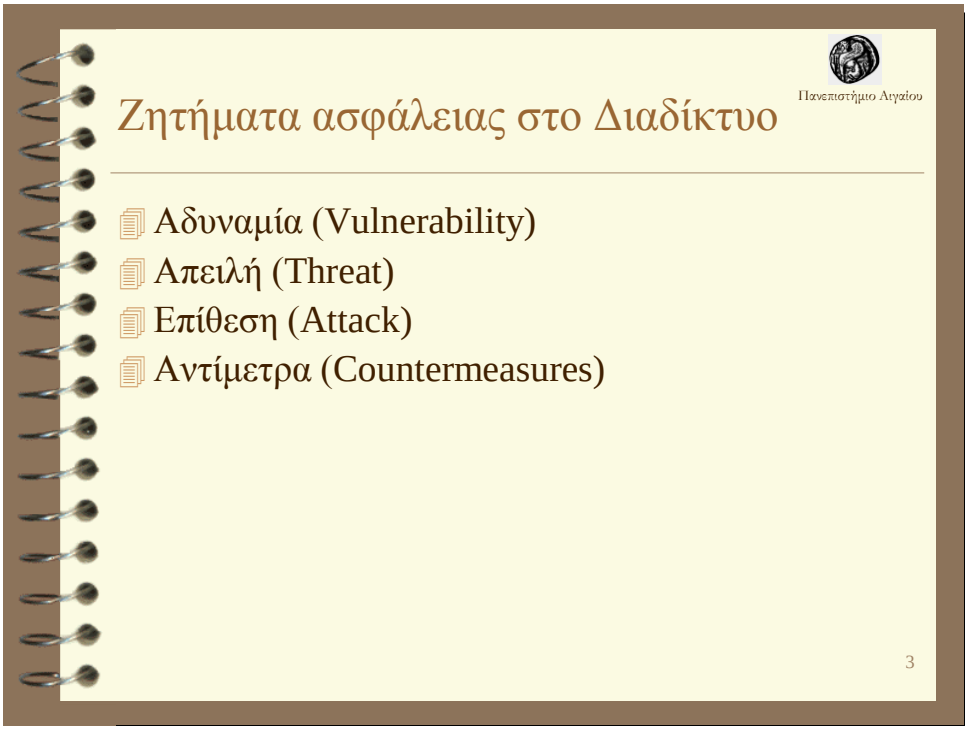
Ασφάλεια Δικτύων Υπολογιστών

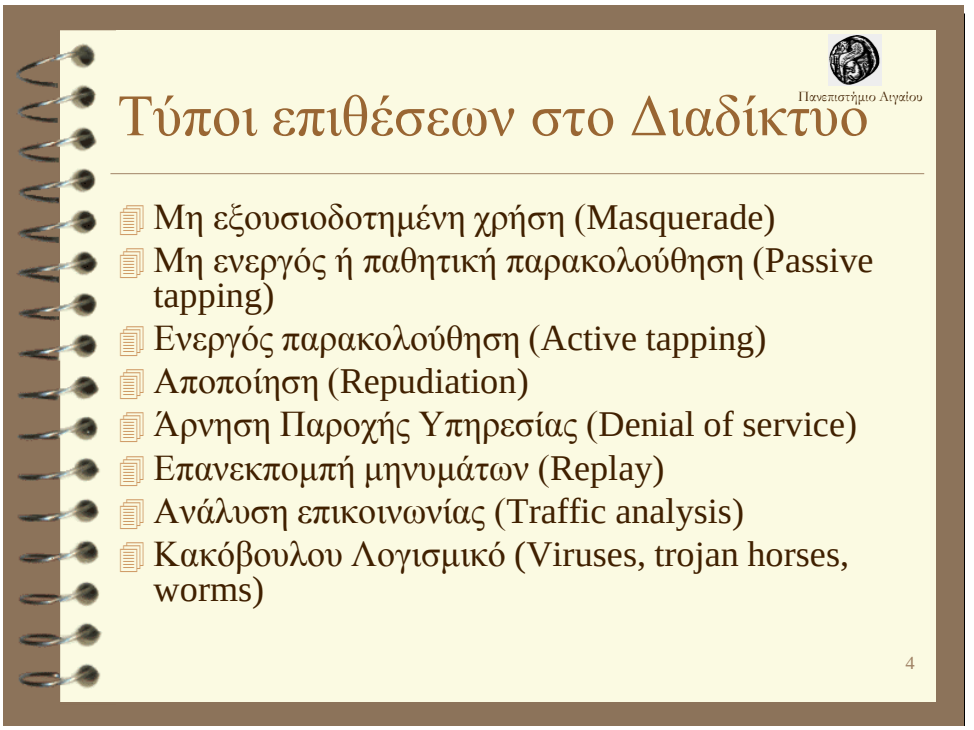
Γιώργος Καρόπουλος
(Διδάσκων Π.Δ. 407/80)
Τμήμα Μηχανικών
Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Αντικείμενο μελέτης

Πανεπιστήμιο Αιγαίου

- Ζητήματα ασφάλειας στο Διαδίκτυο
- Τύποι επιθέσεων στο Διαδίκτυο
- Πρωτόκολλα ασφάλειας ανά επίπεδο δικτύου


Πανεπιστήμιο Αιγαίου
Ζητήματα ασφάλειας στο Διαδίκτυο
Αδυναμία (Vulnerability)
Απειλή (Threat)
Επίθεση (Attack)
Αντίμετρα (Countermeasures)
3


Πανεπιστήμιο Αιγαίου
Τύποι επιθέσεων στο Διαδίκτυο
Μη εξουσιοδοτημένη χρήση (Masquerade)
Μη ενεργός ή παθητική παρακολούθηση (Passive tapping)
Ενεργός παρακολούθηση (Active tapping)
Αποποίηση (Repudiation)
Άρνηση Παροχής Υπηρεσίας (Denial of service)
Επανεκπομπή μηνυμάτων (Replay)
Ανάλυση επικοινωνίας (Traffic analysis)
Κακόβουλου Λογισμικό (Viruses, trojan horses, worms)
4

Πρωτόκολλα Ασφάλειας

Πανεπιστήμιο Αιγαίου

- Επιπέδου Πρόσβασης Δικτύου
- Επιπέδου Internet
- Επιπέδου Μεταφοράς
- Επιπέδου Εφαρμογής και υπεράνω αυτού

Πρωτόκολλα Ασφάλειας Πρόσβασης Δικτύου

Πανεπιστήμιο Αιγαίου

- Γνωστότερα πρωτόκολλα: Ethernet, Point-to-Point Protocol (PPP)
- Πρόβλημα: κάποιος ευρισκόμενος σε μία χώρα επιθυμεί να συνδεθεί μέσω του φορητού υπολογιστή του στο εταιρικό εσωτερικό δίκτυο (π.χ. για πρόσβαση σε e-mails ή αρχεία)
- Λύσεις:
  - PPP ανάμεσα στο χρήστη και την εταιρεία μέσω PSTN ή ISDN
    - + διαθεσιμότητα, απλότητα
    - - ασφάλεια, κόστος
  - Χρήση ενός Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network – VPN): ενθυλάκωση ενός δοθέντος πρωτοκόλλου επιπέδου δικτύου μέσα σε PPP, η προστασία μέσω κρυπτογράφησης των πλαισίων του PPP και η ενθυλάκωση των δεδομένων με βάση ένα πρωτόκολλο διέλευσης (tunneling) που τυπικά είναι το πρωτόκολλο IP, αλλά θα μπορούσε να είναι και το ATM ή το Frame Relay. Αυτή η προσέγγιση είναι γνωστή ως *διέλευση δευτέρου επιπέδου* (Layer 2 Tunneling – L2TP) επειδή τη δίοδο διαπερνά συνήθως ένα πρωτόκολλο δευτέρου επιπέδου (π.χ. το PPP).

Πρωτόκολλα Ασφάλειας Πρόσβασης Δικτύου

- Συμμετέχουσες οντότητες
  - απομακρυσμένο σύστημα (remote system) ή ένας εξυπηρετούμενος μέσω τηλεφώνου (dial-up client)
  - συγκεντρωτής πρόσβασης L2TP (L2TP Access Concentrator - LAC)
  - εξυπηρέτης δικτύου L2TP (L2TP Network Server - LNS)

7

Πρωτόκολλα Ασφάλειας Επιπέδου Internet

- IP Security protocol
  - Ο μηχανισμός *Authentication Header - AH* παρέχει αυθεντικοποίηση προέλευσης δεδομένων και υπηρεσίες ακεραιότητας δεδομένων χωρίς σύνδεση.
  - Ο μηχανισμός *Encapsulating Security Payload - ESP* παρέχει υπηρεσίες εμπιστευτικότητας δεδομένων χωρίς σύνδεση.
    - κατάσταση μεταγωγής - transport mode
    - κατάσταση διόδου - tunnel mode
  - Από κανέναν από τους δύο αυτούς μηχανισμούς ασφάλειας δεν παρέχεται αποτελεσματική προστασία έναντι της ανάλυσης κυκλοφορίας δεδομένων (traffic analysis)
  - Βασίζονται στον συσχετισμό ασφάλειας (Security Association – SA)

8

Πρωτόκολλα Ασφάλειας Επιπέδου Internet

- Security Association – SA: κοινό σύνολο παραμέτρων ασφάλειας
  - Αλγόριθμος αυθεντικοποίησης, κατάσταση (mode) και κλειδιά για τον AH μηχανισμό.
  - Αλγόριθμος κρυπτογράφησης, κατάσταση και κλειδιά για τον ESP μηχανισμό.
  - Το μέγεθος και η παρουσία ή απουσία του διανύσματος συγχρονισμού του αλγορίθμου κρυπτογράφησης ή διανύσματος αρχικοποίησης (initialization vector - IV) για τον ESP μηχανισμό.
  - Η διάρκεια ζωής των κλειδιών και του SA ως συνόλου.
  - Η διεύθυνση πηγής (source address) του SA. Στην περίπτωση που περισσότεροι από ένας ξενιστές υπολογιστές (host) μοιράζονται τον ίδιο SA, αυτή μπορεί επίσης να είναι μία διεύθυνση δικτύου ή υποδικτύου.
  - Το επίπεδο ευαισθησίας των ασφαλών δεδομένων, όπως Confidential, Secret, Unclassified. Αυτή η παράμετρος απαιτείται μόνον αν οι εξυπηρέτες απαιτούν την παροχή υποστήριξης πολυεπίπεδης ασφάλειας (Multilevel Security - MLS) σε περιβάλλον υποχρεωτικού ελέγχου προσπέλασης (Mandatory Access Control).
- Δείκτης παραμέτρων ασφάλειας (Security Parameters Index - SPI)

9

Πρωτόκολλα Ασφάλειας Επιπέδου Internet

- Πρωτόκολλο Διαχείρισης Κλειδιού Internet (Internet Key Management Protocol - IKMP): γιατί;
  - Modular Key Management Protocol – MKMP
  - Simple Key-management for Internet Protocols – SKIP
  - Photuris
  - Secure Key Exchnage Mechanism – SKEME
  - Internet Security Association Key Management Protocol – ISAKMP
  - OAKLEY
  - IKE/IKEv2: ISAKMP/ OAKLEY

10

Πρωτόκολλα Ασφάλειας Επιπέδου Μεταφοράς

- Secure Shell – SSH
- Secure Sockets Layer/Transport Layer Security – SSL/TLS
- Private Communication Technology - PCT

11

Πρωτόκολλα Ασφάλειας Επιπέδου Μεταφοράς

- Secure Shell – SSH
  - πρόγραμμα το οποίο μπορεί να χρησιμοποιηθεί για να συνδεθεί μία οντότητα ασφαλώς με μία απομακρυσμένη μηχανή, να εκτελεί εντολές σε αυτήν και να μεταφέρει αρχεία από μία μηχανή σε μία άλλη
  - παρέχει ισχυρή αυθεντικοποίηση, αλλά και ασφαλή επικοινωνία (εμπιστευτικότητα, ακεραιότητα δεδομένων) διαμέσου μη ασφαλών διαύλων
  - χρησιμοποιεί μη αυτοματοποιημένα διανεμημένα δημόσια κλειδιά
  - δωρεάν και εμπορική έκδοση
  - RSA και Blowfish, DES, ή Triple-DES σε CBC κατάσταση
- Πρωτόκολλο επιπέδου μεταφοράς SSH (SSH Transport Layer Protocol): παρέχει κρυπτογραφημένη αυθεντικοποίηση host, καθώς επίσης και εμπιστευτικότητα και προστασία ακεραιότητας δεδομένων, ενώ δεν παρέχει αυθεντικοποίηση χρήστη
- SSH πρωτόκολλο αυθεντικοποίησης (SSH Authentication Protocol) : σχεδιάστηκε να εκτελείται πάνω από το πρωτόκολλο επιπέδου μεταφοράς SSH για να παρέχει αυθεντικοποίηση χρήστη

12

Πρωτόκολλα Ασφάλειας Επιπέδου Μεταφοράς

- Secure Sockets Layer/Transport Layer Security – SSL/TLS
  - Το SSL στρωματοποιείται στην κορυφή μίας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που παρέχεται από το TCP/IP
  - ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή
  - αμοιβαία αυθεντικοποίηση με κρυπτογραφία δημόσιου κλειδιού
  - προστασία εμπιστευτικότητας των μεταδιδόμενων δεδομένων
  - προστασία ακεραιότητα των μεταδιδόμενων δεδομένων
  - δεν παρέχει προστασία έναντι επιθέσεων ανάλυσης κυκλοφορίας (traffic analysis)
- SSL record protocol
  - υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων
- SSL handshake protocol
  - πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών
  - διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας και την αντίστοιχη κατάσταση στα δύο άκρα της σύνδεσης

Πρωτόκολλα Ασφάλειας Επιπέδου Εφαρμογής

- Δύο κύριες προσεγγίσεις:
  - ανεξάρτητα σε κάθε εφαρμογή
  - γενικευμένο σύστημα ασφάλειας το οποίο μπορεί να χρησιμοποιηθεί για την ενσωμάτωση των υπηρεσιών ασφάλειας μέσα σε διαφορετικές εφαρμογές

Πρωτόκολλα Ασφάλειας Επιπέδου Εφαρμογής

- Telnet
  - πάνω από SSL/TLS
  - S/RLogin από την Baltimore Technologies Ltd.
  - Telnet λογισμικό για 4.4BSD UNIX με χρήση πρωτοκόλλου Interlock
  - Secure RPC Authentication - SRA
    - πριν από λίγα χρόνια ανακοινώθηκε επιτυχής κρυπτανάλυση του SRA
    - το Secure RPC και συνεπώς και το SRA είναι ευάλωτα σε επιθέσεις τύπου ενδιαμέσου
  - Secure Telnet - STEL
  - όλα τα παραπάνω χρησιμοποιούν μία Diffie-Hellman ανταλλαγή κλειδιών για να μεταβιβάζουν ένα κλειδί συνόδου και αυτό το κλειδί συνόδου χρησιμοποιείται στη συνέχεια για να κρυπτογραφεί, είτε μόνο τις πληροφορίες αυθεντικοποίησης, είτε ολόκληρη την Telnet σύνοδο

15

Πρωτόκολλα Ασφάλειας Επιπέδου Εφαρμογής

- E-mail
  - η τεχνική επίτευξης από άκρη-σε-άκρη ασφάλειας ηλεκτρονικών μηνυμάτων είναι η χρήση ψηφιακού φακέλου (digital enveloping)
  - Privacy Enhanced Mail – PEM
  - Pretty Good Privacy – PGP
  - Secure Multipurpose Internet Mail Extensions - S/MIME

16

Πανεπιστήμιο Αιγαίου

Privacy Enhanced Mail – PEM

- ενσωμάτωσή του στην υπάρχουσα υποδομή ηλεκτρονικού ταχυδρομείου βασιζόμενη σε SMTP
- τα ασφαλή μηνύματα θα πρέπει να συμπεριλαμβάνονται ως τμήματα του σώματος των προτυποποιημένων ηλεκτρονικών μηνυμάτων
- εμπιστευτικότητα δεδομένων, αυθεντικοποίηση μηνύματος, ακεραιότητα δεδομένων και μη-αποποίηση αποστολής
- απαιτεί PKI
- δεν παρέχει υποστήριξη για δυαδικές επισυνάψεις (binary attachments) και τύπους MIME

17

Πανεπιστήμιο Αιγαίου

Pretty Good Privacy - PGP

- προϊόν λογισμικού
- υπηρεσίες εμπιστευτικότητας δεδομένων, αυθεντικοποίηση μηνυμάτων, ακεραιότητα δεδομένων και μη-αποποίησης αποστολής, μέσω κρυπτογράφησης και ψηφιακών φακέλων
- ασφάλεια σε ηλεκτρονικά μηνύματα, αλλά και κρυπτογράφηση τοπικών αρχείων
- αποσπασμένες ψηφιακές υπογραφές
- ιεραρχία πιστοποιητικών VS ιστός εμπιστοσύνης

18

Πανεπιστήμιο Αιγαίου

Secure MIME – S/MIME

- Μεγαλύτερη έμφαση στη διαλειτουργικότητα: S/MIME Interoperability Center της RSA Data Security, Inc.
- περισσότερο ευέλικτες ιεραρχίες πιστοποιητικών
- Τα PGP και S/MIME χρησιμοποιούν διαφορετική δομή μηνυμάτων
- ύπαρξη ολοκληρωμένης υποδομής δημόσιων κλειδιών

19

Πανεπιστήμιο Αιγαίου

Δοσοληψίες στον Παγκόσμιο Ιστό

- Secure HTTP (S-HTTP)
  - Το S-HTTP παρέχει τρεις υπηρεσίες προστασίας περιεχομένου μηνύματος: ψηφιακή υπογραφή, αυθεντικοποίηση και κρυπτογράφηση
  - ευέλικτο ως προς τους μηχανισμούς ασφάλειας και τους κρυπτογραφικούς αλγορίθμους που υποστηρίζει
  - η ευρεία διάδοση και χρήση του SSL έχει εκτοπίσει σε σημαντικό βαθμό τη χρήση του S-HTTP

20

Σύστημα Ονοματοδοσίας - DNS

- DNS Security (DNSSEC)
  - κρυπτογραφία δημόσιου κλειδιού και ψηφιακές υπογραφές για την παροχή υπηρεσιών ακεραιότητας δεδομένων και αυθεντικοποίησης για πληροφορίες που περιέχονται στο DNS και μεταφέρονται με το DNS πρωτόκολλο
  - δεν παρέχει υπηρεσίες ελέγχου προσπέλασης και διασφάλισης της ιδιωτικότητας
  - προκαλεί αυξημένο φόρτο εργασίας

21

Σύστημα αυθεντικοποίησης και διανομής κλειδιών

- Kerberos
  - έχει παρουσιαστεί σε προηγούμενη διάλεξη

22