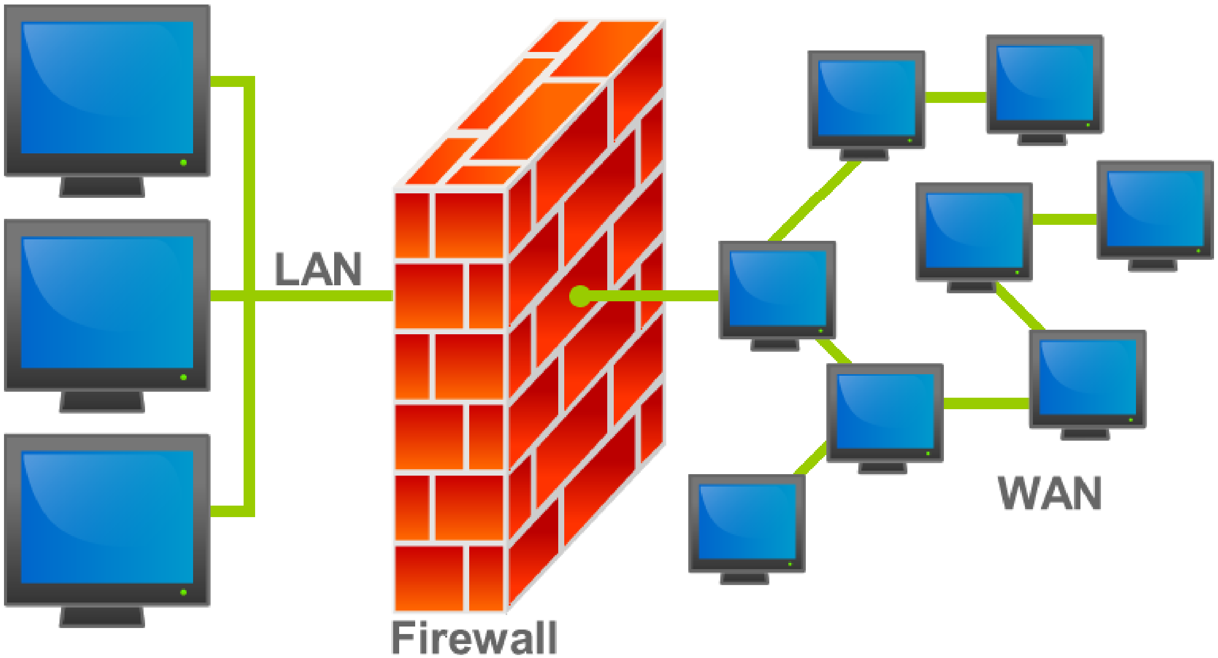
Δομή Encapsulating Security Payloads

(πηγή: http://en.wikipedia.org/wiki/IPsec)

Τείχος προστασίας - Firewall

- Ο όρος firewall εμφανίστηκε στις αρχές του 20ού αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα, ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς
- Πλέον σημαίνει το λογισμικό ή υλικό, που παρεμβάλλεται μεταξύ δικτύων υπολογιστών, και επιβλέπει την κυκλοφορία, βασιζόμενο σε ένα σύνολο κανόνων
- Βασικός στόχος: η ρύθμιση της κυκλοφορίας μεταξύ δικτύων διαφορετικών επιπέδων εμπιστοσύνης
- Παράδειγμα: το Internet, που είναι ένα δίκτυο χωρίς εμπιστοσύνη, και ένα εσωτερικό δίκτυο, που αποτελεί ζώνη υψηλότερης εμπιστοσύνης

Firewall



source: http://commons.wikimedia.org/wiki/File:Firewall.png

Το firewall παρεμβάλλεται μεταξύ δικτύων υπολογιστών

Οφέλη

- Ένα firewall μπορεί να μας προσφέρει :
  - Ένα σημείο εφαρμογής των αποφάσεων, που αφορούν την ασφάλεια
  - Ένα μέσο για την εφαρμογή της πολιτικής ασφάλειας
  - Ένα τρόπο καταγραφής της δικτυακής κίνησης
  - Ένα φράγμα σε ανεπιθύμητες επιθέσεις

Αδυναμίες

- Ένα firewall δεν μπορεί να μας προστατέψει από:
  - Εσωτερικούς χρήστες, που σκοπεύουν να επιτεθούν
  - Συνδέσεις, που δεν περνούν από αυτό
  - Εντελώς νέους τύπους απειλών-επιθέσεων
  - Από όλους τους ιούς
  - Λάθη στο σχεδιασμό, τη λειτουργία ή τις ρυθμίσεις του

