

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια Δικτύων Η/Υ
εναντίον
Ευελιξίας στο δικτυακό περιβάλλον
άρα
Μειωμένη Παραγωγικότητα

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Ασφαλισμένο το κτήριο στο οποίο
είναι εγκατεστημένο το δίκτυο Η/Υ.

**Από προσωπικό
ασφαλείας ή σύστημα
συναγερμού.**

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Ασφαλείς χώροι (κλειδωμένοι), της σημαντικής δικτυακής υποδομής (π.χ. computer room, PABX room)



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Ελεγχος πρόσβασης (access control)
στα άτομα που επιτρέπεται να
εισέλθουν στο computer room.

(Καταχώρηση εισόδου/εξόδου)



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Κλειδωμένα ικριώματα (racks) και
κατανεμητές που δεν βρίσκονται στο
computer room.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

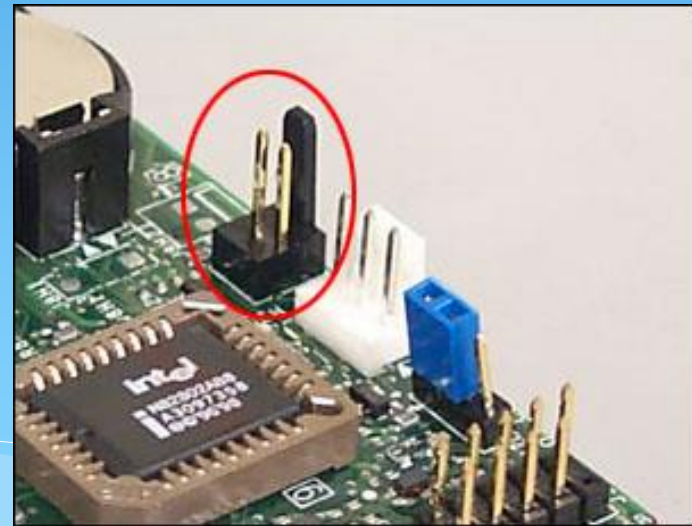
Κλειδωμένα κουτιά Η/Υ που δεν βρίσκονται στο computer room.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Κουτιά Η/Υ με Case Intruder (CI)
διακόπτη που συνδέεται στη μητρική
πλακέτα (1/2).



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Κουτιά Η/Υ με Case Intruder (CI) διακόπτη που συνδέεται στη μητρική πλακέτα (2/2).

Παραμετροποιείται στο BIOS.
Μετά το άνοιγμα (και
κλείσιμο) του πλαινού
καλύμματος του κουτιού
εμφανίζεται σχετικό μήνυμα
κατά την επόμενη εκκίνηση
του Η/Υ. Το σχετικό μήνυμα
μπορεί να βρεθεί και μέσα από
το Λ.Σ. Windows όπου με
κάποια δικτυακή εφαρμογή
μπορεί να ενημερωθεί κάποιος
απομακρυσμένα.

```
ASUS P5K SE ACPI BIOS Revision 1402
CPU : Intel(R) Pentium(R) D CPU 3.00GHz
Speed : 3.00 GHz    Count : 2
```

```
Entering SETUP ...
Press F8 for BBS POPUP
Press ALT+F2 to execute ASUS EZ Flash
DDR2-800 in Single-Channel Mode
Initializing USB Controllers .. Done.
1024MB OK
```

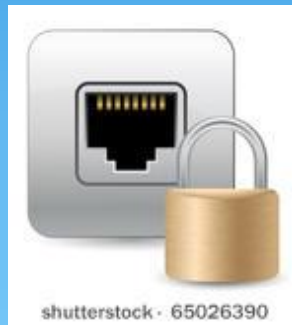
```
Auto-Detecting SATA 1...IDE Hard Disk
SATA 1: ST3160211AS 3.AAE
        Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK
Auto-detecting USB Mass Storage Devices ..
00 USB mass storage devices found and configured.
```

```
Chassis intruded !
Fatal Error... System Halted.
```

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Να μην υπάρχουν μη επιτηρούμενες,
ελεύθερες, και ενεργές δικτυακές
πρίζες



Να μη μπορεί ο επισκέπτης (guest)
να συνδεθεί στο δίκτυο του χώρου
χωρίς άδεια.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

φυσικός τρόπος

Να μην υπάρχει ασύρματο τοπικό δίκτυο (WiFi).

Εάν επιβάλλεται η ύπαρξή του, τότε πρέπει να έχει ισχυρότατους περιορισμούς.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια διακινούμενων πληροφοριών και εξασφάλιση παροχής δικτυακών υπηρεσιών μόνο σε εξουσιοδοτημένους χρήστες (1/5).

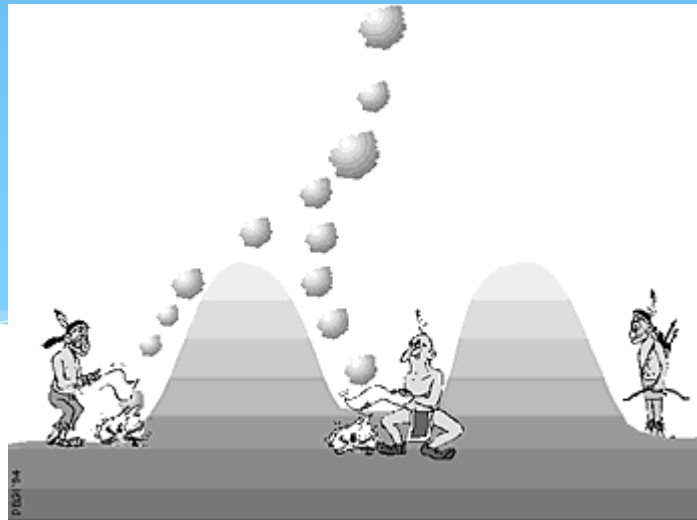
Αυθεντικότητα (Authenticity): Η αποφυγή ατελειών και ανακρίβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων ή αποστολής μιας πληροφορίας.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια διακινούμενων πληροφοριών και εξασφάλιση παροχής δικτυακών υπηρεσιών μόνο σε εξουσιοδοτημένους χρήστες (2/5).

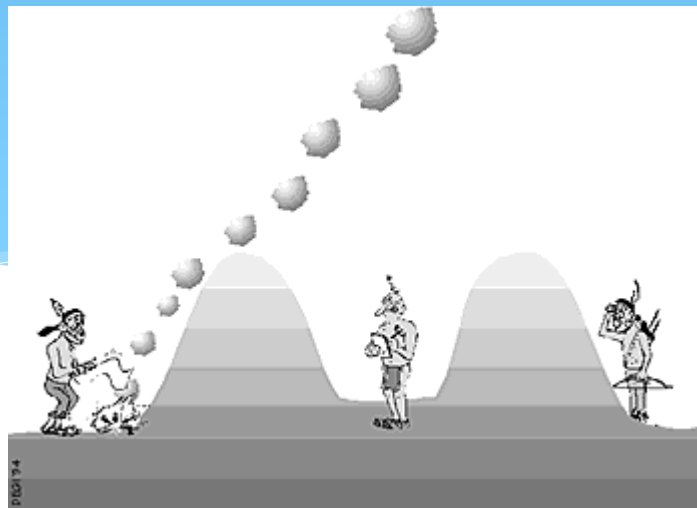
Ακεραιότητα (Integrity): Η διασφάλιση ότι τα δεδομένα έχουν υποστεί αλλαγές μόνο από εξουσιοδοτημένα άτομα.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια διακινούμενων πληροφοριών και εξασφάλιση παροχής δικτυακών υπηρεσιών μόνο σε εξουσιοδοτημένους χρήστες (3/5).

Εμπιστευτικότητα (Confidentiality):
Ο περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια διακινούμενων πληροφοριών και εξασφάλιση παροχής δικτυακών υπηρεσιών μόνο σε εξουσιοδοτημένους χρήστες (4/5).

Μη άρνηση ταυτότητας (Non repudiation):
Η δυνατότητα απόδοσης πράξεων σε συγκεκριμένο χρήστη.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Ασφάλεια διακινούμενων πληροφοριών και εξασφάλιση παροχής δικτυακών υπηρεσιών μόνο σε εξουσιοδοτημένους χρήστες (5/5).

Εγκυρότητα (Validity): Η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας = Αυθεντικότητα + Ακεραιότητα .



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (1/7)

Μόνο συγκεκριμένοι χρήστες πρέπει να έχουν πρόσβαση στο δίκτυο Η/Υ.

Με τη σημερινή διείσδυση των πληροφοριακών συστημάτων σχεδόν όλοι οι υπάλληλοι μιας επιχείρησης είναι και χρήστες του δικτύου των υπολογιστών αυτής.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (2/7)

Οι χρήστες πρέπει να χρησιμοποιούν
διαπιστευτήρια (credentials).

Όνομα χρήστη - Username

Κωδικός πρόσβασης - Password

Επιβαλλόμενη αλλαγή του κωδικού πρόσβασης στους χρήστες
ανά τακτά χρονικά διαστήματα.

Οι χρήστες ξεχνούν τους κωδικούς πρόσβασης αμέσως μετά την
αλλαγή.

Μεγάλο πρόβλημα για τους Διαχειριστές του δικτύου Η/Υ.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (3/7)

Οι χρήστες πρέπει να έχουν
διαβαθμισμένη πρόσβαση στο δίκτυο
Η/Υ.

Να μην έχουν όλοι οι χρήστες απεριόριστη πρόσβαση
στους τομείς (Domains)
και τους διαμοιραζόμενους πόρους του δικτύου Η/Υ.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

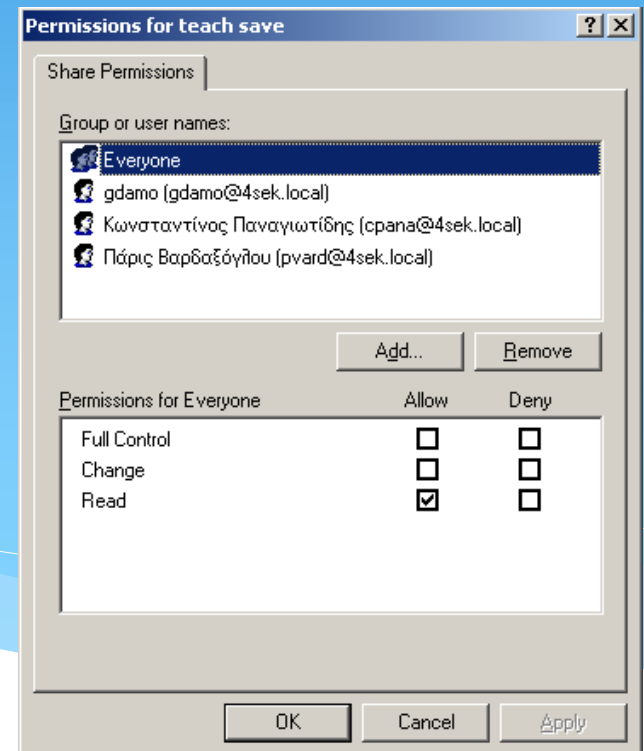
μέσω λογισμικού

Χρήστες (4/7)

Οι χρήστες πρέπει να έχουν πολύ συγκεκριμένα δικαιώματα κατά την πρόσβαση στα κοινόχρηστα (αρχεία και φακέλους) του δικτύου Η/Υ (1/2).

Π.χ.. Στον φάκελο teach save όλοι οι χρήστες του δικτύου (ομάδα: Everyone) έχουν δικαιώματα:

Ανάγνωσης
(Read: **✓**Allow).



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (5/7)

Οι χρήστες πρέπει να έχουν πολύ συγκεκριμένα δικαιώματα κατά την πρόσβαση στα κοινόχρηστα (αρχεία και φακέλους) του δικτύου Η/Υ (2/2).

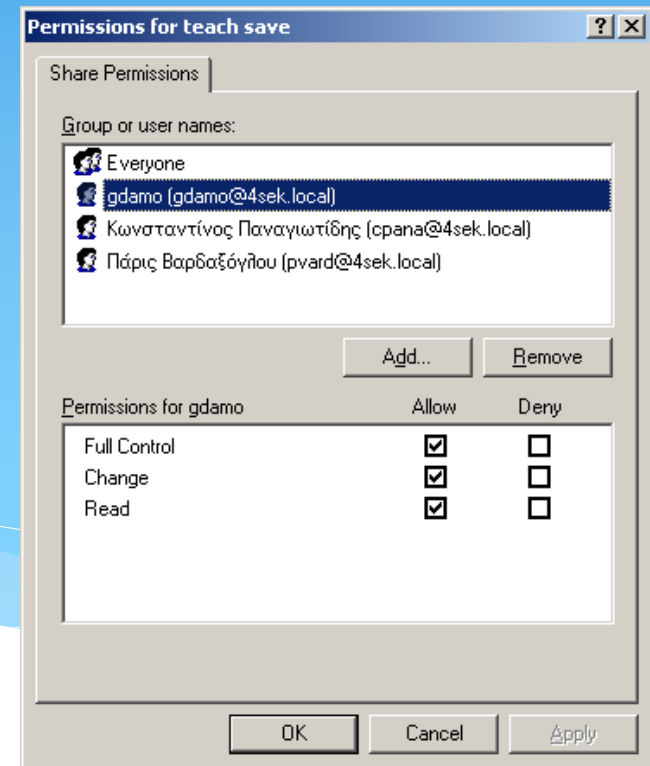
Π.χ.. Στον φάκελο teach save ο συγκεκριμένος χρήστης του δικτύου (χρήστης: gdamo) έχει δικαιώματα:

Πλήρους Ελέγχου ,

Τροποποίησης,

και Ανάγνωσης

(Full Control, Change, Read: ✓Allow).



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (6/7)

Εκπαίδευση των χρηστών στη μη διάδοση των διαπιστευτηρίων στο εταιρικό περιβάλλον αλλά και πολύ περισσότερο εκτός αυτού.

Σε εταιρικό περιβάλλον:

- Αμελή χρήση αυτών καθώς οι άλλοι χρήστες δεν έχουν την ευθύνη αυτών.
- Κακόβουλη χρήση τους από δυσαρεστημένους συναδέλφους.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Χρήστες (7/7)

Εκπαίδευση των χρηστών στη μη διάδοση των διαπιστευτηρίων εντός και εκτός εταιρικού περιβάλλοντος δια της Κοινωνικής Μηχανικής (Social Engineering).

Η πιο διαδεδομένη περίπτωση: Phishing

1. Ψευδής αποστολή email από φαινομενικά έγκυρο site σχετικά με κάποιο εταιρικό πρόβλημα.
2. Ζητείται από τον χρήστη να εισάγει τα διαπιστευτήριά του.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (1/6)

Μέσω του Event Viewer (tab: Security) μπορούμε να δούμε τους χρήστες που έχουν διαπιστευθεί στο δίκτυο Η/Υ.

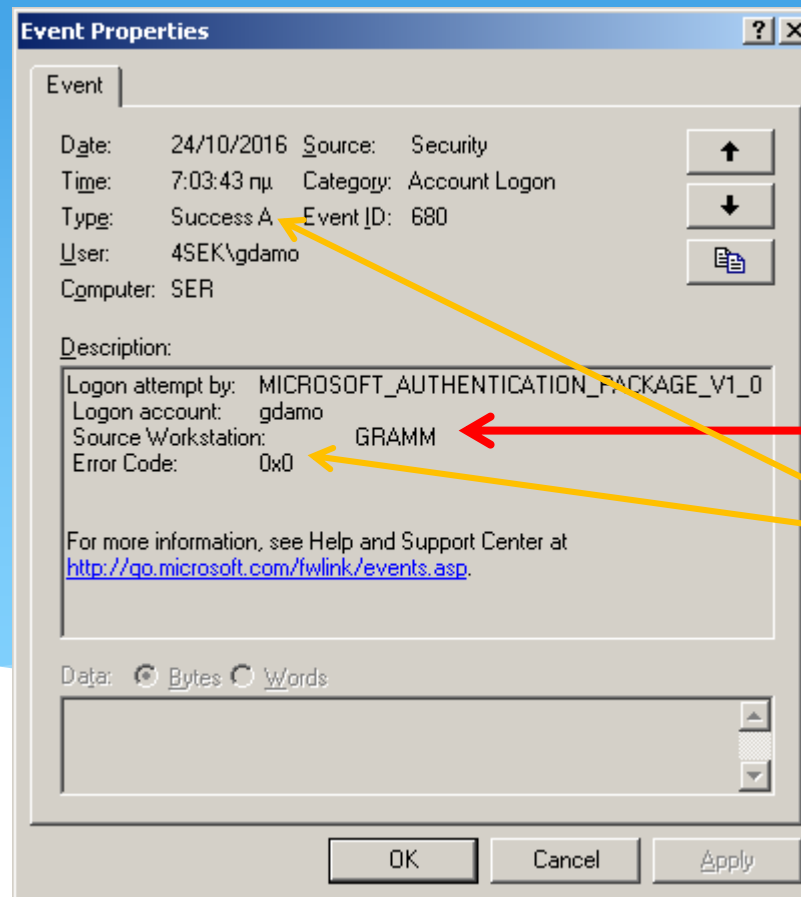
Event Viewer

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (2/6)

Αυθεντικοποίηση
του χρήστη



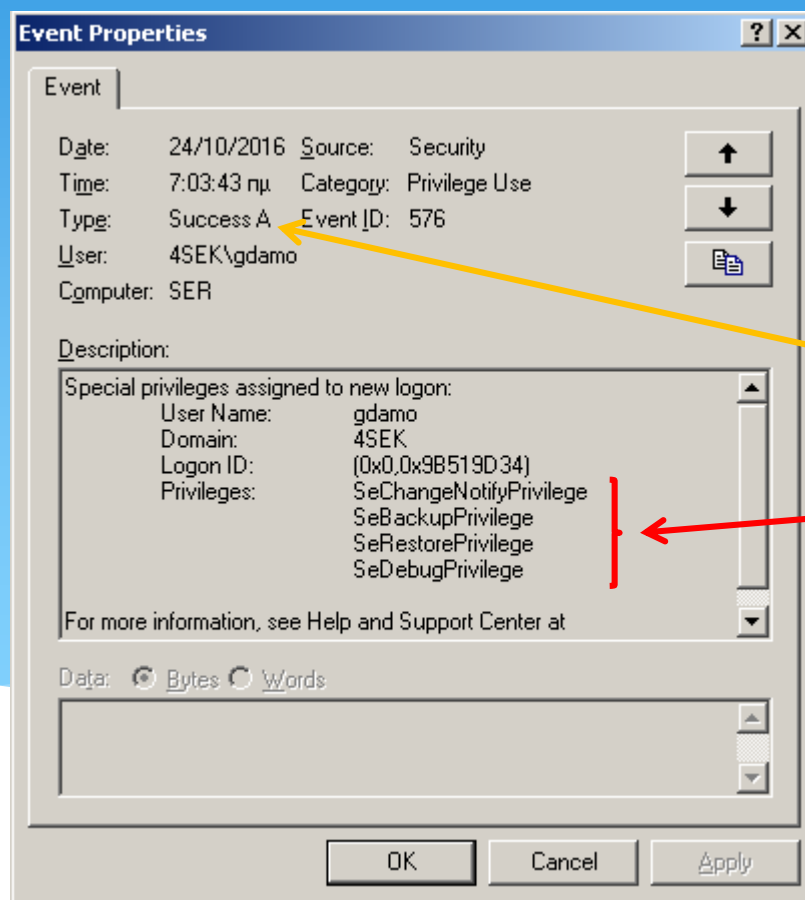
Όνομα
Η/Υ του χρήστη
Επιτυχής

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (3/6)

Εκχώρηση
δικαιωμάτων
στον
αυθεντικοποιημένο
χρήστη



Επιτυχής

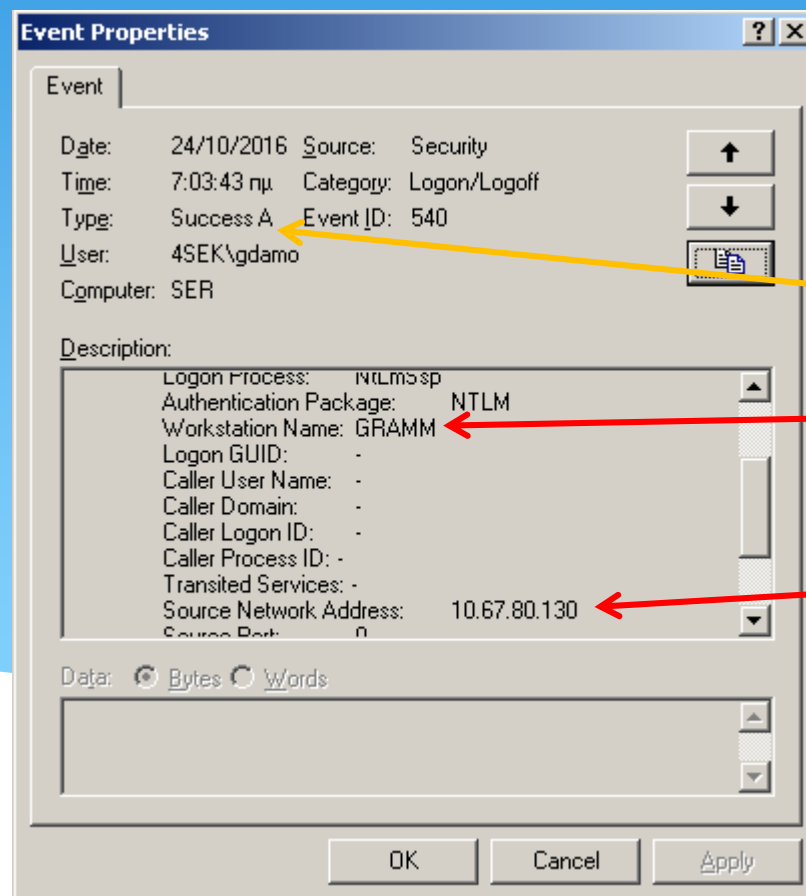
Δικαιώματα
του χρήστη

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (4/6)

Επιτυχής δικτυακή
σύνδεση
του χρήστη



Επιτυχής
Ονομα
Η/Υ του χρήστη

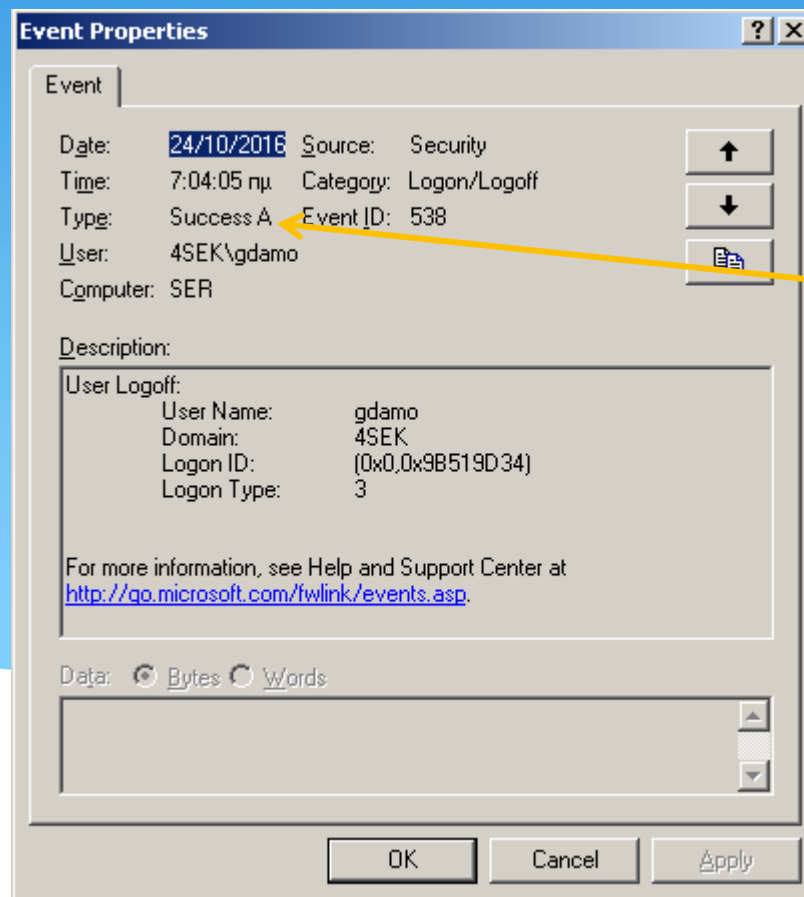
IP διεύθυνση του
Η/Υ του χρήστη

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (5/6)

Προσωρινή
αποσύνδεση
του χρήστη
λόγω
ανενεργούς
δικτυακής
σύνδεσης



Επιτυχής

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Καταλογογράφηση Login/Logoff των Χρηστών (6/6)

Λόγω του μεγάλου πλήθους των σχετικών εγγραφών του Event Viewer δεν είναι εύκολη η συστηματική χρήση αυτού του εργαλείου.

Υπάρχουν εφαρμογές (όχι από την Microsoft, 3rd party software applications) που αναλαμβάνουν την συστηματοποιημένη και εύληπτη ανάδειξη και παρουσίαση των πληροφοριών που μας ενδιαφέρουν.

(π.χ. Ο xxx χρήστης είναι συνδεδεμένος;
Πόσο χρόνο είναι συνδεδεμένος;
Ποια ώρα συνδέθηκε; κ.α.)

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Ενημερωμένο Λειτουργικό Σύστημα.
Updated O.S.

Ενημερωμένα Λειτουργικά
Συστήματα και στον Server και στα
Workstations για την επιδιόρθωση
security Bugs τα οποία οδηγούν σε
vulnerabilities του δικτύου Η/Υ.

Το vulnerability είναι συνδυασμός
τριών στοιχείων:

1. Το Hardware/software του Η/Υ
έχει κάποιο σφάλμα ασφάλειας.
2. Κάποιος κακόβουλος χρήστης
το γνωρίζει.
3. Αυτός ο κακόβουλος χρήστης
έχει την ικανότητα να το
εκμεταλλευθεί.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Anti-Virus Server-Client

1. Τα Client antivirus εγκαθίστανται σε σταθμούς εργασίας και ενημερώνονται από το Server antivirus.

2. Το μέρος του Server antivirus εκτελεί έλεγχο στους σταθμούς εργασίας (σπανιότερα).

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Firewall (Networking)

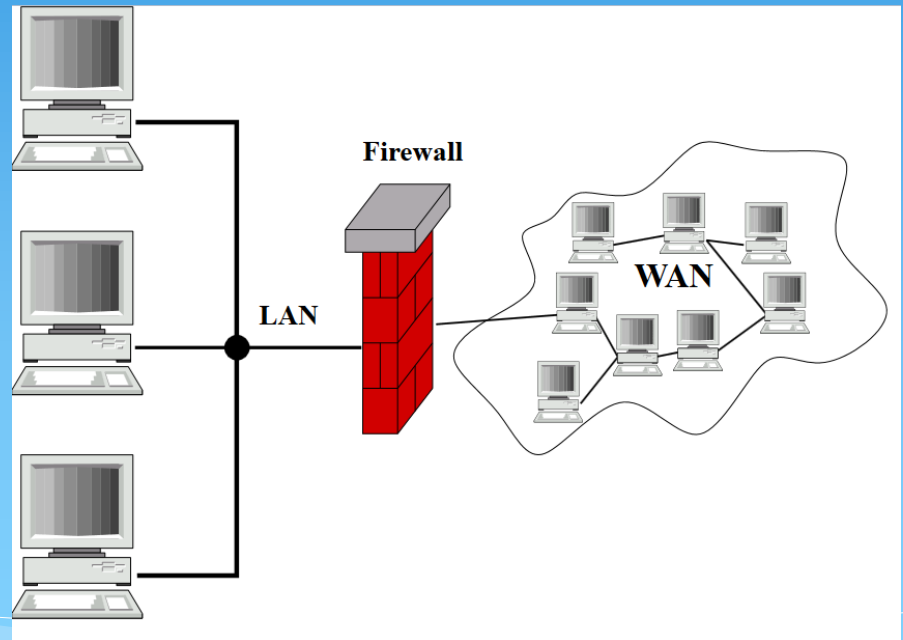
Το τείχος προστασίας είναι ένα λογισμικό που παρακολουθεί την κίνηση του δικτύου εφαρμόζοντας σε κάθε πακέτο δεδομένων ένα σύνολο κανόνων.

Οι κανόνες αποφασίζουν εάν ένα πακέτο μπορεί να περάσει, ή αν θα απορριφθεί.

Συνήθως το τείχος προστασίας τοποθετείται ανάμεσα σε ένα δίκτυο που είναι αξιόπιστο (LAN), και σ' ένα άλλο που είναι λιγότερο αξιόπιστο (INTERNET).

Όταν πρέπει να προστατευθεί ένα μεγάλο δίκτυο, το λογισμικό τείχους προστασίας τρέχει συχνά σε έναν υπολογιστή που δεν κάνει τίποτα άλλο (Hardware-based Firewall).

Το firewall προστατεύει ένα τμήμα του δικτύου από μη εξουσιοδοτημένη πρόσβαση.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks, VPN)

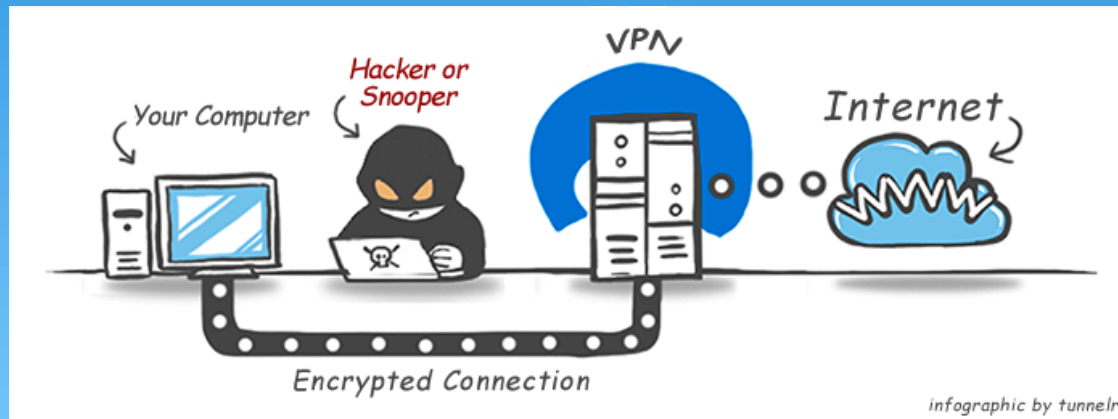
Με τη βοήθεια των
Εικονικών Ιδιωτικών
Δικτύων
δημιουργούμε
ασφαλείς «συνδέσεις»
μεταφοράς δεδομένων
μέσω του ανασφαλούς
Διαδικτύου.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks, VPN)

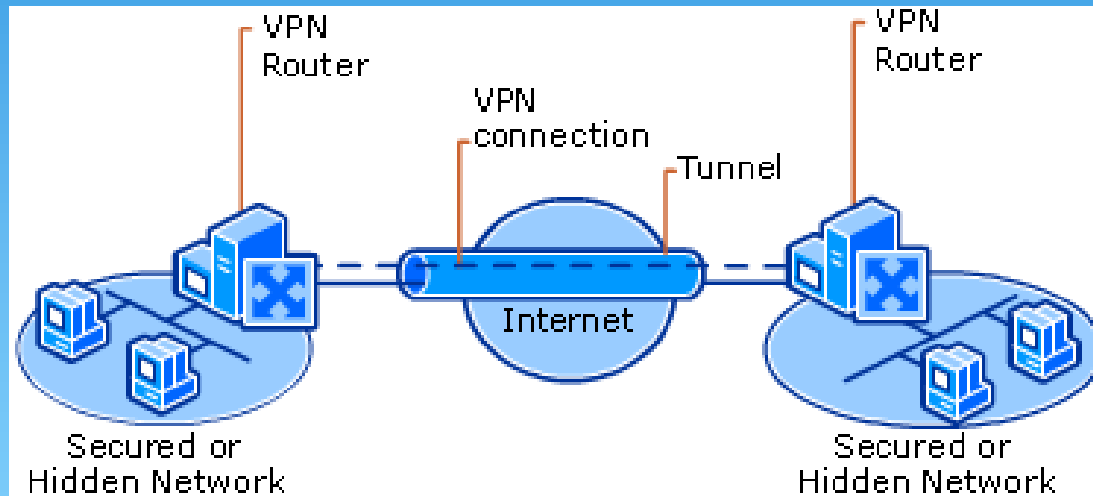


Δημιουργία ασφαλούς όδευσης
(tunnel) με τη χρήση
ισχυρότατης κρυπτογράφησης.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks, VPN) Εταιρικό περιβάλλον (1/2)



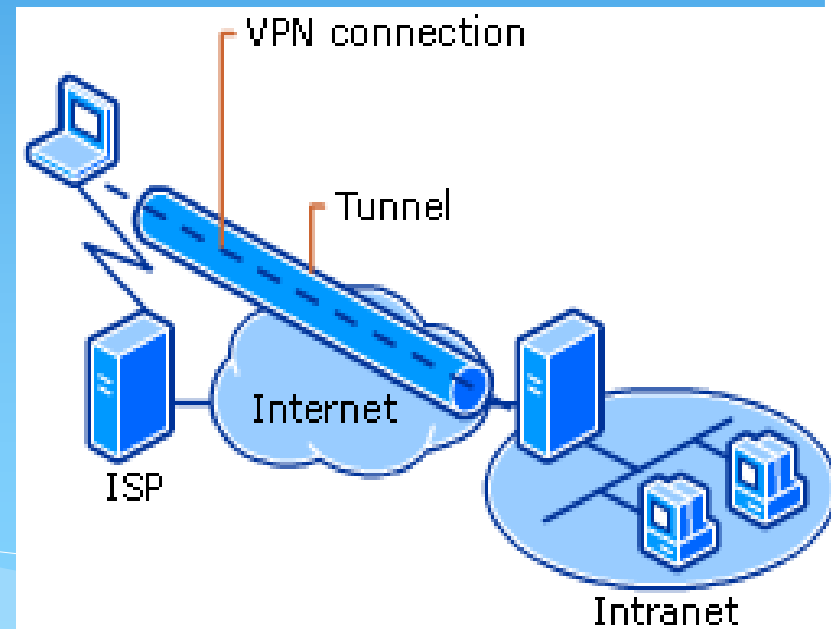
Η εταιρία διασυνδέει ασφαλώς
δύο απομακρυσμένα δίκτυα
Η/Υ μέσω του Διαδικτύου.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks, VPN) Εταιρικό περιβάλλον (2/2)

Απομακρυσμένος
υπάλληλος της εταιρίας
διασυνδέεται ασφαλώς
με το δίκτυο Η/Υ μέσω
του Διαδικτύου.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Έλεγχος της ακεραιότητας και της γνησιότητας των λογισμικών που εγκαθίστανται σε Η/Υ.

Integrity and Authenticity (1/3)

Ο έλεγχος της ακεραιότητας του λογισμικού και της γνησιότητας του δημιουργού αυτού, είναι σημαντικά χαρακτηριστικά που δεν ακολουθούνται ενιαία από όλους.

Η διπλανή εικόνα μας καλύπτει μόνο αν έχουμε αποκτήσει το CD/DVD εγκατάστασης από τον δημιουργό.

Υπάρχει πρόβλημα εάν «κατεβάζουμε» λογισμικό από το διαδίκτυο.

Ακόμα και αν βλέπουμε τη διπλανή εικόνα δεν είναι σίγουρος ο δημιουργός.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Έλεγχος της ακεραιότητας και της γνησιότητας των λογισμικών που εγκαθίστανται σε Η/Υ.

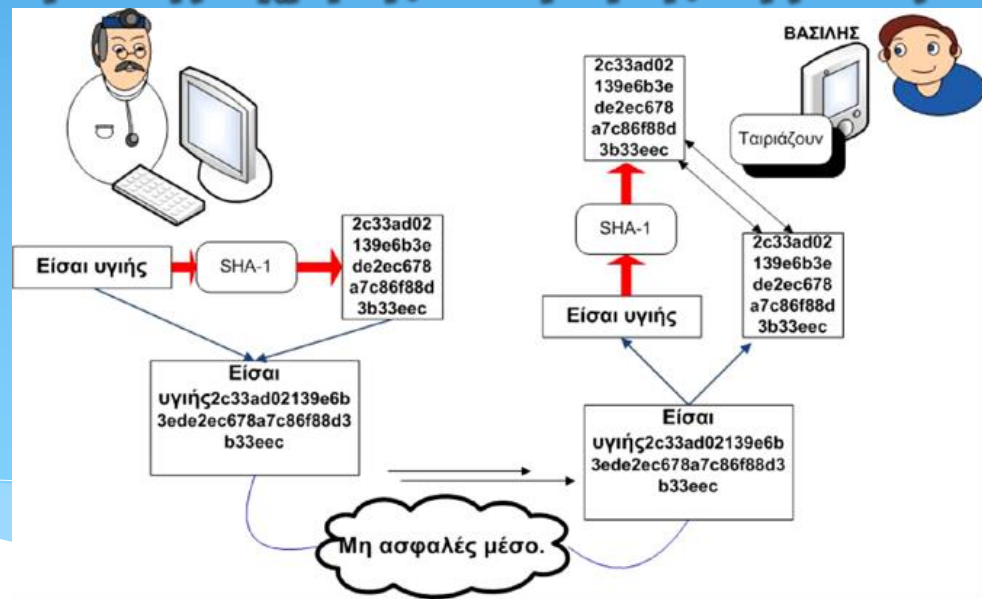
Integrity and Authenticity (2/3)

Ο έλεγχος της ακεραιότητας του λογισμικού και της γνησιότητας του δημιουργού αυτού, είναι σημαντικά χαρακτηριστικά που δεν ακολουθούνται ενιαία από όλους.

Παράδειγμα χρήσης συνάρτησης κερματισμού.

Πρέπει να χρησιμοποιηθούν αλγόριθμοι και συναρτήσεις κερματισμού (π.χ. Secure Hash Algorithm (SHA)) και από τα δύο μέρη.

Η διαδικασία όμως αυτή δεν ακολουθείται από όλους τους δημιουργούς λογισμικού.



Βλέπε εφαρμογή Checksum Utility σε σχέση με το site: <https://www.fosshub.com/qBittorrent.html>.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Έλεγχος της ακεραιότητας και της γνησιότητας των λογισμικών
που εγκαθίστανται σε Η/Υ.

Integrity and Authenticity (3/3)

**Προσοχή!!!! Δεν κρυπτογραφούμε το αποστελλόμενο
αρχείο.**

**Ο αποστολέας του αρχείου με τη χρήση της συνάρτησης
κερματισμού (Hash Function) δημιουργεί μια σύνοψη
μηνύματος (Message Digest) την οποία αποστέλλει μαζί με
το αρχείο.**

**Ο παραλήπτης εφαρμόζει την ίδια συνάρτηση κερματισμού
στο ληφθέν αρχείο και η παραγόμενη σύνοψη μηνύματος
πρέπει να είναι ίδια με την ληφθείσα σύνοψη μηνύματος.**

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (1/37)

Κρυπτογράφηση (Encryption): Η κρυπτογράφηση είναι η διαδικασία με την οποία μετατρέπονται τα αρχικά δεδομένα (*plaintext*) σε μορφή (κρυπτόγραμμα-*ciphertext*) η οποία δεν μπορεί πλέον να γίνει κατανοητή χωρίς να αποκρυπτογραφηθεί.



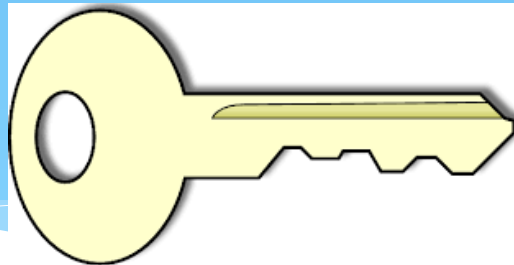
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (2/37)

Η κρυπτογράφηση γίνεται με τη βοήθεια αλγορίθμου, το αποτέλεσμα του οποίου πρέπει να αντιστραφεί ώστε να παράγει ξανά τα αρχικά δεδομένα εισόδου.

Για την κρυπτογράφηση και την αποκρυπτογράφηση χρησιμοποιείται “κλειδί”.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (3/37)

Αποκρυπτογράφηση (Decryption): Προφανώς η αντίστροφη διαδικασία της κρυπτογράφησης. Ο αλγόριθμος δέχεται ως είσοδο τα κρυπτογραφημένα δεδομένα (κρυπτόγραμμα-ciphertext) και με τη βοήθεια του κλειδιού (το οποίο προφανώς είναι διαθέσιμο μόνο σε εξουσιοδοτημένα άτομα) τα μετατρέπει ξανά στα κανονικά δεδομένα (plaintext).



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (4/37)

Κλειδί (Key): Στο πεδίο της κρυπτογράφησης, το κλειδί είναι ένας ψηφιακός κωδικός (ένας αριθμός από bits) ο οποίος χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (5/37)

Συμμετρική Κρυπτογράφηση (1/4)

Εξασφαλίζει μόνο την εμπιστευτικότητα της μεταδιδόμενης πληροφορίας.

Χρησιμοποιείται το ίδιο ακριβώς κλειδί (Secret key) τόσο για την κρυπτογράφηση (plaintext $\rightarrow$ ciphertext) όσο και για την αποκρυπτογράφηση (ciphertext $\rightarrow$ plaintext).

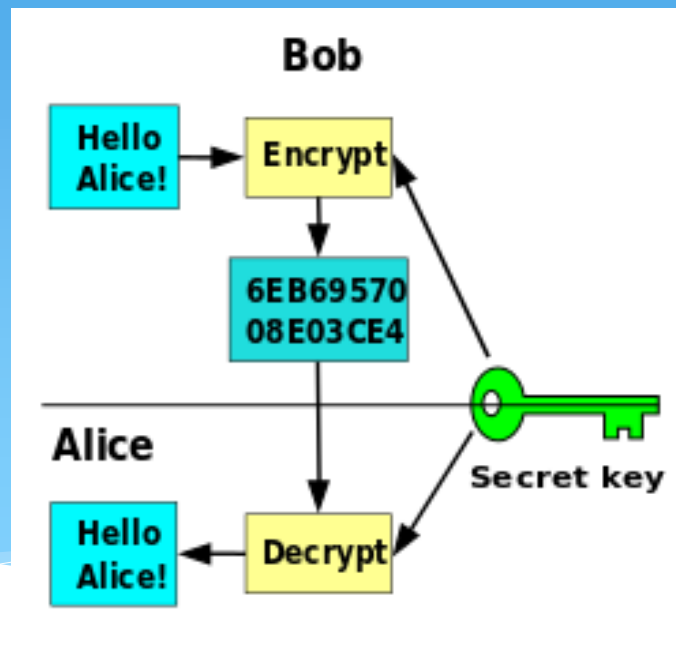
Μυστικό Κλειδί (Secret Key): Ψηφιακός κωδικός που είναι γνωστός και στα δύο μέρη (αλλά μόνο σε αυτά) προκειμένου να τον χρησιμοποιήσουν σε ανταλλαγή δεδομένων με χρήση κρυπτογράφησης / αποκρυπτογράφησης.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (6/37)

Συμμετρική Κρυπτογράφηση (2/4)



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (7/37)

Συμμετρική Κρυπτογράφηση (3/4)

Πρόβλημα

Κατά την αποστολή του Μυστικού Κλειδιού στο
απέναντι άκρο του Καναλιού Επικοινωνίας αυτό
μπορεί να υποκλαπεί.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (8/37)

Συμμετρική Κρυπτογράφηση (4/4)

Μερικοί από τους πιο διαδεδομένους αλγόριθμους συμμετρικής κρυπτογράφησης είναι:

- DES, Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων
- 3DES, Triple DES
- IDEA, International Data Encryption Algorithm, Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων.

Οι παραπάνω αλγόριθμοι δέχονται ως είσοδο μηνύματα μεγέθους 64 bits.
Αν το μήνυμα είναι μεγαλύτερο από 64 bits, θα πρέπει να σπάσει σε κομμάτια των 64 bits.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (9/37)

Ασυμμετρική Κρυπτογράφηση (1/20)

Εξασφαλίζει:

την εμπιστευτικότητα της μεταδιδόμενης πληροφορίας,
ή/και την αυθεντικότητα του αποστολέα.

Η κρυπτογράφηση αυτή χρησιμοποιεί διαφορετικά κλειδιά για την
κρυπτογράφηση και την αποκρυπτογράφηση .



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (10/37)

Ασυμμετρική Κρυπτογράφηση (2/20)

Δημόσιο Κλειδί (Public Key): Το δημόσιο μας κλειδί το γνωρίζει ο καθένας, και συνήθως χρησιμοποιείται για να "κλειδώνει" (κρυπτογραφεί) τα δεδομένα. Όποιος θέλει να μας στείλει κρυπτογραφημένα δεδομένα, χρησιμοποιεί το δημόσιο μας κλειδί για να τα κλειδώσει.

Ιδιωτικό Κλειδί (Private Key): Το ιδιωτικό μας κλειδί που δεν το γνωρίζει κανείς άλλος χρησιμοποιείται για να αποκρυπτογραφεί και να υπογράψει τα δεδομένα.

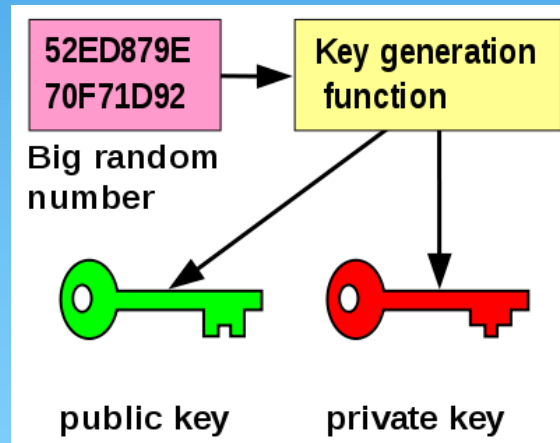
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (11/37)

Ασυμμετρική Κρυπτογράφηση (3/20)

Παραγωγή, στον Η/Υ μας, ζεύγους Δημόσιου/Ιδιωτικού Κλειδιού.



Τα Δημόσια Κλειδιά μεταφορτώνονται σε ειδικούς εξυπηρετητές, τους λεγόμενους **keyservers** όπου μπορεί όποιος θέλει να τα αναζητήσει και να τα ανακτήσει ή το αποστέλουμε μόνο σ' αυτόν με τον οποίο μας ενδιαφέρει να επικοινωνούμε.

Το Ιδιωτικό κλειδί δεν δημοσιεύεται και προστατεύεται συνήθως με κωδικό.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

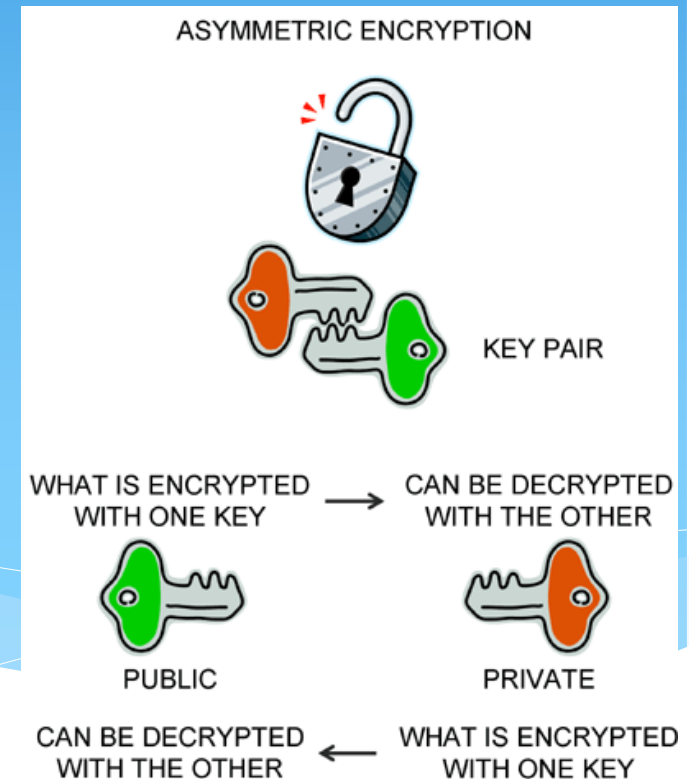
Κρυπτογράφηση\Αποκρυπτογράφηση (12/37)

Ασυμμετρική Κρυπτογράφηση (4/20)

Το δημιουργημένο ζεύγος Δημόσιου/Ιδιωτικού Κλειδιού δρα «συμπληρωματικά».

Ότι κρυπτογραφείται με το Δημόσιο Κλειδί
αποκρυπτογραφείται μόνο από το
αντίστοιχο Ιδιωτικό Κλειδί.

Ότι κρυπτογραφείται με το Ιδιωτικό Κλειδί
αποκρυπτογραφείται μόνο από το
αντίστοιχο Δημόσιο Κλειδί.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (13/37)

Ασυμμετρική Κρυπτογράφηση (5/20)

Όταν κρυπτογραφούμε δεδομένα με το Δημόσιο Κλειδί το οποίο είναι διαθέσιμο σε όλους...



δεν μπορούν να αποκρυπτογραφηθούν με το Δημόσιο Κλειδί.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (14/37)

Ασυμμετρική Κρυπτογράφηση (6/20)

Όταν κρυπτογραφούμε δεδομένα με το Ιδιωτικό Κλειδί...



δεν μπορούν να αποκρυπτογραφηθούν με το Ιδιωτικό Κλειδί.



Αλλα, αυτή η περίπτωση δεν μας ενδιαφέρει.
Το Ιδιωτικό Κλειδί δεν είναι διαθέσιμο στον καθένα.

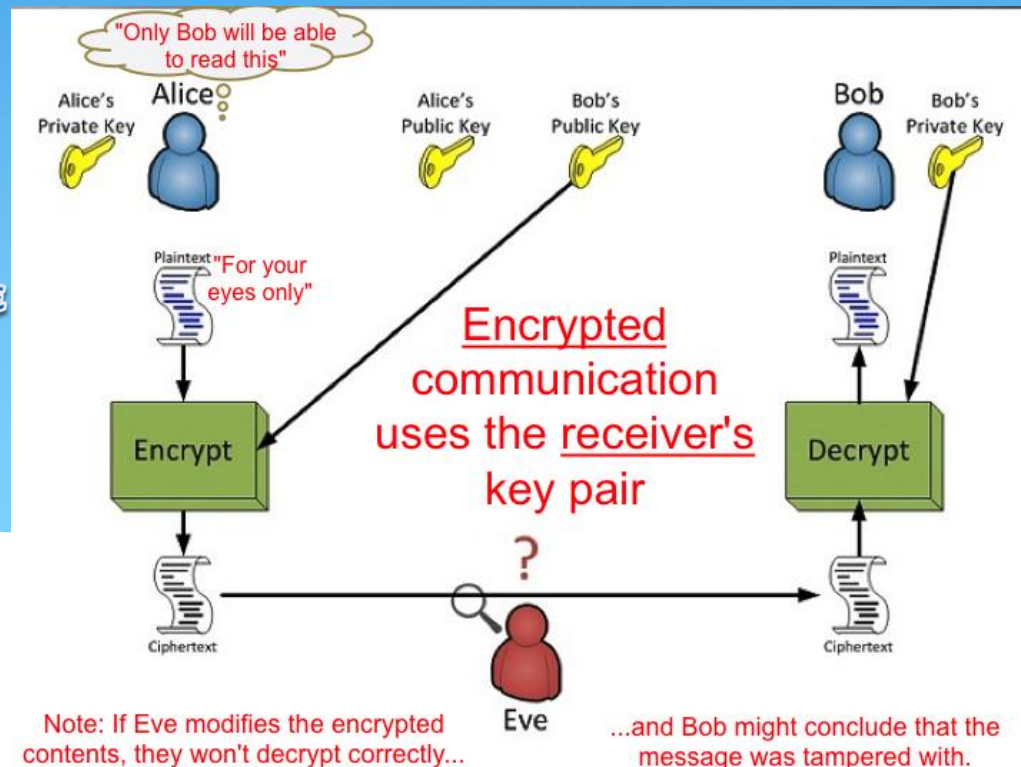
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (15/37)

Ασυμμετρική Κρυπτογράφηση (7/20)

Εμπιστευτικότητα της επικοινωνίας.



Η Alice κρυπτογραφεί τα δεδομένα με το Δημόσιο Κλειδί του Bob και τα στέλνει στον Bob.

Ο Bob λαμβάνει τα κρυπτογραφημένα δεδομένα από την Alice και τα αποκρυπτογραφεί με το Ιδιωτικό του Κλειδί.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

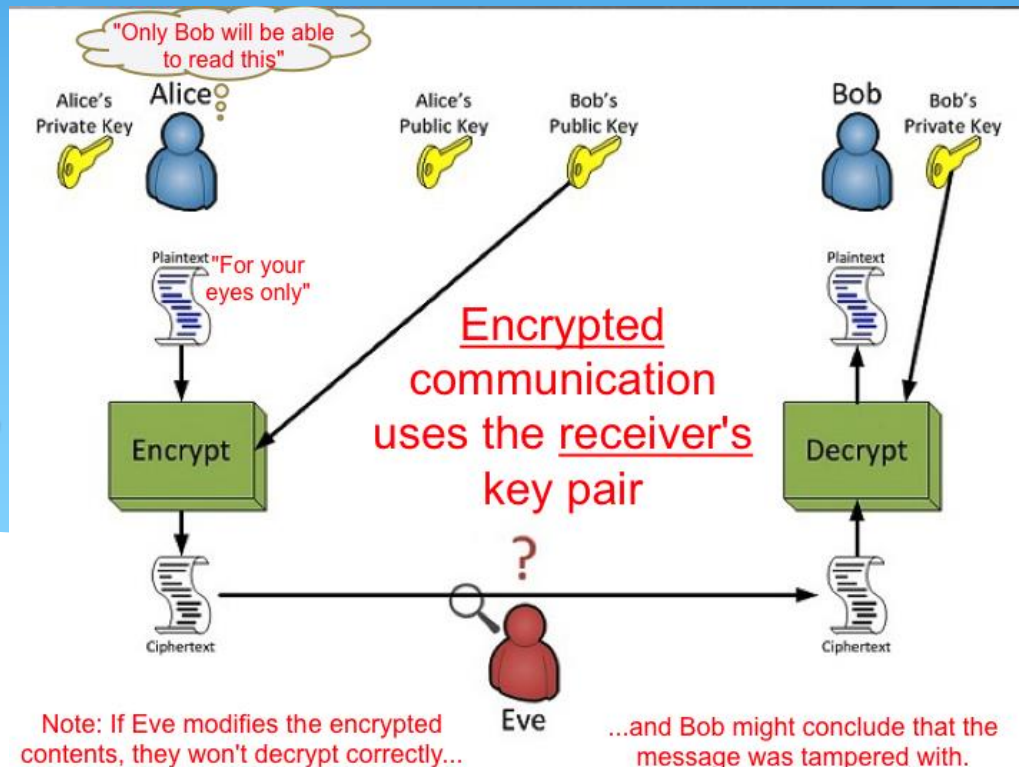
μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (16/37)

Ασυμμετρική Κρυπτογράφηση (8/20)

Εμπιστευτικότητα της επικοινωνίας.

Η Alice είναι σίγουρη ότι τα δεδομένα μπορούν να αποκρυπτογραφηθούν μόνο από τον Bob.



Ο Bob δεν είναι σίγουρος ότι τα κρυπτογραφημένα δεδομένα προέρχονται από την Alice. Οποιοσδήποτε με το δημοσιευμένο Δημόσιο Κλειδί του Bob μπορεί να στείλει τα κρυπτογραφημένα δεδομένα προφασιζόμενος την Alice.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

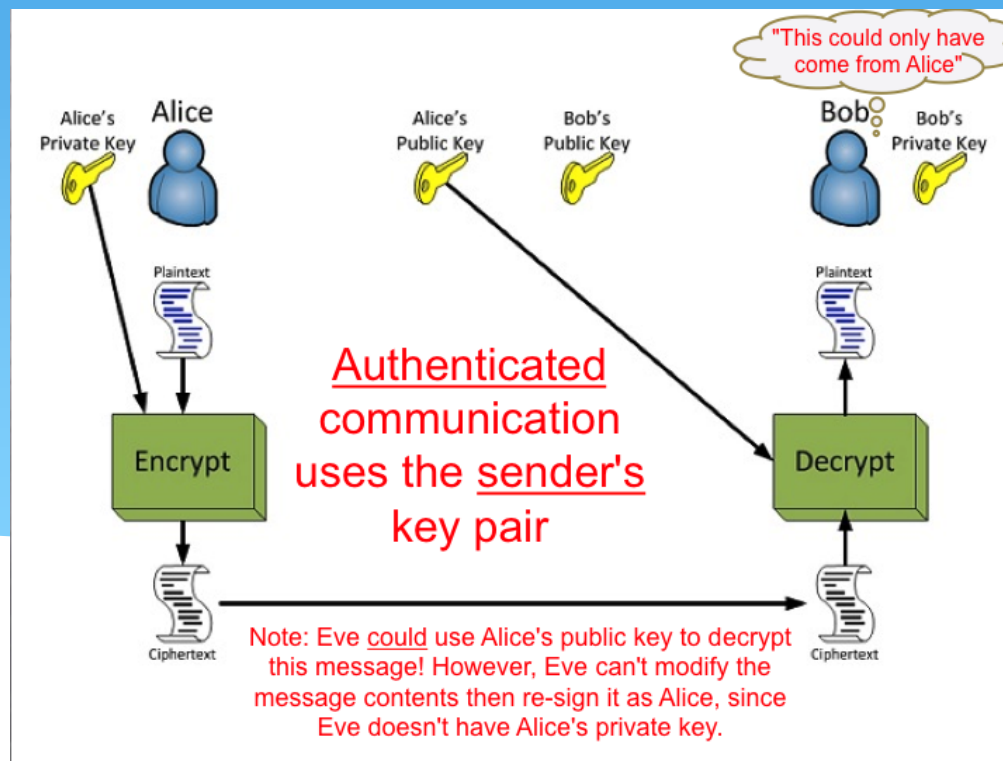
μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (17/37)

Ασυμμετρική Κρυπτογράφηση (9/20)

Αυθεντικότητα της επικοινωνίας.

Η Alice κρυπτογραφεί τα δεδομένα με το Ιδιωτικό της Κλειδί και τα στέλνει στον Bob.



Ο Bob λαμβάνει τα κρυπτογραφημένα δεδομένα από την Alice και τα αποκρυπτογραφεί με το Δημόσιο Κλειδί της Alice.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

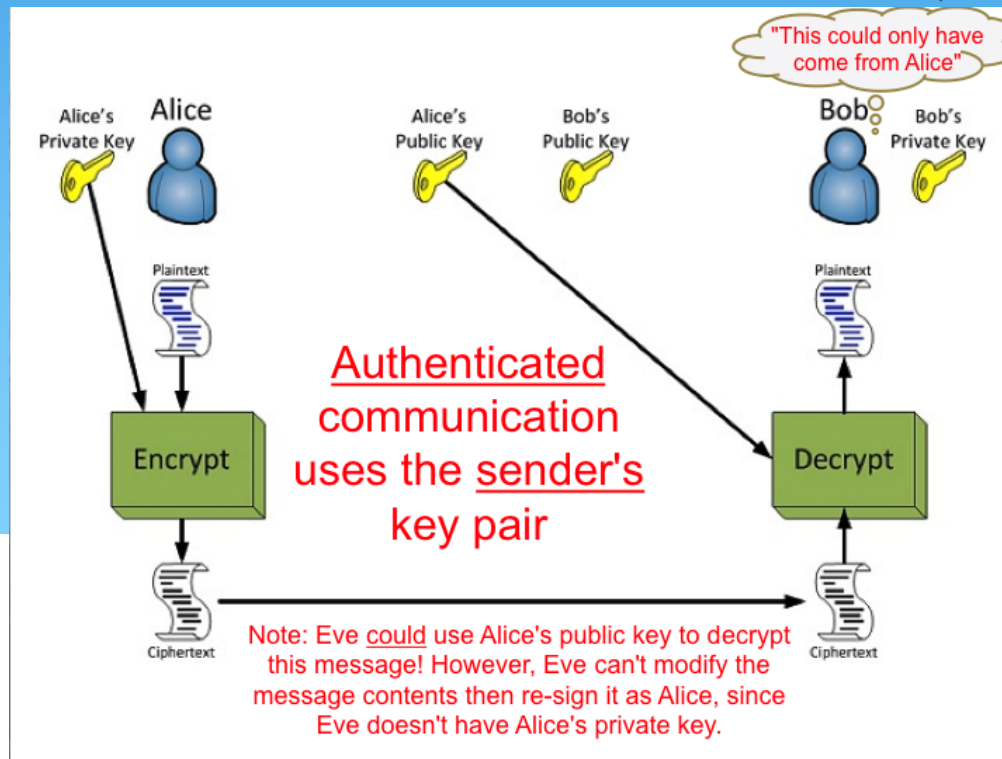
μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (18/37)

Ασυμμετρική Κρυπτογράφηση (10/20)

Αυθεντικότητα της επικοινωνίας.

Η Alice δεν είναι σίγουρη ότι τα δεδομένα της δεν θα αποκρυπτογραφηθούν από κάποιον άλλο αφού το Δημόσιο Κλειδί της είναι δημοσιευμένο.



Ο Bob είναι σίγουρος ότι τα κρυπτογραφημένα δεδομένα προέρχονται από την Alice.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (19/37)

Ασυμμετρική Κρυπτογράφηση (11/20) [Ψηφιακή Υπογραφή (1/7)]

Πλευρά Alice

Ιδιωτικό Κλειδί της Alice

Q2uBfGRau6/XJyZhcF5abo7b37I5hr3EmwGykdyk8G

Μήνυμα

The quick
brown fox
jumps over
the lazy
dog.

Συνάρτηση
κερματισμού

SHA-1

Σύνοψη
Μηνύματος

21a57f2fe76
5e1ae4a8bf1
5d73fc1bf2a
533f547f234
3d12a499d9

Αλγόριθμος
κρυπτογράφησης

crypto

Ψηφιακή
Υπογραφή

MIIB6gYJKoZIhvc
NAQcColIB2zCCA
dcCAQExCzAIBgU
rDgMCGgUAMAs
GCSqGSib3
DQEHATGCAbYwg
gGyAgEBMIGcMIG
GEwJVUzEOMAw

Βήμα 1: Παραγωγή Σύνοψης Μηνύματος.

Βήμα 2: Κρυπτογράφηση της Σύνοψης Μηνύματος με το Ιδιωτικό Κλειδί για την παραγωγή της Ψηφιακής Υπογραφής.

Βήμα 3: Αποστολή Μηνύματος και Ψηφιακής Υπογραφής στον Bob.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (20/37)

Ασυμμετρική Κρυπτογράφηση (12/20) Ψηφιακή Υπογραφή (2/7)

Κανάλι Επικοινωνίας



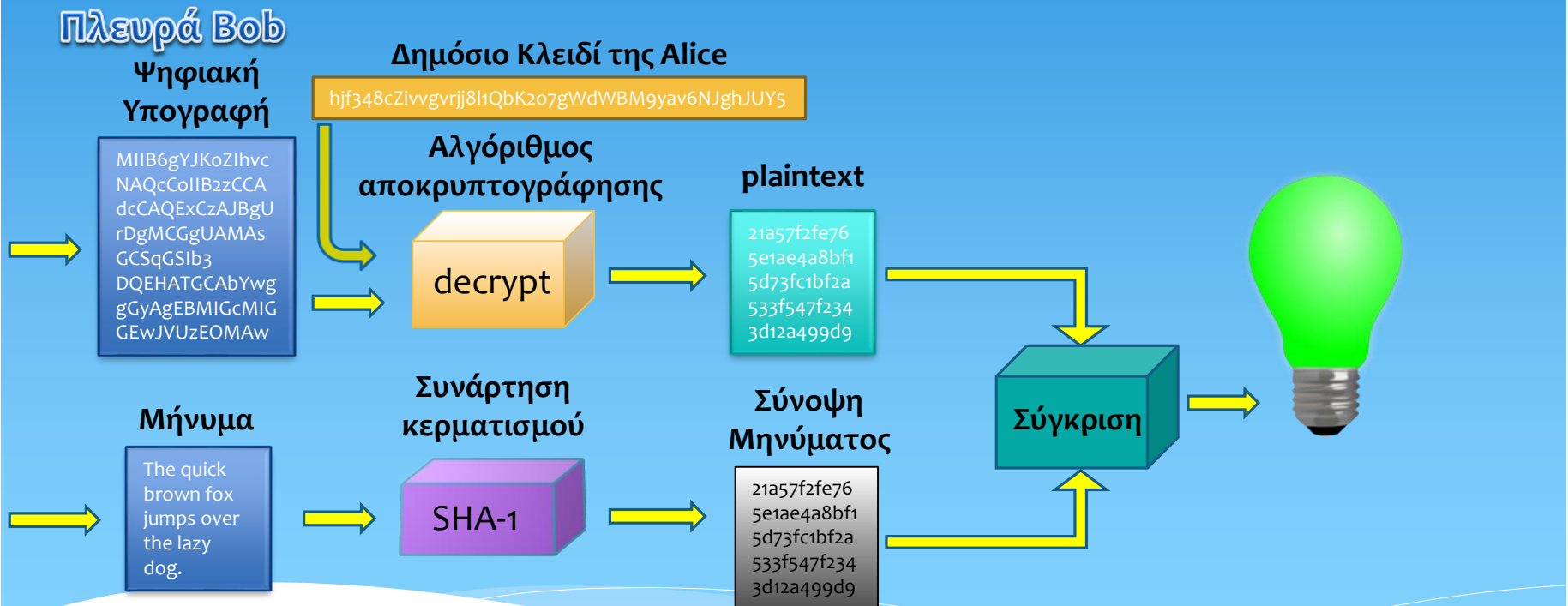
Κανείς δεν παρενοχλεί την επικοινωνία.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (21/37)

Ασυμμετρική Κρυπτογράφηση (13/20) Ψηφιακή Υπογραφή (3/7)



Βήμα 4: Ο Bob, με το Δημόσιο Κλειδί της Alice, αποκρυπτογραφεί την Ψηφιακή Υπογραφή και αναδεικνύει την ληφθείσα Σύνοψη του Μηνύματος.

Βήμα 5: Παραγωγή Σύνοψης Μηνύματος από το ληφθέν Μήνυμα.

Βήμα 6: Σύγκριση των δύο Συνόψεων Μηνύματος.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (22/37)

Ασυμμετρική Κρυπτογράφηση (14/20) Ψηφιακή Υπογραφή (4/7)

Κανάλι Επικοινωνίας

Μήνυμα

The quick
brown fox
jumps over
the lazy
dog.



Τροποποιημένο
Μήνυμα

The quick
brown fox
jumps over
the lazy
hound.

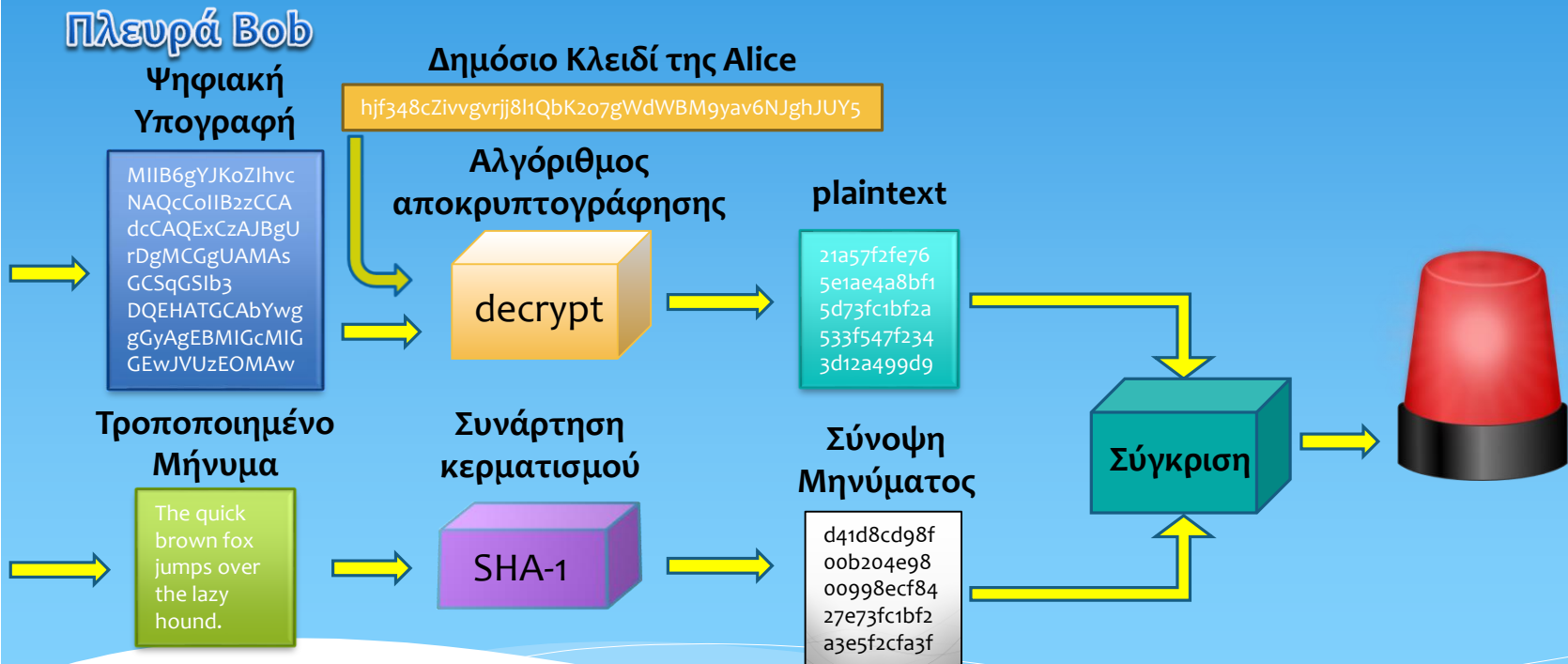
Ο κακός παρενοχλεί την επικοινωνία
τροποποιώντας το μη κρυπτογραφημένο μήνυμα (plaintext).

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (23/37)

Ασυμμετρική Κρυπτογράφηση (15/20) Ψηφιακή Υπογραφή (5/7)



Βήμα 4: Ο Bob, με το Δημόσιο Κλειδί της Alice, αποκρυπτογραφεί την Ψηφιακή Υπογραφή και αναδεικνύει την ληφθείσα Σύνοψη του Μηνύματος.

Βήμα 5: Παραγωγή Σύνοψης Μηνύματος από το ληφθέν Τροποποιημένο Μήνυμα.

Βήμα 6: Σύγκριση των δύο Συνόψεων Μηνύματος.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (24/37)

Ασυμμετρική Κρυπτογράφηση (16/20) Ψηφιακή Υπογραφή (6/7)

Μέχρι τώρα έχουμε καταδείξει ότι εξασφαλίσθηκαν τα εξής:

Ακεραιότητα του Μηνύματος (Integrity).

Εάν ο κακός τροποποιήσει το Μήνυμα (plaintext),
οι δύο Συνόψεις του Μηνύματος θα είναι διαφορετικές.

Δεν διανοείται ο κακός να προσπαθήσει
να τροποποιήσει τη Ψηφιακή Υπογραφή (ciphertext).

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (25/37)

Ασυμμετρική Κρυπτογράφηση (17/20) Ψηφιακή Υπογραφή (7/7)

Μέχρι τώρα έχουμε καταδείξει ότι εξασφαλίσθηκαν τα εξής:

Αυθεντικότητα & Μη Αρνηση Ταυτότητας του αποστολέα του Μηνύματος (Authentication & Non Repudiation).

Αφού χρησιμοποιούμε το Δημόσιο Κλειδί της Alice για να αποκρυπτογραφήσουμε την ληφθείσα Σύνοψη του Μηνύματός της είμαστε σίγουροι για την Αυθεντικότητα του αποστολέα.

Η Alice δεν Μπορεί να Αρνηθεί την Ψηφιακή της Υπογραφή (Ταυτότητα).
Κανείς άλλος δεν κατέχει το Ιδιωτικό της Κλειδί για να κρυπτογραφήσει τη Σύνοψη του Μηνύματός της

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (26/37)

Ασυμμετρική Κρυπτογράφηση (18/20)

Πρόβλημα

Ο κακός δεν έχει τη δυνατότητα να αλλάξει το περιεχόμενο του Μηνύματος της Alice

αλλά μπορεί να το διαβάσει!!!!!!

Δεν ισχύει η Εμπιστευτικότητα του Μηνύματος (Confidentiality).

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (27/37)

Λύση Ασυμμετρική Κρυπτογράφηση (19/20)

Μια πιθανή λύση είναι η κρυπτογράφηση του Μηνύματος και της Ψηφιακής Υπογραφής της Alice με το Δημόσιο Κλειδί του Bob.

Ο Bob τα αποκρυπτογραφεί με το Ιδιωτικό του Κλειδί και ακολουθείται η διαδικασία που παρουσιάστηκε πριν.

Είναι πιθανόν, στη πράξη, να πρόκυψη πρόβλημα αποκρυπτογράφησης που σχετίζεται με την πολυπλοκότητα του Ιδιωτικού Κλειδιού της Alice και του Δημοσίου Κλειδιού του Bob.

Προσοχή!!!. Η Σύνοψη Μηνύματος της Alice κρυπτογραφείται πρώτα με το Ιδιωτικό Κλειδί της Alice και μετά, στα πλαίσια αυτής της λύσης, κρυπτογραφείται με το Δημόσιο Κλειδί του Bob.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (28/37)

Ασυμμετρική Κρυπτογράφηση (20/20)

Μερικοί από τους πιο διαδεδομένους αλγόριθμους ασυμμετρικής κρυπτογράφησης είναι:

- RSA (Rivest, Shamir, and Adleman)
- DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm
- ElGamal

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (29/37)

Η συμμετρική κρυπτογράφηση:

Δεν απαιτεί μεγάλη υπολογιστική ισχύ.

Χρησιμοποιείται συνήθως για κρυπτογράφηση αρχείων μεγάλου όγκου δεδομένων.

Υπάρχει πρόβλημα στην αποστολή του Μυστικού Κλειδιού.

Η ασυμμετρική κρυπτογράφηση:

Απαιτεί μεγάλη υπολογιστική ισχύ.

Δεν υπάρχει πρόβλημα στην διανομή του Δημόσιου Κλειδιού.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (30/37)

Ψηφιακά Πιστοποιητικά (1/8)

**Αλλά ποια είναι αυτή η Alice που λέει
ότι είναι η Alice;;;;;**

Είναι υπαρκτό φυσικό ή νομικό πρόσωπο;;;;;;;;;;

Προσοχή!!!! Δεν αμφισβητούμε ότι το μήνυμα προέρχεται από την Alice και ότι δεν έχει αλλοιωθεί, αλλά αυτά που γράφει η Alice μπορεί να μην ισχύουν καθώς η πραγματική της ταυτότητα δεν είναι γνωστή.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (31/37)

Ψηφιακά Πιστοποιητικά (2/8)

Η Ψηφιακή Υπογραφή της Alice μας πιστοποιεί ότι το μήνυμα το έστειλε η Alice αφού μπορώ να το αποκρυπτογραφήσω με το Δημόσιο Κλειδί αυτής.

Αλλά δεν ξέρουμε τίποτα για την πραγματική της ταυτότητα και τις επιδιώξεις της

Η Alice μπορεί να παραγάγει όσα δικά της Δημόσια Κλειδιά θέλει.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (32/37)

Ψηφιακά Πιστοποιητικά (3/8)

Ετσι τίθεται το ζήτημα της ύπαρξης μιας (ή περισσότερων) Ανεξάρτητων και Επίσημων Αρχών που θα αναλάβουν να πιστοποιούν τα Δημόσια Κλειδιά των φυσικών ή νομικών προσώπων.

Certificate Authority - CA

Δηλαδή αυτές οι Αρχές εκδίδουν Ψηφιακά Πιστοποιητικά για αυτά τα πρόσωπα.

Ετσι η Alice δεν είναι μια άυλη υπόσταση του Διαδικτύου αλλά μια οντότητα που μπορούμε να βρούμε να χρειασθεί.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (33/37)

Ψηφιακά Πιστοποιητικά (4/8)

Δηλαδή τα Ψηφιακά Πιστοποιητικά είναι ηλεκτρονικά έγγραφα τα οποία συνδέουν ένα δημόσιο κλειδί με μια ταυτότητα, δηλαδή πληροφορίες για το άτομο ή τον οργανισμό στον οποίο ανήκει το κλειδί.

Προσοχή!!!!!! Η CA δεν συμμετέχει στην επικοινωνία της Alice με του Bob, απλώς πιστοποιεί την ταυτότητα της Alice.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (34/37)

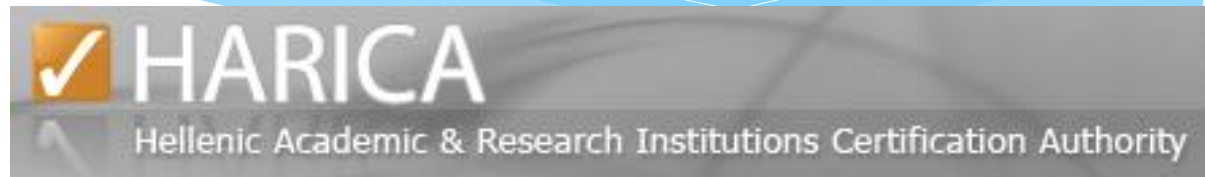
Ψηφιακά Πιστοποιητικά (5/8)



Αυτές οι Αρχές μπορεί να είναι
αλλά και

Ιδιωτικές

Δημόσιες.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (35/37)

Ψηφιακά Πιστοποιητικά (6/8) Αρχή λειτουργίας.

1. Η CA δημιουργεί ένα δικό της set Δημόσιου και Ιδιωτικού Κλειδιού.
2. Η CA φυλάσσει το Ιδιωτικό της Κλειδί στη βάση δεδομένων της.
3. Η CA ενσωματώνει το Δημόσιο Κλειδί της (υπό μορφή Ψηφιακού Πιστοποιητικού) στους διαφόρους browsers.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (36/37)

Ψηφιακά Πιστοποιητικά (7/8) Αρχή λειτουργίας.

1. Ένα eshop θέλει να πιστοποιηθεί από τη CA. Δημιουργεί ένα δικό του set Δημόσιου και Ιδιωτικού Κλειδιού. Το Ιδιωτικό Κλειδί αποθηκεύεται τοπικά.
2. Το Δημόσιο Κλειδί μαζί με την ταυτότητα του eshop αποστέλλεται στην CA.



3. Η CA παράγει μια σύνοψη για το eshop με το δικό της Ιδιωτικό Κλειδί (Ψηφιακή Υπογραφή) την οποία προσθέτει στο Δημόσιο Κλειδί από το eshop.
4. Αυτό το Ψηφιακά Υπογεγραμμένο Δημόσιο Κλειδί επιστρέφεται στο eshop.

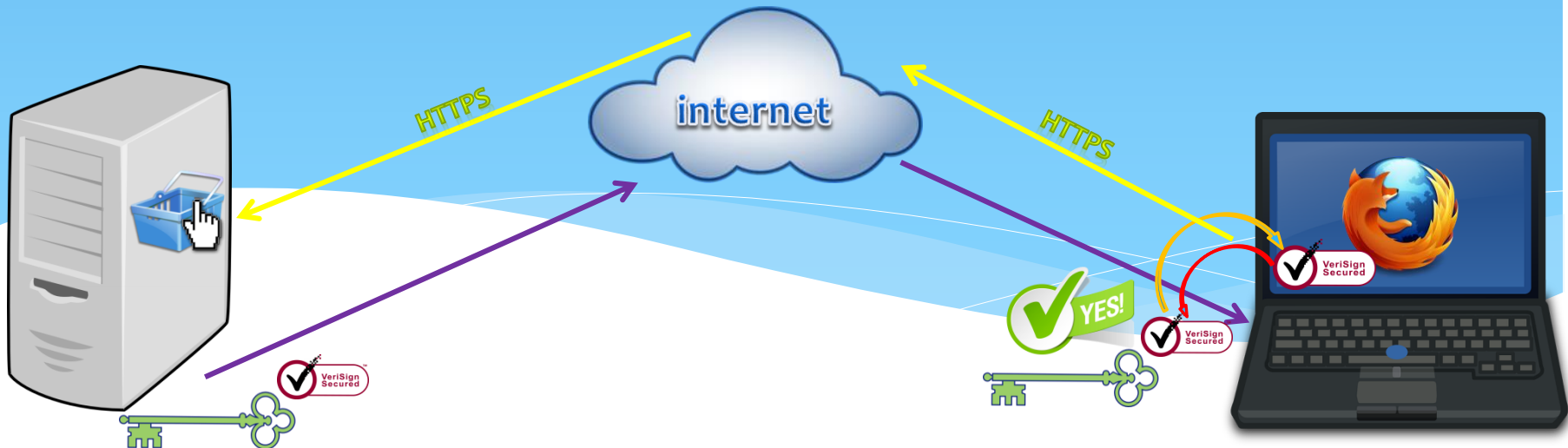
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Κρυπτογράφηση\Αποκρυπτογράφηση (37/37)

Ψηφιακά Πιστοποιητικά (8/8) Αρχή λειτουργίας.

1. Ένας αγοραστής από τον Η/Υ του, επικοινωνεί με το eshop για αγορές μέσω του https.
2. Από το eshop αποστέλλεται το Ψηφιακά Υπογεγραμμένο Δημόσιο Κλειδί στον Η/Υ του αγοραστή.
3. Όταν παραληφθεί αυτό, ελέγχεται με το εγκατεστημένο Ψηφιακό Πιστοποιητικό από την CA, επαληθεύοντας τη σύνοψη που έχει παραχθεί με το Ιδιωτικό Κλειδί της CA και έχει επισυναφθεί στο Δημόσιο Κλειδί του eshop.

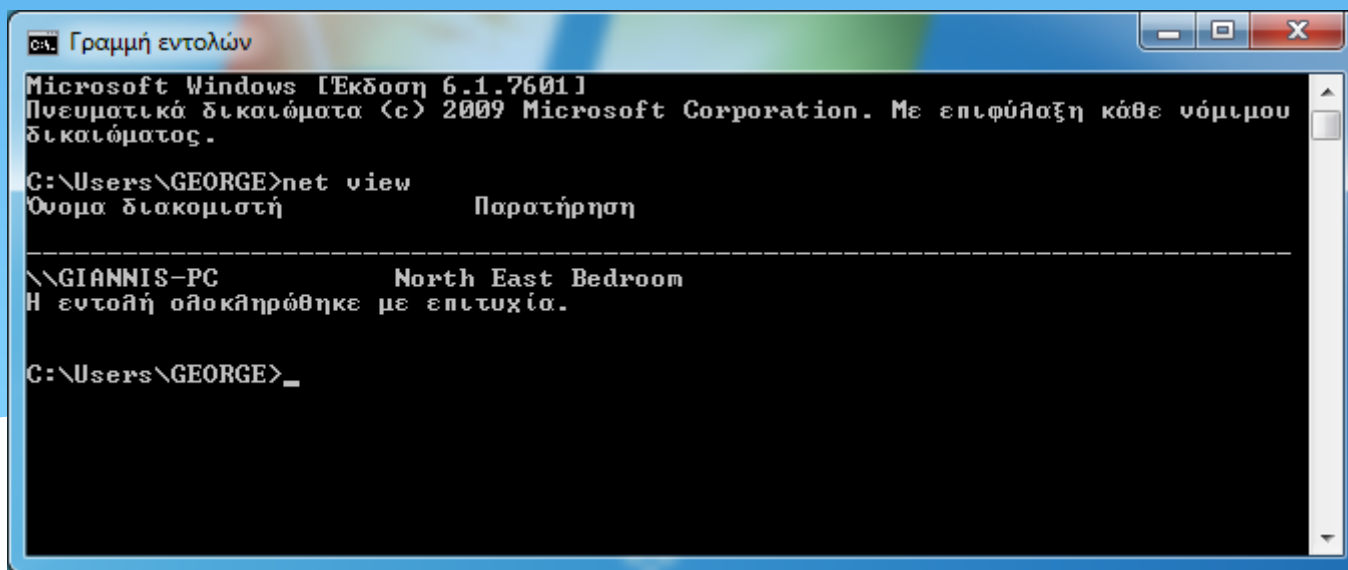


ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Δικτυακές εντολές σε περιβάλλον cmd. (1/4)
net view (1/2)

Με τη χρήση αυτής της εντολής μπορούμε να
δούμε τα ονόματα (και την περιγραφή) των
υπολογιστών του δικτύου μας που «τρέχουν»
Λ.Σ. Windows.



```
cmd. Γραμμή εντολών
Microsoft Windows [Έκδοση 6.1.7601]
Πνευματικά δικαιώματα (c) 2009 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου
δικαιώματος.

C:\Users\GEORGE>net view
Όνομα διακομιστή          Παρατήρηση
-----
\\GIANNIS-PC              North East Bedroom
Η εντολή ολοκληρώθηκε με επιτυχία.

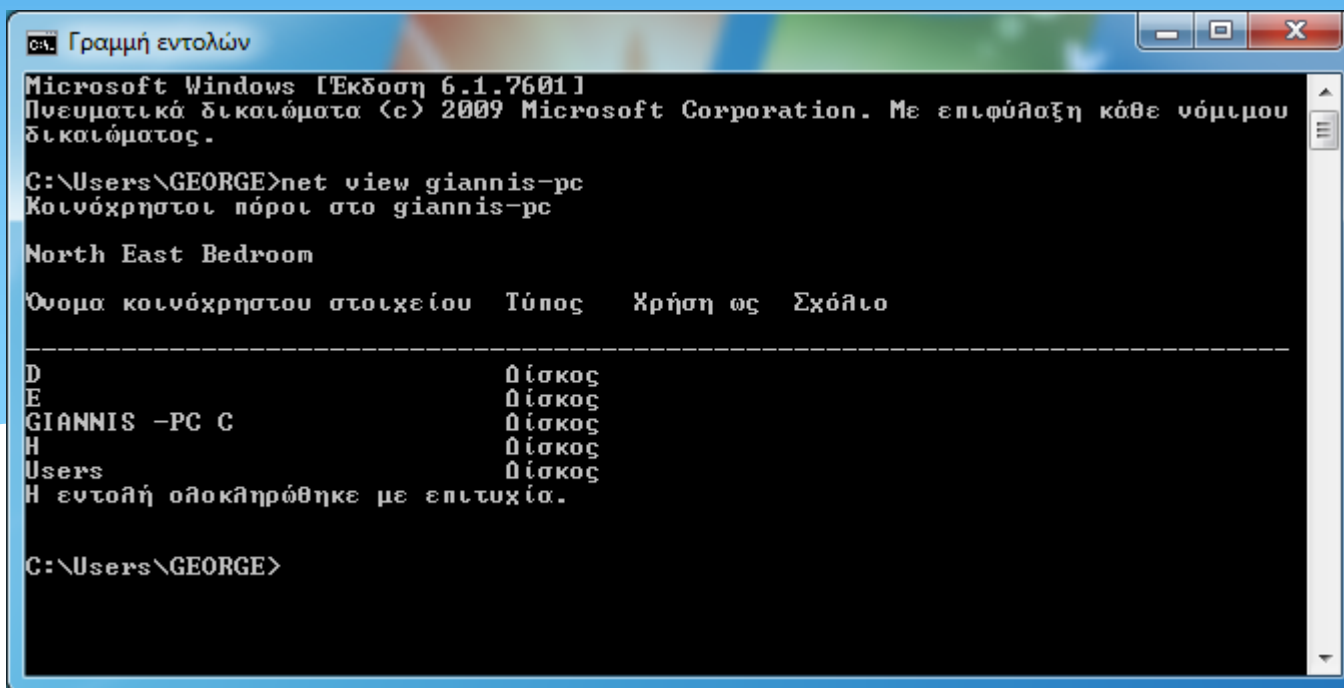
C:\Users\GEORGE>_
```

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Δικτυακές εντολές σε περιβάλλον cmd. (2/4)
net view (2/2)

Με τη χρήση της ίδιας εντολής παραθέτοντας και το όνομα του υπολογιστή μπορούμε να δούμε τα τυχόν κοινόχρηστα στοιχεία (φάκελοι ,αρχεία) αυτού του υπολογιστή.



```
C:\> Γραμμή εντολών

Microsoft Windows [Έκδοση 6.1.7601]
Πνευματικά δικαιώματα (c) 2009 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου
δικαιώματος.

C:\Users\GEORGE>net view giannis-pc
Κοινόχρηστοι πόροι στο giannis-pc

North East Bedroom

Όνομα κοινόχρηστου στοιχείου  Τύπος  Χρήση ως  Σχόλιο
-----
D                               Δίσκος
E                               Δίσκος
GIANNIS -PC C                   Δίσκος
H                               Δίσκος
Users                           Δίσκος
Η εντολή ολοκληρώθηκε με επιτυχία.

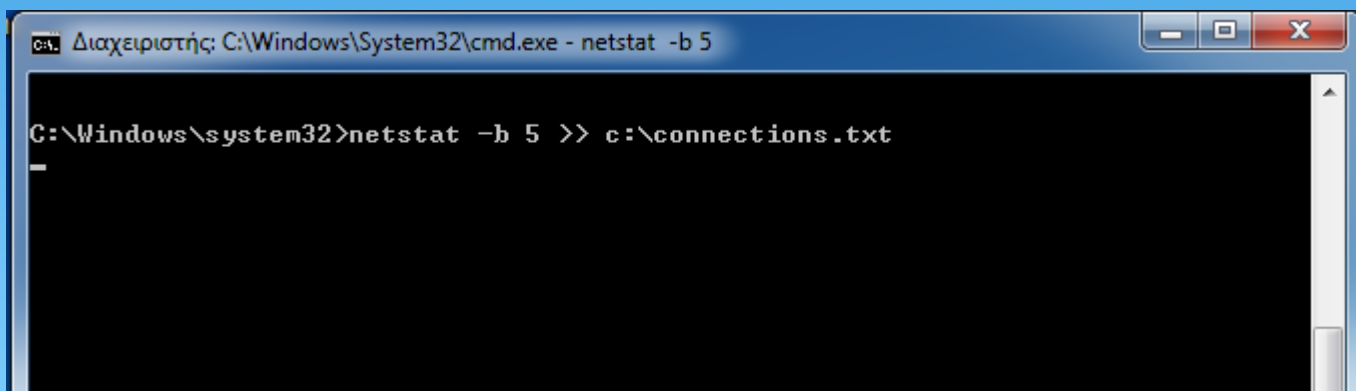
C:\Users\GEORGE>
```

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Δικτυακές εντολές σε περιβάλλον cmd. (3/4)
netstat -b (1/2)

Ανοίγουμε με διαχειριστικά δικαιώματα το Command Prompt και εισάγουμε την εντολή όπως φαίνεται:



```
Διαχειριστής: C:\Windows\System32\cmd.exe - netstat -b 5

C:\Windows\system32>netstat -b 5 >> c:\connections.txt
-
```

Η εντολή αυτή, κάθε 5 sec, εγγράφει στο αρχείο connections.txt ποια προγράμματα του Η/Υ επικοινωνούν μέσω δικτύου.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Δικτυακές εντολές σε περιβάλλον cmd. 4/4)
netstat -b (2/2)

Ανοίγοντας το αρχείο μπορούμε να δούμε ποια προγράμματα επικοινωνούν μέσω δικτύου.

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	192.168.1.100:2924 [msfeedssync.exe]	204.245.162.25:80	ESTABLISHED	2104
TCP	192.168.1.100:2558 c:\windows\system32\WS2_32.dll C:\WINDOWS\system32\WININET.dll [svchost.exe]	207.68.172.236:80	CLOSE_WAIT	1684
TCP	192.168.1.100:2916 [Dreamweaver.exe]	204.14.90.25:21	CLOSE_WAIT	2144

Έτσι μπορούμε να εντοπίσουμε ένα πιθανό πρόγραμμα τύπου malware.

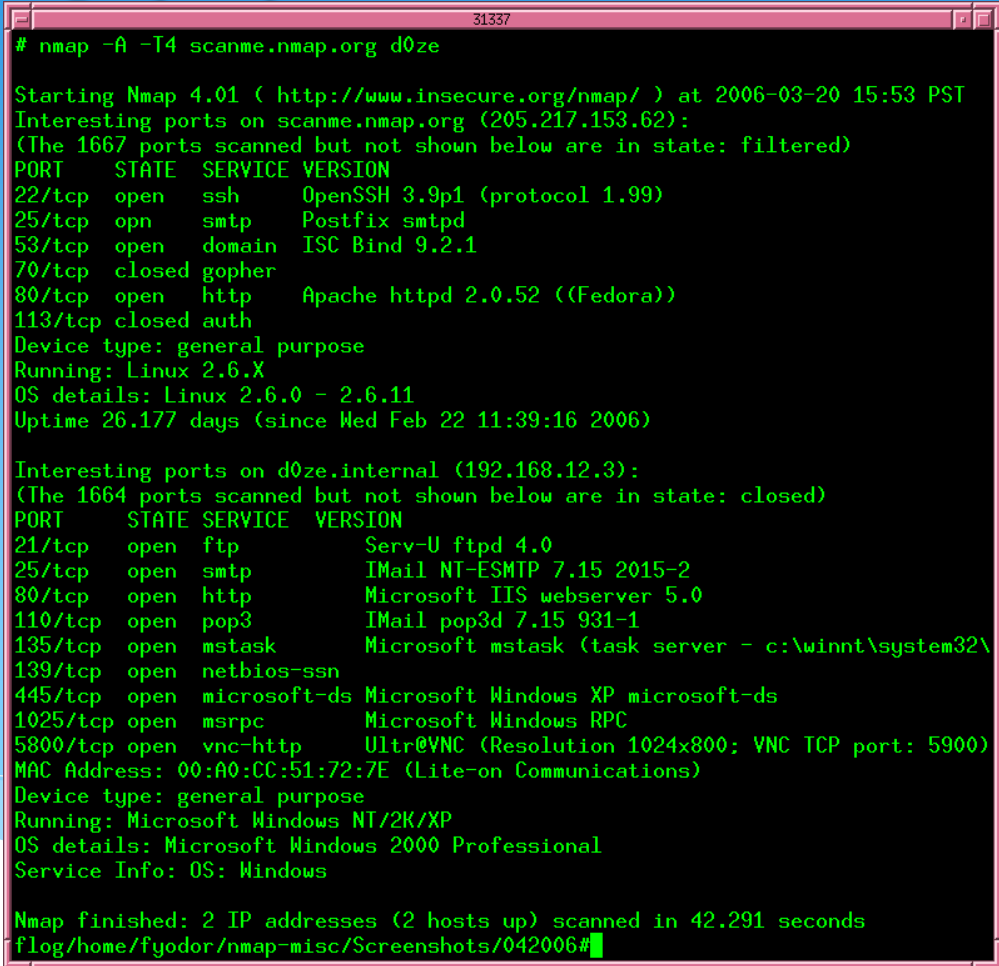
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Nmap (1/7)

Το Nmap είναι μια εφαρμογή
(Command Line Interface)
ελέγχου δικτύων Η/Υ.
Χρησιμοποιεί τα IP πακέτα
έτσι ώστε:

να ανακαλύψει τις συσκευές
που είναι σε λειτουργία στο
δίκτυο,
τον τύπο του λειτουργικού
συστήματος που τρέχουν,
τις ενεργές υπηρεσίες αυτών,
εάν υπάρχει firewall κ.α.



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    opn   smtp      Postfix smtpd
53/tcp    open  domain    ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http      Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       Serv-U ftpd 4.0
25/tcp    open  smtp      IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http      Microsoft IIS webserver 5.0
110/tcp   open  pop3      IMail pop3d 7.15 931-1
135/tcp   open  mstask     Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc      Microsoft Windows RPC
5800/tcp  open  vnc-http   Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

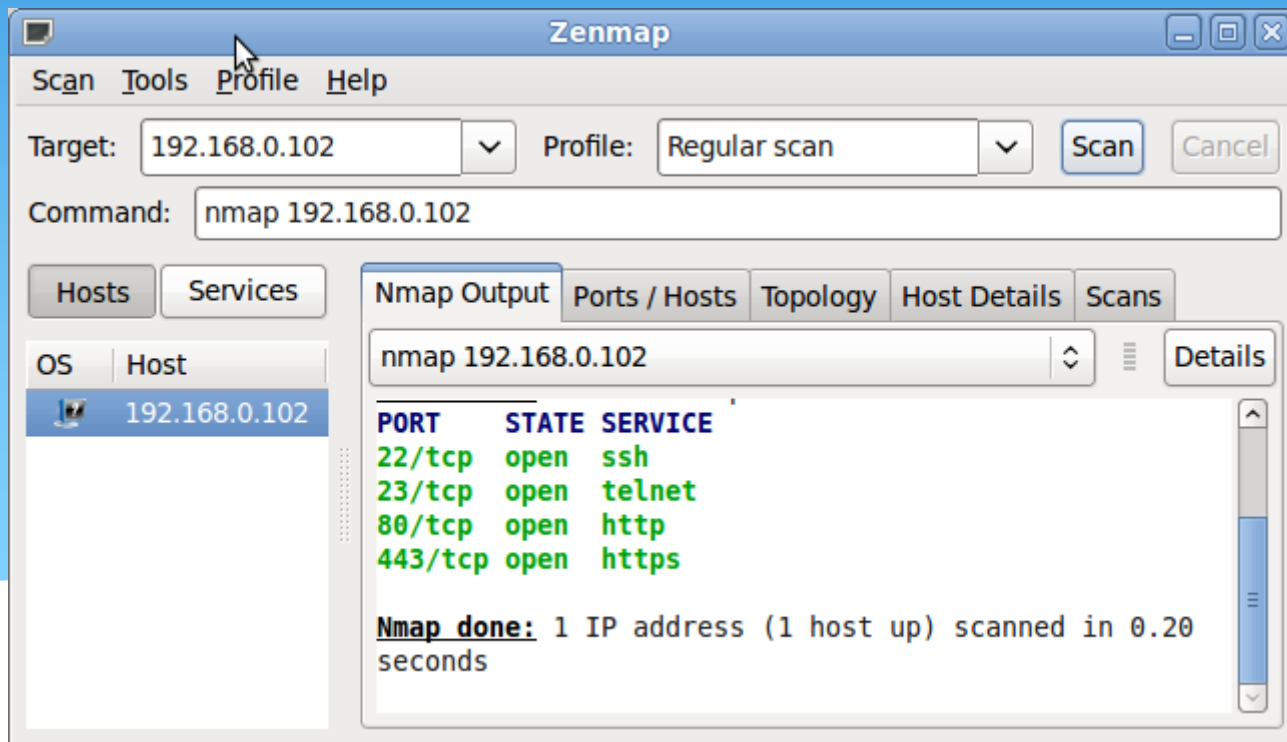
Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (2/7)

Το Zenmap είναι η παραθυρική (Graphical User Interface) εκδοχή του Nmap.

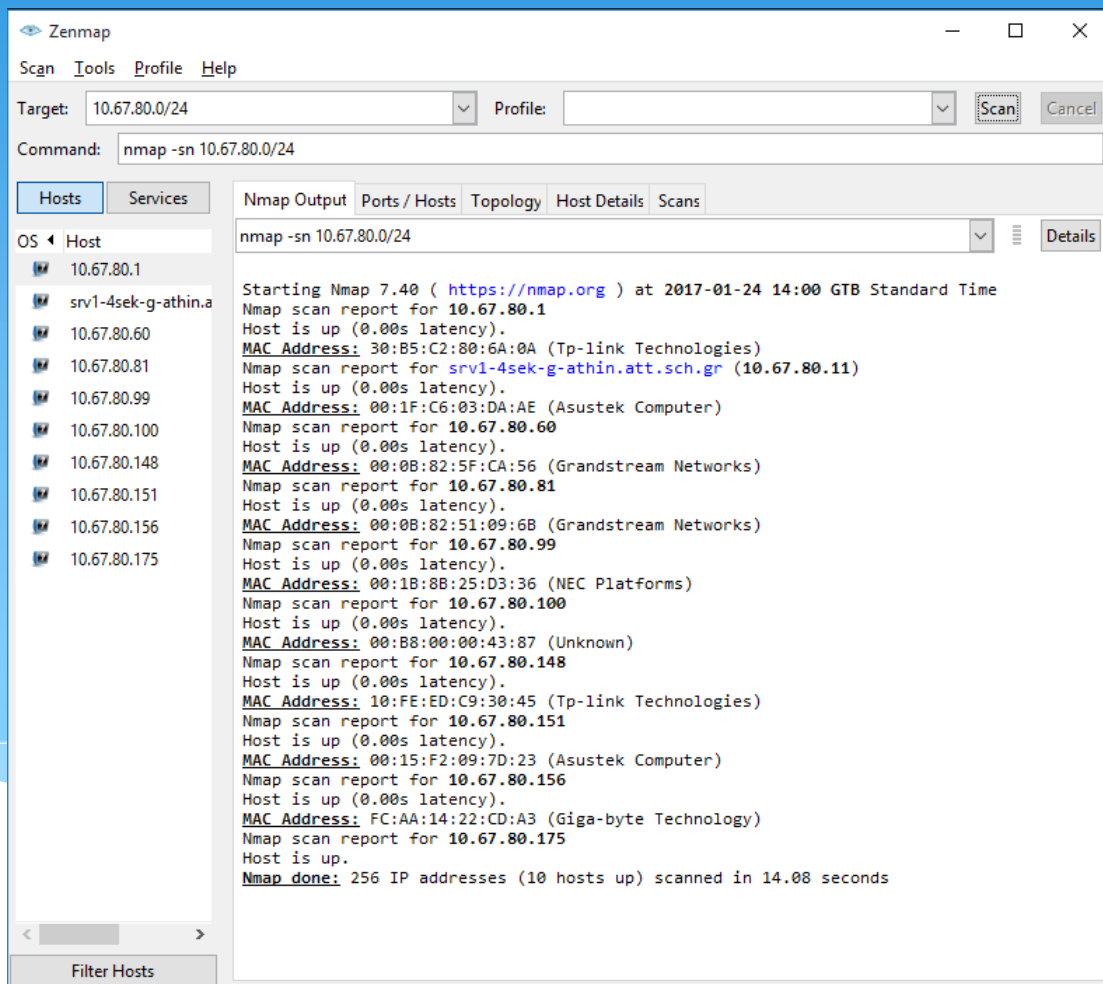


ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (3/7)

Αυτή η επιλογή λέει
στο nmap να
εκτελέσει μόνο ping
scan, και στη
συνέχεια να τυπώσει
τον αριθμό των Η/Υ
που ανταποκρίθηκαν.

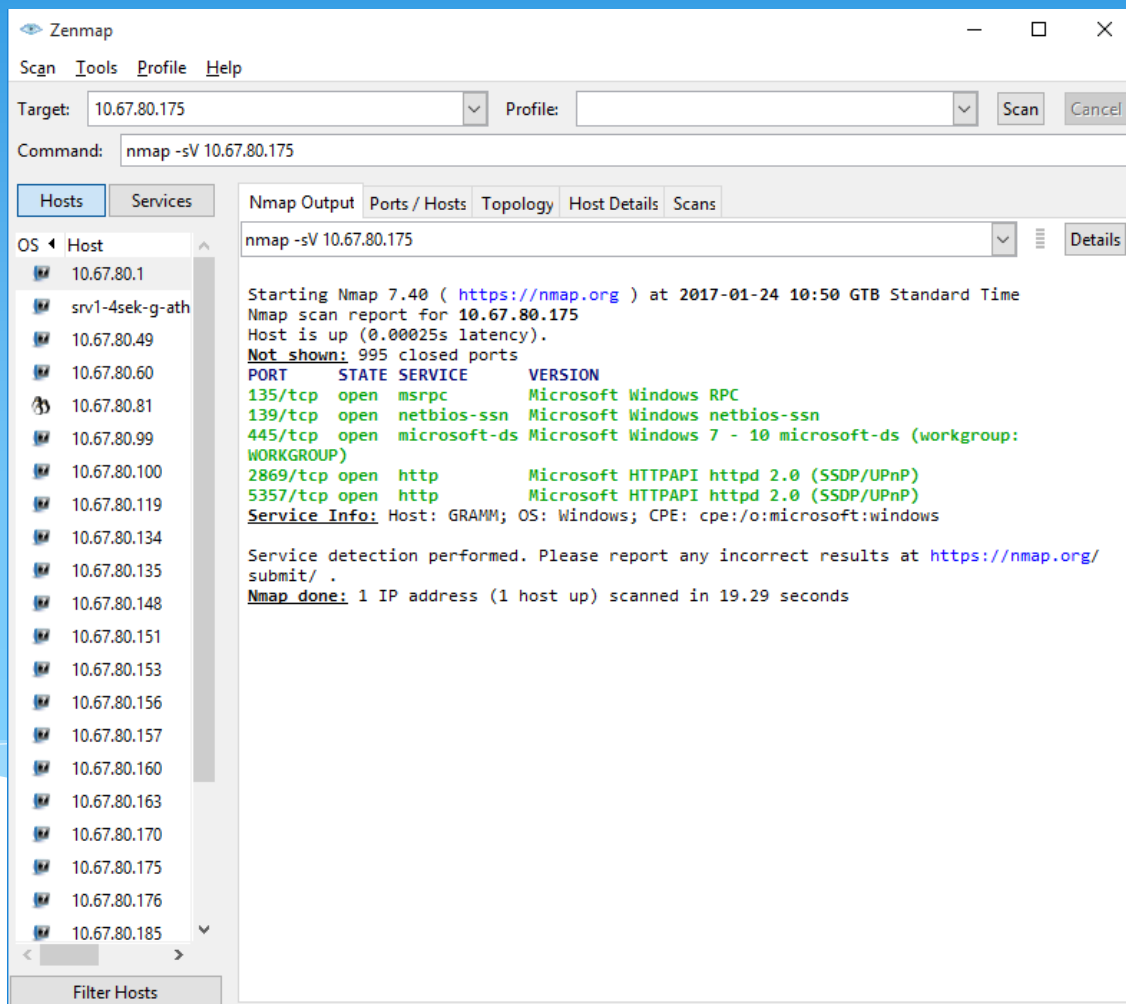


ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (4/7)

Το nmap μπορεί αν
μας εμφανίσει τις
υπηρεσίες και τις
εκδόσεις τους που
τρέχουν στις
πόρτες που βρέθηκαν
ανοικτές.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (5/7)

Port Scanning

Το nmap χωρίζει τις θύρες σε 6 κατηγορίες:

- open. Μια εφαρμογή τρέχει πίσω από τη θύρα και δέχεται συνδέσεις.
- closed. Η θύρα είναι ανοικτή, αλλά δεν υπάρχει κάποια εφαρμογή που να τη χρησιμοποιεί.
- Filtered. Το nmap δε μπορεί να αποφασίσει αν η θύρα είναι ανοικτή γιατί κάποια φίλτρα πακέτων εμποδίζουν τα πακέτα του να φτάσουν στον προορισμό.
- Unfiltered. Η θύρα είναι προσβάσιμη αλλά το nmap δε μπορεί να αποφασίσει αν είναι ανοικτή ή όχι.
- open|filtered. Το nmap δεν είναι δυνατό να αποφασίσει αν η συγκεκριμένη πόρτα είναι ανοικτή ή φιλτραρισμένη.
- closed|filtered. Το nmap δεν είναι δυνατό να αποφασίσει αν η συγκεκριμένη πόρτα είναι κλειστή ή φιλτραρισμένη.

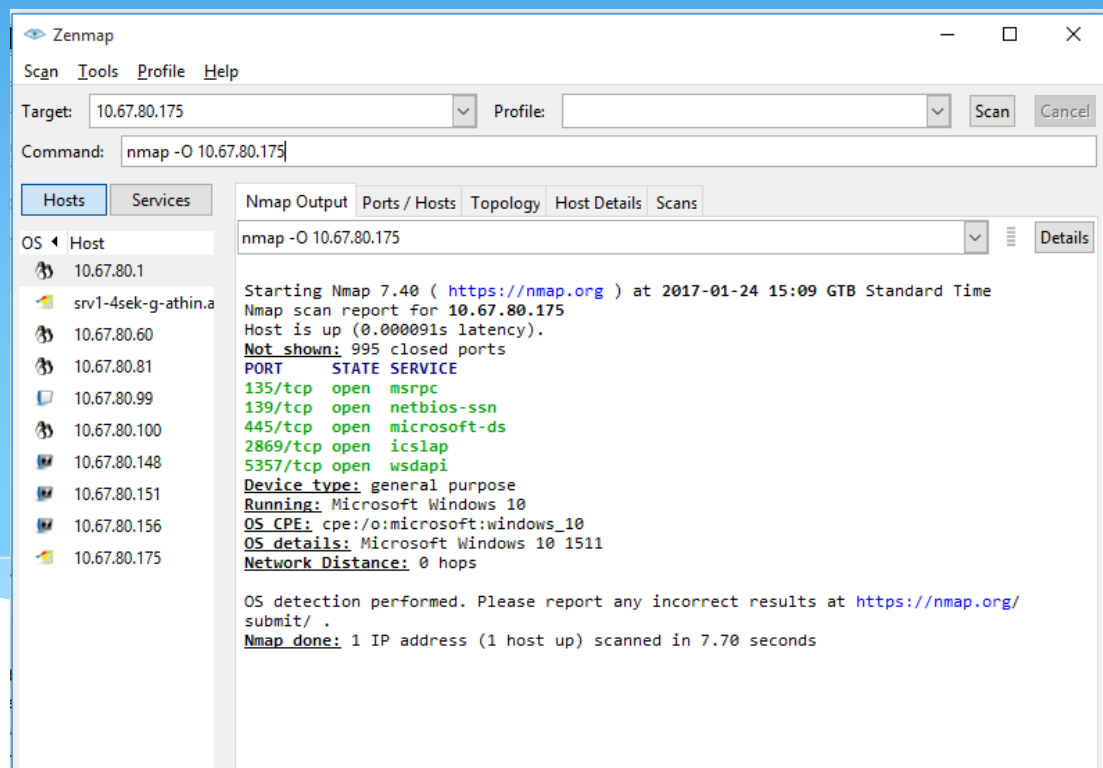
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (6/7)

Το nmap μπορεί να εντοπίσει και το λειτουργικό σύστημα που ένας Η/Υ

ή τα λειτουργικά συστήματα των Η/Υ ενός δικτύου.



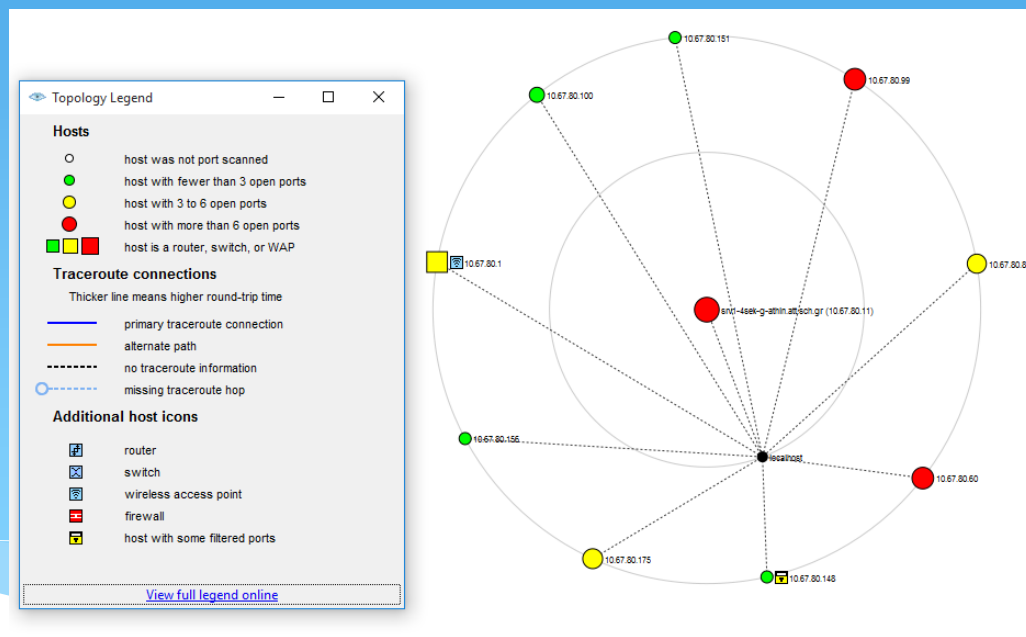
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Zenmap (7/7)

Τοπολογία δικτύου Η/Υ.

(Μεγαλύτερος κύκλος περισσότερα ports ανοικτά)



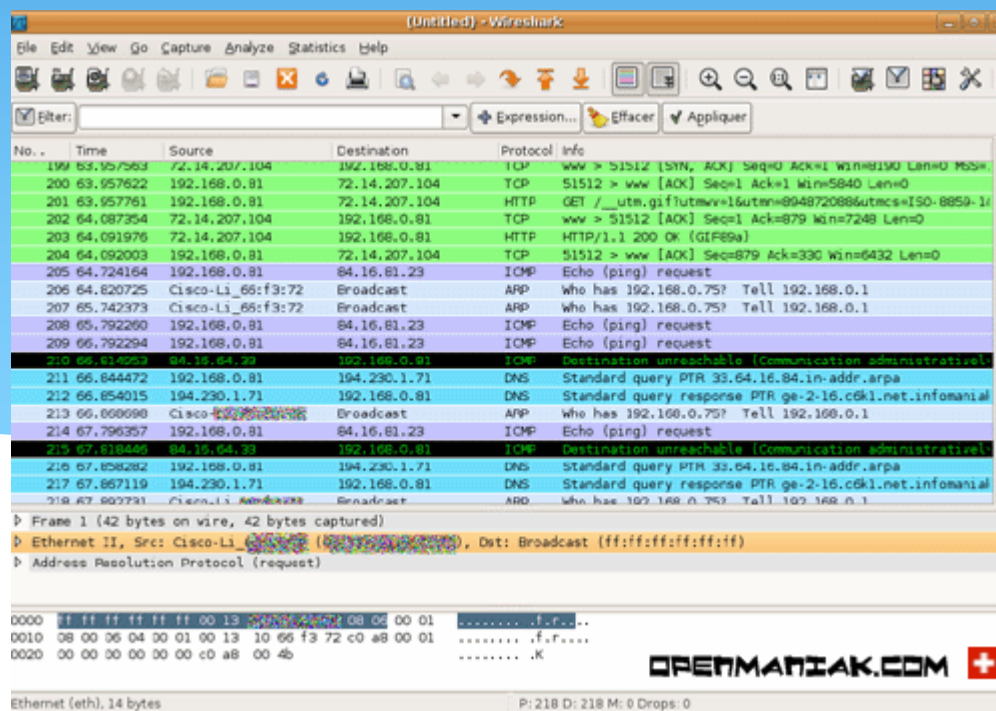
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Wireshark (1/2)

Η εφαρμογή Wireshark είναι ίσως ο δημοφιλέστερος από τους sniffers που κυκλοφορούν σήμερα.

Πρόκειται για ένα λογισμικό ανοιχτού κώδικα που κάποιος μπορεί να κατεβάσει και να εγκαταστήσει στον υπολογιστή του από την σελίδα <http://www.wireshark.org/>.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

μέσω λογισμικού

Wireshark (2/2)

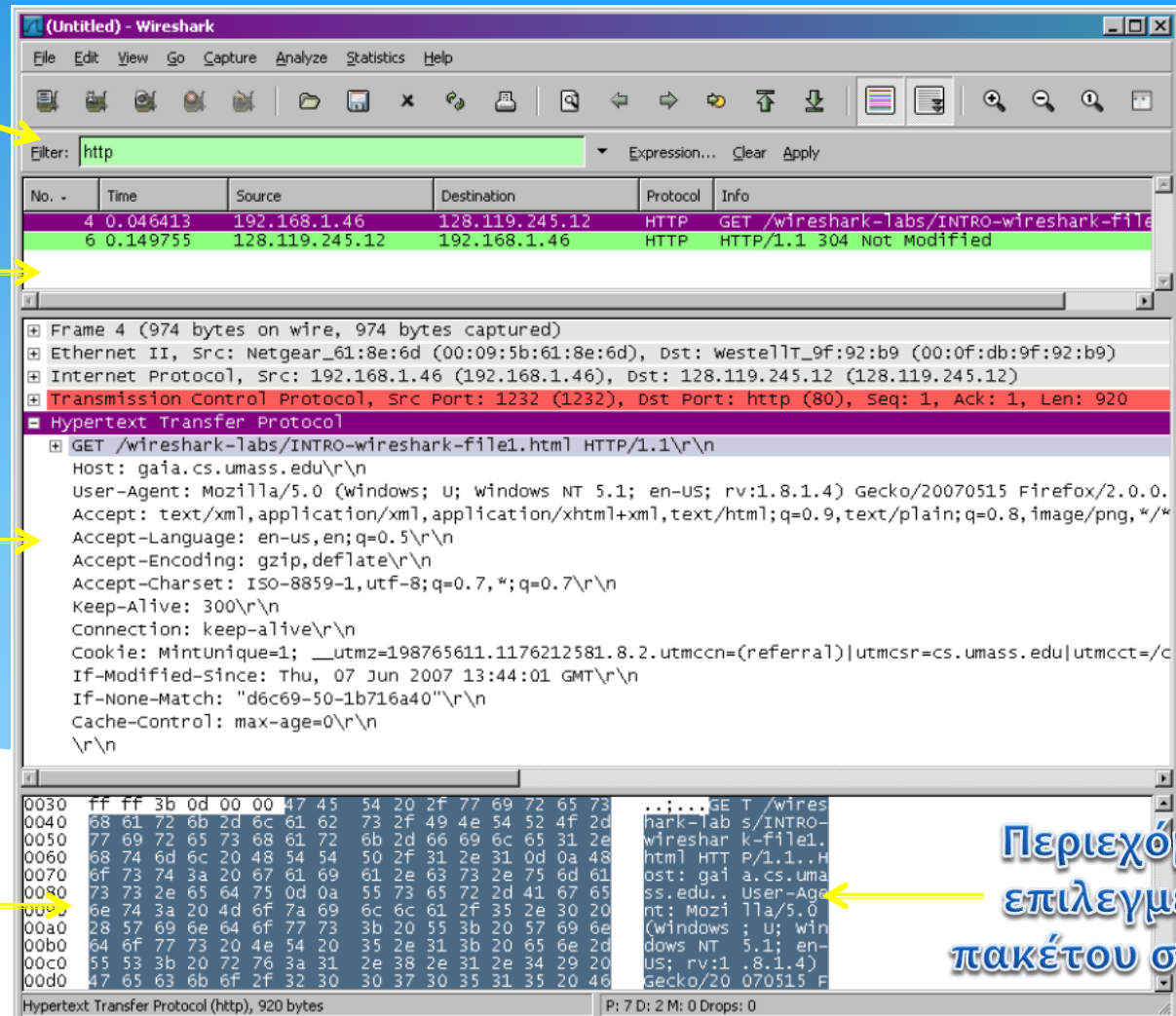
Φίλτρο

Συλλεχθέντα
πακέτα http

Λεπτομέρειες
επιλεγμένου
πακέτου

Περιεχόμενο
επιλεγμένου
πακέτου σε hex

Περιεχόμενο
επιλεγμένου
πακέτου σε ASCII



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (1/19) (Disaster Recovery)

Τα δίκτυα Η/Υ σκοπό έχουν την υποστήριξη της Επιχειρηματικής Δραστηριότητας μιας εταιρείας η οποία παράγει έργο και κέρδη.

Τα δίκτυα Η/Υ σκοπό έχουν την υποστήριξη της λειτουργίας μιας Δημόσιας Υπηρεσίας για να παρέχει υπηρεσίες στους πολίτες.

Τώρα πλέον, περισσότερο από ποτέ, τα δίκτυα Η/Υ παρέχουν το έργο των Επιχειρήσεων και τις υπηρεσίες του Δημοσίου προς τους πελάτες τους και τους πολίτες.

(π.χ. Τράπεζες, eshops, Εφορεία, Ε.Ο.Π.Υ.Υ., κ.α.)

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (2/19) (Disaster Recovery)

«Καταστροφή» ονομάζουμε κάθε σοβαρή δυσλειτουργία του δικτύου Η/Υ μιας Εταιρείας ή Δημόσιου Οργανισμού.

Κανονικά θα έπρεπε να υπάρχει πάντα ένα σχέδιο αποφυγής των «Καταστροφών» του δικτύου Η/Υ.

Οσο καλά όμως και να είναι οργανωμένο ένα σχέδιο αποφυγής των «Καταστροφών» του δικτύου Η/Υ, η «Καταστροφή» αυτή του δικτύου Η/Υ πρέπει να θεωρούμε δεδομένο ότι θα συμβεί.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (3/19) (Disaster Recovery)

Για να αντιμετωπίσουμε την σχεδόν αναπόφευκτη «Καταστροφή» του δικτύου Η/Υ θα πρέπει να υπάρχει ένα σχέδιο δράσεων για την Αποκατάσταση αυτής.
(Disaster Recovery Plan – DRP)

Παράλληλα με τη δράση του σχεδίου αποκατάστασης αυτής της «Καταστροφής» του δικτύου Η/Υ θα πρέπει να υπάρχει πάντα και ένα σχέδιο δράσης για την Επιχειρηματική Συνέχεια μιας Εταιρείας ή της «Υπηρεσιακής» Συνέχειας ενός Δημόσιου Οργανισμού.
(Business Continuity Plan – BCP)

Βέβαια αυτό το δεύτερο σχέδιο δράσης δεν είναι αντικείμενο σχεδιασμού του διαχειριστή του δικτύου Η/Υ, αλλά εκπονείται σε συνεργασία με αυτόν.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (4/19) (Disaster Recovery)

Βασικό χαρακτηριστικό του Σχεδίου Ανάκαμψης από την «Καταστροφή» του δικτύου Η/Υ είναι η τήρηση του Εφεδρικού Αντιγράφου των Πληροφοριών (Information Backup)

Η δημιουργία Αντιγράφων Ασφάλειας του Πληροφοριακού Συστήματος (και Εφεδρικών Αντιγράφων Ασφαλείας, επίσης) είναι μια απαίτηση (must) αφού χρησιμοποιούμε Η/Υ - «τελεία και παύλα».

Πρέπει να υπάρχει συγκεκριμένη πολιτική τήρησης Αντιγράφων Ασφαλείας ανάλογα με την Εταιρεία ή την Υπηρεσία.

Συνηθίζεται να τηρούνται περισσότερα από ένα Αντίγραφα Ασφαλείας, με ένα πάντα, να φυλάσσεται σε προστατευμένο χώρο εκτός του Main Site της Εταιρείας ή της Υπηρεσίας ώστε να μην επηρεαστεί από τυχόν καταστροφή αυτού του site.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (5/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Βλάβες των Servers ή/και του ενεργού δικτυακού εξοπλισμού.

Μητρικές πλακέτες
Σκληροί δίσκοι
Τροφοδοτικά
κ.α.

Hub
Switches
Routers
κ.α.

Για τους Servers πλεονασμός στα Τροφοδοτικά και οι Σκ. Δίσκοι σε RAID1.

Standby Servers (Domain Controller, D.N.S.).

Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

Υπαρξη ανταλλακτικών (Μητρικές πλακέτες, Σκληροί δίσκοι Τροφοδοτικά κ.α.)
και μηχανημάτων (Servers, Hub, Switches, Routers κ.α.) on site.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (6/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση

Bugs

στο software

και στο firmware.

Λογισμικό
Εφαρμογών και
Λειτουργικού
Συστήματος

Ενεργού δικτυακού
εξοπλισμού,
συνήθως

Πάντα ενημερωμένο Λογισμικό.

Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (7/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Κακόβουλη επίθεση στο δίκτυο Η/Υ (Hackers, Crackers, Hacktivists).

1/2
Malware



Χρήση Antimalware λογισμικού.

Επανεγκατάσταση Λειτουργικών Συστημάτων και Εφαρμογών Λογισμικού.

Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (8/19)
(Disaster Recovery)

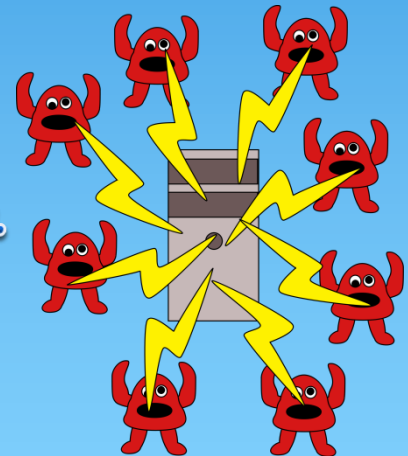
Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Κακόβουλη επίθεση στο δίκτυο Η/Υ (Hackers, Crackers, Hacktivists).

2/2
DOS, DDOS

Αποκατάσταση των Πρωτοκόλλων Επικοινωνίας με τον ISP.

Αποκατάσταση λειτουργίας του Firewall

Αποκατάσταση λειτουργίας των Εφαρμογών Λογισμικού



Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (9/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Διακοπή Παροχής Ισχύος στο Computer Room.



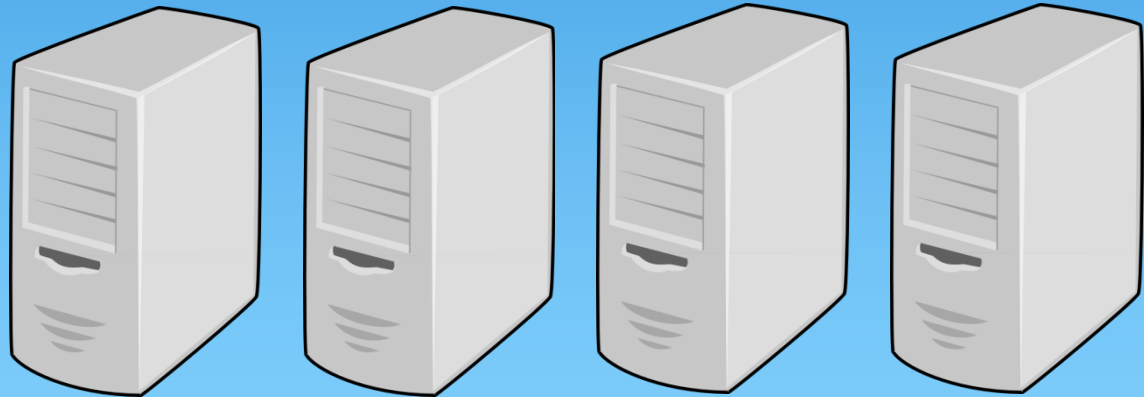
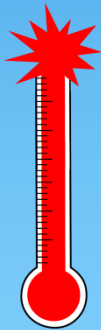
Τοπική Αδιάλειπτη Παροχή Ισχύος (UPS) στο Computer Room.

Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (10/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Βλάβη στο Σύστημα Ψύξεως του Computer Room.

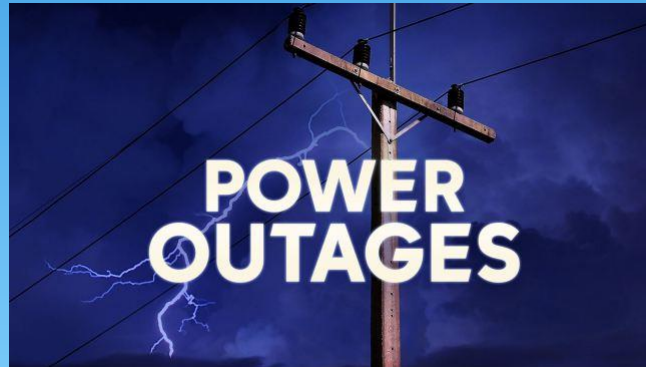


Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (11/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Διακοπή Παροχής Ισχύος στο κτήριο του δικτύου Η/Υ.



Τοπική Αδιάλειπτη Παροχή Ισχύος (UPS) στο Computer Room.

Αδιάλειπτη Παροχή Ισχύος (UPS) του κτηρίου.

Γεννήτρια (+εφεδρική Γεννήτρια) Παροχής Ισχύος του κτηρίου.

Συμφωνία με εταιρείες παροχής τεχνικής εξυπηρέτησης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (12/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Πρόκληση Πυρκαγιάς στο κτήριο του δικτύου Η/Υ.



Ένα άλλο site της Εταιρείας/Υπηρεσίας σε άλλο κτήριο αναλαμβάνει μέρος του φόρτου εργασίας του δικτύου Η/Υ του κυρίως κτηρίου της Εταιρείας/Υπηρεσίας.

Εάν δεν υπάρχει άλλο κτήριο της Εταιρείας/Υπηρεσίας πρέπει να υπάρχει πρόβλεψη για στήσιμο Server, ακόμα και στο σπίτι υπαλλήλου, για την παροχή στοιχειώδους web υπηρεσίας προς τους πελάτες/πολίτες .

Συμφωνία με εταιρείες παροχής web υποστήριξης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (13/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Πλημμύρα στο κτήριο του δικτύου Η/Υ.



Ένα άλλο site της Εταιρείας/Υπηρεσίας σε άλλο κτήριο αναλαμβάνει μέρος του φόρτου εργασίας του δικτύου Η/Υ του κυρίως κτηρίου της Εταιρείας/Υπηρεσίας.

Εάν δεν υπάρχει άλλο κτήριο της Εταιρείας/Υπηρεσίας πρέπει να υπάρχει πρόβλεψη για στήσιμο Server, ακόμα και στο σπίτι υπαλλήλου, για την παροχή στοιχειώδους web υπηρεσίας προς τους πελάτες/πολίτες .

Συμφωνία με εταιρείες παροχής web υποστήριξης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (14/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Σεισμός ή άλλη δομική βλάβη στο κτήριο του δικτύου Η/Υ.



Ένα άλλο site της Εταιρείας/Υπηρεσίας σε άλλο κτήριο αναλαμβάνει μέρος του φόρτου εργασίας του δικτύου Η/Υ του κυρίως κτηρίου της Εταιρείας/Υπηρεσίας.

Εάν δεν υπάρχει άλλο κτήριο της Εταιρείας/Υπηρεσίας πρέπει να υπάρχει πρόβλεψη για στήσιμο Server, ακόμα και στο σπίτι υπαλλήλου, για την παροχή στοιχειώδους web υπηρεσίας προς τους πελάτες/πολίτες .

Συμφωνία με εταιρείες παροχής web υποστήριξης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (15/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση
Τρομοκρατική ενέργεια στο κτήριο του δικτύου Η/Υ.



Ένα άλλο site της Εταιρείας/Υπηρεσίας σε άλλο κτήριο αναλαμβάνει μέρος του φόρτου εργασίας του δικτύου Η/Υ του κυρίως κτηρίου της Εταιρείας/Υπηρεσίας.

Εάν δεν υπάρχει άλλο κτήριο της Εταιρείας/Υπηρεσίας πρέπει να υπάρχει πρόβλεψη για στήσιμο Server, ακόμα και στο σπίτι υπαλλήλου, για την παροχή στοιχειώδους web υπηρεσίας προς τους πελάτες/πολίτες .

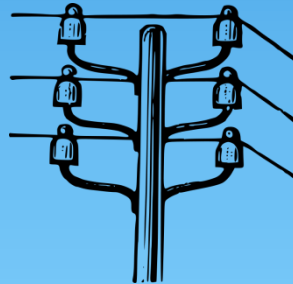
Συμφωνία με εταιρείες παροχής web υποστήριξης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (16/19)
(Disaster Recovery)

Πιθανές αιτίες «Καταστροφών» του δικτύου Η/Υ και Αποκατάσταση

Αποκοπή της Τηλεπικοινωνιακής Σύνδεσης
του κτηρίου του δικτύου Η/Υ.



Ένα άλλο site της Εταιρείας/Υπηρεσίας σε άλλο κτήριο αναλαμβάνει μέρος του φόρτου εργασίας του δικτύου Η/Υ του κυρίως κτηρίου της Εταιρείας/Υπηρεσίας.

Εάν δεν υπάρχει άλλο κτήριο της Εταιρείας/Υπηρεσίας πρέπει να υπάρχει πρόβλεψη για στήσιμο Server, ακόμα και στο σπίτι υπαλλήλου, για την παροχή στοιχειώδους web υπηρεσίας προς τους πελάτες/πολίτες .

Συμφωνία με εταιρείες παροχής web υποστήριξης 24x7x365
με ανταπόκριση σε συγκεκριμένο χρονικό διάστημα.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (17/19)
(Disaster Recovery)

Emergency Data and Telecom Center

Γενικά κάθε Εταιρεία/Υπηρεσία με έντονη «δικτύωση» Η/Υ οφείλει να έχει σχεδιάσει την εναλλακτική της λειτουργία (έστω και σε υποτυπώδη μορφή) σε άλλο site της Εταιρείας/Υπηρεσίας και σε περίπτωση που αυτό δεν υπάρχει, σε ένα οποιοσδήποτε άλλο κατάλληλο χώρο.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (18/19)

(Disaster Recovery)

Emergency Data and Telecom Center

Δεν αρκεί όμως μόνο η αρχική προετοιμασία αυτού του εναλλακτικού κέντρου τηλεπικοινωνιακής δικτύωσης .

Απαιτείται η συστηματική: συντήρηση, αναβάθμιση και δοκιμαστική λειτουργία.



ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Αποκατάσταση Καταστροφών (19/19) (Disaster Recovery)

Γενικά δεν υπάρχει κάποια σαφής και καθιερωμένη μορφή του σχεδίου αποφυγής καταστροφών και ανάκαμψης από αυτές.

Ο Σχεδιασμός και η Υλοποίηση αυτών εξαρτώνται από:

τη Δομή του Πληροφοριακού Συστήματος

τη Σπουδαιότητα αυτού

το Κόστος Υλοποίησης

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ Η/Υ

Βιβλιογραφία

1. www.wikipedia.org
2. Τεχνολογία Δικτύων Επικοινωνιών, Α' Τάξη 2^{ου} Κύκλου Τ.Ε.Ε. Τομέα ΗΛΕΚΤΡΟΝΙΚΩΝ (Κεφάλαιο 8)
3. Δίκτυα Υπολογιστών, Γ' Τάξη Τομέα ΠΛΗΡΟΦΟΡΙΚΗΣ (Κεφάλαιο 8)
4. Δίκτυα Υπολογιστών II, Γ' Τάξη Τομέα ΠΛΗΡΟΦΟΡΙΚΗΣ (Κεφάλαιο 8) (Ανεπίσημο βοήθημα, Μανώλης Κιαγιάς)
5. http://ikee.lib.auth.gr/record/131056/files/243_Computer_Networks_Vulnerability_Assessment.pdf
6. NMAP, Tutorial and Examples, Γιώργος Καππές
7. Εικόνες από το Διαδίκτυο.