Πρώτη γενιά – Packet Filters

- Εμφανίστηκαν στα τέλη της δεκαετίας του 1980, όταν ακόμη το Internet ήταν σε πρώιμα στάδια και είχαν παρατηρηθεί αρκετά κενά ασφαλείας στο Διαδίκτυο
- Πρώτη γενιά – packet filters:
  - Τα packet filter firewalls ενεργούν στα πακέτα, που αντιπροσωπεύουν τη βασική πληροφορία, δηλαδή στα πακέτα, που μεταφέρουν τα δεδομένα μεταξύ των υπολογιστών
  - Διαβάζουν τα πακέτα δεδομένων και εάν ένα πακέτο ταιριάζει με κάποιο κανόνα το απορρίπτουν
  - Ο διαχειριστής ορίζει τους κανόνες
  - Δεν εξετάζεται εάν ένα πακέτο είναι μέρος ενός ρεύματος κυκλοφορίας δεδομένων

Δεύτερη γενιά-"Stateful" filters

- Τα firewall της δεύτερης γενιάς δρουν, όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες:
  - Εξετάζουν την κατάσταση (state) του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε
  - Αποθηκεύουν δομές δεδομένων στη μνήμη με πληροφορίες σχετικά με την κατάσταση της σύνδεσης (πίνακες κατάστασης)
  - Όταν ένα firewall λαμβάνει ένα πακέτο, ελέγχει πρώτα αν ανήκει σε υπάρχουσα κατάσταση στον πίνακα. Εάν ναι, τότε γίνεται αποδεκτό
  - Διαφορετικά, συγκρίνεται με βάση τους κανόνες του firewall για την αποδοχή ή την απόρριψή του

Τρίτη γενιά - Application layer

- Η τρίτη γενιά firewall βασίζεται στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI
- Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση
- Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές, που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μίας υπηρεσίας

Τέταρτη γενιά

- Διαθέτουν γραφικό περιβάλλον μέσω του οποίου ο χρήστης κάνει τις επιλογές του και θέτει τους κανόνες βάσει τον οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις
- Μπορούν πλέον να ενσωματωθούν στο λειτουργικό σύστημα και συνεργάζονται στενά με άλλα συστήματα ασφαλείας

Λειτουργίες firewall σε γραφικό περιβάλλον

Παράδειγμα λειτουργιών firewall σε γραφικό περιβάλλον

(πηγή: https://en.wikipedia.org/wiki/Firewall_%28computing%29#/media/File:Gufw_10.04.4.png)

Proxy Firewalls

- Ένας άλλος τύπος firewall είναι το proxy firewall, όπου κάθε πακέτο σταματά στο firewall
- Το πακέτο εξετάζεται και συγκρίνεται με τους κανόνες, που διαμορφώνονται από το firewall
- Εάν το πακέτο περάσει τις «εξετάσεις», επαναδημιουργείται και στέλνεται
- Επειδή κάθε πακέτο καταστρέφεται και επαναδημιουργείται, αποτρέπονται οι άγνωστες επιθέσεις, που βασίζονται στις αδυναμίες του πρωτοκόλλου TCP/IP

Λειτουργικά όρια των firewalls

- Τα firewalls δεν μπορούν να εμποδίσουν μια σειρά από περιστατικά και ενέργειες, όπως:
  - Την πειρατεία συνόδου, όπου ο επιτιθέμενος παίρνει τον έλεγχο από έναν νόμιμο χρήστη
  - Το network data sniffing (ή snooping)
  - Την επαναδρομολόγηση δικτυακών δεδομένων
  - Τη μεταμφίεση δικτυακών δεδομένων (spoofing)
  - Τη διαρροή πληροφοριών, σε τρίτους, από νόμιμα εξουσιοδοτημένους χρήστες
  - Την αποδοχή «μολυσμένων αρχείων», χωρίς προηγούμενο έλεγχό τους
  - Τις εσωτερικές επιθέσεις

Σύντομη ανασκόπηση

- Εισαγωγή
- Κρυπτογράφηση
- SSL
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Ασφάλεια σε επίπεδο δικτύου
- Τείχος προστασίας

Βιβλιογραφία

- Σημειώσεις μαθήματος (Κεφάλαιο 10)
- Βιβλία:
  - Computer Networks, Andrew S. Tanenbaum, David J. Wetherall
  - Data and Computer Communications, W. Stallings
  - Security Engineering, Anderson
  - Cryptography Engineering: Design Principles and Practical Applications, N. Ferguson, B. Schneier, T. Kohno
  - Network security: private communication in a public world, C. Kaufman, R. Perlman, M. Speciner

Links

- Links
  - http://ru6.cti.gr/ru6/bouras/undergraduate-courses/diktua-dhmosias-xrhshs-kai-diasundesh-diktuwn?language=el (Δικτυακός τόπος μαθήματος)
  - http://www.cs.cmu.edu/~srini/15-441/F02/lectures/lec21-security.ppt (Presentation on Network Security)
  - http://www.cs.uiuc.edu/class/sp07/cs498ia/slides/CS461-09.Cryptography.ppt (Presentation on Cryptography algorithms)
  - http://www.cs.northwestern.edu/~ychen/classes/mitp-458/firewalls.ppt (Presentation on Firewalls)

Ερωτήσεις

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο την αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σημειώματα

Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση 2.0.

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης