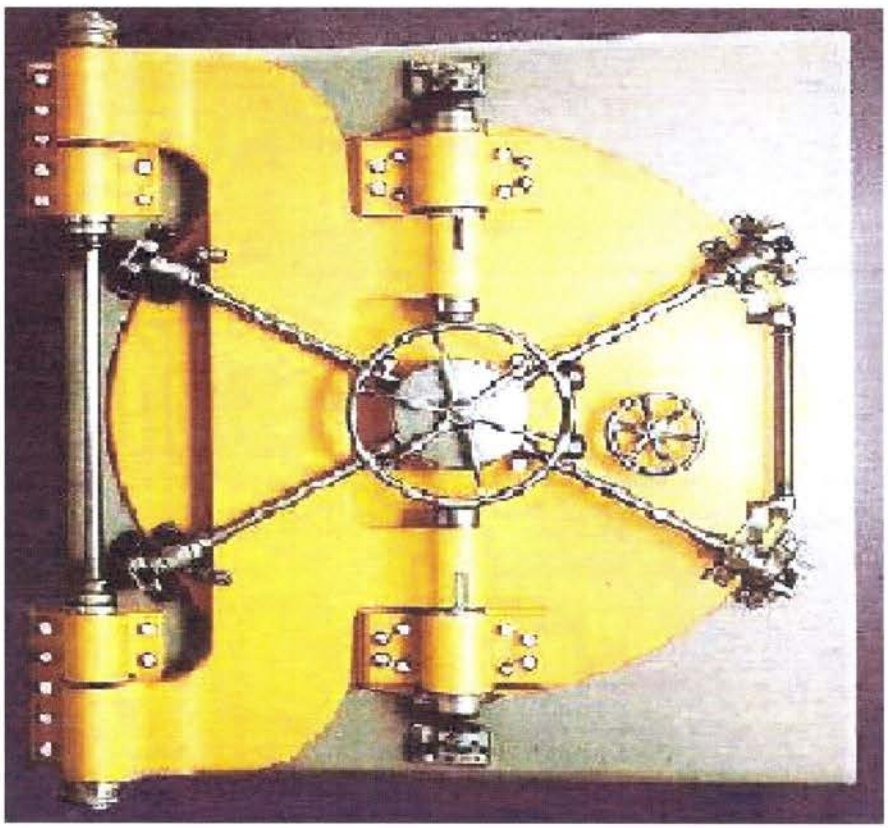
Τ.Ε.Ι. ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ ( Σ.Δ.Ο.)
*ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ*

**T.E.I. of EPIRUS**
SCHOOL OF MANAGEMENT AND ECONOMICS
*DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT*



# WIN: Πόσο Ασφαλείς Είμαστε?

**ΚΑΡΒΟΥΝΙΔΟΥ ΜΑΡΙΑ – ΝΑΣΙΟΣ ΑΘΑΝΑΣΙΟΣ**

**ΑΡΤΑ ~ ΣΕΠΤΕΜΒΡΙΟΣ 2004**

**ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ**

Όλες οι προτάσεις οι οποίες παρουσιάζονται σε αυτό το κείμενο και οι οποίες ανήκουν σε άλλους αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα. Τα υπόλοιπα είναι επινόηση των γραφόντων οι οποίοι φέρουν και την καθολική ευθύνη για αυτό το κείμενο και δηλώνουν υπεύθυνα ότι δεν υπάρχει λογοκλοπή για αυτό το κείμενο.

1) Ονοματεπώνυμο : Καρβουνίδου Μαρία

Υπογραφή……. Ημερομηνία……...

2)Ονοματεπώνυμο : Νάσιος Αθανάσιος

Υπογραφή……. Ημερομηνία……...

## ABSTRACT ~ ΠΕΡΙΛΗΨΗ

Το θέμα “Win: Πόσο Ασφαλείς Είμαστε ?” αναφέρει τρόπους προστασίας των χρηστών του Λειτουργικού Συστήματος των Windows από επιτιθέμενους οι οποίοι επιδιώκουν να εκμεταλλευτούν τα κενά ασφαλείας και τις ευπάθειες που αυτά παρουσιάζουν

Οι επιθέσεις έχουν διάφορες μορφές, είτε μέσω ηλεκτρονικού ταχυδρομείου, είτε μέσω εκμετάλλευσης κάποιων αδυναμιών του κώδικα του Λειτουργικού Συστήματος όσο ο υπολογιστής είναι on-line.

Οι χρήστες έχουν αρκετούς τρόπους για να προστατευτούν από αυτές τις επιθέσεις και να κάνουν τα συστήματα τους ασφαλέστερα. Μερικοί από τους τρόπους αυτούς είναι η εγκατάσταση firewall, η χρησιμοποίηση smartcard, οι ισχυροί κωδικοί πρόσβασης, τα ενημερωμένα antivirus κ.τ.λ.

Το θέμα δημιουργήθηκε με σκοπό την ενημέρωση των χρηστών υπολογιστικών συστημάτων ώστε να γνωρίζουν καλύτερα τους κινδύνους που απειλούν την ασφάλεια των δεδομένων τους και την ιδιωτικότητά τους και να λάβουν τα απαραίτητα μέτρα προστασίας ώστε να αποφύγουν τις δυσάρεστες συνέπειες μίας “ηλεκτρονικής επίθεσης”

# ΠΕΡΙΕΧΟΜΕΝΑ

# 1. ΕΙΣΑΓΩΓΗ

Γιατί το πρόβλημα *ασφάλειας της πληροφορίας* είναι τόσο μεγάλο; Γιατί δεν υπάρχει σχεδόν καμιά ανθρώπινη δραστηριότητα που να μην υποστηρίζεται από κάποιο είδος υπολογιστικού συστήματος, ενώ η απίστευτα μεγάλη ροή και συγκέντρωση πληροφοριών, η διεύρυνση των δικτύων επικοινωνίας πληροφοριών και η διαφαινόμενη έξαρση της χρήσης βάσεων πληροφοριών από το σπίτι και το κινητό τηλέφωνο συνθέτουν την εικόνα, "πληροφοριοποιημένης" κοινωνίας. Γιατί θα πρέπει να ασχολούμαστε; Στην καθημερινή ζωή ο άνθρωπος εξυπηρετείται από απειρία συσκευών και συστημάτων αυτόματης επεξεργασίας πληροφοριών τα οποία περιέχουν δεδομένα πολύτιμα. Μερικά από τα συστήματα τα οποία βασίζονται σε υπολογιστές είναι:

- Συστήματα μεταφορών
- Συστήματα και οικονομικές εγγραφές προσώπων και εταιριών
- Συστήματα επεξεργασίας πιστωτικών καρτών
- Μηχανές αυτόματων συναλλαγών (ATMs)
- Το διεθνές δίκτυο τηλεπικοινωνιών
- Επικοινωνίες έκτακτων αναγκών(166)
- Συστήματα υπεύθυνα για την αποθήκευση και μεταφοράς δεδομένων
- Μονάδων υγείας
- Συστήματα ενεργειακής διαχείρισης
- Συστήματα γενικής επεξεργασίας μισθοδοσιών
- Συστήματα έκδοσης εισιτηρίων

Αν παραβιαστεί ένα από αυτά τα συστήματα από κάποιον τότε θα μπορούσε να δει θέματα υγείας για οποιονδήποτε. Να κλέψει χρήματα από τον τραπεζικό λογαριασμό μας. Να κλέψει από τις πιστωτικές μας κάρτες. Να κάνει το τηλέφωνό μας κοινής χρήσης. Να εκδώσει εισιτήρια στο όνομά του ή να διακόψει το ηλεκτρικό μας ρεύμα. Με λίγα λόγια να γίνει πραγματικός κίνδυνος. Οι περισσότεροι έχουν ήδη προσπαθήσει επιτυχώς κάποιες από αυτές τις ενέργειες. Πολλά από αυτά έχουν ήδη συμβεί. Αυτό κάνει ιδιαίτερα αισθητή στις επιχειρήσεις και στα άτομα την ανάγκη διασφάλισης αμεροληψίας και έχει κατ΄ επέκταση, αύξησε σημαντικά το ενδιαφέρον και την αναγκαιότητα για τα θέματα ασφάλειας της πληροφορίας. Όταν προσπαθούμε να ασφαλίσουμε περιβάλλοντα enterprise αντιμετωπίζουμε προβλήματα στις ακόλουθες κατηγορίες:

- Προβληματικές διατάξεις και ρυθμίσεις δικτύων και κόμβων
- Ελαττώματα λειτουργικών συστημάτων και εφαρμογών

- Ατέλειες στις προσπάθειες ποιοτικών υπηρεσιών και την ανταπόκριση των κατασκευαστών.
- Έλλειψη ικανών ανθρώπων στον χώρο

Στο παρόν σύγγραμμα θα ασχοληθούμε κυρίως με τα προβλήματα και τις ατέλειες ως αναφορά την ασφάλεια σε υπολογιστικά συστήματα με λειτουργικό σύστημα windows, που η χρήση τους προορίζεται κυρίως ως ατομική (PC), μετέχούν ή όχι σε ένα τοπικό δίκτυο και έχουν πρόσβαση στο διαδίκτυο.

# ΚΕΦΑΛΑΙΟ 1ο

# 2. ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ WINDOWS & ΑΣΦΑΛΕΙΑ

## 2.1. Λειτουργικό σύστημα (Operating System)

Ένα υπολογιστικό σύστημα μπορεί να θεωρηθεί ότι αποτελείται από:

- Το υλικό (hardware)
- Τα προγράμματα εφαρμογών (application programs)
- Το λειτουργικό σύστημα (operating system)

Το υλικό αποτελείται από το σύνολο των συσκευών που απαρτίζουν το υπολογιστικό σύστημα.

Τα προγράμματα εφαρμογών γράφονται από τους χρήστες και καθορίζουν τον τρόπο χρησιμοποίησης των συσκευών για την επίλυση υπολογιστικών προβλημάτων.

Το λειτουργικό σύστημα είναι ένα σύνολο προγραμμάτων που παρεμβάλλεται μεταξύ του υλικού και του χρήστη (ή των προγραμμάτων εφαρμογών) για να ελέγχει και να καθοδηγεί τη λειτουργία του υπολογιστή.

Ένα λειτουργικό σύστημα διαχειρίζεται και φροντίζει την αρμονική συνεργασία των “μέσων” του υπολογιστή, με σκοπό την πραγματοποίηση των “εργασιών” που ζητούν οι χρήστες, όπως εκτέλεση προγραμμάτων, αντιγραφή αρχείων, εκτυπώσεις κ.λ.π. Λέγοντας “μέσα” εννοούμε τη μνήμη, την κεντρική μονάδα επεξεργασίας και τις διάφορες περιφερειακές συσκευές. Η κάθε ζητούμενη “εργασία” αντιμετωπίζεται από το λειτουργικό σύστημα σαν ένα ή περισσότερα “καθήκοντα” που πρέπει να πραγματοποιηθούν. Το κάθε “καθήκον” επιτυγχάνεται με μια διεργασία, δηλαδή την εκτέλεση ενός ή περισσοτέρων σχετικών προγραμμάτων.

Μία επιπρόσθετη ευθύνη του λειτουργικού συστήματος είναι η εποπτεία “διαλόγου” ανάμεσα το χρήστη και τον υπολογιστή. Για να διευκολύνει το χρήστη, δημιουργεί το κατάλληλο περιβάλλον εργασίας του χρήστη ώστε να τον απαλλάσσει από τις λεπτομερείς γνώσεις του λειτουργικού συστήματος. Πολλές φορές, αν κάποιος ζητήσει από ένα χρήστη να του περιγράψει τον υπολογιστή πάνω στον οποίο εργάζεται, θα του δοθεί μία περιγραφή με τα χαρακτηριστικά του λειτουργικού συστήματος που χρησιμοποιεί. Αυτό δείχνει την στενή σχέση της έννοιας του λειτουργικού συστήματος και της έννοιας του υπολογιστή.

Λειτουργικό σύστημα λοιπόν είναι ένα σύνολο προγραμμάτων που δέχεται τις διαταγές των χρηστών, τις μεταφράζει στις αντίστοιχες διεργασίες που πρέπει να εκτελεστούν, δραστηριοποιεί για τον σκοπό αυτό τα κατάλληλα “μέσα” του υπολογιστή και φροντίζει για την αρμονική συνεργασία τους.

Μετά τα παραπάνω είναι φανερό ότι οι βασικοί στόχοι ενός λειτουργικού συστήματος είναι:

- Η αποδοτική λειτουργία του υπολογιστικού συστήματος και
- Η διευκόλυνση του χρήστη.

Πολλές φορές οι δύο στόχοι είναι αλληλοσυγκρουόμενοι, αφού παρατηρείται η ευκολία του χρήστη να επιτυγχάνεται σε βάρος της αποδοτικότητας και αντίστροφα.

## 2.2. Η ιστορία των WINDOWS

Στις 10 Νοεμβρίου,1983, η Microsoft ανήγγειλε τα Microsoft Windows®, μια επέκταση του λειτουργικού συστήματος MS-DOS® που θα παρείχε ένα λειτουργικό γραφικό περιβάλλον για τους χρήστες των ηλεκτρονικών υπολογιστών. Με τα Windows, η εποχή γραφικής διεπαφής με τον χρήστη (graphical user interface -GUI) στη Microsoft είχε αρχίσει. Πολλοί χρήστες PC εντόπισαν το λειτουργικό σύστημα της Microsoft Windows® στην έκδοση του 1990 των Windows 3.0, την πρώτη ευρέως διαδεδομένη εκδοχή των Windows. Εντούτοις, η Microsoft ανήγγειλε αρχικά το προϊόν παραθύρων επτά χρόνια νωρίτερα και κυκλοφόρησε την πρώτη έκδοση το 1985. Τα Windows 1.0 ήταν το νέο προϊόν που αποτελούταν από παράθυρα και γραφική διεπαφή με τον χρήστη (GUI).

**1985: Windows 1.0**

Η πρώτη έκδοση των Windows παρείχε ένα νέο περιβάλλον λογισμικού για την ανάπτυξη και το τρέξιμο των εφαρμογών που χρησιμοποιούσαν bitmap εικόνες και συσκευές ποντικιού

**1987: Windows 2.0**

Τα Windows 2.0 εκμεταλλεύθηκαν τη βελτιωμένη ταχύτητα του επεξεργαστή 286 της Intel, και την επεκταθείσα μνήμη. Οι δια-επικοινωνίες έγιναν πραγματοποιήσιμες μέσω της δυναμικής ανταλλαγής στοιχείων (Dynamic Data Exchange- DDE)

**1990: Windows 3.0**

Η τρίτη και σημαντικότερη έκδοση της πλατφόρμας Windows από τη Microsoft πρόσφερε βελτιωμένη απόδοση, προηγμένα γραφικά με 16 χρώματα, και πλήρη υποστήριξη του ισχυρότερου επεξεργαστή της Intel, τον 386 καθώς επίσης και ένα ευρύ φάσμα χρήσιμων δυνατοτήτων και λειτουργιών, που περιλαμβάνουν:

- Program Manager, File Manager, και Print Manager.
- ένα εντελώς ξαναγραμμένο περιβάλλον ανάπτυξης εφαρμογής.
- ένα βελτιωμένο σύνολο εικονιδίων των Windows.

**1993: Windows for Workgroups 3.11**

Αυτή η έκδοση πρόσθεσε την υποστήριξη για δικτύωση ομάδων εργασίας. Για πρώτη φορά, οι βασισμένα σε Windows υπολογιστές ήταν δίκτυο-ενήμεροι και έγιναν ένα αναπόσπαστο τμήμα της αναδυόμενης εξέλιξης των client/server υπολογιστών.

**1993: Windows NT 3.1**

Αντίθετα από τα Windows 3,1, τα WINDOWS NT 3.1 ήταν ένα τριανταδυάμπιτο λειτουργικό σύστημα.

Τα WINDOWS NT ήταν το πρώτο λειτουργικό σύστημα παραθύρων που συνδύαζε την υποστήριξη για επιχειρησιακές εφαρμογές των client/server με τις κύριες προσωπικές εφαρμογές παραγωγικότητας της βιομηχανίας. Επιπλέον, το λειτουργικό σύστημα έδωσε νέο έδαφος στην ασφάλεια, τη δύναμη των λειτουργικών συστημάτων, την απόδοση, την εξελιξιμότητα υπολογιστών γραφείου, και την αξιοπιστία. Τα νέα χαρακτηριστικά γνωρίσματα περιέλαβαν εφαρμογές όπως, την ενσωματωμένη δικτύωση, την ασφάλεια περιοχών των κεντρικών υπολογιστών, OS/2 και τα υποσυστήματα POSIX, την υποστήριξη για τις πολλαπλάσιες αρχιτεκτονικές επεξεργαστών, και το σύστημα αρχείων NTFS

**1993: Windows NT Workstation 3.5**

Η κυκλοφορία των Windows NT Workstation 3.5 παρείχε τον υψηλότερο βαθμό προστασίας μέχρι τότε για τις κρίσιμες επιχειρησιακές εφαρμογές και τα δεδομένα. πρόσφερε επίσης τις τριανταδυάμπιτες βελτιώσεις απόδοσης και την καλύτερη υποστήριξη εφαρμογών, συμπεριλαμβανομένης της υποστήριξης για τους print servers και του NetWare αρχείου

**1995: Windows 95**

Τα WINDOWS 95 ήταν ο διάδοχος στα τρία υπάρχοντα γενικής χρήσης λειτουργικά συστήματα υπολογιστών γραφείου από τα Windows, Ενσωμάτωσαν έναν τριανταδυάμπιτο TCP/IP σωρό (Transmission Control Protocol/Internet Protocol) για την υποστήριξη διαδικτύου, τη δικτύωση dial-up και τις νέες ικανότητες Plug and Play που το κατέστησαν εύκολο για τους χρήστες στο να εγκαθιστούν υλικό και λογισμικό. Το τριανταδυάμπιτο

λειτουργικό σύστημα πρόσφερε επίσης τις ενισχυμένες ικανότητες πολυμέσων και ενσωματωμένη τη δικτύωση.

**1996: Windows NT Workstation 4.0**

Αυτή η βελτίωση στο λειτουργικό σύστημα επιχειρησιακών υπολογιστών γραφείου έφερε αυξανόμενη ευκολία της χρήσης και απλοποίησε τη διαχείριση, την υψηλότερη απόδοση δικτύων, και τα εργαλεία για intranets (εσωτερικά διαδίκτυα επιχειρήσεων)

**1998: Windows 98**

Τα Windows 98 ήταν η αναβάθμιση των Windows 95. Ήταν η πρώτη έκδοση των Windows που σχεδιάστηκε ειδικά για τους καταναλωτές. Με τα Windows 98, οι χρήστες θα μπορούσαν να βρουν πληροφορίες ευκολότερα για τους υπολογιστές τους καθώς επίσης και για το διαδίκτυο. Άλλες βελτιώσεις πάνω στην ευκολία στην χρήση, περιέλαβαν τη δυνατότητα του γρηγορότερου ανοίγματος και κλεισίματος των εφαρμογών, την υποστήριξη για την ανάγνωση των δίσκων DVD, και η υποστήριξη για συσκευές USB.

**1999: Windows 98 Second Edition**

Τα Windows 98 SE, ήταν μια επαυξητική αναπροσαρμογή στα Windows 98. Βοήθησαν στη βελτίωση της online εμπειρίας των χρηστών με τον Internet Explorer 5.0 και Microsoft Windows NetMeeting® 3.0. Περιέλαβε επίσης τη Microsoft DirectX® API 6,1, η οποία παρείχε ότι βελτίωση της υποστήριξης για τα πολυμέσα των Windows, και πρόσφερε τις ικανότητες οικιακής δικτύωσης μέσω της διανομής σύνδεσης με το διαδίκτυο (Internet connection sharing -ICS).

**2000: Windows Millennium Edition (Windows Me)**

Σχεδιασμένα για τους οικιακούς χρήστες ηλεκτρονικών υπολογιστών, τα Windows Me πρόσφεραν στους καταναλωτές μουσική, βίντεο, αύξηση της οικιακής δικτύωσης και βελτιώσεις αξιοπιστίας. Τα Windows Me ήταν το τελευταίο λειτουργικό σύστημα της Microsoft που βασίζεται στη βάση του κώδικα των WINDOWS 95. Η Microsoft ανήγγειλε ότι όλα τα μελλοντικά προϊόντα λειτουργικών συστημάτων θα βασίζονταν στα WINDOWS NT και Windows 2000 kernel.

**2000: Windows 2000 Professional**

Τα Windows 2000 πρόσθεσαν σημαντικές βελτιώσεις στην αξιοπιστία, την ευκολία της χρήσης και τη συμβατότητα διαδικτύου. Μεταξύ άλλων βελτιώσεων, τα Windows 2000 Professional απλούστευσαν τη διαδικασία της εγκατάστασης υλικού με την προσθήκη της υποστήριξης για μια ευρεία ποικιλία νέου υλικού Plug and Play, συμπεριλαμβανομένης της προηγμένης δικτύωσης και των ασύρματων προϊόντων, των συσκευών USB, των συσκευών IEEE 1394, και των υπέρυθρων συσκευών.

**2001: Windows XP**

Με την κυκλοφορία των Windows XP τον Οκτώβριο του 2001, η Microsoft συγχώνευσε δύο γραμμές λειτουργικών συστημάτων των Windows της για τους οικιακούς χρήστες και για τις επιχειρήσεις, ενώνοντας τις γύρω από τη βάση κώδικα των Windows 2000.

**2001: Windows XP Professional**

Τα Windows XP Professional φέρουν τη σταθερότητα των Windows 2000 στον υπολογιστή γραφείου, ενισχύοντας την αξιοπιστία, την ασφάλεια, και την απόδοση. Με ένα φρέσκο σχεδιασμό περιβάλλοντος, τα Windows XP Professional περιλαμβάνουν τα χαρακτηριστικά για την επιχείρηση των οικιακών υπολογιστών συμπεριλαμβανομένης της μακρινής υποστήριξης υπολογιστών γραφείου, ένα κρυπτογραφικό σύστημα αρχείων, το system restore και προχωρημένα χαρακτηριστικά δικτύωσης. Οι βασικές αυξήσεις για τους κινητούς χρήστες περιλαμβάνουν την ασύρματη υποστήριξη δικτύωσης 802.1x, τον Windows Messenger, και τη Remote Assistance.

## *2.3. **Ασφάλεια***

Ο όρος ασφάλεια, περιγράφει την τεχνική και τις μεθόδους που χρησιμοποιούνται για να αποτρέψουν την προσπέλαση σε αρχεία ή τη χρήση ενός υπολογιστικού συστήματος από μη εξουσιοδοτημένα άτομα, ή ακόμη και την αποφυγή απώλειας ή καταστροφής του υλικού ή δεδομένων του (π.χ. φυσικές καταστροφές).

Οι απαιτήσεις για ασφάλεια προσδιορίζονται:

- ***μυστικότητα*** *(secrecy):* απαιτείται η πληροφορία να είναι προσπελάσιμη για ανάγνωση μόνον από εξουσιοδοτημένους χρήστες. Αυτού του είδους η πρόσβαση περιλαμβάνει την εκτύπωση, την προβολή και άλλες φορές ακόμη και την αποκάλυψη ύπαρξης κάποιου είδους πληροφορίας.
- ***ακεραιότητα*** *(integrity):* απαιτείται οι πόροι του συστήματος (data, processes κλπ) να μπορούν να τροποποιηθούν μόνον από εξουσιοδοτημένους χρήστες. Η τροποποίηση περιλαμβάνει την

εγγραφή, τροποποίηση, αλλαγή κατάστασης (status), διαγραφή και δημιουργία.

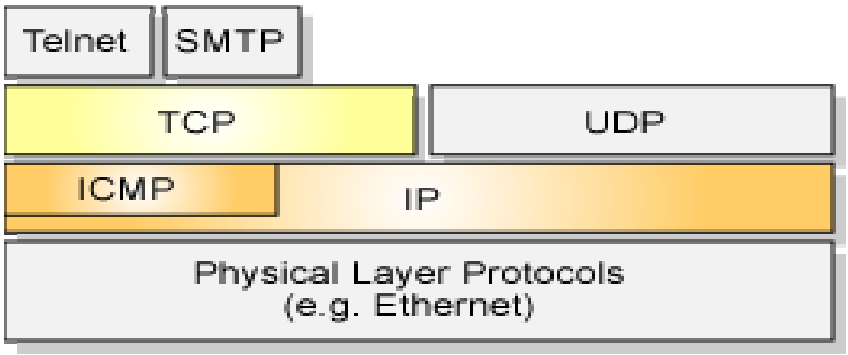
- ***διαθεσιμότητα*** *(availability):* απαιτείται οι πόροι του συστήματος να είναι διαθέσιμοι στους εξουσιοδοτημένους χρήστες

## *2.4. Πρωτόκολλα ~ Κατηγορίες επιθέσεων*

Χαρακτηριστικά, οι επιθέσεις ταξινομούνται από τα χαρακτηριστικά τους. Δύο από αυτά τα χαρακτηριστικά περιγράφονται παρακάτω

**Ανίχνευση (Scanning):** Η ανίχνευση, ή footprinting, είναι μέρος της αρχικής διαδικασίας συλλογής πληροφοριών για έναν χάκερ. Προτού να μπορέσουν οι χάκερ να επιτεθούν σε ένα σύστημα, πρέπει να συγκεντρώσουν τις πληροφορίες για το σύστημα, όπως το σχεδιάγραμμα του δικτύου, τον τύπο των λειτουργικών συστημάτων, τις υπηρεσίες που είναι διαθέσιμες σε εκείνα τα συστήματα, τους χρήστες σε εκείνα τα συστήματα, και τα λοιπά. Με βάση τις πληροφορίες που συγκεντρώνονται, οι χάκερ μπορούν να συναγάγουν τις πιθανές ευπάθειες του συστήματος και να επιλέξουν την καλύτερη μέθοδο επίθεσης για το επιλεγμένο σύστημα στόχων

**Επιθέσεις άρνησης των υπηρεσιών:** Συχνά, οι επιτιθέμενοι στοχεύουν σε συγκεκριμένα συστήματα, που τα παραβιάζουν και έτσι να μπορούν να χρησιμοποιηθούν για συγκεκριμένους λόγους. Συχνά, η ασφάλεια των διαχειριστών εκείνων των συστημάτων θα αποτρέψει τους επιτιθεμένους από το κέρδος του ελέγχου ενός συστήματος. Αλλά με τις επιθέσεις άρνησης των υπηρεσιών, οι επιτιθέμενοι δεν χρειάζεται να αποκτήσουν πρόσβαση σε ένα σύστημα. Ο στόχος είναι απλά να υπερφορτωθεί ένα σύστημα ή ένα δίκτυο έτσι ώστε να μην μπορεί να παρέχει την υπηρεσία του άλλο. Οι επιθέσεις άρνησης των υπηρεσιών μπορεί να έχουν διαφορετικούς στόχους, συμπεριλαμβανομένης της κατανάλωσης εύρους ζώνης και της στέρησης των πόρων.




**Εικόνα 2-1: Η δομή των πρωτοκόλλων**

### *2.4.1. Χρησιμοποίηση ICMP*

Επειδή είναι προσανατολισμένο στην αποστολή πακέτων, το ICMP είναι αναξιόπιστη υπηρεσία host-to-host διαγραμμάτων σε ένα σύστημα διασυνδεόμενων δικτύων και δεν προσφέρει καμία εγγύηση παράδοσης. Το ICMP χρησιμοποιεί τη βασική υποστήριξη του IP σαν να ήταν ένα πρωτόκολλο πιο υψηλού επιπέδου. Εντούτοις, το ICMP είναι ένα αναπόσπαστο τμήμα του IP -- που βασικά σημαίνει ότι τα πακέτα ICMP χρησιμοποιούν την επικεφαλίδα του IP για τη μετάδοση -- και πρέπει να εφαρμοστεί από κάθε ενότητα IP. Χαρακτηριστικά, το ICMP χρησιμοποιείται για να αναφέρει τα λάθη στην επεξεργασία διαγραμμάτων δεδομένων σε έναν host. Μερικές λειτουργίες του ICMP περιλαμβάνουν:

- **Μήνυμα απρόσιτου προορισμού (Destination Unreachable Message):** Εάν, σύμφωνα με τους πίνακες δρομολόγησης της πύλης, η διεύθυνση προορισμού που διευκρινίζεται στο διάγραμμα δεδομένων που διαβιβάζεται δεν είναι εφικτή στην πρόσβαση, θα επιστρέψει ένα μήνυμα (**Destination Unreachable Message)** ICMP στον προορισμό του αρχικού host, που ενημερώνει το ότι η παράδοση πακέτων δεν ήταν επιτυχής.

- **Μήνυμα Υπερβαίνοντος χρόνου(Time Exceeded Message):** Κάθε IP διάγραμμα δεδομένων περιέχει έναν τομέα στην επικεφαλίδα του, που προσδιορίζει πόσο περισσότερο το διάγραμμα δεδομένων πρόκειται να παραμείνει στο διαδίκτυο προτού να απορριφθεί. Ο χρόνος που το διάγραμμα δεδομένων παραμένει στο διαδίκτυο μετριέται σε hops όπου ένα hop αντιπροσωπεύει μια πύλη στην πορεία του διαγράμματος δεδομένων στον κόμβο προορισμού. Όταν ένα διάγραμμα δεδομένων προωθείται από μια πύλη, μειώνει την τιμή του στο πεδίο του χρόνου ζωής κατά ένα. Εάν η πύλη που επεξεργάζεται ένα διάγραμμα δεδομένων καθορίζει ότι το πεδίο του χρόνου ζωής στην IP επικεφαλίδα του διαγράμματος δεδομένων είναι 0, απορρίπτει το διάγραμμα δεδομένων και ειδοποιεί τον αποστολέα host στέλνοντας ένα μήνυμα υπερβαίνοντος χρόνου.

- **Μηνύματα Echo Request και Echo Reply:** Εάν ο Host A θέλει να ανακαλύψει εάν ο Host B είναι ενεργός, ο Host A θα στείλει ένα ICMP μήνυμα Echo Request στον Host B. Ο Host B θα απαντήσει με ένα μήνυμα ICMP Echo Reply για να δείξει ότι είναι ενεργός. Αυτό το μήνυμα είναι συνήθως γνωστό ως ping packet.

Αυτοί δεν είναι οι μόνοι τύποι μηνυμάτων που χρησιμοποιούνται από το ICMP. Παρ' όλα αυτά η περιγραφή τους βοηθά στην κατανόηση των επιθέσεων που θα παρουσιαστούν παρακάτω

### *2.4.2. Επίθεση Απρόσιτου προορισμού*

**Κατηγορία:** Επίθεση άρνησης των υπηρεσιών

**Περιγραφή:** το ICMP μήνυμα απρόσιτου προορισμού δίνει σε μια πύλη που προσπαθεί να προωθήσει ένα μήνυμα, ένα εργαλείο που ενημερώνει τον αποστολέα ότι το μήνυμα δεν μπορεί να παραδοθεί επειδή ο host που προσδιορίστηκε στη διεύθυνση προορισμού του διαγράμματος δεδομένων δεν μπόρεσε να προσεγγιστεί.
Μια "επίθεση απρόσιτου προορισμού" θα μπορούσε να είναι κάπως έτσι: Υποθέτουμε ότι η πύλη G συνδέει δύο δίκτυα: Το δίκτυο 10.1.0.0 και το δίκτυο 10.2.0.0. Υποθέτουμε ότι ο Host A, του οποίου η διεύθυνση είναι 10.1.23.3 (επομένως ανήκει στο δίκτυο 10.1.0.0), θέλει να στείλει ένα διάγραμμα δεδομένων στον Host B, του οποίου η διεύθυνση είναι 10.2.156.34 (επομένως ανήκει στο δίκτυο 10.2.0.0). Κατά μήκος της διαδρομής του, το διάγραμμα δεδομένων θα σταλεί στην πύλη G, η οποία στη συνέχεια θα το προωθήσει στον host του προορισμού του.
Εάν ένας εισβολέας αποκτούσε πρόσβαση σε έναν host στο δίκτυο 10.1.0.0, θα μπορούσε να μεταδίδει ένα " μήνυμα απρόσιτου προορισμού" δηλώνοντας ότι η πύλη G δεν είναι προσβάσιμη σε όλους τους hosts στο δίκτυο που είναι. Αυτό θα έκανε την πύλη G και το δίκτυο 10.2.0.0 προσωρινά μη διαθέσιμο, καθιστώντας αδύνατη την διαβίβαση οποιουδήποτε μηνύματος από το δίκτυο 10.1.0.0 στο δίκτυο 10.2.0.0.
Το κίνητρο πίσω από αυτήν την επίθεση είναι απλά να τεθεί ένα δίκτυο ή μια υπηρεσία προσωρινά εκτός λειτουργίας. Είναι ιδιαίτερα επικίνδυνο επειδή ο επιτιθέμενος δεν χρειάζεται μια ισχυρή μηχανή ή μια ισχυρή σύνδεση δικτύων για να εκτελέσει αυτήν την επίθεση.

### *2.4.3. Επίθεση Smurf*

**Κατηγορία:** Επίθεση άρνησης των υπηρεσιών
**Περιγραφή:** Η επίθεση Smurf είναι μια τρομακτική μορφή επίθεσης άρνησης των υπηρεσιών λόγω των επιπτώσεων διευρύνσεως της. Η επίθεση Smurf χρησιμοποιεί τα μηνύματα echo του ICMP. Όπως περιγράφεται ανωτέρω, κάθε φορά που στέλνεται ένα μήνυμα αιτήματος (Echo Request) από τον Host A στον Host B, ο Host B θα επιστρέψει ένα μήνυμα απάντησης (Echo Reply) που δείχνει ότι είναι ενεργός. Το όνομα "επίθεση Smurf" προέρχεται από το όνομα ενός εκ των προγραμμάτων εκμετάλλευσης των αδυναμιών των συστημάτων -- αποκαλούμενα *smurf* --τα οποία κάνουν χρήση οι επιτιθέμενοι για να εκτελέσουν αυτήν την επίθεση.
Πριν γίνει αναφορά με λεπτομέρειες σε αυτήν την επίθεση πρέπει να γίνει κατανοητή η έννοια του όρου spoofing. Το spoofing μπορεί να ερμηνευθεί ως όρος ασφάλειας δικτύων που χρησιμοποιείται για “πλαστογράφηση”. Σημαίνει ότι για τους επιτιθεμένους υπάρχει ένας τρόπος κατασκευής δικτυακών διαγραμμάτων δεδομένων που περιέχουν λανθασμένα στοιχεία. Παραδείγματος χάριν, ο επιτιθέμενος θα μπορούσε να στείλει ένα διάγραμμα δεδομένων από τον Host A στον Host B, αλλά χρησιμοποιώντας τη διεύθυνση IP του Host C στον τομέα διευθύνσεων της επικεφαλίδας προέλευσης των διαγραμμάτων δεδομένων. Με αυτόν τον τρόπο, ο Host B σκέφτεται το πακέτο προήλθε από τον Host C αντί του Host A. Στην ουσία, ο Host C έχει "υποδυθεί" τον Host A χωρίς ο Host B να το έχει αντιληφθεί.
Γνωρίζοντας αυτό, γίνεται η υπόθεση ότι ένας επιτιθέμενος κατασκευάζει έναν ICMP μήνυμα echo πού περιέχει στην επικεφαλίδα του την πλαστή διεύθυνση προέλευσης κάποιου αυθαίρετου Host A, όπως π.χ του 192.168.2.2.

Περαιτέρω υποθέτουμε ότι εκείνος ο Host A βρίσκεται στο δίκτυο 192.168.2.0, και ότι ο επιτιθέμενος στέλνει το διάγραμμα δεδομένων στη διεύθυνση της δικτυακής μετάδοσης αυτού του δικτύου αντί σε έναν συγκεκριμένο Host. Με την αποστολή αυτού του διαγράμματος δεδομένων στη διεύθυνση μετάδοσης του δικτύου, το διάγραμμα δεδομένων θα μεταδίδεται σε κάθε Host σε αυτό το δίκτυο, και κάθε Host σε αυτό το δίκτυο θα επιστρέψει ένα μήνυμα απάντησης (Echo Reply) στον υποτιθέμενο αποστολέα, Host A. Υποθέτοντας ότι υπάρχουν 255 υποδίκτυα, κάθε ένα από τα οποία περιέχουν 255 υπολογιστές, πάνω από *65.000* υπολογιστές θα έστελναν ένα μήνυμα απάντησης στον Host A -- και αυτό γίνεται εάν ο επιτιθέμενος μεταδώσει μόνο ένα πλαστό διάγραμμα δεδομένων (255 * 255 = 65,025). Με την αύξηση της μετάδοσης του αριθμού των πλαστών πακέτων ή του μεγέθους της δικτυακής μετάδοσης, μπορεί να γίνει εύκολα αντιληπτό ότι αυτή μπορεί να είναι μια πολύ σοβαρή μορφή επίθεσης.
Το κίνητρο μιας επίθεσης Smurf είναι το ίδιο με πριν. Γίνεται εύκολα αντιληπτό ότι ένας επιτιθέμενος θα μπορούσε να θέσει εκτός λειτουργίας ακόμη και έναν κεντρικό υπολογιστή δικτύου αρκετά μεγάλης υπολογιστικής δύναμης λόγω των αποτελεσμάτων της διευρύνσεως της επίθεσης. Πάλι, ο επιτιθέμενος απαιτεί πολύ λίγους πόρους.

### *2.4.4. Πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol)-TCP*

Το πρωτόκολλο TCP παρέχει μια προσανατολισμένη προς τη σύνδεση, αξιόπιστη, υπηρεσία παράδοσης ροής στα packet-switched δίκτυα υπολογιστών. Αυτό σημαίνει ότι οι διαμορφώσεις του TCP εγγυούνται την παράδοση χωρίς το διπλασιασμό, κανένα λάθος μετάδοσης, και τα δεδομένα διαβιβάζονται με τη σωστή σειρά. Το TCP παρέχει περαιτέρω την αφαίρεση θυρών, η οποία επιτρέπει σε έναν host να ανοίξει πολλαπλές συνδέσεις TCP παράλληλα. Από αυτό γίνεται αντιληπτό ότι το TCP προσδιορίζεται από την διεύθυνση προέλευσης και προορισμού. Η διεύθυνση /θύρα των ζευγών IP καλείται *υποδοχή (socket*.).
Το TCP αλληλεπιδρά με το στρώμα IP κάτω από και τα πρωτοκόλλα του στρώματος παρουσίασης - και εφαρμογής- (όπως Telnet και SMTP) Σχήμα 1.
Πριν συνεχίσουμε, θα ήταν χρήσιμο να αναφερθούν μερικές πτυχές του TCP λεπτομερέστερα, κάτι το οποίο είναι απαραίτητο για την κατανόηση των επιθέσεων που θα συζητηθούν κατωτέρω. Ειδικότερα αυτό θα είναι το σχεδιάγραμμα των πακέτων TCP (αποκαλούμενα τομείς- *segments*), για το πώς οι συνδέσεις TCP στήνονται μεταξύ των hosts, και πώς διακόπτονται.

### *Σχεδιάγραμμα των πακέτων TCP*

Όπως το διάγραμμα δεδομένων IP, ο τομέας του TCP αποτελείται από μια μερίδα επικεφαλίδων, ένα προαιρετικό τμήμα (επιλογών), και τη τμήμα δεδομένων.Μερικοί από τους σημαντικούς τομείς της επικεφαλίδας του TCP είναι οι εξής:

- **Θύρα προέλευσης (Source port):** Ο αριθμός θύρας που ανατίθεται στην εικονική σύνδεση στον host με την αρχική σύνδεση.

- **Θύρα προορισμού (Destination port):** Ο αριθμός θύρας προορισμού. Αυτός θα οριστεί επίσης από τον host με την αρχική σύνδεση. Παραδείγματος χάριν, εάν ανοίξει μια σύνδεση Telnet σε έναν συγκεκριμένο host, η θύρα προορισμού θα τεθεί η 23,

- **Αριθμός ακολουθίας και αριθμός αναγνώρισης (Sequence number and acknowledgment number):** Δύο αριθμοί ακολουθίας χρησιμοποιούνται από τον αποστολέα και το δέκτη για να εξασφαλίσουν ότι κανένα πακέτο δεν χάνεται, ότι δεν υπάρχει κανένας διπλασιασμός, και ότι τα πακέτα μπορούν να συγκεντρωθούν εκ νέου στη σωστή σειρά στον κόμβο προορισμού

- **Σημαίες (Flags):** Αυτός ο τομέας περιέχει έξι bits ελέγχου:
    - **URG:** Υποδεικνύει στο δέκτη να κάνει την επείγουσα επεξεργασία εφ' όσον υπάρχουν δεδομένα που καταστρέφονται.
    - **ACK:** Υποδεικνύει ότι ο τομέας αριθμού αναγνώρισης είναι σημαντικός. Αν το bit ειναι 1 πάει να πεί ότι το acknowledgement number είναι έγκυρο. Αν είναι 0 ο τομέας δεν περιέχει επαλήθευση και έτσι αγνοείται το περιεχόμενο του πεδίου acknowledgement number.
    - **PSH:** Υποδεικνύει ότι τα δεδομένα πρέπει να διαβιβαστούν στο δέκτη αμέσως.
    - **RST:** Υποδεικνύει ότι η σύνδεση πρόκειται να επαναρυθμιστεί αμέσως. Ουσιαστικά χρησιμοποιείται για να υποδηλώνει connection request και connection accepted με το bit ACK να διαχωρίζει τις δυο αυτές περιπτώσεις.
    - **SYN:** Ταξινομεί τις περιπτώσεις που οι αριθμοί ακολουθίας πρέπει να συγχρονιστούν.
    - **FIN:** Υποδεικνύει ότι δεν θα υπάρξουν άλλα δεδομένα από τον αποστολέα (δηλαδή η σύνδεση θα διακοπεί.


**Εικόνα 2.2 Η επικεφαλίδα TCP**

Αυτοί είναι σημαντικοί τομείς στην επικεφαλίδα του TCP και παρακάτω θα φανεί καλύτερα η χρησιμότητα τους:

## *Οργάνωση και διακοπή των συνδέσεων TCP*

**Οργάνωση σύνδεσης:** Η οργάνωση μιας σύνδεσης TCP πραγματοποιείται από μια "συμφωνία" κατανεμημένη σε τρία στάδια, μεταξύ ενός πελάτη (client) που θέλει να εγκαταστήσει τη σύνδεση και τον κεντρικό υπολογιστή (server) που έρχεται σε επαφή με τον πελάτη. Για να γίνει η αρχή, χρειάζεται ένας κεντρικός υπολογιστής που προσφέρει μια υπηρεσία σε μία συγκεκριμένη θύρα π.χ η υπηρεσία Telnet που υπακούει στη θύρα 23. Όταν ένας client θέλει να ανοίξει μια σύνδεση σε έναν server, στέλνει ένα αίτημα σύνδεσης σε αυτόν τον server. Αυτό σημαίνει ότι ένα πακέτο TCP με το σύνολο SYN σημαιών στέλνεται στον server. Ο server απαντά με ένα πακέτο όπου τίθενται οι σημαίες SYN και ACK. Τέλος, ο πελάτης επιβεβαιώνει αυτό με την αποστολή ενός πακέτου TCP πίσω στον server με το σύνολο σημαιών ACK. Μετά από αυτό, καθιερώνεται η σύνδεση μεταξύ του client και του server.

**Κλείσιμο σύνδεσης:** Μόλις σταλούν όλα τα στοιχεία, ένας από τους συνεργάτες της επικοινωνίας θα θελήσει να διακόψει τη σύνδεση. Γίνεται η υπόθεση ότι ο client θέλει να τερματίσει τη σύνδεση. Θα το κάνει αυτό με την αποστολή ενός πακέτου TCP με το σύνολο των FIN σημαιών στον server. Ο server θα το αναγνωρίσει αυτό με την επιστροφή ενός πακέτου με το σύνολο σημαιών ACK. Από αυτό το σημείο στον client δεν θα σταλούν άλλα δεδομένα από τον server. Θα αναγνωρίζει μόνο τα δεδομένα με κενούς τομείς, που στέλνονται από τον server. Όταν ο server διακόπτει το ρεύμα του, η σύνδεση είναι κλειστή.

Με την κατανόηση των παραπάνω, μπορούν πιο εύκολα να γίνουν κατανοητά τα παραδείγματα επιθέσεων TCP που ακολουθούν:

### *2.4.5. Ανίχνευση TCP SYN (TCP SYN scanning)*

**Κατηγορία:** Ανίχνευση θυρών

**Περιγραφή:** Η ανίχνευση TCP SYN είναι μια παραλλαγή της ανίχνευσης θυρών. Η ανίχνευση θυρών χρησιμοποιείται για να ελέγξει εάν οι θύρες σε έναν δεδομένο host είναι ανοικτές. Η συγκέντρωση αυτού του είδους πληροφοριών είναι μέρος του footprinting, στο οποίο έγινε αναφορά παραπάνω (Κατηγορίες επιθέσεων) και χρησιμοποιούνται για να πάρουν πρόσθετες πληροφορίες για έναν host.

Γνωρίζοντας ποιες θύρες είναι ανοικτές σε έναν host είναι ένα σημαντικό πρώτο βήμα για έναν επιτιθέμενο για να διαπιστώσει τις πιθανές ευπάθειες στον host-στόχο.
Η απλούστερη μορφή μιας ανίχνευσης θυρών TCP είναι να ανοιχτεί μια σύνδεση σε όλες τις θύρες σε έναν host. Εάν το άνοιγμα μιας σύνδεσης σε μια δεδομένη θύρα πετυχαίνει, ένας επιτιθέμενος ξέρει ότι η υπηρεσία είναι διαθέσιμη. Εντούτοις, ο επιτιθέμενος θέλει γενικά να εκτελέσει μια ανίχνευση θυρών χωρίς να ενημερώσει τον ανιχνευόμενο host ότι αυτός ανιχνεύεται, δεδομένου ότι τα λειτουργικά συστήματα ή και κάποια εργαλεία να καταγράψουν αυτόν τον τύπο δραστηριότητας και επομένως να αντιληφθούν μια ανίχνευση θυρών. Σε αυτό το σημείο, θα περιγραφεί μια μορφή ανίχνευσης θυρών που χρησιμοποιείται από τους επιτιθεμένους και δεν μπορεί εύκολα να ανιχνευθεί από τον host-στόχο.
Η ανίχνευση TCP SYN είναι επίσης γνωστή ως κατά το ήμισυ ανοικτή (half open) ανίχνευση. Όπως το όνομα μαρτυρά, ο επιτιθέμενος ανοίγει τη σύνδεση μόνο στα μισά της διαδρομής. Για να επιτύχει αυτό, ο επιτιθέμενος στέλνει ένα πακέτο TCP με το σύνολο σημαιών SYN στον host-στόχο, ακριβώς όπως κατά άνοιγμα μιας κανονικής σύνδεσης TCP. Στην απάντηση, ο ανιχνευόμενος host επιστρέφει ένα πακέτο με τα σύνολα των SYN και ACK σημαιών εάν η θύρα είναι ανοικτή. Εάν η θύρα δεν είναι ανοικτή, στέλνει ένα πακέτο με το σύνολο των σημαιών RST και ACK.
Μόλις επιστρέψει ο ανιχνευόμενος host ένα πακέτο SYN/ ACK, η σύνδεση θα πάει σε μια εν αναμονή κατάσταση στην πλευρά του server, δείχνοντας ότι η σύνδεση είναι στο στάδιο της εγκατάστασης, αλλά δεν εγκαθίσταται πλήρως ακόμα. Εντούτοις, σε απάντηση του πακέτου SYN /ACK ο επιτιθέμενος θα στείλει ένα πακέτο με το σύνολο σημαιών RST και ACK. Αυτό θα προκαλέσει τον ανιχνευόμενο host να κλείσει την κατά το ήμισυ εγκατεστημένη σύνδεση πάλι.
Η ιδέα είναι να ανακαλυφθούν ποιες θύρες είναι ανοικτές σε έναν συγκεκριμένο host-στόχο, αλλά αυτό γίνεται με έναν τέτοιο περίπλοκο τρόπο που ο επιτεθέμενος host ή ένα χαμηλής ποιότητος εργαλείο ανίχνευσης παρείσφρησης δεν μπορεί να παρατηρήσει.

### *2.4.6. Πλημμύρα SYN (SYN flooding)*

**Κατηγορία:** Επίθεσης άρνησης των υπηρεσιών

**Περιγραφή:** Προτού γίνει μόδα η επίθεση Smurf, η επίθεση πλημμύρων SYN ήταν η πιο καταστρεπτική επίθεση άρνησης των υπηρεσιών. Όπως αναφέρεται παραπάνω, όταν θέλει ο Host A να εγκαταστήσει μια σύνδεση TCP στον Host προορισμού D, στέλνει πρώτα ένα τομέα του TCP με το σύνολο των σημαιών SYN. Κατά τη λήψη αυτού του τομέα, ο Host D τον αναγνωρίζει με την επιστροφή ενός πακέτου με το σύνολο των σημαιών SYN και ACK. Αλλά ο Host D βάζει επίσης την εν αναμονή -- εν μέρει ανοιγμένη -- σύνδεση σε μια ουρά εκκρεμής-σύνδεσης. Η σύνδεση κρατιέται σε μια κατάσταση αναμονής καθώς περιμένει την αναγνώριση από το δημιουργό της, τον Host A.
Ο Host D περιμένει την αναγνώριση να φθάσει για μια ορισμένη περίοδο διαλείμματος, χαρακτηριστικά οποτεδήποτε από 75 δευτερόλεπτα έως και 25 λεπτά στις σπασμένες εφαρμογές IP. Δεδομένου ότι η ουρά της εκκρεμής-σύνδεσης έχει μόνο ένα περιορισμένο μέγεθος, θα γεμίσει τελικά. Έτσι γίνεται αντιληπτό ότι ο επιτιθέμενος θα πρέπει μόνο να στείλει μερικά πακέτα SYN κάθε δέκα δευτερόλεπτα ή παραπάνω και έτσι να θέσει εκτός λειτουργίας μία συγκεκριμένη θύρα. Αυτή η μέθοδος επίθεσης είναι μια πολύ σοβαρή μορφή επίθεσης άρνησης των υπηρεσιών, δεδομένου ότι το επιτεθέμενο σύστημα δεν θα είναι σε θέση ποτέ να καθαρίσει τη ουρά ανεκτέλεστης παραγγελίας πριν να λάβει τα νέα πακέτα SYN, και επομένως δεν θα είναι σε θέση να ανταποκριθεί σε οποιαδήποτε άλλα αιτήματα.
Το κίνητρο είναι σαφές και σε αυτήν την περίπτωση. Ο επιτιθέμενος θέλει να θέσει μια ορισμένη υπηρεσία -- παραδείγματος χάριν έναν Web server – εκτός λειτουργίας. Πάλι, βλέπουμε ότι αυτή η επίθεση μπορεί να εκτελεσθεί με πολύ λίγους πόρους εκ μέρους του επιτιθεμένου.

### *2.4.7. **IP** spoofing*

Ένας μεγάλος αριθμός επιθέσεων χρησιμοποιεί την αλλαγή της πηγής της διεύθυνσης IP. Το πρωτόκολλο TCP/IP δεν έχει κανέναν τρόπο να ελέγξει εάν η διεύθυνση πηγής IP στην επικεφαλίδα του πακέτου ανήκει πραγματικά στη μηχανή που το στέλνει. Μερικές από τις επιθέσεις που εκμεταλλεύονται την IP spoofing είναι:

## *Ανιχνεύσεις UDP*

Λόγω του σχεδιασμού του UDP, η ανίχνευση αυτού του πρωτοκόλλου, είναι αρκετά πιο αργή και παράγει πολλά ψευδές θετικά. Αυτό οφείλεται στο γεγονός ότι το UDP είναι ένα πρωτόκολλο χωρίς σύνδεση που σημαίνει ότι όταν μια θύρα είναι ανοικτή δεν είναι απαραίτητο να στείλει μια επιβεβαίωση ότι το πακέτο UDP παραλήφθηκε. Οι περισσότερες εφαρμογές UDP στέλνουν ένα πακέτο μηνύματος απρόσιτου προορισμού ICMP όταν η θύρα είναι κλειστή. Τα Firewalls πρέπει να διαμορφωθούν για να μην αποκρίνονται στη θύρα απρόσιτου προορισμού ICMP - αυτό θα δυσκόλευε πολύ στους χάκερ που χρησιμοποιούν την παραδοσιακή ανίχνευση UDP. Εκτός από αυτό, υπάρχουν πολλά μηχανήματα ρύθμισης ICMP μηνυμάτων, που σημαίνει ότι η ανίχνευση τέτοιων μηχανών είναι μια πολύ αργή διαδικασία.

### *2.4.8. Buffer overflow σε ένα συστατικό του Distributed Component Object Model (DCOM)*

#### 2.4.8.1. Τι είναι μια υπερχείλιση Buffer Overflow

Μια υπερχείλιση buffer είναι ένα λάθος ενός προγραμματιστή που μπορεί να προέλθει από διάφορα προβλήματα. Όπως το όνομα υπονοεί, το θεμελιώδες ζήτημα είναι ότι ένα πρόγραμμα προσπαθεί να αποθηκεύσει περισσότερα δεδομένα σε έναν buffer από ότι ο buffer σχεδιάστηκε για να κρατήσει. Αυτό το λάθος μπορεί να πάρει πολλές διαφορετικές μορφές. Ενώ μερικά από τα κατασκευάσματα που προκαλούν αυτόν τον τύπο προβλήματος είναι προφανή, άλλα μπορούν είναι εξαιρετικά δύσκολο να βρεθούν.

Για να εκμεταλλευτεί μια υπερχείλιση buffer, ένας επιτιθέμενος θα πρέπει να δημιουργήσει ένα ειδικά επεξεργασμένο μήνυμα που αναγκάζει περισσότερα στοιχεία να αποθηκεύονται σε έναν buffer από ότι ο buffer σχεδιάστηκε να κρατήσει. Ο υπερβολικά μεγάλος αριθμός δεδομένων καταλήγει να μπαίνει πάνω από διάφορες άλλες μερίδες της μνήμης. Εάν αυτή η μερίδα της μνήμης περιέχει οδηγίες που για να εκτελέσει, ο υπολογιστής θα προσπαθήσει να ερμηνεύσει τα δεδομένα που στέλνονται από τον επιτιθέμενο ως οδηγίες και να τα εκτελέσει. Σε μερικές περιπτώσεις, είναι δυνατό να επικαλυφθεί ο buffer με δεδομένα που είναι πραγματικά εκτελέσιμος κώδικας προγράμματος, κάτι που αναγκάζει τον υπολογιστή να εκτελέσει τον αυθαίρετο κώδικα. Αυτό είναι γνωστό ως "εκμεταλλεύσιμη" υπερχείλιση buffer.

## *2.5. Τι πρέπει να κάνουν οι Administrators*

Κατά πολύ ο σημαντικότερος παράγοντας στην καταπολέμηση αυτών των ζητημάτων είναι να επιδιορθωθούν όλα τα τρωτά συστήματα στο περιβάλλον το συντομότερο δυνατόν. Ενώ διάφοροι μετριασμοί είναι διαθέσιμοι, δεν υπάρχει κανένα υποκατάστατο της εγκατάστασης του patch. Ακόμα κι ένα σύστημα που δεν συνδέεται άμεσα με το διαδίκτυο, θα μπορούσε ακόμα να είναι τρωτό στην επίθεση από τα έμπιστα συστήματα.Εκείνα τα συστήματα περιλαμβάνουν χαρακτηριστικά άλλους hosts σε ένα εταιρικό ενδοδίκτυο (intranet), τους hosts που συνδιαλέγονται μέσα σε ένα δίκτυο μέσω VPN ή dial-in, και οποιοδήποτε άλλο host που μπορούν να φτάσουν πίσω από το firewall που προστατεύει ένα δίκτυο από το διαδίκτυο. Επιπλέον, μετριασμοί, που μπορούν να θέσουν εκτός λειτουργίας το Remote Procedure Call RPC ή/και το Distributed Component Object Model DCOM σε ένα ενδοδίκτυο, μεταβάλλουν πολλά χαρακτηριστικά και αποτρέπουν μερικά μέρη του συστήματος να λειτουργήσουν κανονικά. Επομένως, η προτιμημένη προσέγγιση είναι η εγκατάσταση του patch σε όλα τα συστήματα το συντομότερο δυνατόν .

### 2.5.1. Ανίχνευση των τρωτών συστημάτων

Υπάρχουν διάφοροι τρόποι να ανιχνευθεί εάν σε ένα σύστημα έχει εγκατασταθεί patch. Η απλούστερη μέθοδος για να αξιολογηθεί ένα σύστημα είναι να χρησιμοποιηθεί το Windows Update, (http://windowsupdate.microsoft.com). Εντούτοις, για πελάτες με μεγάλες εγκαταστάσεις, καταλληλότερες είναι άλλες μέθοδοι. Στα μεγάλα δίκτυα όπου είναι παρούσα μια διοικητική υποδομή δικτύων, οι administrators μπορούν να ανιχνεύσουν το patch με την έρευνα των ακόλουθων κλειδιών του μητρώου:

- **Windows Server 2003**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP1\KB824146
- **Windows XP Gold**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\KB824146
- **Windows XP SP1**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB824146
- **Windows XP 64-bit Edition, Version 2003**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP1\KB824146
- **Windows 2000**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB824146
- **Windows NT 4.0 Workstation, SP6a**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Hotfix\824146
- **Windows NT 4.0 Server, SP6a**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Hotfix\824146
- **Windows NT 4.0, Terminal Services Edition, SP6a**
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Hotfix\824146

# ΚΕΦΑΛΑΙΟ 2ο

# 3. ΤΡΟΠΟΙ ΕΙΣΒΟΛΗΣ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ

## 3.1. Γνωστές τρύπες Ασφάλειας

Είναι λογικό οι επιτιθέμενοι σε ένα σύστημα να είναι πάντα ένα βήμα μπροστά από τους αμυνόμενους οι οποίοι τις περισσότερες φορές βρίσκουν εκ των υστέρων τρόπο να αποκρούσουν τις επιθέσεις. Με την κυκλοφορία ενός νέου ιού ή της εκμετάλλευσης κάποιας αδυναμίας του κώδικα των windows κατόπιν ακολουθεί και η κυκλοφορία κάποιου patch το οποίο θα υπερασπιστεί το σύστημα φτάνει αυτό να μην έχει ήδη μολυνθεί**.**

### *3.1.1. ActiveX*

Η τεχνολογία ActiveX χρησιμοποιείται στο πρόγραμμα πλοήγησης Internet Explorer, στο πρόγραμμα ηλεκτρονικού ταχυδρομείου Outlook Express καθώς και σε πολλές άλλες εφαρμογές των Windows, επιτρέποντας τη μεταξύ τους συνεργασία. Οι εντολές ActiveX μπορούν να ενεργοποιηθούν αυτόματα όταν ο χρήστης επισκέπτεται ένα δικτυακό τόπο. Οι ActiveX ενσωματώνονται στον κώδικα HTML ενός δικτυακού τόπου υπό τη μορφή εντολών γλώσσας script (π.χ. javascript), ή μέσω της ετικέτας (tag) OBJECT της HTML. Η ιδιότητά τους αυτή να εκτελούνται αυτόματα τις καθιστά καλό όπλο στα χέρια των επίδοξων χάκερ.

### *3.1.2. Remote procedure Call*

Η ατέλεια εντοπίστηκε στο στοιχείο των Windows που επιτρέπει σε άλλους υπολογιστές να αποκτούν πρόσβαση σε κοινόχρηστους φακέλους και εκτυπωτές και να ζητούν από το λειτουργικό σύστημα την εκτέλεση ενεργειών (Remote procedure Call). Το κενό ασφάλειας ενυπάρχει και στη νέα έκδοση του λειτουργικού για διακομιστές Windows Server 2003. «*Θα έδινε στον επιτιθέμενο τη δυνατότητα να προχωρήσει σε οποιαδήποτε ενέργεια στον διακομιστή*» αναφέρει ανακοίνωση της Microsoft. «*Για παράδειγμα, ο επιτιθέμενος θα μπορούσε να παραποιήσει ιστοσελίδες, να διαγράψει το σκληρό δίσκο, ή να προσθέσει νέους χρήστες στην ομάδα των διαχειριστών του συστήματος*» προσθέτει. Τα Windows Server 2003, που κυκλοφόρησαν τον Απρίλιο, είναι η πρώτη έκδοση του λειτουργικού που κυκλοφόρησε αφότου η Microsoft παρουσίασε το πρόγραμμα Trustworthy Computing initiative για τη βελτίωση της αξιοπιστίας και της ασφάλειας του λογισμικού.

### *3.1.3. JVM (Java Virtual Machine)*

Ένα σοβαρό κενό ασφάλειας στην JVM (Java Virtual Machine) των Windows μπορεί να επιτρέψει σε hackers να αποκτήσουν τον πλήρη έλεγχο ενός PC. Για να εκμεταλλευτεί κανείς αυτό το κενό ασφάλειας δημιουργεί αρχικά μία

'κατάλληλα' διαμορφωμένη σελίδα του Web, την οποία και χρησιμοποιεί για να διεισδύσει σε άλλους υπολογιστές. Το κενό ασφάλειας εμφανίζεται σε διάφορες τάξεις objects που συνοδεύουν την Java. Για την αντιμετώπισή του η Microsoft προτείνει τα εξής: Όποιος διαθέτει έκδοση της JVM προγενέστερη της 3805, πρέπει να κατεβάσει κατ' αρχάς την τελευταία έκδοση από το Internet και στη συνέχεια το patch. Όποιος διαθέτει την έκδοση 3805 ή μεταγενέστερη πρέπει να εγκαταστήσει μόνο το patch. Τόσο η τρέχουσα έκδοση της JVM όσο και το patch εγκαθίστανται μέσω της λειτουργίας 'Windows Update' ή με μία επίσκεψη στο windowsupdate.microsoft.com.

## *3.2. **Ιοί Υπολογιστών***

Στη βασικότερη έννοια, οι ιοί υπολογιστών είναι προγράμματα ή μακροεντολές που κάνουν ενέργειες (συχνά καταστροφικές) που δεν τις περιμένουμε. Μπορεί να εμφανίζουν προσβλητικά ή πολιτικά μηνύματα στην οθόνη, να διαγράφουν αρχεία από τον σκληρό δίσκο ή να σβήνουν το λειτουργικό σύστημα του υπολογιστή. Ορισμένα προγράμματα ιών λειτουργούν με καθυστέρηση, οπότε με τη χρησιμοποίηση τους τα περνάνε και σε άλλους, πριν να γίνει αντιληπτό. Πολλά από αυτά είναι ύπουλα , αλλάζοντας αργά, επιλεγμένα αρχεία ώσπου μια μέρα το σύστημά δε δουλεύει. Οι παραλλαγές είναι πολλές αλλά το τελικό αποτέλεσμα είναι το ίδιο: διακοπή ή καταστροφή των λειτουργιών του υπολογιστή.

Το όνομα ιός είναι άκρως κατάλληλο. Οι ιοί υπολογιστών μιμούνται την συμπεριφορά των βιολογικών ιών κατά πολλούς τρόπους. Όπως ο ιός της γρίπης κολλάει σε ένα ανθρώπινο ξενιστή, έτσι και οι ιοί υπολογιστών κολλούν σε προγράμματα ή σε αρχεία. Επίσης σαν τον ιό της γρίπης οι ιοί υπολογιστών είναι κολλητικοί και μερικοί χρησιμοποιούν πόρους ενός συστήματος ξενιστή για να αναπαραχθούν.

Ένας ορισμός της έννοιας ιός του υπολογιστή είναι: «*ένα πρόγραμμα που αναπαράγεται προσβάλλοντας-μολύνοντας άλλα προγράμματα ώστε να περιέχουν ένα αντίγραφο του ιού*».

Η μόλυνση περιγράφεται και ως προσκόλληση του προγράμματος του ιού σε ένα ή περισσότερα προγράμματα στο προσβαλλόμενο σύστημα. Ωστόσο η λέξη προσκόλληση δεν είναι σωστή γιατί η λέξη επισύναψη έχει μάλλον άλλη σημασία όταν μιλάμε για email. Καλύτερα είναι να μιλήσουμε για μια αλυσίδα εντολής. Ο κώδικας του ιού ενσωματώνεται μέσα στην αλυσίδα της εντολής ούτως ώστε όταν τρέξει το νόμιμο αλλά μολυσμένο πρόγραμμα, να εκτελείται και ο κώδικας του ιού.

### *3.2.1. Γιατί υπάρχουν οι ιοί*

Οι άνθρωποι δημιουργούν ιούς υπολογιστών για διάφορους λόγους. Τα κίνητρα περιλαμβάνουν, χωρίς να παίζει ρόλο η σειρά που αναφέρονται:

- Εκδίκηση εναντίον ενός συγκεκριμένου συστήματος ή ομάδας χρηστών υπολογιστών
- Επιθυμία να ακουστεί το όνομα τους (αν και είναι ανώνυμοι)

- Φάρσες
- Πολιτικές πράξεις
- Πειραματισμούς («να δω αν μπορώ να το κάνω»)

Ο λαϊκός τύπος έχει σκιαγραφήσει τους δημιουργούς ιών σαν έξυπνους παλιάνθρωπους. Οι δημοσιογράφοι δε, έχουν δηλώσει ότι ορισμένοι δημιουργοί ιών είναι ανικανοποίητοι στις προσωπικές τους ζωές και ενεργούν από μια βαθιά ανάγκη να έχουν τον έλεγχο των πραγμάτων.

Όποιοι και να είναι οι λόγοι που οι προγραμματιστές δημιουργούν ιούς και προγράμματα Δούρειους Ίππους, οι λόγοι αυτοί δεν παίζουν κανένα ρόλο αν ο χρήστης κολλήσει ένα ιό. Έτσι, πρέπει να υπάρχει κάθε δυνατή προφύλαξη για την αποφυγή τους.

### *3.2.2. Ποια Είδη Ιών Υπάρχουν*

Οι ιοί υπάρχουν σε πολλές παραλλαγές. Ορισμένοι ενεργοποιούνται μόνο ορισμένες ημερομηνίες (όπως για παράδειγμα ο διαβόητος ιός της ημέρας του Κολόμβου). Άλλοι εκτελούνται μόνο όταν εκτελεστεί ένα συγκεκριμένο πρόγραμμα, ή όταν ένα πρόγραμμα καλεί μια λειτουργία του συστήματος. Άλλοι πάλι ενεργοποιούνται μόλις γίνεται εκκίνηση του συστήματος. Οι ιοί χωρίζονται σε κλάσεις βάση των ακόλουθων χαρακτηριστικών:

**Α)** Σύμφωνα με το περιβάλλον στο οποίο λειτουργούνε οι ιοί χωρίζονται στις παρακάτω κατηγορίες:

- Ιοί αρχείων (**File**) είτε μολύνουν εκτελέσιμα αρχεία με πολλούς τρόπους (parasitic – ο πιο κοινός τύπος ιού), είτε δημιουργούν αντίγραφα αρχείων (companion virii), ή χρησιμοποιούν συγκεκριμένα χαρακτηριστικά του συστήματος (link virii).
- Ιοί εκκίνησης (**Boot**) είτε αποθηκεύουν τον εαυτό τους στον τομέα εκκίνησης (boot sector) του σκληρού δίσκου, ή στο Master Boot Record, ή αλλάζουν τον δείκτη ενός ενεργού boot sector.
- **Macro ιοί** Μολύνουν αρχεία κειμένου, αρχεία λογιστικών φύλλων (excel) και αρχεία βάσεων δεδομένων
- Ιοί δικτύου (**Network)** χρησιμοποιούν πρωτόκολλα και εντολές δικτύων ή ηλεκτρονικό ταχυδρομείο για να εξαπλωθούν.

**Β)** Ο δεύτερος μεγάλος διαχωρισμός γίνεται σύμφωνα με το λειτουργικό σύστημα (OPERATING SYSTEM**)** ή την έκδοση (version) των προσβαλλόμενων αρχείων. Ανάλογα με αν οι ιοί λειτουργούνε σε Dos, Windows 3.xx, 95, 98, 2000, Xp, OS/2, Linux κλπ. Μπορεί κάποιοι macro ιοί να προσβάλουν αρχεία Office 97, άλλοι μόνο Office Xp κλπ.

Οι ιοί εκκίνησης πάλι, μπορεί να είναι εξειδικευμένοι ανάλογα με το σύστημα αρχείων και να προσβάλλουν ένα συγκεκριμένο.

**Γ)** Ανάλογα με τους αλγόριθμους λειτουργίας ξεχωρίζουμε τις παρακάτω κατηγορίες:

- **TSR** ικανότητα (**Terminate and stay resident**)
- η χρήση αλγορίθμων απόκτυψης (**Stealth algorithms)**
- Χρήση **πολυμορφισμού και απόκρυψης εαυτού**
- η χρήση **μη τυπικών** μηχανισμών

Ένας **TSR ιός**, αφού μολύνει ένα υπολογιστή, αφήνει ένα κομμάτι του μόνιμα φορτωμένο στη μνήμη RAM το οποίο παρεμβάλλεται στις κλήσεις του συστήματος προς τα αρχεία και ενσωματώνει τον εαυτό του στον στόχο. Οι TSR ιοί μένουν στη μνήμη και παραμένουν ενεργοί μέχρι να κλείσει ο υπολογιστής ή μέχρι να γίνει επανεκκίνηση. Μερικοί ιοί αφήνουν μερικά κομμάτια τους στη μνήμη αλλά δεν τα χρησιμοποιούν για να μεταδώσουν τον εαυτό τους, αυτοί δεν θεωρούνται ιοί TSR.

Οι ιοί μακροεντολών θεωρούνται TSR ιοί γιατί παραμένουν στη μνήμη του υπολογιστή κατά τη διάρκεια που τρέχει το πρόγραμμα επεξεργασίας, το οποίο παίζει το ρόλο του λειτουργικού συστήματος και όταν λέμε «κλείσιμο υπολογιστή» εννοούμε το κλείσιμο του προγράμματος επεξεργασίας.

Η χρήση των **αλγορίθμων απόκρυψης** επιτρέπει στους ιούς να καλύπτουν μερικά ή ολικά τα ίχνη τους στο λειτουργικό σύστημα. Ο πιο κοινός αλγόριθμος απόκρυψης είναι η παρεμβολή στις κλήσεις του λειτουργικού συστήματος από και προς τα μολυσμένα αρχεία. Σ΄ αυτές τις περιπτώσεις οι ιοί είτε «θεραπεύουν» προσωρινά τον εαυτό τους είτε υποκαθιστούν τον εαυτό τους με «καθαρά» κομμάτια πληροφορίας. Σε περιπτώσεις ιών μακροεντολών η πιο συνηθισμένη τεχνική είναι να απενεργοποιούν τα μενού ViewMacro. Για την ιστορία, από τους πρώτους ιούς με αλγόριθμους απόκρυψης (Stealth Virus ) ήταν ο “Frodo”[1] και ο πρώτος stealth boot ιός ήταν ο “Brain”[2].

Σχεδόν όλα τα είδη ιών χρησιμοποιούν τεχνικές απόκρυψης και πολυμορφισμού για να κάνουν την ανίχνευσή τους πιο δύσκολη. Οι πολυμορφικοί ιοί είναι πραγματικά δύσκολο να ανιχνευτούν, κανένα τμήμα τους δε μένει χωρίς αλλαγές και στις περισσότερες περιπτώσεις δύο δείγματα του ίδιου ιού δεν θα έχουν ούτε ένα κοινό σημείο μετά από σύγκριση. Αυτό επιτυγχάνεται με κρυπτογράφηση του κυρίως κορμού του ιού και επιπρόσθετα κάνοντας τροποποιήσεις στη ρουτίνα αποκρυπτογράφησης.

Μια μεγάλη ποικιλία **μη τυπικών τεχνικών** χρησιμοποιείται από διάφορους ιούς για να κρύψουν τον εαυτό τους όσο βαθύτερα γίνεται στον πυρήνα του λειτουργικού συστήματος όπως πχ. ο "3APA3A" (προσβάλει το αρχείο io.sys), ή να κάνουν τη θεραπεία ακόμα πιο δύσκολη, γράφοντας τον εαυτό τους στο Flash Bios.[3]

[1] http://www.f-secure.com/v-descs/frodo.shtml

[2] http://www.europe.f-secure.com/v-descs/brain.shtml

[3] http://www.europe.f-secure.com/v-descs/3apa3a.shtml

**Δ**) Βάσει των Καταστροφικών ικανοτήτων οι ιοί ταξινομούνται ως εξής:

- **άκακοι**: δεν έχουν καμιά επίπτωση στον υπολογιστή εκτός του ότι γεμίζουν το σκληρό δίσκο ως αποτέλεσμα της εξάπλωσης τους
- **όχι επικίνδυνοι**: περιορίζονται στο να γεμίζουν το σκληρό δίσκο και εμφανίζονται με μερικά γραφικά, ήχους ή άλλες άκακες λειτουργίες όπως ανοιγοκλείσιμο cd-rom κλπ.
- **Επικίνδυνοι** ιοί οι οποίοι μπορεί να διακόψουν τη λειτουργία του υπολογιστή
- **Πολύ επικίνδυνοι** ιοί οι οποίοι προκαλούν απώλειες ή καταστροφή δεδομένων, και διαγραφή ζωτικών πληροφοριών σε περιοχές του συστήματος. Υπάρχουν κάποιο ιοί που σβήνουνε το Flash Bios του υπολογιστή καταστρέφοντας έτσι τη μητρική πλακέτα του υπολογιστή. Φήμες αναφέρουν ότι κάποιοι ιοί μπορούν να προκαλέσουν μηχανικές βλάβες σε κάποια είδη σκληρών δίσκων προκαλώντας συντονισμό!

Στην πραγματικότητα κανένας ιός δεν μπορεί να θεωρηθεί αβλαβής αφού εισέρχεται χωρίς να το θέλει ο χρήστης στο σύστημα και μπορεί να προκαλέσει προβλήματα τα οποία δεν έχουν προβλεφθεί.

Εκτός από τους ιούς υπάρχουν και άλλα «βλαβερά» προγράμματα όπως οι Δούρειοι ίπποι (Trojan Horses), κρυφά διαχειριστικά προγράμματα (BackDoors), προγράμματα κλοπής κωδικών και άλλων πληροφοριών (keyloggers) κλπ. Πρέπει να γίνει σαφές ότι ένας ιός μπορεί να περιλαμβάνει οποιαδήποτε από τα παραπάνω χαρακτηριστικά και λειτουργίες

### *3.2.3. Τι Ενέργειες Κάνουν*

Οι ενέργειες που μπορεί να κάνει ένας ιός ποικίλλουν. Όπως θα περιγραφεί στις επόμενες ενότητες, καταστρέφουν δεδομένα, κλέβουν πληροφορίες, παρενοχλούν ή αποτρέπουν την λειτουργία του υπολογιστή ή κάνουν παράξενα πράγματα όπως να επανεκκινούν τον υπολογιστή ή να κάνουν την οθόνη να τρεμοπαίζει. Ορισμένοι απλώς σας ενοχλούν διακόπτοντας την λειτουργία του υπολογιστή .

Ένα πράγμα που δεν κάνουν οι ιοί υπολογιστών είναι να καταστρέψουν τον υλικό εξοπλισμό. Επίσης δεν μπορούν να καταστρέψουν φυσικά τους δίσκους. Τα δεδομένα των δίσκων μπορούν να καταστραφούν και οι συσκευές, όπως η οθόνη και ο εκτυπωτής, μπορούν να κάνουν πράγματα που δεν είναι αναμενόμενα αλλά δεν γίνεται καμία φυσική καταστροφή.

### *3.2.4. Οι Καταστροφείς*

Ο καλύτερος τύπος ιού είναι αυτός που καταστρέφει δεδομένα, διαγράφει όλα τα αρχεία σε ένα κατάλογο ή σε ένα σκληρό δίσκο ή διαβρώνει ή διαγράφει αρχεία συστήματος, μόλις εκτελεστεί ένα πρόγραμμα στο οποίο είναι προσαρτημένος. Άλλοι ιοί δημιουργούν προοδευτικά μεγαλύτερα κομμάτια αρχείων στον σκληρό δίσκο, προσπαθώντας να τον γεμίσουν. Ορισμένοι αλλάζουν, χωρίς να το καταλάβει ο χρήστης αρκετά αρχεία προγραμμάτων ή

συστήματος στον σκληρό δίσκο, δημιουργώντας ίσως αντίγραφα των εαυτών τους μέσα σε καθένα από αυτά τα προγράμματα, μέχρι να επιτευχθεί ένας συγκεκριμένος σκοπός - οπότε κανένα από τα αρχεία να μην δουλεύει.

### *3.2.5. Αυτοαναπαραγόμενοι Ιοί*

Οι αυτοαναπαραγόμενοι ιοί είναι ιδιαίτερα κακόβουλοι, επειδή μπορούν να ενεδρεύουν σε δεκάδες ή και εκατοντάδες αρχεία του συστήματος. Ακόμη και αν αντιμετωπιστούν μια ή δύο εμφανίσεις ενός αυτοαναπαραγόμενου ιού, θα υπάρχουν πιθανώς και άλλες. Ορισμένοι μπορεί να παραμένουν σε ορισμένα προγράμματα. Οι Δούρειοι Ίπποι έχουν γραφεί με σαφή στόχο την κλοπή ονομάτων και κωδικών πρόσβασης χρηστών από online υπηρεσίες ή παροχείς υπηρεσιών internet. Οι χρήστες του AOL είναι ένας δημοφιλής στόχος για τέτοια προγράμματα, τα οποία εκτελούνται στο παρασκήνιο, όταν ο χρήστης βρίσκεται online και στέλνει με email ή με άλλο τρόπο το όνομα και τον κωδικό πρόσβασης του στο άτομο πίσω από το πρόγραμμα. (Προς μεγάλη ειρωνεία, ένα από τα πιο επιτυχημένα και απειλητικά προγράμματα ήταν αυτό που υποσχόταν δωρεάν πρόσβαση στο AOL. Χιλιάδες άνθρωποι το φόρτωσαν και το εκτέλεσαν.)

Μερικοί ενδιαφέροντες ιοί μακροεντολών και προγράμματα Δούρειοι Ίπποι έχουν χρησιμοποιηθεί επίσης για να κλέψουν δεδομένα - κυρίως για να τα χρησιμοποιήσουν για αυτοαναπαραγωγή. Ένας από αυτούς τους ιούς επιτέθηκε σε ένα συγκεκριμένο πρόγραμμα email το Outlook Express, και χρησιμοποίησε τις καταχωρίσεις του βιβλίου διευθύνσεων του για να στείλει αντίγραφα του εαυτού του σε άλλους, ώστε να μολύνει κάθε υπολογιστή και να συνεχίσει την διαδικασία. Τελικά η μόλυνση έφτασε σε χιλιάδες υπολογιστές.

### *3.2.6. Φανατικοί Λήψης Ελέγχου*

Οι χειρότεροι ιοί μπορούν να καταλάβουν τον υπολογιστή και να εκτελούν ή να κλείνουν προγράμματα με τυχαίο τρόπο. Ορισμένοι ιοί είναι προγραμματισμένοι να κάνουν αυτά τα πράγματα, απλώς για να τα κάνουν. Άλλοι εκτελούν προγράμματα μια συγκεκριμένη ώρα, για να κλέψουν δεδομένα. Υπάρχουν επίσης προγράμματα Δούρειοι Ίπποι που εργάζονται στο παρασκήνιο για να στείλουν με email κλεμμένα δεδομένα, όπως περιγράψαμε προηγουμένως, και να υποκλέψουν οικονομικά δεδομένα από συγκεκριμένα πακέτα λογισμικού.

### *3.2.7. Ιοί Μακροεντολών*

Μια μακροεντολή είναι μια σειρά εντολών, επιλογών μενού και /ή άλλες ενέργειες που έχουν καταγραφεί εκ των προτέρων. Οι περισσότερες μακροεντολές είναι συγκεκριμένες για ένα δεδομένο πρόγραμμα (όπως για το *word* ή το EXCEL) και χρησιμοποιούνται για να απλοποιήσουν συχνά χρησιμοποιούμενες αλληλουχίες εντολών. Για παράδειγμα, μια μακροεντολή μπορεί να χρησιμοποιείται για να δημιουργεί μια ταχυδρομική λίστα από μια απλή λίστα ονομάτων και διευθύνσεων σε ένα αρχείο επεξεργαστή κειμένου. Με μια μακροεντολή, αντί να γίνεται σημείωση, αντιγραφή και επικόλληση κάθε ονόματος και διεύθυνσης, πρέπει να γίνουν αυτά τα βήματα μόνο μια φορά. Καταγράφονται τα βήματα που απαιτούνται, και ο χρήστης έχει μια μακροεντολή που μπορεί να εκτελέσει για καθορισμένα ονόματα και

διευθύνσεις, χρησιμοποιώντας πολύ λιγότερες πληκτρολογήσεις και εξοικονομώντας χρόνο.

Οι μακροεντολές είναι προφανώς πολύ χρήσιμες, και μπορούν να βρεθούν πολλές για φόρτωση στο web. Φυσικά, πολλοί ιοί κρύβονται μέσα σε μακροεντολές πολλών δημοφιλών προγραμμάτων. Οι ιοί μακροεντολών μπορούν να κάνουν μερικές χρήσιμες εργασίες, αλλά ταυτόχρονα καταστρέφουν ή κλέβουν δεδομένα. Υπάρχουν μερικοί πολύ γνωστοί ιοί που μολύνουν το word και το excel σε χιλιάδες εταιρικά συστήματα χρηστών, οι οποίοι εμφανίστηκαν στα τέλη της δεκαετίας του 90.

Οι μακροεντολές μπορούν να ληφθούν σε email, ή μπορούν να προστεθούν στο πρόγραμμα στόχου από ένα άλλο πρόγραμμα Δούρειο Ίππο. Και με τους δύο τρόπους, μπορούν να προκαλέσουν πολλά προβλήματα σε τμήματα πληροφορικής εταιρειών αλλά και στην λειτουργία των οικιακών υπολογιστών, κάνοντας θορύβους και δίνοντας μηνύματα σφάλματος, ή ανοιγοκλείνοντας παράθυρα. Υπάρχουν όμως ορισμένοι ιοί, που κάνουν αυτές τις παρεμβολές σκόπιμα.

Ακόμη και τέτοιοι "ακίνδυνοι" ιοί- που δεν καταστρέφουν δεδομένα - είναι ενοχλητικοί. Μπορεί να γίνεται καλωσόρισμα του χρήστη από ένα υβριστικό ή πολιτικό μήνυμα κάθε μέρα που εκκινεί τον υπολογιστή. Ακόμη χειρότερα, μπορεί ο χρήστης να βλέπει το ίδιο μήνυμα συνεχώς μετά από ένα ορισμένο αριθμό πληκτρολογήσεων, ενώ γίνεται χρησιμοποίηση του επεξεργαστή κειμένου.

### *3.2.8. Ιοί Μικροεφαρμογών: Μια Πιθανή Μάστιγα*

Οι μικροεφαρμογές (applets) είναι μικρά προγράμματα που στέλνονται στο σύστημά από ιστοσελίδες και εκτελούνται στον εξεταστή . Έχουν γραφεί σε ειδικές γλώσσες συγγραφής script που καλούνται JAVA, JAVASCRIPT και activex. (οι μικροεφαρμογές ActiveX επίσημα ονομάζονται *μηχανισμοί* - controls*.)* Οι μικροεφαρμογές χρησιμοποιούνται για οτιδήποτε από την παραγωγή φορμών μέχρι την παροχή μικρών παραθύρων για ειδικές πληροφορίες. Επίσης μπορούν να χρησιμοποιηθούν για τη δημιουργία κίνησης, ακόμη και για την πλοήγηση μέσα σε ένα δικτυακό τόπο.

Η συνεχώς αυξανόμενη δημοφιλία των μικροεφαρμογών java, javascript και των μηχανισμών ActiveX έχει δημιουργήσει αρκετά θέματα ασφάλειας. Ίσως η πιο γνωστή περίπτωση ήταν στις αρχές του 1997, όταν τα μέλη μιας ομάδας Γερμανών εισβολέων υπολογιστών (HACKERS) ανακοίνωσε ένα τρόπο εκμετάλλευσης μιας αδυναμίας στα ActiveX της Microsoft, που θα τους επέτρεπε να βρουν ένα τρόπο για να εισβάλουν σε ορισμένους τύπους μεταφοράς χρημάτων. Αυτή η τρύπα ασφάλειας από τότε κλείστηκε, αλλά υπάρχουν και θα υπάρξουν και άλλες.

Ακόμη και ένα πραγματικό χαρακτηριστικό ασφάλειας των ActiveX είναι μάλλον άχρηστο, επειδή οι περισσότεροι χρήστες του microsoft internet explorer δεν ξέρουν πώς να το χρησιμοποιήσουν. Το χαρακτηριστικό ασφάλειας χρησιμοποιεί ψηφιακές υπογραφές (κωδικοποιημένη επαλήθευση μιας ταυτότητας, που παρέχεται από ένα δικτυακό τόπο), για επαλήθευση ότι το άτομο που δημιούργησε ένα δεδομένο script ή μηχανισμό είναι το ίδιο άτομο

που το έστειλε στον αποδέκτη. Ακόμη όμως και αν υλοποιηθούν αυτές οι υπογραφές, ένας πεπειραμένος εισβολέας μπορεί να τις παρακάμψει.

Επίσης, οι ψηφιακές υπογραφές δεν αποτρέπουν κανένα από το να δημιουργήσει ένα καταστροφικό μηχανισμό ActiveX, που μπορεί να διαγράψει ή να διαβρώσει σημαντικά αρχεία. Η java έχει μια παρόμοια καταστροφική δυνατότητα, αν και καυχάται ότι προσεγγίζει καλύτερα το θέμα της ασφάλειας.

Όλα αυτά δείχνουν ότι οι τρύπες ασφάλειας δεν είναι οι μόνοι πιθανοί κίνδυνοι που παρέχονται από τα ActiveX και την java. Τόσο η java όσο και τα Activex μπορούν να μεταφέρουν προγράμματα στο σύστημα, και το τι κάνουν εκεί είναι ένα τελείως ανοικτό θέμα. Αυτό σημαίνει, βασικά, ότι αυτά τα προγράμματα μπορούν να κάνουν σχεδόν οτιδήποτε. Αυτό δημιουργεί την δυνατότητα να περιέχουν ιούς. Η symantec και άλλες εταιρίες αναπτύσσουν ή έχουν αναπτύξει πρόσφατα σαρωτές ιών που παρέχουν ανίχνευση πραγματικού χρόνου και δυνατότητα προστασίας από τέτοιους ιούς.

Η javascript, μια νέα γλώσσα αυτής της κατηγορίας συγγραφής script, περιέχει τους δικούς της πιθανούς κινδύνους. Ανάμεσα σε άλλα πράγματα, μια ιστοσελίδα με τον σωστό κώδικα javascript μπορεί να καταλάβει τον εξεταστή και να ανοίξει μέσω αυτού οποιαδήποτε σελίδα επιθυμεί ο ιδιοκτήτης της ιστοσελίδας - ακόμη και μια σελίδα χωρίς μενού ή μηχανισμούς, χωρίς κάποιο τρόπο να ξεπεραστεί. Αν κλείσει ο εξεταστής, οι εντολές της javascript απλώς θα τον ξανανοίξουν. Παρόμοια πράγματα μπορούν να γίνουν με τη javascript σε μηνύματα email που στέλνονται στο πρόγραμμα email του netscape.

## *3.3. Πώς Μπορεί να Μπει ένας Ιός στο Σύστημά ;*

Ένας ιός συνήθως εισέρχεται σε ένα σύστημα μεταμφιεσμένος σε πρόγραμμα ή μακροεντολή. Για παράδειγμα, μπορεί να γίνει φόρτωση ενός αρχείου που αναφέρεται σαν παιχνίδι και ονομάζεται fungame.EXE. Μπορεί να εκτελεστεί και, ενώ προσπαθεί ο χρήστης να καταλάβει πώς να παίξει το παιχνίδι, το πρόγραμμα μπορεί να εργάζεται στο φόντο διαγράφοντας όλα τα αρχεία στον τρέχοντα κατάλογο - ή σε όλους τους καταλόγους - ή να προσαρτά ένα ιό στο αρχείο εκκίνησης. (Όπως αναφέρετε παρακάτω, Δούρειος Ίππος είναι ένα άλλο, παλιότερο και πιο κατάλληλο όνομα γι' αυτό το είδος ιού.)

Η πλειοψηφία των ιών και των προγραμμάτων Δούρειων ίππων μεταμφιέζονται σε προγράμματα δημόσιας περιοχής ή δημόσιας χρήσης για να ενθαρρύνουν την διανομή τους. Μερικά μεταμφιέζονται ή ενσωματώνονται μέσα σε νόμιμα ή παράνομα αντίτυπα εμπορικού λογισμικού. Επίσης, μερικά προγράμματα ιών έχουν σχεδιαστεί ώστε να εκμεταλλεύονται την ανθρώπινη απληστία, προσποιούμενα ότι είναι προγράμματα που βοηθούν στην εισβολή σε δικτυακούς τόπους ή στην απόσπαση δωρεάν χρόνου από ένα παροχέα υπηρεσιών ή από μια online υπηρεσία, ή προσφέροντας κάποιο άλλο κέρδος.

### *3.3.1. Φορτώσεις*

Για τους περισσότερους ιούς, οι φορτώσεις είναι ο κύριος τρόπος για να μπουν μέσα σε ένα υπολογιστή, εν μέρει επειδή τόσο πολλά αρχεία στις μέρες μας δίνονται με φορτώσεις. Ο κύριος λόγος όμως, είναι ότι ένα αρχείο που μεταφέρει ένα ιό διαδίδεται ταχύτερα online σε σχέση με την μετάδοση σε άλλα μέσα. Επειδή αυτοί που δημιουργούν ιούς υπολογιστών θέλουν να γίνουν γνωστοί, οι περισσότεροι στοχεύουν στον online κόσμο, σαν σημείο διανομής των δημιουργιών τους.

Οι ιοί που διαχέονται online έχουν επίσης την μεγαλύτερη πιθανότητα μακροβιότητας. Χρειάζεται πολύς χρόνος από την αρχική ανακάλυψη ενός ιού σε μια φόρτωση πριν να καταστραφεί και η τελευταία του εμφάνιση. Πολλοί άνθρωποι που τον φορτώνουν δεν εργάζονται online ή δεν δίνουν σημασία σε online πηγές πληροφοριών, και μερικοί από αυτούς τον εκφορτώνουν κάπου αλλού, βάζοντας τον σε online υπηρεσίες ή σε δικτυακούς τόπους, από όπου άλλοι ανυποψίαστοι χρήστες μπορούν να τον φορτώσουν. Έτσι κάθε νέα εκφόρτωση πολλαπλασιάζει τον πιθανό αριθμό υπολογιστών που εκτίθενται στον ιό. Μερικοί επίσης μπορεί να στείλουν τον ιό με email σε φίλους τους.

### *3.3.2. Προσαρτήσεις Email*

Οι ιοί μπορούν να βρεθούν σε προγράμματα ή αρχεία που προσαρτώνται σε μηνύματα email.

Η απλή ανάγνωση ενός μηνύματος δεν θα ενεργοποιήσει τον ιό, αλλά όμως το άνοιγμα του προσαρτημένου μολυσμένου αρχείου και /ή η εκτέλεση του προσαρτημένου προγράμματος (ή μακροεντολής) θα τον ενεργοποιήσουν.

Τα προγράμματα που προσαρτώνται σε μηνύματα email αυξάνονται σε συχνότητα τις περιόδους των μεγάλων διακοπών. Αν και τέτοιες προσαρτήσεις μπορεί να φαίνονται αβλαβείς και κατάλληλες για την συγκεκριμένη περίοδο, είναι καλύτερο να διαγραφούν. Ακόμη και αν ο αποστολέας του αρχείου είναι γνωστός, πρέπει να υπάρχει μεγάλη προσοχή από τον παραλήπτη γιατί πιθανώς να προωθεί κάτι που του στάλθηκε με τον ίδιο τρόπο και μπορεί να μην έχει ελέγξει για να δει αν το αρχείο είναι ένας ιός.

### *3.3.3. Αρχεία Κοινής Χρήσης σε ένα Δίκτυο*

Τα αρχεία κοινής χρήσης σε ένα δίκτυο συχνά διαχέουν ιούς γρήγορα. Πρέπει να υπάρχει προσοχή στην πολιτική του διαχειριστή του συστήματος σε ότι αφορά αρχεία κοινής χρήσης, απειλές από ιούς και σχετικά θέματα. Θα πρέπει να αποφεύγεται η εκτέλεση προσαρτήσεων email στο δίκτυο, και να γίνεται ειδοποίηση του διαχειριστή του συστήματος αμέσως μόλις βρεθεί ένα ύποπτο αρχείο.

### *3.3.4. Δίσκοι Κοινής Χρήσης*

Αντίθετα, οι ιοί που διαχέονται σε δίσκους, διαχέονται πολύ αργά. Οι ιδιοκτήτες υπολογιστών δεν μοιράζονται προγράμματα σε δίσκους όσο έκαναν παλιότερα, τώρα που ό,τι τους είναι χρήσιμο βρίσκεται, δωρεάν. Αλλά η διάχυση ιών μέσω δίσκων κοινής χρήσης δεν έχει εξαλειφθεί.

Ένας φίλος ή συνεργάτης μπορεί, χωρίς να το ξέρει, να έχει φορτώσει ένα μολυσμένο πρόγραμμα και να το δώσει σε μια δισκέτα, πριν να καταλάβει τι

είναι. Επίσης, κάποιος μπορεί να δίνει αντίγραφα ενός δημοφιλούς προγράμματος κοινής χρήσης, χωρίς να ξέρει ότι το πρόγραμμα είναι μολυσμένο.

Στις σπάνιες περιπτώσεις που ένας ιός εισδύσει μέσα σε μια δισκέτα ή ένα cd-rom που έχει παραχθεί εμπορικά, τότε σχεδόν κάθε αντίγραφο του μπορεί να καταστραφεί γρήγορα, επειδή οι εκδότες του λογισμικού παρακολουθούν προσεκτικά, που πηγαίνουν τα προϊόντα τους. (Αυτό συνέβη ήδη. Πολλές φορές, ένας κακόβουλος υπάλληλος μιας εταιρίας έχει τροποποιήσει ένα εμπορικό προϊόν, πριν να αναπαραχθεί για πώληση.)

## *3.4. Προστασία από Ιούς*

Η προστασία είναι πάντα η καλύτερη θεραπεία. Μπορούν να γίνουν πολλά πράγματα για την αποτροπή προγράμματα ιών από το να μπουν στα δεδομένα ή στο σύστημα .

Πριν να προχωρήσουμε, πρέπει να σημειωθεί ότι οι υπολογιστές δεν μπορούν να πιάσουν ιό ή να προσβληθούν με την απλή κλήση σε μια online υπηρεσία ή σε ένα παροχέα υπηρεσιών internet. Οι ιοί και τα προγράμματα Δούρειοι ίπποι που έχουν φορτωθεί δεν είναι επικίνδυνα παρά μόνο αν γίνει εκτέλεση τους. (Υπάρχει η πιθανότητα ένα απομακρυσμένο σύστημα να στέλνει εντολές στο σύστημα μέσω ορισμένων ειδών λογισμικού επικοινωνιών, αλλά οι online υπηρεσίες και οι παροχείς υπηρεσιών δεν έχουν καθοριστεί ώστε να καταστρέφουν τα δεδομένα).

**Ύστερα από αυτά ακολουθούν μερικές σημαντικές συμβουλές για προστασία από ιούς:**

- Αν δεν υπάρχει πρόγραμμα προστασίας από ιούς στο σύστημα, πρέπει να γίνει εγκατάσταση ενός τέτοιου προγράμματος και καθώς και συχνή ενημέρωση του.
- Αν το πρόγραμμα προστασίας από ιούς παρέχει αυτόματη, πλήρη προστασία, θα πρέπει να γίνει ενεργοποίηση της. Ρόλος της είναι να σαρώνει αυτόματα τις φορτώσεις που γίνονται, και να παρακολουθεί τα αρχεία και τα προγράμματα μέσα στο σύστημα.
- Πρέπει να υπάρχει προσοχή με αυτά που φορτώνονται στον υπολογιστή. Αν υπάρχουν απορίες για ένα πρόγραμμα σε μια βάση δεδομένων φόρτωσης, θα πρέπει ο ενδιαφερόμενος να ρωτήσει ένα διαχειριστή συστήματος (δηλαδή το άτομο που λειτουργεί ένα δικτυακό τόπο ή μια online υπηρεσία όπου βρέθηκε το πρόγραμμα) αν έχει χρησιμοποιήσει το πρόγραμμα και το βρήκε *ασφαλές.* Επίσης να ρωτηθούν και άλλοι χρήστες για το πρόγραμμα. (Γενικά, αν ένα πρόγραμμα έχει πολλές φορτώσεις - οι μετρητές φορτώσεων για προγράμματα σε βάσεις δεδομένων είναι ορατοί σε μερικά συστήματα - και δεν υπάρχουν παράπονα για αυτό σε κανένα ηλεκτρονικό πίνακα ανακοινώσεων, τότε μάλλον μπορεί να γίνει φόρτωση του με ασφάλεια.)

- Αν ληφθεί ένα email με ένα προσαρτημένο αρχείο από κάποιον που είναι άγνωστος, τότε καλό θα είναι να διαγραφεί το αρχείο αμέσως. Αν το αρχείο είναι από κάποιον γνωστό, θα πρέπει να ρωτηθεί από πού το πήρε και αν το έχει εξετάσει για ιούς.
- Αν ένας φίλος ή ένας συνεργάτης έδωσε μια δισκέτα με ένα πρόγραμμα, καλό θα είναι να ερωτηθεί αν ξέρει αν το πρόγραμμα είναι ασφαλές. Το έχει εκτελέσει αυτός; Το έχει ελέγξει για ιούς; Ξέρει από πού πήρε το πρόγραμμα;
- Πριν να εκτελεστεί ένα πρόγραμμα, θα πρέπει να γίνει προσεκτική εξέταση των αρχείων στην αρχειοθήκη του προγράμματος και ανάγνωση των τυχόν αρχείων read-me ή παρόμοιων - οι συγγραφείς προγραμμάτων δημόσιας περιοχής ή δημόσιας χρήσης συνήθως περιλαμβάνουν μια περιγραφή με μεγέθη αρχείων, των αρχείων που περιέχονται μέσα σε μια αρχειοθήκη προγράμματος. Αν υπάρχουν αρχεία που δεν περιλαμβάνονται στην περιγραφή, να μην χρησιμοποιηθεί το πρόγραμμα.
- Ακόμη και αν ένα πρόγραμμα δεν είναι άμεσα ύποπτο, συνίσταται η σάρωση του χρησιμοποιώντας ένα από τα προγράμματα προστασίας από ιούς. (Ορισμένα μπορούν να τεθούν ώστε να σαρώνουν αρχειοθήκες και προγράμματα ενώ γίνεται φόρτωση τους).
- Αν είναι δυνατό, να γίνεται εκτέλεση του προγράμματος από δισκέτα την πρώτη φορά.
- Αν ένα πρόγραμμα είναι ύποπτο πως μεταφέρει ιούς, να μην χρησιμοποιηθεί αλλά να σαρωθεί με ένα ή περισσότερα προγράμματα προστασίας από ιούς.
- Όταν γίνεται αγορά ενός εμπορικού προγράμματος, να γίνεται έλεγχος για να υπάρχει σιγουριά ότι τη ταινία ασφαλείας δεν είναι σπασμένη - ούτε στο εξωτερικό πακέτο, ούτε στο εσωτερικό, που περιέχει τις δισκέτες ή το cd-rom.

### *3.4.1. Λογισμικό Προστασίας από Ιούς*

Πριν να μπούμε σε λεπτομέρειες για λογισμικό προστασίας από ιούς, θέλουμε να δώσουμε μια ιδέα του τι μπορεί να κάνει ένα τέτοιο πρόγραμμα. Παρακάτω γίνεται αναφορά στις λειτουργίες που μπορούν να προσφέρουν προγράμματα προστασίας από ιούς:

- Αναζήτηση σε ύποπτα προγράμματα ιών για ενσωματωμένα μηνύματα που εμφανίζονται συνήθως από προγράμματα ιών.
- Αναζήτηση σε ύποπτα προγράμματα ιών για συναρτήσεις και λειτουργίες που μπορούν να καταστρέψουν τα δεδομένα (όπως εντολές διαγραφής ή μορφοποίησης δίσκων).
- Έλεγχο των αρχείων συστήματος για αλλαγές.

- Μπλοκάρισμα ύποπτου προγράμματος ιού από έκδοση πιθανώς καταστροφικών εντολών.
- Τοποθέτηση προγραμμάτων ιών σε "καραντίνα", όπου δεν μπορούν να εκτελεστούν.
- Κατάργηση ιών από το σύστημα .
- Επιδιόρθωση αρχείων καταστραμμένων από ένα ιό (αυτό περιλαμβάνει νόμιμα προγράμματα, που μερικές φορές λειτουργούν σαν "ξενιστές" για ιούς, όπως και αρχεία δεδομένων).
- Σάρωση φορτωμένων αρχείων και προσαρτήσεων email για ιούς.
- Σάρωση καθορισμένων μονάδων δίσκων, φακέλων και /ή αρχείων κατ' απαίτηση, ή με βάση ένα προκαθορισμένο πρόγραμμα.
- Ενημέρωση με την εντολή του χρήστη , ή με βάση ένα προκαθορισμένο πρόγραμμα.
- Αυτόματη προστασία του συστήματος, παρακολουθώντας προγράμματα, αρχεία και πόρους συστήματος.

3.4.1.1. Τα πιο αξιόλογα γενικά προγράμματα προστασίας από ιούς είναι:

- Karpersky Antivirus
- McAfree virusScan online
- McAfree Virus Scan Deluxe for Windows 95/98
- Norton Antivirus
- F-Secure Antivirus
- Panda Antivirus

## *3.5. Τι είναι Δούρειος Ίππος;*

Είναι δύσκολο να οριστεί τι είναι ένας Δούρειος Ίππος. Ένας Δούρειος ίππος (Trojan horse), όπως υποδηλώνει το όνομα του, είναι μία εφαρμογή η οποία κρύβει μία δυσάρεστη έκπληξη. Πρόκειται συνήθως για μία διεργασία ή λειτουργία της οποίας προστίθεται σκόπιμα από τον δημιουργό του Δούρειου Ίππου και εκτελεί μία δραστηριότητα για την οποία δεν είναι ενήμερος ο χρήστης (και την οποία κατά πάσα πιθανότητα δεν θα ενέκρινε). Η κρυφή λειτουργία είναι αυτή που κάνει ένα τέτοιο πρόγραμμα Δούρειο Ίππο .Η αναπαραγωγή είναι μια απόλυτη αξία. Κάποιο πρόγραμμα είτε αναπαράγεται είτε δεν αναπαράγεται. Η ζημιά και η πρόθεση όμως δεν είναι απόλυτες αξίες, τουλάχιστον όσον αφορά τη λειτουργία του προγράμματος.

Επειδή ο ιός I LOVE YOU παρουσίαζε τον εαυτό του σαν ένα έγκυρο μήνυμα e-mail (ο κώδικας του ιού ήταν αποθηκευμένος σ' ένα αρχείο συνημμένο στο μήνυμα), ορισμένοι τον αντιμετώπισαν σαν Δούρειο Ίππο, αν και ένα μήνυμα e-mail δεν είναι εφαρμογή. Άλλα παραδείγματα εχθρικού κώδικα θολώνουν ακόμη περισσότερο την διαχωριστική γραμμή· ένα τέτοιο παράδειγμα είναι μία επίθεση στην οποία ο τύπος MIME ενός συνημμένου δήλωνε τον ιό σαν ένα πρόγραμμα πολυμέσων, όταν στην πραγματικότητα ήταν εκτελέσιμος κώδικας (και διατηρούσε την επέκταση .EXE). Επειδή εξ ορισμού τα Windows ενεργοποιούν τα αρχεία πολυμέσων το εκτελέσιμο κατάφερε να περάσει από τους συνήθεις ελέγχους ασφάλειας των συνημμένων, και επειδή είχε επέκταση .exe τα Windows το εκτέλεσαν όπως και οποιοδήποτε άλλο πρόγραμμα, πράγμα το οποίο οδήγησε στην μόλυνση του συστήματος. Η πρώτη νύξη για τη φύση των δούρειων προγραμμάτων μας πηγαίνει στην αρχαία ιστορία και στην κλασική μυθολογία.

### *3.5.1. Σε τι διαφέρουν οι ιοί από τους δούρειους ίππους*

Ένας Δούρειος Ίππος διαφέρει από έναν ιό στο ότι δεν αναπαράγεται και δεν προσαρτά τον εαυτό του σε άλλα αρχεία. Ένας Δούρειος Ίππος είναι μία αυτόνομη εφαρμογή της οποίας η "βόμβα" περιλαμβάνεται στον αρχικό πηγαίο κώδικα. Δεν απαιτείται η εκτέλεση ενός άλλου προγράμματος για να γίνει καταστροφική.

Στο Unix έχουν δημιουργηθεί ορισμένοι Δούρειοι Ίπποι για την αντικατάσταση υπαρχουσών εφαρμογών δικτύου. Ένας εισβολέας μπορεί να αντικαταστήσει την διεργασία του Telnet server (telnetd) με μία άλλη διεργασία, δικής του έμπνευσης. Αν και το πρόγραμμα λειτουργεί πανομοιότυπα με το telnetd, στο παρασκήνιο υποκλέπτει όλα τα ονόματα σύνδεσης και τους κωδικούς πρόσβασης των χρηστών που πιστοποιούνται στο σύστημα. Επίσης, ένας εισβολέας θα μπορούσε να αντικαταστήσει την client εφαρμογή Telnet δίνοντας έγκυρες πληροφορίες λογαριασμών σε απομακρυσμένα συστήματα. Δηλαδή, ο εισβολέας μπορεί να διεισδύσει συστηματικά σε κάθε server ενός δικτύου.

Υπήρξαν επίσης παραδείγματα Δούρειων Ίππων οι οποίοι σχεδιάστηκαν με στόχο να είναι εξαιρετικά καταστροφικοί. Για παράδειγμα, τον Απρίλιο του 1997 πολλοί άνθρωποι έπεσαν θύματα του Δούρειου Ίππου AOL4FREE.COM. Ενώ οι χρήστες πίστευαν ότι είχαν βρει ένα βοήθημα το οποίο θα τους παρείχε έναν δωρεάν λογαριασμό στην AOL, στην πραγματικότητα αυτό που *λάμβαναν* ήταν ένα θαυμάσιο εργαλείο για την διαγραφή όλων των αρχείων που υπήρχαν στον τοπικό τους δίσκο. Αμέσως μόλις έτρεχαν το πρόγραμμα, αυτό διέγραφε μόνιμα όλα τα αρχεία από την μονάδα δίσκου C.

### *3.5.2. Δούρειοι Ίπποι μέσω ...κατασκευαστών ;*

Φυσικά, δεν γράφονται όλοι οι Δούρειοι Ίπποι από κακόβουλους χάκερ. Για παράδειγμα, ορισμένοι χρήστες διαπίστωσαν με μεγάλη τους έκπληξη ότι όταν έμπαιναν στο Microsoft Network, το λογισμικό αυτής της υπηρεσίας έκανε μία πλήρη καταγραφή του εξοπλισμού και του λογισμικού τους, συμπεριλαμβανομένων των εφαρμογών της Microsoft αλλά και άλλων ανταγωνιστικών προϊόντων. Όταν ο χρήστης συνδέονταν στο δίκτυο οι πληροφορίες αυτές προωθούνταν αυτόματα στην Microsoft, η οποία θα μπορούσε έτσι να ελέγξει εάν έχουν αποκτηθεί οι απαιτούμενες άδειες χρήσης των προϊόντων της. Αν και η Microsoft ισχυρίστηκε ότι οι πληροφορίες αυτές συλλέγονταν με μοναδικό σκοπό την τεχνική υποστήριξη, πολλοί άνθρωποι θεώρησαν αυτή την ενέργεια καθαρή παραβίαση της ιδιωτικότητάς τους.

Σε πολλές άλλες περιπτώσεις οι κατασκευαστές εξοπλισμού και λογισμικού προσθέτουν επιπλέον λειτουργικότητα στα προϊόντα τους, με αντίτιμο την παραβίαση της ασφάλειας των συστημάτων των πελατών τους. Για παράδειγμα, τον Μάιο του 1998 έγινε γνωστό ότι η 3COM, καθώς και ορισμένοι άλλοι κατασκευαστές εξοπλισμού δικτύωσης συμπεριλάμβαναν λογαριασμούς υπό μορφή "πίσω πόρτας" για την πρόσβαση στα switches και στους routers που διέθεταν. Αυτοί οι μη-τεκμηριωμένοι *λογαριασμοί είναι* συνήθως αόρατοι για τον τελικό χρήστη και δεν μπορούν να διαγραφούν ή να απενεργοποιηθούν. Και σ' αυτή την περίπτωση, οι κατασκευαστές των προϊόντων ισχυρίστηκαν ότι είχαν δημιουργήσει τις "πίσω πόρτες" για λόγους που σχετίζονταν με την τεχνική υποστήριξη (π.χ. στην περίπτωση που ένας επόπτης ξεχάσει έναν κωδικό πρόσβασης). Ωστόσο, αυτές οι "πίσω πόρτες" αφήνουν τα προϊόντα τους εντελώς εκτεθειμένα και τους επόπτες ανυποψίαστους.

Τέτοιου είδους δραστηριότητες κυμαίνονται σε μία "γκρίζα" ζώνη, μεταξύ της τεχνικής υποστήριξης και των Δούρειων Ίππων. Αν και αυτές οι μη-τεκμηριωμένες "πίσω πόρτες" προστίθενται από καθ' όλα αξιόπιστους και έγκριτους κατασκευαστές, αποτελούν κίνδυνο για την ασφάλεια και αφήνουν εντελώς ανυποψίαστο τον πελάτη για τους πιθανούς κινδύνους. Η δυνατότητα πρόσβασης μέσω "πίσω πόρτας" είναι κάτι το οποίο πολλοί επόπτες συστημάτων θα ήθελαν να απενεργοποιήσουν, αλλά για να γίνει αυτό θα πρέπει πρώτα να μάθουν την ύπαρξη τους.

### *3.5.3. Πώς θα ανιχνευθεί ένας Δούρειος Ίππος;*

Η ανίχνευση ενός δούρειου ίππου είναι εύκολη. Το λογισμικό antivirus συνήθως ανιχνεύει μερικούς Δούρειους ίππους χρησιμοποιώντας λίγο πολύ τις ίδιες τεχνικές που χρησιμοποιεί για να ανιχνεύει ιούς. Ωστόσο η αναγνώριση κάποιου γνωστού Δούρειου ίππου δεν είναι πάντα η καλύτερη άμυνα. Η ανίχνευση παλαιότερων και γνωστών Δούρειων Ίππων είναι (θεωρητικά απλή, με την προϋπόθεση όμως ότι πάντα τηρούνταν όλες οι πρακτικές ασφαλείας).

Οι περισσότερες μέθοδοι ανίχνευσης στα συμβατικά πολυχρηστικά συστήματα απορρέουν από μια βασική αρχή που συχνά αναφέρεται ως συμφιλίωση αντικειμένου, δηλαδή, ρωτώντας συχνά: "Είναι όλα όπως τα άφησα;" Αυτή είναι περίπου η λειτουργία του: τα αντικείμενα είναι οι

περιοχές του συστήματος, δηλαδή τα αρχεία ή οι κατάλογοι. Η συμφιλίωση είναι η διαδικασία σύγκρισης των αντικειμένων αυτών με φωτογραφία - αντίτυπο-στιγμιότυπο των ίδιων αντικειμένων που είχε ληφθεί σε προηγουμένη χρονική στιγμή, όταν ακόμα ήταν βέβαιο ότι το προστατευόμενο αντικείμενο βρισκόταν σε "καθαρή" κατάσταση συχνότερα η διαδικασία αυτή περιγράφεται ως συμφιλίωση αντικειμένου είναι γνωστή ως ανίχνευση αλλαγής, έλεγχος ακεραιότητας, ή διαχείριση ακεραιότητας και ολοκλήρωση. Οι έννοιες αυτές δεν είναι απαραίτητα ταυτόσημες.

**Ανίχνευση αλλαγής** απλώς αναφέρεται σε κάθε τεχνική που προειδοποιεί τον χρήστη ότι κάποιο αντικείμενο έχει αλλάξει ή αλλοιωθεί κατά κάποιον τρόπο.

**Έλεγχος ακεραιότητας** έχει το ίδιο νόημα βασικά, αλλά συχνά υιοθετεί πιο εξεζητημένη προσέγγιση, ανιχνεύοντας όχι μόνο τις αλλαγές και τις απόπειρες συγκάλυψης τους, αλλά και διασφαλίζοντας ότι το λογισμικό που αναφέρει την αλλαγή δεν είναι και αυτό υπονομευόμενο.

**Διαχείριση ακεραιότητας** και **ολοκλήρωσης** είναι ένας περισσότερο γενικός όρος. Μπορεί να περιλαμβάνει όχι μόνο την ανίχνευση των μη εξουσιοδοτημένων αλλαγών, αλλά και άλλες μεθόδους διατήρησης της ακεραιότητας και της ολοκλήρωσης του συστήματος. Οι μέθοδοι αυτές μπορεί να περιλαμβάνουν κάποιες ή όλες από τις παρακάτω: τήρηση αξιόπιστων και έμπιστων εφεδρικών αρχείων, μπλοκάρισμα άγνωστων προσπαθειών διείσδυσης στην είσοδο (π.χ. τρέχοντας τα αρχεία του συστήματος από οδηγούς ή από μέσα μόνο ανάγνωσης ή ανανεώνοντας τα αρχεία του συστήματος μόνο από αξιόπιστα και έμπιστα μέσα μονό ανάγνωσης), τήρηση αυστηρών ελέγχων πρόσβασης, προσεκτική εφαρμογή των αντιδότων του κατασκευαστή για να καλυφθεί κάθε τρωτό σημείο καλοσχεδιασμένο σύστημα διαχείρισης των αλλαγών, χρησιμοποιώντας μόνο ενυπόγραφο (έμπιστο) κώδικα.

Μια απλή μέθοδος ελέγχου της ακεραιότητας των αρχείων βασίζεται σε αναφορές για την κατάσταση των αρχείων. Οι έλεγχοι της ακεραιότητας των αρχείων είναι λιγότερο ή περισσότερο πολύπλοκοι. Παραδείγματος χάριν μπορεί χονδρικά να ελεγχθεί η ακεραιότητα κάποιου αρχείου χρησιμοποιώντας κάποιους από τους εξής δείκτες:

- ημερομηνία τελευταίας τροποποίησης του αρχείου
- ημερομηνία δημιουργίας του αρχείου
- μέγεθος αρχείου

Δυστυχώς, καμία από τις ανωτέρω τρεις μεθόδους δεν συνιστά σωστή άμυνα έναντι περισσότερο ύπουλων και μελετημένων επιθέσεων. Κάθε φορά που αλλάζει ένα αρχείο, αλλάζουν οι τιμές του. π.χ. κάθε φορά που ανοίγει, τροποποιείται και αποθηκεύεται το αρχείο, αποτυπώνεται η ημερομηνία της τελευταίας αλλαγής. Η ημερομηνία αυτή όμως αλλοιώνεται εύκολα, αλλάζοντας το χρονικό αποτύπωμα του αρχείου. Αλλάζοντας απλά την ώρα του συστήματος, γίνεται εφαρμογή των αλλαγών, κατόπιν αρχειοθέτηση του αρχείου, και ρύθμιση πάλι της ώρας του συστήματος. Ακόμα καλύτερα μάλιστα, εάν γίνει ανάκτηση και αποθήκευση των στοιχείων για την ημερομηνία και την ώρα με στάνταρ συναρτήσεις βιβλιοθήκης της C (για παράδειγμα), τροποποίηση ή

αντικατάσταση του αντικειμένου, και αποκατάσταση της ημερομηνίας τροποποίησης του αρχείου. Σε σύστημα ενός χρήστη (π.χ. MS-DOS) με ελάχιστους ή μηδενικούς ελέγχους πρόσβασης, η δυσκολία είναι μηδαμινή. Για τους λόγους αυτούς ο έλεγχος της ημερομηνίας της τελευταίας τροποποίησης ενός αρχείου είναι μάλλον αναξιόπιστος τρόπος ανίχνευσης μιας καίριας αλλαγής. Ακόμα, η τελευταία ημερομηνία που τροποποιήθηκε το αρχείο δεν αποκαλύπτει κάτι σημαντικό, εάν το ίδιο το αρχείο παρέμεινε αναλλοίωτο (δηλαδή απλώς αντιγράφηκε, διαβάστηκε ή ταχυδρομήθηκε). Από την άλλη όμως, εάν υπάρχει ανισοτιμία μεταξύ της ημερομηνίας τροποποίησης που επέστρεψε το σύστημα και της ημερομηνίας τροποποίησης που κατέγραψε κάποιο πρόγραμμα παρακολούθησης του συστήματος, οι πιθανότητες είναι σοβαρές να έχει υπάρξει κακόβουλη ενέργεια.

Ένας άλλος τρόπος ελέγχου της ακεραιότητας ενός αρχείου είναι ο έλεγχος του μεγέθους του. Ωστόσο και η τιμή αυτή μπορεί εύκολα να αλλοιωθεί, είτε περικόπτοντας είτε διογκώνοντας το ίδιο το αρχείο, είτε αλλάζοντας την τιμή που αναφέρεται από το λειτουργικό σύστημα.

Υπάρχουν όμως και μερικοί άλλοι δείκτες, π.χ. η χρησιμοποίηση αθροισμάτων ελέγχου. Είναι περισσότερο αξιόπιστα από τις τιμές ημερομηνίας και ώρας, όμως και αυτά αλλοιώνονται. Ένα βασικό σύστημα checksum (ή ένα λογισμικό ανίχνευσης αλλαγών που να βασίζεται σε αθροίσματα ελέγχου) πρέπει να τηρείται σε απόλυτα έμπιστο περιβάλλον, για να χρησιμοποιείται με ασφάλεια, δηλαδή σε ξεχωριστό server ή ακόμα και σε ξεχωριστό μέσο, στο οποίο πρόσβαση να έχουν μόνο χρήστες του βασικού καταλόγου ή άλλοι εξίσου έμπιστοι χρήστες. Τα αθροίσματα ελέγχου λειτουργούν αποτελεσματικά και ενδείκνυνται για τον έλεγχο κάθε μεταφερομένου αρχείου π.χ. από το σημείο Α στο σημείο Β, αλλά δεν είναι κατάλληλα για εφαρμογές υψηλής ασφαλείας. Απλώς δεν είναι σχεδιασμένα για να προφυλάσσουν από κακόβουλες επιθέσεις.

## *3.6. Worms*

Κατά παράδοση, *ένα* worm (σκουλήκι) θεωρούνταν σαν μία εφαρμογή η οποία μπορούσε να αναπαράγει τον εαυτό της μέσω μιας μόνιμης ή dial-up σύνδεσης δικτύου. Ανόμοια με έναν ιό ο οποίος εξαπλώνει τον εαυτό του στον σκληρό δίσκο ή στο σύστημα αρχείων ενός υπολογιστή, ένα worm είναι ένα αυθύπαρκτο και αυτουποστηριζόμενο πρόγραμμα. Ένα τυπικό worm διατηρεί μόνο ένα λειτουργικό αντίγραφο του εαυτού του ενεργό στην μνήμη και δεν χρειάζεται καν να γραφτεί στον δίσκο. Ωστόσο, τα τελευταία χρόνια η διαχωριστική γραμμή *ανάμεσα* στα worms και στους ιούς έγινε πολύ θολή, ξεκινώντας από την πολύ γνωστή περίπτωση της Melissa. Η Melissa ήταν ένα υβρίδιο worm/ιού το οποίο μπορούσε να μολύνει ένα σύστημα (σαν ένας ιός), τροποποιώντας τα έγγραφα ώστε να περιέχουν αποσπάσματα από την τηλεοπτική εκπομπή The Simpsons. Αλλά μπορούσε επίσης να χρησιμοποιήσει το Βιβλίο Διευθύνσεων του Microsoft Outlook και του Outlook Express για να στείλει τον εαυτό της (σαν ένα worm) σε άλλα συστήματα του δικτύου, τα οποία μολύνονταν από ένα έγγραφο συνημμένο στο μήνυμα. Το 2000 ο ιός I LOVE YOU, ένα ακόμη υβρίδιο ιού/worm, προκάλεσε σημαντική ζημιά διαγράφοντας αρχεία μορφής JPEG και MP3 από υπολογιστές σε όλο τον κόσμο. (Ορισμένοι ισχυρίζονται ότι ο ιός I LOVE YOU ήταν επίσης μία

μορφή Δούρειου Ίππου επειδή παρουσίαζε τον εαυτό του σαν ένα καθ' όλα έγκυρο μήνυμα e-mail). Επίσης, ενώ η Melissa περιόριζε τον εαυτό της στις πρώτες 50 διευθύνσεις του Βιβλίου Διευθύνσεων ενός χρήστη, ο ιός I LOVE YOU χρησιμοποιούσε όλες τις διευθύνσεις που έβρισκε.

Το Code Red, ένα worm το οποίο γνώρισε αρκετή δημοσιότητα (μαζί με τον διάδοχο του, Code Red II), ήταν επίσης μία συνδυασμένη μορφή απειλής η οποία περιλάμβανε επιθέσεις άρνησης εξυπηρέτησης, παραποίηση ιστοσελίδων και έναν Δούρειο Ίππο ο οποίος εκτελούνταν μετά από την κύρια επίθεση.

Ο Nimda, ένας από τους ιούς με συχνή παρουσία το 2001, είχε πρωτοποριακή συμπεριφορά όσον αφορά στον τρόπο με τον οποίο τροποποιούσε υπάρχοντα web sites ώστε να παρέχουν μολυσμένο κώδικα σε client συστήματα. Αφού μολύνονταν, τα client συστήματα αναζητούσαν άλλα ευάλωτα web sites και ο κύκλος της μόλυνσης συνεχίζονταν.

Στα τέλη του 2001 άρχισε να κυκλοφορεί ένα νέο worm με όνομα Klez (το οποίο συνέχιζε να είναι αρκετά ενεργό και το καλοκαίρι του 2002). Έχοντας δυνατότητα να απενεργοποιεί τα προγράμματα ανίχνευσης /εξάλειψης ιών (μαζί με άλλα, καθ' όλα έγκυρα προγράμματα), το worm Klez μπορεί να παρουσιάσει τον εαυτό του στους χρήστες ακόμη και σαν μία διόρθωση (patch) για την θωράκιση των συστημάτων τους έναντι του εαυτού του!

**ΣΗΜΕΙΩΣΗ** Το όνομα worm προέρχεται από μία ιστορία γραμμένη το 1975 από τον John Brunner, με τίτλο "The Shockwave Rider". Ο ήρωας αυτής της ιστορίας χρησιμοποιούσε ένα πρόγραμμα με όνομα "tapeworm" για να καταστρέψει το δίκτυο υπολογιστών μιας φασιστικής κυβέρνησης καθεστώτος και την ελευθέρωση των πολιτών. Πριν από την δημοσίευση αυτής της ιστορίας δεν υπήρχε καθολικά αποδεκτό όνομα γι' αυτή την κατηγορία προγραμμάτων (για μία ακόμη φορά, η ζωή μιμήθηκε την τέχνη).

### *3.6.1. Το WORM VAMPIRE*

Τα worms δεν θεωρούνταν πάντα κακό πράγμα. Στην δεκαετία του '80, οι John Shock I και Jon Hepps της Xerox έκαναν μία θαυμάσια έρευνα για τα worms, με στόχο να δείξουν πόσο ευεργετικά θα μπορούσαν να είναι αυτά τα προγράμματα. Για τον σκοπό αυτό δημιούργησαν πολλά προγράμματα worm και τα χρησιμοποίησαν για την εποπτεία και διαχείριση του δικτύου υπολογιστών της ίδιας της Xerox. Το αποτελεσματικότερο από αυτά ήταν το worm vampire. Αυτό το worm κάθονταν αδρανές κατά την διάρκεια της ημέρας, όταν ο βαθμός χρήσης του δικτύου ήταν υψηλός. Την νύχτα όμως το worm ξυπνούσε και χρησιμοποιούσε τον άεργο χρόνο της CPU για να ολοκληρώσει πολύπλοκες εργασίες. Το επόμενο πρώτο worm vampire αποθήκευε την δουλειά του και πήγαινε για ύπνο. Το worm vampire ήταν εξαιρετικά αποτελεσματικό, μέχρι την ημέρα που οι υπάλληλοι της Xerox έφτασαν στην δουλειά τους και διαπίστωσαν ότι όλα τα συστήματα υπολογιστών είχαν καταρρεύσει λόγω κάποιας διεργασίας η οποία δεν λειτουργούσε σωστά. Όταν επανεκκίνησαν τα συστήματα, κατέρρευσαν

αμέσως και πάλι από το worm. Αυτό είχε σαν αποτέλεσμα την απομάκρυνση του worm απ' όλα τα συστήματα του δικτύου και τον τερματισμό της σχετικής έρευνας.

### *3.6.2. Το "Μεγάλο" INTERNET WORM*

Μέχρι τις 3 Νοεμβρίου του 1988, ελάχιστη ήταν η προσοχή που έδιναν οι άνθρωποι στα worms. Αυτή ήταν η ημέρα που παρουσιάστηκε το "Μεγάλο Σκουλήκι" στο Internet. Σε λιγότερο από έξι ώρες, αυτό το 99 γραμμών πρόγραμμα κατάφερε κυριολεκτικά να θέσει εκτός λειτουργίας 6,000 συστήματα Sun και VAX συνδεδεμένα στο Internet.

Το πρόγραμμα αυτό γράφτηκε από τον Robert Morris, γιο ενός από τους πλέον αξιόλογους ειδικούς στην ασφάλεια που υπήρχαν στις Η.Π.Α. εκείνη την εποχή. Έχει ειπωθεί ότι η συγγραφή του worm δεν ήταν μία κακόβουλη ενέργεια, αλλά η προσπάθεια ενός γιου να βγει από την σκιά του πατέρα του. Το σκεπτικό αυτό υποστηρίζεται και από τον ίδιο τον κώδικα του worm, επειδή το πρόγραμμα αυτό δεν εκτελούσε σκόπιμα καταστροφικές ενέργειες. Αυτό που έκανε το συγκεκριμένο worm ήταν απλό: εκκινούσε μία μικρή διεργασία, η οποία έτρεχε στο παρασκήνιο, σε κάθε μηχανή που συναντούσε. Το πείραμα αυτό θα περνούσε πιθανώς εντελώς απαρατήρητο, εάν δεν υπήρχε μία μικρή αβλεψία στον προγραμματισμό του worm. Πριν μολύνει ένα σύστημα, το worm δεν έλεγχε εάν το σύστημα ήταν ήδη μολυσμένο. Αυτή η αβλεψία οδήγησε στην πολλαπλή μόλυνση συστημάτων. Ενώ η μία εμφάνιση του worm έθετε ελάχιστο φόρτο στον επεξεργαστή, οι δεκάδες - ή πιθανώς εκατοντάδες - απανωτές μολύνσεις μπορούσαν να "γονατίσουν" ένα σύστημα. Οι επόπτες συστημάτων βρέθηκαν μπλεγμένοι σε μία άνιση μάχη. Αφού καθάριζαν και επανεκκινούσαν ένα σύστημα, αυτό μολύνονταν ξανά, πολύ γρήγορα. Όταν ανακάλυψαν ότι το worm χρησιμοποιούσε τρωτά σημεία του Send mail για να μεταφερθεί από σύστημα σε σύστημα, πολλοί επόπτες αντέδρασαν αποσυνδέοντας τα συστήματα τους από το Internet, ή θέτοντας εκτός λειτουργίας τα συστήματα ηλεκτρονικού ταχυδρομείου. Κατά πάσα πιθανότητα η αντίδραση αυτή έκανε περισσότερη ζημιά παρά καλό, επειδή ουσιαστικά απομόνωνε τα συστήματα καθιστώντας αδύνατη την λήψη ενημερωμένων πληροφοριών για το worm, συμπεριλαμβανομένων και πληροφοριών για την αποτροπή περαιτέρω μόλυνσης.

Απ' όλο το χάος που ακολούθησε μετά από αυτό το περιστατικό, προέκυψαν αρκετά καλά πράγματα. Χρειάστηκε ένα επεισόδιο τόσο μεγάλου εύρους για να αλλάξει το σκεπτικό των ανθρώπων όσον αφορά στα τρωτά σημεία των υπολογιστικών τους συστημάτων. Εκείνη την εποχή τέτοιου είδους τρωτά σημεία θεωρούνταν απλώς "σφάλματα" (bugs) δευτερεύουσας σημασίας. Το περιστατικό με το "Μεγάλο Σκουλήκι" του Internet βοήθησε στο να προσδιοριστούν με σαφέστερο τρόπο αυτές οι αδυναμίες. Χάρη σ' αυτό το περιστατικό δημιουργήθηκε ο οργανισμός CERT (Computer Emergency Response Team), ο οποίος είναι υπεύθυνος για την τεκμηρίωση των προβλημάτων που σχετίζονται με την ασφάλεια των υπολογιστών και βοηθά άλλες εταιρείες και οργανισμούς να λύνουν τέτοια προβλήματα.

### *3.6.3. ΤΟ WORM WANK*

Αν και το "Μεγάλο Σκουλήκι" του Internet είναι το πιο γνωστό παράδειγμα, σίγουρα δεν είναι το χειρότερο worm που υπήρχε ποτέ. Τον Οκτώβριο του 1989, το worm WANK (Worms Against Nuclear Killers) άρχισε να διαδίδεται σε ανυποψίαστα συστήματα. Αν και εξαιρετικά καταστροφικό, το worm αυτό ήταν μοναδικό στο είδος του επειδή μόλυνε μόνο συστήματα DEC και χρησιμοποιούσε μόνο το πρωτόκολλο DECnet (δηλαδή δεν μεταδίδονταν μέσω του IP). Αυτό το worm έκανε τα ακόλουθα:

- Έστελνε e-mail (κατά πάσα πιθανότητα στον δημιουργό του) με το οποίο προσδιόριζε σε ποια συστήματα είχε επιτεθεί, μαζί με τα ονόματα σύνδεσης και τους κωδικούς πρόσβασης που είχε χρησιμοποιήσει.
- Άλλαζε τους κωδικούς πρόσβασης υπαρχόντων λογαριασμών.
- Άφηνε "πίσω πόρτες" για την πρόσβαση στο σύστημα.
- Έβρισκε χρήστες σε τυχαίους κόμβους του δικτύου και τους καλούσε χρησιμοποιώντας το βοήθημα phone.
- Μόλυνε τα COM αρχεία του τοπικού συστήματος έτσι ώστε να έχει την δυνατότητα να ενεργοποιηθεί εκ νέου μελλοντικά, ακόμη και μετά από τον καθαρισμό του συστήματος.
- Άλλαζε την αρχική οθόνη χαιρετισμού, αναφέροντας την ύπαρξη του.
- Τροποποιούσε το script σύνδεσης, έτσι ώστε να δείχνει σαν να είχαν διαγραφεί όλα τα αρχεία ενός χρήστη.
- Έκρυβε τα αρχεία μετά από την σύνδεση, προσπαθώντας να πείσει τον χρήστη ότι τα αρχεία του είχαν διαγραφεί.

Όπως ίσως φαντάζεστε, το worm αυτό κατέστρεψε κάτι περισσότερο από την ημέρα μερικών εποπτών συστημάτων. Χρειάστηκε αρκετός καιρός για την επιτυχημένη εξάλειψη αυτού του worm απ' όλα τα μολυσμένα συστήματα.

## *3.7. **Sniffers***

### *3.7.1. Sniffers: Τι είναι και ποιοι τρόποι προστασίας υπάρχουν*

Ένα sniffer είναι ένα κομμάτι λογισμικού που ‘’οσμίζεται’’ και ελέγχει όλη την κυκλοφορία που ρέει προς και από έναν υπολογιστή που συνδέεται με ένα δίκτυο. Είναι διαθέσιμα για διάφορες πλατφόρμες και σε αρκετά μεγάλες ποικιλίες. Μερικά από τα συνηθέστερα πακέτα είναι αρκετά εύκολο να εφαρμοστούν στην γλώσσα C ή Perl, να χρησιμοποιήσουν μια διεπαφή γραμμών εντολής και να εμφανίσουν τα συλληφθέντα στοιχεία στην οθόνη. Τα πιο σύνθετα προγράμματα χρησιμοποιούν ένα GUI, στατιστικές κυκλοφορίας με χρήση γραφικών παραστάσεων, και προσφέρουν διάφορες επιλογές διαμόρφωσης τους με βάση τις απαιτήσεις του χρήστη. Τα Sniffers είναι επίσης οι μηχανές για άλλα προγράμματα. Τα συστήματα ανίχνευσης παρείσφρησης (IDS) χρησιμοποιούν τα sniffers για να ταιριάξουν πακέτα ενάντια σε ένα σύνολο κανόνων που είναι σχεδιασμένοι να αντιμετωπίζουν οτιδήποτε κακόβουλο ή παράξενο.

Τα προγράμματα χρησιμοποίησης και ελέγχου των δικτύων χρησιμοποιούν συχνά τα sniffers για να συγκεντρώσουν τα απαραίτητα στοιχεία για μετρήσεις και αναλύσεις. Οι αντιπροσωπείες επιβολής νόμου που πρέπει να ελέγχουν το ηλεκτρονικό ταχυδρομείο ,κατά τη διάρκεια των ερευνών, πιθανών χρησιμοποιούν ένα sniffer σχεδιασμένο με σκοπό να συλλαμβάνει την πολύ συγκεκριμένη κυκλοφορία. Τα sniffers ποικίλλουν σημαντικά από άποψη λειτουργικότητας και σχεδίασης. Μερικά αναλύουν ένα μόνο πρωτόκολλο, ενώ άλλα μπορούν να αναλύσουν εκατοντάδες. Ως γενικό κανόνα, τα πλέον σύγχρονα sniffers θα αναλύουν τουλάχιστον τα εξής πρωτόκολλα:

- Standard Ethernet
- TCP/IP
- IPX
- DECNet

Γνωρίζοντας ότι τα sniffers αρπάζουν απλά τα δεδομένα των δικτύων, μπορούμε να δούμε πώς λειτουργούν.

### *3.7.2. Πώς λειτουργεί ένα Sniffer;*

Προτού να γίνει η εξερεύνηση του τρόπου λειτουργίας ενός sniffer, είναι χρήσιμο να εξεταστεί τι επιτρέπει στο εργαλείο αυτό να λειτουργήσει. Κατά τη διάρκεια των κανονικών εργασιών όπως η πλοήγηση και η ανταλλαγή μηνυμάτων στο Web, οι υπολογιστές επικοινωνούν συνεχώς με άλλες μηχανές. Προφανώς, ένας χρήστης πρέπει να είναι σε θέση να δει όλη την κυκλοφορία πρός ή από τη μηχανή του. Παρ'όλα αυτά, τα περισσότερα PCs, βρίσκονται σε ένα τοπικό δίκτυο(LAN), που σημαίνει ότι μοιράζονται μια σύνδεση με διάφορους άλλους υπολογιστές. Εάν στο δίκτυο δεν υπάρχει switch (ένα switch είναι μια συσκευή που φιλτράρει και προωθεί πακέτα μεταξύ των τμημάτων του LAN), η κυκλοφορία που προορίζεται για οποιαδήποτε υπολογιστή ή τομέα μεταδίδεται σε κάθε υπολογιστή σε εκείνο τον τομέα. Αυτό σημαίνει ότι ένας υπολογιστής "βλέπει" τα δεδομένα να ταξιδεύουν προς και από κάθε ένα από τους γείτονές του, αλλά τα αγνοεί, εκτός αν έχει εντολή για το αντίθετο.

Τώρα μπορεί να γίνει ανάλυση ενός sniffer για να γίνει κατανοητή η λειτουργία του. Το πρόγραμμα sniffer λέει σε έναν υπολογιστή, συγκεκριμένα στην κάρτα δικτύου του, να σταματήσει να αγνοεί όλη την κυκλοφορία που κατευθύνεται σε άλλους υπολογιστές και να δώσει προσοχή σε αυτούς .Το Κάνει αυτό με την τοποθέτηση της κάρτας δικτύου σε μια κατάσταση αδιακρισίας. Μόλις μια κάρτα δικτύου είναι σε κατάσταση αδιακρισίας (promiscuous), μια θέση που απαιτεί προνόμια administrative ή root, ένας υπολογιστής μπορεί να δει όλα τα στοιχεία που διαβιβάζονται στον τομέα του. Το πρόγραμμα τότε αρχίζει την ανάγνωση όλων των πληροφοριών που εισάγονται στο PC μέσω της κάρτας δικτύων. Τα δεδομένα που ταξιδεύουν κατά μήκος του δικτύου έρχονται ως πλαίσια (frames), ή πακέτα, υπερχειλίσεις από bits που είναι μορφοποιημένα για συγκεκριμένα πρωτόκολλα. Λόγω αυτής της αυστηρής μορφοποίησης, ένα sniffer μπορεί να "ξεφλουδίσει" τα στρώματα της ενθυλάκωσης και να

αποκωδικοποιήσει τις σχετικές πληροφορίες που αποθηκεύονται σε: υπολογιστές προέλευσης, υπολογιστές προορισμού, στοχευόμενων αριθμό θυρών, ωφέλιμο φορτίο, εν ολίγοις - κάθε κομμάτι πληροφορίας που ανταλλάχθηκε μεταξύ δύο υπολογιστών.

### *3.7.3. Πώς μοιάζουν τα Sniffed δεδομένα ?*

Είναι εύκολο να κατανοηθούν οι έννοιες που συζητούνται παραπάνω με την παρακολούθηση ενός sniffer σε δράση. Οι πληροφορίες στο ακόλουθο παράδειγμα είναι αποτέλεσμα της χρησιμοποίησης tcpdump, ένα πρόγραμμα που ήταν στο προσκήνιο αρκετές φορές κάποτε και είναι διαθέσιμο για πολλές πλατφόρμες. Αυτό το συγκεκριμένο κομμάτι είναι μια συντομευμένη ανταλλαγή μεταξύ μιας μηχανής και του κεντρικού υπολογιστή δικτύου SecurityFocus.

21:06:30.786814 0:1:3:e5:46:6b 0:4:5a:d1:46:ad 0800 650: 192.168.1.3.32946 >

66.38.151.10.80: P [tcp sum ok] 1:585(584) ack 336 win 64080 <nop,nop,timestamp 608776

899338> (DF) (ttl 64, id 7468, len 636)

| | | |
|---|---|---|
| 0x0000 | 4500 027c 1d2c 4000 4006 8074 c0a8 0103 | E..\|.,@.@..t.... |
| 0x0010 | 4226 970a 80b2 0050 54ac b070 78ef d6c3 | B&.....PT..px... |
| 0x0020 | 8018 fa50 c663 0000 0101 080a 0009 4a08 | ...P.c.....J. |
| 0x0030 | 000d b90a 4745 5420 2f63 6f72 706f 7261 | ....GET./corpora |
| 0x0040 | 7465 2f69 6d61 6765 732f 6275 696c 642f | te/images/build/ |
| 0x0050 | 626c 6c74 5f72 645f 312e 6769 6620 4854 | bllt_rd_1.gif.HT |
| 0x0060 | 5450 2f31 2e31 0d0a 486f 7374 3a20 7777 | TP/1.1..Host:.ww |
| 0x0070 | 772e 7365 6375 7269 7479 666f 6375 732e | w.securityfocus. |
| 0x0080 | 636f 6d0d 0a55 7365 722d 4167 656e 743a | com..User-Agent: |
| 0x0090 | 204d 6f7a 696c 6c61 2f35 2e30 2028 5831 | .Mozilla/5.0.(X1 |
| 0x00a0 | 313b 2055 3b20 4c69 6e75 7820 6936 3836 | 1;.U;.Linux.i686 |

21:06:30.886814 0:4:5a:d1:46:ad 0:1:3:e5:46:6b 0800 402: 66.38.151.10.80 >

192.168.1.3.32949: P [tcp sum ok] 2363393025:2363393361(336) ack 1437810754 win 8616

<nop,nop, timestamp 899338 608766> (ttl 61, id 10825, len 388)

| | | |
|---|---|---|
| 0x0000 | 4500 0184 2a49 0000 3d06 b74f 4226 970a | E...*I..=..OB&.. |
| 0x0010 | c0a8 0103 0050 80b5 8cde 8401 55b3 4042 | .....P.....U.@B |
| 0x0020 | 8018 21a8 0543 0000 0101 080a 000d b90a | ..!..C..... |
| 0x0030 | 0009 49fe 4854 5450 2f31 2e31 2032 3030 | ..I.HTTP/1.1.200 |
| 0x0040 | 204f 4b0d 0a41 6765 3a20 320d 0a41 6363 | .OK..Age:.2..Acc |
| 0x0050 | 6570 742d 5261 6e67 6573 3a20 6279 7465 | ept-Ranges:.byte |
| 0x0060 | 730d 0a44 6174 653a 2054 7565 2c20 3132 | s..Date:.Tue,.12 |

| | | |
|---|---|---|
| 0x0070 | 2046 6562 2032 3030 3220 3033 3a30 343a | .Feb.2002.03:04: |
| 0x0080 | 3538 2047 4d54 0d0a 436f 6e74 656e 742d | 58.GMT..Content- |
| 0x0090 | 4c65 6e67 7468 3a20 3433 0d0a 436f 6e74 | Length:.43..Cont |
| 0x00a0 | 656e 742d 5479 7065 3a20 696d 6167 652f | ent-Type:.image/ |
| 0x00b0 | 6769 660d 0a53 6572 7665 723a 2041 7061 | gif..Server:.Apa |
| 0x00c0 | 6368 652f 312e 332e 3232 2028 556e 6978 | che/1.3.22.(Unix |
| 0x00d0 | 2920 6d6f 645f 7065 726c 2f31 2e32 360d | ).mod_perl/1.26. |

Αυτό το απόσπασμα παρουσιάζει δύο πακέτα: ένα αίτημα HTTP από τον πελάτη και την απάντηση του κεντρικού υπολογιστή. Σημείωση ότι οι πρώτες-πρώτες γραμμές κάθε οσμισμένου πακέτου παρέχουν μια περίληψη της συναλλαγής: χρονοσφραγίδες, διευθύνσεις της MAC προέλευσης και προορισμού, διευθύνσεις πηγής και προορισμού IP και διάφορα άλλα bits πληροφοριών. Οι αριθμημένες γραμμές (0x00 ##) δείχνουν τα στοιχεία που διαβιβάζονται από κάθε πακέτο με το δεκαεξαδικό σύστημα. Επιπλέον, εντοπίζεται μια ASCII αποκωδικοποίηση του ωφέλιμου φορτίου - ένα κατάλληλο χαρακτηριστικό γνώρισμα για τους crackers και τους αδιάκριτους γείτονες που παρακολουθούν το δίκτυο.

### *3.7.4. Γιατί θα πρέπει οι χρήστες να ενδιαφερθούν;*

Στο κανονικό τοπικό LAN υπάρχουν χιλιάδες πακέτα που ανταλλάσσονται από τις πολλούς υπολογιστές κάθε λεπτό, τα οποία είναι άφθονος ανεφοδιασμός για οποιοδήποτε επιτιθέμενο. Οτιδήποτε διαβιβάζεται πέρα από το δίκτυο θα είναι τρωτό - κωδικοί πρόσβασης, ιστοσελίδες, queries βάσεων δεδομένων και μηνύματα. Ένα sniffer μπορεί εύκολα να προσαρμοστεί για να συλλάβει συγκεκριμένη κυκλοφορία όπως τις συνόδους Telnet ή το ηλεκτρονικό ταχυδρομείο. Μόλις συλληφθεί η κυκλοφορία, οι crackers μπορούν γρήγορα να εξαγάγουν τις πληροφορίες που χρειάζονται - logins, κωδικοί πρόσβασης και το κείμενο των μηνυμάτων. Και οι χρήστες πιθανώς δεν ξέρουν ποτέ ότι τα συστήματα τους παραβιάστηκαν. Τα sniffers δεν προκαλούν καμία ζημία ή διαταραχή σε ένα περιβάλλον δικτύων.

### *3.7.5. Τι Επίπεδα Κινδύνου Αναπαριστούν τα Sniffers;*

Τα sniffers αντιπροσωπεύουν ένα υψηλό επίπεδο κινδύνου, γιατί:

- Μπορούν να συλλάβουν ονόματα και κωδικούς πρόσβασης λογαριασμών.
- Μπορούν να συλλάβουν εμπιστευτικές ή ιδιόκτητες πληροφορίες.
- Μπορούν να χρησιμοποιηθούν για να παραβιάσουν την ασφάλεια γειτονικών δικτύων ή για να αποκτήσουν προνομιακή πρόσβαση.

Στην πραγματικότητα, η ύπαρξη ενός αναρμόδιου sniffer στο δίκτυο μπορεί να δηλώνει ότι το σύστημα έχει ήδη εκτεθεί.

# ΚΕΦΑΛΑΙΟ 3ο

## *4. E-MAIL*

### 4.1. **Απειλές μέσω ηλεκτρονικού ταχυδρομείου**

Ποικίλα διαφορετικά στοιχεία αποδυναμώνουν το εταιρικό σύστημα ηλεκτρονικού ταχυδρομείου και ενώ μερικά είναι ευρέως γνωστά - όπως οι ιοί ηλεκτρονικού ταχυδρομείου - άλλα τείνουν να αγνοούνται. Τα ηλεκτρονικά ταχυδρομεία που φέρνουν τα επιθετικά μηνύματα ή οι εμπιστευτικές εταιρικές πληροφορίες μπορούν να δημιουργήσουν μεγάλη αναστάτωση και έξοδα για μια επιχείρηση που δεν έχει εξοπλίσει τον κεντρικό υπολογιστή ταχυδρομείου της (mail server) με τα κατάλληλα εργαλεία. Το ίδιο πράγμα πηγαίνει για τους spammers που χρησιμοποιούν το σύστημα ηλεκτρονικού ταχυδρομείου στην εργασία για να στείλουν χιλιάδες αζήτητα μηνύματα ηλεκτρονικού ταχυδρομείου. Και τι γίνεται με τις μεγάλες ζημιές και την απώλεια χρόνου που προκαλείται από τους ιούς ηλεκτρονικού ταχυδρομείου, που φαίνεται κάνουν συχνότερες τις εμφανίσεις τους αυτές τις μέρες;

Κάποιες επιχειρήσεις βασίζονται σε μια ψεύτικη αίσθηση ασφάλειας με την εγκατάσταση ενός firewall. Αυτό είναι ένα καλό βήμα για να προστατεύσουν το ενδοδίκτυό τους (intranet), αλλά δεν είναι αρκετό: Τα Firewalls αποτρέπουν την πρόσβαση στο δίκτυο από τους αναρμόδιους χρήστες. Αλλά δεν ελέγχουν το περιεχόμενο του mail που στέλνεται και που παραλαμβάνεται από εκείνους που είναι εξουσιοδοτημένοι να χρησιμοποιούν το σύστημα, παραδείγματος χάριν. Περισσότερα στοχοθετημένα μέτρα απαιτούνται για να αντιδράσουν σε αυτό και σε άλλες τρύπες ασφάλειας σε ένα εταιρικό δίκτυο.

#### *4.1.1. Η απειλή διαρροής των πληροφοριών*

Οι οργανισμοί αποτυγχάνουν συχνά να αναγνωρίσουν ότι υπάρχει ένας μεγαλύτερος κίνδυνος κλοπής κρίσιμων δεδομένων από μέσα από την επιχείρηση παρά από το εξωτερικό.

Οι διάφορες μελέτες έχουν δείξει πώς οι υπάλληλοι χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο για να στείλουν τις εμπιστευτικές εταιρικές πληροφορίες. Είτε επειδή είναι δυσαρεστημένοι και εκδικητικοί, ή επειδή αποτυγχάνουν να αντιληφθούν τον ενδεχομένως επιβλαβή αντίκτυπο μιας τέτοιας πρακτικής, οι υπάλληλοι χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο για να μοιραστούν το ευαίσθητα δεδομένα που προορίστηκαν επίσημα να παραμείνουν στο εσωτερικό της επιχείρησης.

### *4.1.2. Η απειλή των emails που περιέχουν κακόβουλο ή δυσάρεστο περιεχόμενο*

Τα emails που φέρνουν τις ευαίσθητες πληροφορίες, ή τα αζήτητα μηνύματα (spam) που στέλνονται από τους εταιρικούς χρήστες δεν είναι το μόνο πρόβλημα που μια επιχείρηση πρέπει να αντιμετωπίσει όσον αφορά τη χρήση ηλεκτρονικού ταχυδρομείου από τους υπάλληλους. Τα emails που στέλνονται από το προσωπικό μπορούν να περιέχουν ρατσιστικό, φυλετικό ή άλλο δυσάρεστο υλικό και θα μπορούσαν να αποδειχθούν εξίσου ενοχλητικά.

Αυτός ο παράγοντας απασχόλησε κατά τη διάρκεια της πολύ-κοινοποιημένης περίπτωσης ενάντια στην εταιρία της Microsoft, όταν η αμερικανική κυβέρνηση παρουσίασε ως στοιχεία τα περιεχόμενα των emails που γράφτηκαν από κορυφαίους ανώτερους υπαλλήλους της Microsoft που περιγράφουν τα σχέδια της εταιρίας για να ανατρέψει τους ανταγωνιστές.

Βάσει του βρετανικού νόμου, οι εργοδότες θεωρούνται αρμόδιοι για τα emails που γράφονται από τους υπαλλήλους κατά τη διάρκεια της απασχόλησής τους, είτε ο εργοδότης συγκατατέθηκε με το email ή όχι. Εκτός αυτού, τα επιθετικά emails μπορούν να προκαλέσουν ιδιαίτερη ζημία στο περιβάλλον εργασίας, απλά με την δημιουργία μιας δυσάρεστης, εχθρικής ή μη επαγγελματικής ατμόσφαιρας.

### *4.1.3. Η απειλή των ιών*

Οι ιοί είναι ένας σημαντικός κίνδυνος ασφάλειας του ηλεκτρονικού ταχυδρομείου που οι επιχειρήσεις απλά δεν μπορούν να αντέξουν οικονομικά να αγνοήσουν. Πάνω από 11.000 διαφορετικοί ιοί υπολογιστών υπάρχουν μέχρι σήμερα και περίπου 300 νέοι δημιουργούνται κάθε μήνα. Τα αποτελέσματά τους κυμαίνονται από αμελητέα ως ενοχλητικά, ακόμα και καταστρεπτικά.

Η έκταση του προβλήματος είναι τόσο μεγάλη που σήμερα πολλές επιχειρήσεις έχουν αρχίσει ακόμη και να απαγορεύουν τη χρήση των συνημμένων ηλεκτρονικού ταχυδρομείου, καθώς εκεί είναι όπου οι ιοί ενσωματώνονται συχνά. Εκτός αν είναι προειδοποιημένοι, γενικά οι χρήστες είναι απληροφόρητοι ότι έχουν λάβει έναν ιό έως ότου ανοίγουν τη μολυσμένη σύνδεση (attachment). Στο μεταξύ, είναι πάρα πολύ αργά: ο ιός ενεργοποιείται και αρχίζει να αναλαμβάνει δράση, μολύνοντας εντελώς το σκληρό δίσκο και το δίκτυο μηνυμάτων.

Ο κίνδυνος των ιών που διαβιβάζονται μέσω των μακροεντολών, μια άλλη κοινή μορφή μετάδοσης ιών, είναι ότι επιτρέπουν στο χρήστη να συνεχίσει να εργάζεται και να μοιράζει έγγραφα. Με αυτόν τον τρόπο, ο ιός διαδίδεται γρηγορότερα, μολύνοντας όλο και περισσότερους χρήστες.

### *4.1.4. Η απειλή του spam*

Αν είσαστε online για περισσότερο από μερικούς μήνες, τότε πιθανώς θα έχετε την εξής εμπειρία: Συνδέεστε για να ελέγξετε το email σας, και σας περιμένουν νέα μηνύματα - πολλά νέα μηνύματα, και κανένα από κάποιον που να ξέρετε. Οι επικεφαλίδες θεμάτων λένε κάτι σαν: "Make Money While You Sleep", "Earn a Thousand Dollars Every Time the Phone Rings" ή "Retire Next Week!".

Αυτά τα μηνύματα ονομάζονται *spam.* (Το όνομα είναι μια αναφορά σε ένα αστείο των Month Python, όπου μια ομάδα Βίκινγκς που τραγουδούσαν "spam, spam, spam" διέκοπταν συνέχεια ένα δείπνο. Το spam στο Internet είναι πολύ παρόμοιο - άχρηστα λόγια, χωρίς καμία επικοινωνία.) Το spam υπερφορτώνει συστήματα email, ενοχλεί κόσμο και σχεδόν ποτέ δεν έχει σαν αποτέλεσμα, αυτός που το έστειλε να πωλήσει κάτι. Αυτή η έλλειψη αποδοτικότητας είναι ιδιαίτερα αληθής, επειδή τα περισσότερα τέτοια μηνύματα έχουν σχέση με κάποιο είδος πυραμίδας πωλήσεων. Κάθε σημείο πρόσβασης στο δίκτυό παρουσιάζει μια πιθανή απειλή στην ασφάλεια των συστημάτων των χρηστών. Το Spam δεν είναι εξαίρεση. Σε μια προσπάθεια "να ξεχωρίσουν από το πλήθος, οι spammers στέλνουν συχνά τα μηνύματά τους ως μήνυμα HTML, το οποίο μπορεί να εμπεριέχει τον ενσωματωμένο κακόβουλο κώδικα. Άλλα μηνύματα spam περιλαμβάνουν επισυνάψεις που μπορούν να περιέχουν μακρο ιούς. Το μήνυμα Spam μπορεί ακόμα να δείξει στους παραλήπτες τα sites που περιέχουν scripts για να συλλέξουν πληροφορίες, ή να περιλαμβάνει τις συνδέσεις που ισχυρίζονται ότι θα βγάλουν τους χρήστες από τον κατάλογο διευθύνσεων των spammer αλλά στην πραγματικότητα ελέγχουν ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου τους είναι "ενεργή". Οι Spammers χρησιμοποιούν τεχνικές "επίθεσης συγκομιδής" (harvest attack) για να συλλέξουν τις διευθύνσεις από τους εταιρικούς καταλόγους ηλεκτρονικού ταχυδρομείου. Μερικοί spammers χρησιμοποιούν διευθύνσεις νόμιμων επιχειρήσεων, τραπεζών, κ.λπ. και προσπαθούν να συγκεντρώσουν πληροφορίες για πιστωτικές κάρτες και άλλες προσωπικές πληροφορίες. Ακόμα και όταν το spam αποτελείται "μόνο" από απλό κείμενο διαφημίζοντας ένα προϊόν, ο όγκος μπορεί να απειλήσει την ακεραιότητα του δικτύου, προκαλώντας μια απρόσμενη άρνηση των υπηρεσιών.
Όπως και την κατανάλωση του εύρους ζώνης και την επιβράδυνση των συστημάτων ηλεκτρονικού ταχυδρομείου με το spam σπαταλιέται πολύς χρόνος, διότι αναγκάζει τους υπαλλήλους να διαχωρίζουν και να διαγράφουν μεγάλες ποσότητες άχρηστων mail. Αυτό αποδεικνύει την ενόχληση και επιθετικότητα προς τους παραλήπτες οι οποίοι αισθάνονται ότι η ιδιωτική τους ζωή έχει παραβιαστεί και θα μπορούσε επίσης να οδηγήσει σε μια κατάσταση που τα έγκυρα emails να απορρίπτονται μαζί με το άχρηστα emails.

## *4.2. **Προστασία από τις παραβιάσεις ασφάλειας***

### *4.2.1. Εταιρική πολιτική ασφάλειας*

Οι απειλές ασφάλειας είναι πολλές, αλλά οι αποτελεσματικές λύσεις υπάρχουν. Το πρώτο βήμα για την ενίσχυση της ασφάλειας που συστήνεται από τους συμβούλους κυβερνο-ασφάλειας είναι η διατύπωση ενός εταιρικού εγγράφου για την πολιτική που θα ακολουθείται σχετικά με το ηλεκτρονικό

ταχυδρομείο και την χρησιμοποίηση του. Αυτό χρησιμοποιείται για να ενημερώνει όλα τα μέλη της εταιρείας των οποίων οι πρακτικές σχετικά με την διαχείριση του email κρίνονται απαράδεκτες.

Χωρίς να είναι υπερβολικά περιοριστικά, τέτοια έγγραφα πρέπει να παρέχουν τις οδηγίες και τις διαδικασίες που θα πρέπει να ακολουθούνται από τους υπαλλήλους σε σχέση με την χρήση του ηλεκτρονικού ταχυδρομείου τους στον εργασιακό χώρο. Επίσης θα πρέπει να παρασχεθούν παραδείγματα των ειδών των μηνυμάτων ηλεκτρονικού ταχυδρομείου που θα μπορούσαν να αποδειχθούν καταστρεπτικά στην εταιρεία ώστε οι χρήστες να είναι προετοιμασμένοι. Το εξαιρετικά σημαντικό σημείο που υπογραμμίζεται είναι ότι με την υιοθέτηση αυτής της πολιτικής, η επιχείρηση και το προσωπικό της αναμένουν να κερδίσουν με το να εκμεταλλευτούν την ασφάλεια των μηνυμάτων που είναι όσο το δυνατόν πιο δύσκολο να αλλοιωθούν.

Έπειτα, η επιχείρηση πρέπει να αποκτήσει τα νέα εργαλεία ασφάλειας (software ή hardware) για να βοηθήσει να επιβληθούν αυτοί οι κανονισμοί, ενημερώνοντας όλους τους χρήστες ότι αυτό το μέτρο λαμβάνεται.

### *4.2.2. Λογισμικό ασφάλειας*

Οι εταιρίες μπορούν να επιλέξουν από μια μεγάλη γκάμα πακέτων ασφάλειας του ηλεκτρονικού ταχυδρομείου. Μερικές λύσεις δημιουργούνται για να αντιμετωπίσουν μια και μόνο ιδιαίτερη απειλή μόνο ενώ άλλες περιέχουν μια κατάλληλη δέσμη εργαλείων για να διαχειρίζονται τους διάφορους κινδύνους. Εξαρτάται από κάθε εταιρία να επιλέξει το λογισμικό που ανταποκρίνεται καλύτερα στις ανάγκες της.

Όπως πάντα, η τιμή αναγκαστικά είναι ένας από τους καθοριστικούς παράγοντες στην λήψη της σωστής απόφασης. Ένα άλλο ουσιαστικό χαρακτηριστικό στην αναζήτηση του κατάλληλου προϊόντος είναι ότι αυτό θα πρέπει να είναι όσο το δυνατόν απλοποιημένο και φιλικό στο χρήστη. Ένα πακέτο λογισμικού που εγκαθίσταται στο ήδη υπάρχον εταιρικό σύστημα ηλεκτρονικού ταχυδρομείου και είναι εύχρηστο σημαίνει ότι η επιχείρηση μπορεί να απολαμβάνει τα προσφερθέντα οφέλη ασφάλειας αμέσως με την εγκατάσταση. Η παρακάτω παράγραφοι εξετάζουν τα διαφορετικά χαρακτηριστικά γνωρίσματα ασφάλειας ηλεκτρονικού ταχυδρομείου που είναι διαθέσιμα στην αγορά, είτε χωριστά είτε ως τμήμα μιας λύσης.

### *4.2.3. Παρεμπόδιση των διαρροών πληροφοριών*

Ένα ικανοποιητικό εργαλείο ελέγχου είναι απαραίτητο για να αποτρέψει τους χρήστες να αποστέλλουν εμπιστευτικές ή ευαίσθητες εταιρικές πληροφορίες μέσω του ηλεκτρονικού ταχυδρομείου. Αυτό το εργαλείο ανιχνεύει αυτόματα το περιεχόμενο του κάθε μηνύματος που είναι προς αποστολή. Για να είναι αποτελεσματικό, αυτό το εργαλείο πρέπει να συνδέεται με ένα χαρακτηριστικό καραντίνας που απομονώνει τα emails με το ύποπτο περιεχόμενο και τα αποτρέπει από την αποστολή τους εκτός αν ένα εξουσιοδοτημένο πρόσωπο μέσα στην εταιρεία έχει εγκρίνει το μήνυμα.

**Ικανοποιητικός έλεγχος.** Επιπλέον, ένα ικανοποιητικό εργαλείο διαλογής είναι απαραίτητο για να αποτρέψει τους εταιρικούς χρήστες από την αποστολή ή τη λήψη των κακόβουλων, δυσάρεστων, ή ακατάλληλων emails. Αυτό πρέπει να συνδεθεί με ένα ελεγμένο και δοκιμασμένο χαρακτηριστικό καραντίνας που μπλοκάρει τα emails με το ύποπτο περιεχόμενο από την αποστολή ή λήψη τους, εκτός αν ένα εξουσιοδοτημένο πρόσωπο μέσα στην εταιρεία έχει εγκρίνει το μήνυμα πρώτα

### *4.2.4. Προστασία του ηλεκτρονικού ταχυδρομείου από τους ιούς και άλλο MalWare*

Σε παλαιότερους καιρούς, το ηλεκτρονικό ταχυδρομείο θεωρούταν ένα αρκετά ασφαλές μέσο επικοινωνίας. Όμως τα πράγματα έχουν αλλάξει κατά πολύ και στις μέρες μας το άνοιγμα ενός μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να είναι μια ‘’τρομακτική’’ εμπειρία.

Οι συγγραφείς ιών, που συνήθιζαν να διαδίδουν τις εικονικές "ασθένειές τους" μέσω των μολυσμένων δισκετών και των δικτύων, έχουν επωφεληθεί της ευκαιρίας που τίθεται από τα προγράμματα ηλεκτρονικού ταχυδρομείου που υποστηρίζουν τα **συνημμένα αρχεία**, **τα μηνύματα HTML,** και τα **ενσωματωμένα scripts** για να στέλνουν τους ιούς και άλλα κακόβουλα λογισμικά (αποκαλούμενα "malware") σε εκατοντάδες ή χιλιάδες ανθρώπους με μερικές πληκτρολογήσεις. Θα εξετάσουμε το πώς οι ιοί ηλεκτρονικού ταχυδρομείου λειτουργούν και τι μπορούν να κάνουν οι χρήστες για να προστατεύσουν τον υπολογιστή και το δίκτυό τους από αυτούς.

### *4.2.5. Πώς λειτουργούν οι ιοί ηλεκτρονικού ταχυδρομείου*

Υπάρχουν αρκετοί διαφορετικοί τρόποι με τους οποίους οι ιοί μπορούν να εισβάλουν στον υπολογιστή μέσω του ηλεκτρονικού ταχυδρομείου των χρηστών. Μια από τις ποιο διαδεδομένες είναι μέσω των συνημμένων αρχείων. Εάν ο χρήστης ανοίξει ένα εκτελέσιμο αρχείο που είναι συνημμένο με ένα μήνυμα mail, το πρόγραμμα τρέχει και ο ιός κάνει την καταστροφική δουλειά του – σε αρκετές περιπτώσεις δεν κάνει τη ζημία μόνο στ μηχάνημα του συγκεκριμένου χρήστη αλλά και χρησιμοποιεί το βιβλίο διευθύνσεών του ώστε να στέλνει αντίγραφα του εαυτού του σε καθένα με το οποίο ο χρήστης αλληλογραφεί. Αυτά τα μολυσμένα μηνύματα θα εμφανιστούν να είναι από τον ήδη μολυσμένο χρήστη, ακόμα κι αν δεν γνωρίζει και ότι εστάλησαν. Γι’ αυτό πρέπει πάντα να υπάρχει μεγάλη επιφυλακτικότητα στην λήψη μηνύματος με επισυνάψεις, ακόμα και όταν προέρχεται από κάποιον γνωστό. Οι ιοί που λειτουργούν αυτόν τον τρόπο περιλαμβάνουν τους Melissa, Klez, και άλλους.

Η αποφυγή των ιών μέσω των συνημμένων αρχείων θα ήταν εύκολη μόνο αν οι χρήστες δεν άνοιγαν τα συνημμένα τους μηνύματα. Εντούτοις, δεν είναι πάντα αυτό τόσο απλό. Πολλοί από τους χρήστες των οποίων η εργασία εξαρτάται από τη συνεργασία με άλλους μέσα από το διαδίκτυο πρέπει να ανταλλάσσουν συνημμένα μηνύματα. Θα πρέπει ο χρήστης να σημειώνει τον

τύπο αρχείου πριν ανοίξει ένα συνημμένο. Τα εκτελέσιμα είναι πιο πιθανό να είναι επικίνδυνα, αλλά οι συγγραφείς των ιών χρησιμοποιούν τεχνάσματα όπως η προσάρτηση πολλαπλών επεκτάσεων στα αρχεία έτσι ώστε να ξεγελάσουν ότι ένα αρχείο είναι κάτι που στην ουσία δεν είναι. Επειδή ο Windows Explorer και μερικά προγράμματα λογισμικού δεν παρουσιάζουν κοινές επεκτάσεις εξ ορισμού, ένα αρχείο με όνομα letter.txt.exe θα εμφανιστεί να είναι ένα αβλαβές αρχείο κειμένων όταν στην πραγματικότητα είναι ένα αρχείο προγράμματος.

Επειδή το πρόβλημα των ιών στις επισυνάψεις είναι τόσο μεγάλο, η Microsoft έχει κυκλοφορήσει τις πρόσφατες εκδόσεις του Outlook (2002 και πάνω) για να μπλοκάρει αυτόματα τους εκτελέσιμους τύπους αρχείου (exe, .bat, .com, .lnk, .scr, .vbs) και πολλούς άλλους). Αυτό το χαρακτηριστικό γνώρισμα προστίθεται επίσης στο Outlook 2000 με την εγκατάσταση του Service Pack 2 και στο Outlook 98 όταν γίνεται εφαρμογή του Outlook Email Security Update. Δυστυχώς όμως, αυτό δημιουργεί μια κατάσταση όπου η θεραπεία μπορεί να είναι χειρότερη από την ασθένεια εάν πρέπει να αποσταλούν και να ληφθούν οι συγκεκριμένοι τύποι αρχείων. Σε αυτή την περίπτωση, υπάρχουν διάφοροι τρόποι χειρισμού του προβλήματος.

Η απλούστερη μέθοδος είναι να μετονομαστεί το αρχείο με μια διαφορετική επέκταση (π.χ. να μετονομάσει από program.exe σε program.txt) και να ειπωθεί στο πρόσωπο στο οποίο γίνεται η αποστολή του μηνύματος να το μετονομάσει στο αρχικό όνομα του πριν το ‘’κατεβάσει’’.

Στο Outlook 2002, μπορεί ο χρήστης να μεταβάλει το μητρώο (Registry) για να τροποποιήσει τους τύπους αρχείου που θα μπλοκάρονται. Υπάρχουν διάφορα utilities που επιτρέπουν να γίνει το ίδιο πράγμα χωρίς να τροποποιηθεί άμεσα το μητρώο. Μερικά χαρακτηριστικά utilities είναι το Outlook Permissions Add-in, το DetachXP και το Xenos Outlook Security Extension.

Το μπλοκάρισμα των συνημμένων είναι προαιρετικό στο Outlook Express, και το Outlook Web Access δεν περιλαμβάνει μπλοκάρισμα συνημμένων. Έτσι ένας άλλος τρόπος να αποκτηθούν τα συνημμένα είναι να χρησιμοποιηθεί OWA (Outlook Web Access) ή να εισαχθούν τα μηνύματά στο OE από το Outlook.

Ακόμα και αν τα συνημμένα είναι αρχεία εγγράφων, ο χρήστης δεν μπορεί να αισθάνεται απολύτως ασφαλής. Τα έγγραφα Word μπορούν να περιέχουν μακροεντολές (μικρά προγράμματα) που μπορούν να εκτελέσουν τις κακόβουλες εντολές. Αυτοί καλούνται μακρο-ιοί. Ο χρήστης μπορεί να προστατευθεί με τον καθορισμό του μακρο επιπέδου ασφάλειας στο Word (μέσω της διαδρομής -**Tools | Options | Security tab**) στη μέση ή υψηλή επιλογή. Η υψηλή θέτει εκτός λειτουργίας όλες τις ανυπόγραφες μακροεντολές, και η μέση προειδοποιεί πριν τρέξει μια μακροεντολή, όπως φαίνεται στην **Εικόνα 4-1.**

.


**Εικόνα 4-1: Το μενού της μακρο ασφάλειας στο Word με τις επιλογές προστασίας από τους μακρο ιούς(High,Medium,Low)**

Όμως δεν μπορούμε να πούμε ότι τα mail είναι ασφαλή μόνο όταν δεν υπάρχουν συνημμένα αρχεία. Οι ιοί μπορούν επίσης να ενσωματωθούν στο ίδιο το μήνυμα. Αυτό δεν είναι δυνατό σε ένα απλό μήνυμα κειμένου, αλλά τα δημοφιλέστερα πακέτα (Outlook, OE, Eudora) υποστηρίζουν το HTML mail έτσι ώστε να είναι δυνατή η χρησιμοποίηση επιστολόχαρτων, η ενσωμάτωση εικόνων και ήχου, και ούτω καθ' εξής. Ένα μήνυμα HTML μπορεί να περιέχει scripts (προγράμματα) που εκτελούν τους ιούς. Αυτό είναι ένας λόγος που πολλές λίστες ηλεκτρονικού ταχυδρομείου μπλοκάρουν τα HTML μηνύματα.

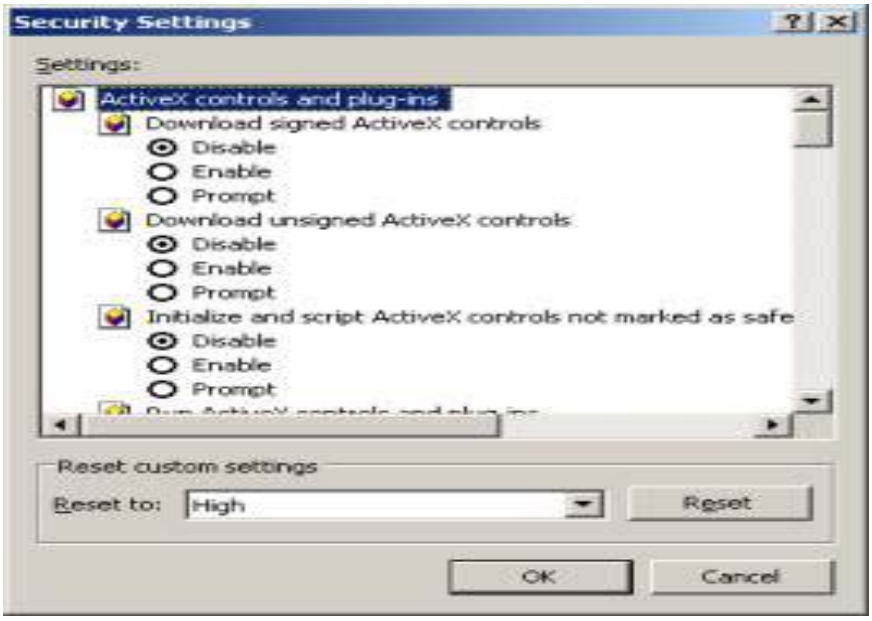
Η πιο πρόσφατη έκδοση του Outlook (2003), επιτρέπει τελικά στους χρήστες να μπλοκάρουν τα μηνύματα HTML. Για να γίνει μετατροπή του εισερχόμενου HTML μηνύματος σε απλό κείμενο στο Outlook 2000, χρησιμοποιείται ο κώδικας VBA. Στο Outlook 2002, μπορεί να χρησιμοποιηθεί ο Rules Wizard με την ενέργεια του τρεξίματος ενός script για να καλέσει μια υπορουτίνα VBA και να εκτελέσει αυτήν την μετατροπή.

Ακόμη και τα σαφή μηνύματα κειμένων μπορούν να περιέχουν URLs που μπορούν να παραπέμπουν σε sites όπου τρέχουν τα scripts και διαδίδουν τους ιούς.

### *4.2.6. Προστατευτικά μέτρα που μπορούν να πάρουν οι χρήστες*

Οι περισσότεροι ιοί είναι προορισμένοι για συγκεκριμένο λειτουργικό σύστημα (δηλαδή ιοί που τρέχουν στα Windows συχνά δεν έχουν επιπτώσεις στους υπολογιστές με λειτουργικό Linux ή Macintosh, και αντίστροφα) και πολλοί είναι επίσης συγκεκριμένοι για ορισμένους πελάτες (clients) ηλεκτρονικού ταχυδρομείου. Το πρώτο βήμα στην προστασία του υπολογιστή από τους ιούς ηλεκτρονικού ταχυδρομείου είναι να εφαρμοστούν όλα τα service packs και τα updates ασφάλειας, εκείνα για το λειτουργικό σύστημα και εκείνα για το λογισμικό του ηλεκτρονικού ταχυδρομείου. Επειδή ο mail client είναι πιθανό να αλληλεπιδρά με τον browser κατά την ανάγνωση μηνυμάτων HTML, πρέπει επίσης να γίνει εφαρμογή των πιο πρόσφατων αναπροσαρμογών (updates) στον Internet Explorer.

Ο mail client πρέπει να διαμορφωθεί έτσι ώστε τα scripts του ActiveX και της Java να μην τρέχουν αυτόματα. Στο Outlook και OE, αυτό γίνεται μέσω των ρυθμίσεων της ζώνης ασφάλειας. Συγκεκριμένα μέσω της διαδρομής (**Tools | Options | Security**). Επιλογή σε ποια περίπτωση να απενεργοποιείται (disable) **το** ActiveX και τα scripts ή ακόμα "υπενθύμιση"(prompt) όπως φαίνεται στην Εικόνα 4-2.




**Εικόνα 4-2: Το μενού Security Settings με τις επιλογές του ActiveX.**

Με το να θέσει ο χρήστης εκτός λειτουργίας (disable) το ActiveX και το scripting στο Outlook ή η απαίτηση μιας υπενθύμισης(prompt)θα αποτρέψουν αυτά τα συστατικά από να εκτελεστούν αυτόματα.Το επόμενο βήμα είναι να εγκατασταθεί ένα καλό **anti-virus** ή ένα πρόγραμμα ασφάλειας ηλεκτρονικού ταχυδρομείου. Αν και ένα πρόγραμμα **anti-virus** θα βοηθήσει, μπορεί να μην είναι αρκετό να προστατεύσει ένα δίκτυο. Σε εκείνη την περίπτωση, ένα περιεκτικότερο "email **firewall**" όπως π.χ. το GFi MailSecurity for Exchange μπορεί να ελέγξει το περιεχόμενο των μηνυμάτων καθώς επίσης και για ιούς.

Όμως, νέοι ιοί δημιουργούνται καθημερινά, έτσι οποιοδήποτε **anti-virus** θα πρέπει να ενημερώνει τα αρχεία του τακτικά.

## *4.3. Εξάλειψη του spam*

### *4.3.1. Αντι-spam τεχνολογίες : Ποιες είναι οι καλύτερες;*

Μερικές τεχνικές ελέγχου spam περιλαμβάνουν:

- **Key word filtering**: είναι ένας τύπος φιλτραρίσματος στρώματος εφαρμογής -application layer filtering (ALF) που επιτρέπει να μπλοκάρονται όλα τα μηνύματα που περιέχουν τις ιδιαίτερες λέξεις κλειδιά ή τις φράσεις που εμφανίζονται συνήθως στο spam (π.χ “Viagra” ή “xxx” κ.τ.λ)
- **Address blocking**: είναι μια μέθοδος φιλτραρίσματος που μπλοκάρει τα μηνύματα από συγκεκριμένες διευθύνσεις IP, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου ή domains των γνωστών spammers.
- **Μαύρη λίστα (Black listing)**: η διατήρηση ενός καταλόγου γνωστών διευθύνσεων των spammers που μπορούν να μοιραστούν και με άλλους, έτσι κάθε χρήστης δεν είναι απαραίτητο να σχηματίσει τον κατάλογο από την αρχή.
- **Λευκή λίστα (White listing**): είναι μια μέθοδος φιλτραρίσματος που, αντί του καθορισμού των ποιών αποστολέων πρέπει να εμποδιστούν, διευκρινίζει ποιοι αποστολείς πρέπει να έχουν την άδεια να στέλνουν μηνύματα.
- **Heuristic filtering (Ευρετικό φιλτράρισμα)**: βασισμένο σε κανόνα φιλτράρισμα που χρησιμοποιεί το ταίριασμα προτύπων που προσδιορίζουν το spam.
- **Bayesian filtering (Μπεϋζιανό φιλτράρισμα)**: "ευφυές" λογισμικό Ένα αποδοτικό αντι - spam εργαλείο χρησιμοποιεί την Μπεϋζιανή (Bayesian) τεχνολογία φιλτραρίσματος που ανιχνεύει τα βασισμένα σε spam μηνύματα. Αντί απλώς να ελέγχει για λέξεις κλειδιά, ένα Μπεϋζιανό φίλτρο λαμβάνει υπόψη ολόκληρο το μήνυμα. Τα Μπεϋζιανά φίλτρα αναγνωρίζονται ευρέως ότι είναι ο καλύτερος τρόπος στην αντιμετώπιση του spam επειδή χρησιμοποιούν τη στατιστική νοημοσύνη για να αναλύουν το περιεχόμενο του email. Μαζί με αυτό, ένα αντι - spam προϊόν πρέπει να αναλύει τις υπογραφές του email και να προσδιορίζει τις βασισμένες σε spam και να είναι ικανό να ανιχνεύσει τις πλαστογραφημένες υπογραφές, την μεταλλαγή του spam, spam σταλμένο από άγνωστα domains. Πρέπει επίσης να επιτρέπει στο χρήστη να διαμορφώνει τις λέξεις κλειδιά για να ελέγχει για spam χρησιμοποιώντας τον έλεγχο της λέξης κλειδιού.
- **Φιλτράρισμα πρόκλησης /απάντησης (Challenge/Response)**: οι απαντήσεις στο email από αποστολείς που είναι εκτός της "λίστας εμπιστοσύνης" με μια πρόκληση, περιλαμβάνοντας συνήθως λύση ενός στόχου που είναι εύκολος για τους ανθρώπους αλλά δύσκολος για αυτοματοποιημένα bots ή scripts.

Παρ' όλα αυτά όμως καμία μέθοδος δεν μπορεί να εξασφαλίσει αποτελεσματικότητα 100% ενάντια στο spam. Οι Spammers αλλάζουν συνεχώς τις διευθύνσεις τους, ενημερώνουν τα περιεχόμενά τους και χρησιμοποιούν τεχνάσματα όπως η ανορθογραφία των βασικών λέξεων ή η χρησιμοποίηση των διαστημάτων ή των περιόδων (π.χ., "v.i.a.g.r.a.") για να παρακάμψουν τα συστήματα που προστατεύονται με φίλτρα.

Ένα ιδιαίτερο πρόβλημα με το λογισμικό φιλτραρίσματος του spam είναι η δυνατότητα *των ψεύτικων – θετικών* (*false positives)* μηνυμάτων που προσδιορίζονται ως spam και παρεμποδίζονται, αλλά που είναι πραγματικά νόμιμα (και μερικές φορές σημαντικά). Το μόνο πράγμα χειρότερο από το να περάσει το spam στα εισερχόμενα μηνύματα του χρήστη είναι να χαθεί ένα κρίσιμο μήνυμα επειδή πιάστηκε από τα φίλτρα κατά του spam. Ανεξάρτητα από τις μεθόδους που χρησιμοποιούνται για να προσδιορίσουν το spam, ένα καλό αντί - spam πρόγραμμα πρέπει να περιλάβει έναν μηχανισμό λευκής λίστας, από τον οποίο οι χρήστες να μπορούν να διευκρινίσουν ότι τα μηνύματα από ορισμένες διευθύνσεις πρέπει να παραδίδονται ανεξάρτητα με το περιεχόμενο τους.

### *4.3.2. Τύποι spam*

Συνήθως σκεφτόμαστε το spam ως ανεπιθύμητο μήνυμα, αλλά είναι κάτι περισσότερο από αυτό. Το Spam μπορεί να ταξινομηθεί με αρκετούς τρόπους:

- **Άχρηστα μηνύματα (Junk mail)**: Μαζικές αποστολές διαφημιστικών ανεπιθύμητων μηνυμάτων από νόμιμες επιχειρήσεις.
- **Μη διαφημιστικά μηνύματα**: Αλληλουχίες γραμμάτων, τοπικοί μύθοι, συλλογές αστείων και άλλες μαζικές αποστολές των ανεπιθύμητων μηνυμάτων χωρίς ένα προφανή εμπορικό κίνητρο.
- **Porno spam**: Μαζικές αποστολές "ενήλικων" διαφημίσεων ή πορνογραφικών εικόνων
- **Spam scams:** Μαζικές αποστολές ψευδών μηνυμάτων ή εκείνων που σχεδιάζονται να αποσπούν από τους χρήστες τις προσωπικές τους πληροφορίες με σκοπό την κλοπή ταυτότητας και άλλες εγκληματικές πράξεις
- **Ο ιός spam** – Μαζικές αποστολές που περιέχουν ιούς, Trojans, κακόβουλα scripts κ.λπ.

# ΚΕΦΑΛΑΙΟ 4ο

# *5. ΠΩΣ ΝΑ ΑΙΣΘΑΝΟΝΤΑΙ ΟΙ ΧΡΗΣΤΕΣ ΑΣΦΑΛΕΙΣ*

## *5.1. Βασικές ρυθμίσεις για περισσότερη ασφάλεια στα συστήματα Win NT/2000/XP;*

Τα ακόλουθα στοιχεία καθιστούν τα WinNT ασφαλέστερα, συμπεριλαμβανομένης της ανίχνευσης καθώς επίσης και της πρόληψης. Αυτά παρατίθενται κατά προσέγγιση κατά σειρά σπουδαιότητας.

- **Εγκατάσταση των πιο πρόσφατων service packs και "hot fixes".**

Οι προμηθευτές θα κυκλοφορήσουν στην αγορά συνήθως τα patches για το λογισμικό τους όταν ανακαλυφθεί μια ευπάθεια σε αυτό. Οι περισσότερες υποστηρίξεις προϊόντων προσφέρουν μια μέθοδο για να πάρει ο χρήστης τα updates και patches. Πρέπει ο χρήστης να είναι σε θέση να λάβει τα updates από το web site του προμηθευτή. Μερικές εφαρμογές θα ελέγξουν αυτόματα για τα διαθέσιμα updates, και πολλοί προμηθευτές προσφέρουν την αυτόματη ανακοίνωση των updates μέσω ενός καταλόγου διευθύνσεων. Έτσι ο χρήστης πρέπει να κοιτάξει στο site του προμηθευτή του τις πληροφορίες για την αυτόματη ανακοίνωση. Εάν κανένας κατάλογος διευθύνσεων ή άλλος αυτοματοποιημένος μηχανισμός ανακοίνωσης δεν προσφέρεται μπορεί να πρέπει να γίνει περιοδικός έλεγχος για updates

- **Χρήση λογισμικού προστασίας εναντίον των ιών (anti-virus)**

Συστήνεται η χρήση του anti-virus σε όλους τους συνδεμένους στο διαδίκτυο υπολογιστές. Πρέπει το λογισμικό αυτό να ενημερώνεται συχνά με updates. Πολλά από τα πακέτα anti-virus υποστηρίζουν αυτόματες ενημερώσεις σε σχέση με νέους ιούς.

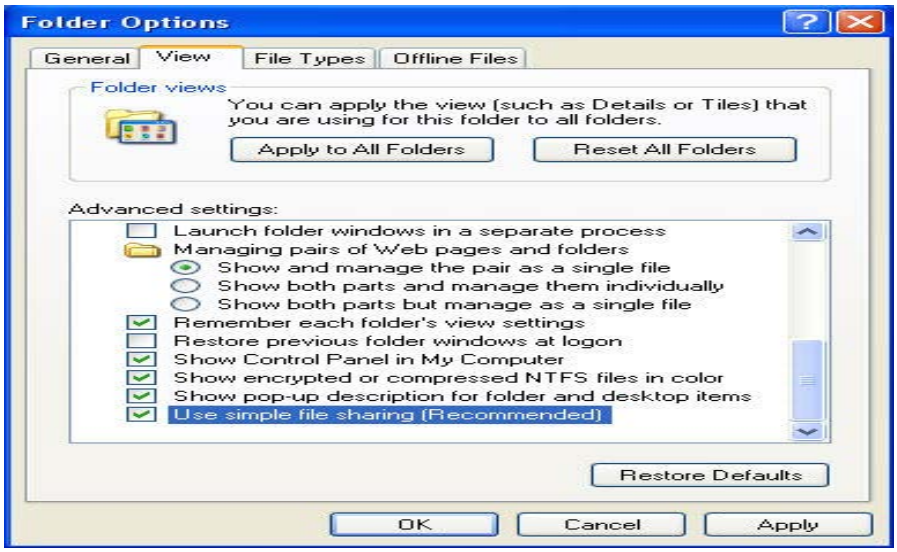
- **Αποφυγή του ανοίγματος προγραμμάτων άγνωστης προέλευσης**

Ο χρήστης δεν θα πρέπει ποτέ να ανοίγει ένα πρόγραμμα εκτός αν ξέρει ότι είναι από ένα πρόσωπο ή μια επιχείρηση που εμπιστεύεται. Επίσης, δεν θα πρέπει να στέλνονται προγράμματα άγνωστης προέλευσης σε φίλους ή σε συναδέλφους απλά επειδή είναι για διασκεδαστικά – μπορεί να περιέχουν ένα πρόγραμμα Trojan horse

5.1.1. Προστασία των κοινόχρηστων αρχείων

Εξ ορισμού, τα Windows XP Professional που δεν συνδέονται με ένα domain χρησιμοποιούν πρότυπο δικτυακής πρόσβασης αποκαλούμενο "Simple File Sharing“, όπου όλες οι προσπάθειες σύνδεσης προς τον υπολογιστή μέσω του δικτύου θα αναγκάζονται να χρησιμοποιούν τον Guest account. Αυτό σημαίνει ότι πρόσβαση στο δίκτυο μέσω του Server Message Block (SMB,

που χρησιμοποιείται για την πρόσβαση σε αρχεία και εκτυπώσεις), καθώς επίσης και η κλήση εξ αποστάσεως διαδικασίας -Remote Procedure Call (RPC, που χρησιμοποιείται από τα περισσότερα εξ-αποστάσεως διαχειριστικά εργαλεία και εξ-αποστάσεως πρόσβαση στο μητρώο) θα είναι μόνο διαθέσιμη στον Guest account. Αυτό είναι ατελές και θα πρέπει να αλλαχθεί. Για να το αλλάξει, πρέπει να ακολουθηθούν τα παρακάτω βήματα: Start => Programs => Accessories => Windows Explorer επιλογή του μενού Tools και επιλογή 'Folder Options'.




**Εικόνα 5-1: Το μενού Folder Options**

Στο πρότυπο Simple File Sharing, οι διαμοιράσεις αρχείων μπορούν να δημιουργηθούν έτσι ώστε η πρόσβαση από το δίκτυο να είναι μόνο ανάγνωσης (read-only), ή η πρόσβαση από το δίκτυο είναι να σε θέση να διαβάσει, να δημιουργήσει, να αλλάξει, και να διαγράψει τα αρχεία. Η απλή διαμοίραση αρχείων προορίζεται για τη χρήση σε ένα εγχώριο δίκτυο και πίσω από firewall, όπως αυτή που παρέχεται από τα Windows XP. Εάν υπάρχει σύνδεση με το Διαδίκτυο, και δεν υπάρχει firewall, πρέπει ο χρήστης να έχει υπόψη του ότι οποιοδήποτε διαμοιράσεις αρχείων δημιουργεί μπορούν να είναι προσιτές σε οποιοδήποτε χρήστη στο διαδίκτυο.

Η σύστασή είναι η απενεργοποίηση της επιλογής Simple File Sharing

Για να τεθεί εκτός λειτουργίας την αυτή η επιλογή ακολουθούνται τα εξής βήματα

Folder Options => View => Στο παράθυρο Advanced Settings απενεργοποίηση της επιλογής Use Simple File Sharingg => κλείσιμο των επιλογών φακέλων

- **Απενεργοποίηση κρυμμένων επεκτάσεων ονομάτων αρχείου**

Τα Windows περιέχουν μια επιλογή το "Hide file extensions for known file types". "Κρύψε τις επεκτάσεις αρχείων για τους γνωστούς τύπους αρχείων". Η επιλογή αυτή είναι ενεργοποιημένη εξ ορισμού, αλλά μπορεί ο χρήστης να θέσει εκτός λειτουργίας αυτή την επιλογή προκειμένου να φανερωθούν οι

επεκτάσεις αρχείων από τα Windows. Μετά από το να θέσουν εκτός λειτουργίας αυτήν την επιλογή, υπάρχουν ακόμα μερικές επεκτάσεις αρχείων που, εξ ορισμού, θα συνεχίσουν να παραμένουν κρυμμένες. Υπάρχει μια τιμή του μητρώου που, εάν τίθεται, θα αναγκάσει τα Windows να κρύψουν ορισμένες επεκτάσεις αρχείων ανεξάρτητα από τις επιλογές διαμόρφωσης του χρήστη αλλού στο λειτουργικό σύστημα. Η τιμή του μητρώου "NeverShowExt" χρησιμοποιείται για να κρύψει τις επεκτάσεις για τους βασικούς τύπους αρχείου Windows. Παραδείγματος χάριν, η ".LNK" επέκταση που συνδέεται με τις συντομεύσεις των Windows παραμένει κρυμμένη ακόμα και αφού έχει κλείσει ένας χρήστης την επιλογή να κρυφτούν οι επεκτάσεις.

5.1.1.1. Χρησιμοποίηση firewall

Η χρήση κάποιου τύπου προϊόντος firewall είναι καθοριστική για το μέγεθος της ασφάλειας σε ένα σύστημα. Οι εισβολείς ανιχνεύουν συχνά τα συστήματα οικιακών χρηστών για τις γνωστές ευπάθειες. Τα firewallς δικτύων μπορούν να παρέχουν κάποιο βαθμό προστασίας ενάντια σε αυτές τις επιθέσεις. Εντούτοις, κανένα firewall δεν μπορεί να ανιχνεύσει ή να σταματήσει όλες τις επιθέσεις, έτσι δεν είναι ικανοποιητικό να εγκατασταθεί ένα firewall και να αγνοηθούν έπειτα όλα τα άλλα μέτρα ασφάλειας

5.1.1.2. Κλείσιμο του υπολογιστή ή αποσύνδεση από το δίκτυο όταν δεν είναι σε χρήση

Κλείσιμο του υπολογιστή ή αποσύνδεση τη διεπαφής Ethernet του όταν δεν την χρησιμοποιούνται. Ένας εισβολέας δεν μπορεί να επιτεθεί στον υπολογιστή εάν αυτός είναι κλειστός ή ειδάλλως εντελώς αποσυνδεμένος από το δίκτυο.

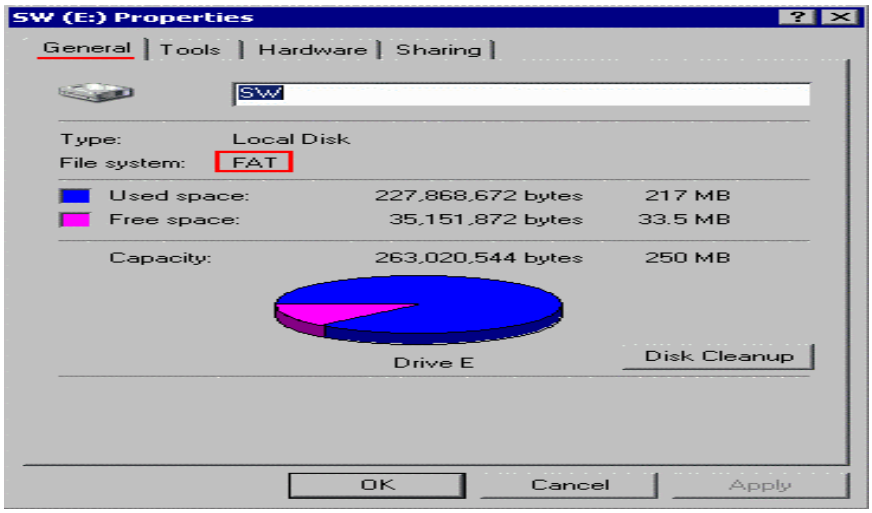
5.1.1.3. Αποφυγή του ανοίγματος επισυνάψεων ηλεκτρονικού ταχυδρομείου

Πριν ανοιχθεί οποιοδήποτε επισύναψη ηλεκτρονικού ταχυδρομείου, ο χρήστης θα πρέπει να είναι σίγουρος ότι ξέρει την πηγή της επισύναψης. Δεν είναι αρκετό που το μήνυμα προέρχεται από μια διεύθυνση που αυτός αναγνωρίζει

5.1.1.4. Απενεργοποίηση της Java, JavaScript, και ActiveX αν είναι δυνατόν

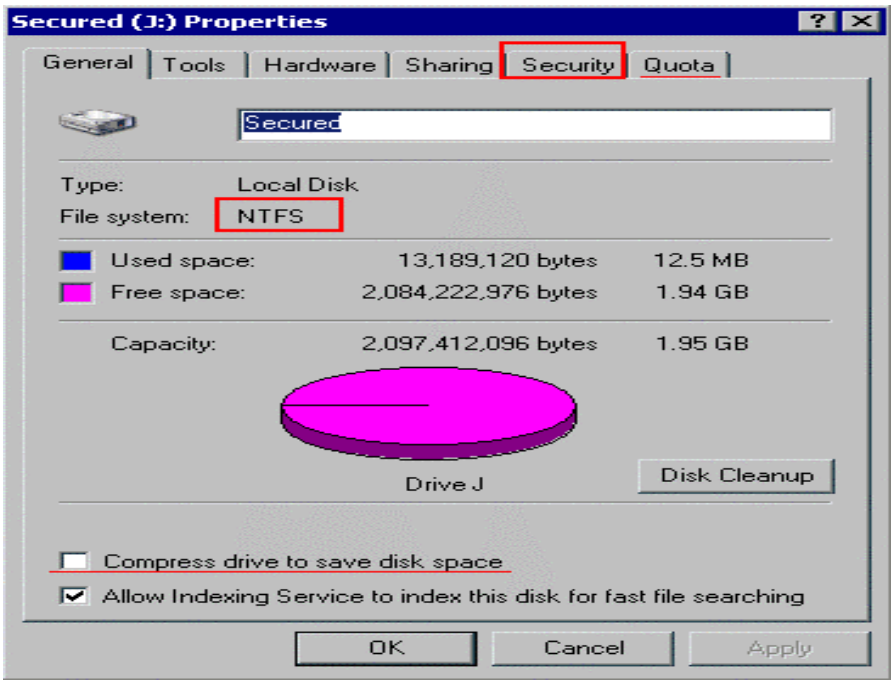
Καλό θα είναι ο χρήστης να γνωρίζει τους κινδύνους που περιλαμβάνονται στη χρήση του "κινητού κώδικα" (mobile code) όπως ActiveX, η Java, και JavaScript. Ένας κακόβουλος web developer μπορεί να επισυνάψει ένα script με κάτι που στέλνεται σε ένα web site, όπως ένα URL, ένα στοιχείο σε μια μορφή, ή μια έρευνα βάσεων δεδομένων. Αργότερα, όταν αποκρίνεται το web site στο χρήστη, το κακόβουλο script μεταφέρεται στον browser του. Ο σημαντικότερος αντίκτυπος αυτής της ευπάθειας μπορεί να αποφευχθεί με το να θέσει ο χρήστης εκτός λειτουργίας όλες τις γλώσσες scripting. Η απενεργοποίηση αυτών των επιλογών θα τον προστατέψει από το αν είναι ευπαθής στα κακόβουλα scripts. Εντούτοις, θα περιορίσει την αλληλεπίδραση που μπορεί ο χρήστης να έχει με μερικά sites. Πολλά νόμιμα sites χρησιμοποιούν scripts που τρέχουν μέσα στον browser για να προσθέσουν χρήσιμα χαρακτηριστικά γνωρίσματα. Με την απενεργοποίηση μπορεί να υποβιβαστεί η λειτουργία αυτών των sites.

- **Χρησιμοποίηση NTFS αντί του FAT**. Η επιλογή Security δεν είναι διαθέσιμη σε δίσκους πού είναι φορμαρισμένοι με FAT ή FAT32




**Εικόνα 5-2: Το μενου Properties του σκληρού δίσκου φορμαρισμένου σε FAT**

Αντιθέτως η επιλογή Security είναι διαθέσιμη σε δίσκους πού είναι φορμαρισμένοι με NTFS. Υπάρχουν επίσης και άλλες επιλογές όπως συμπίεση δίσκων/αρχείων



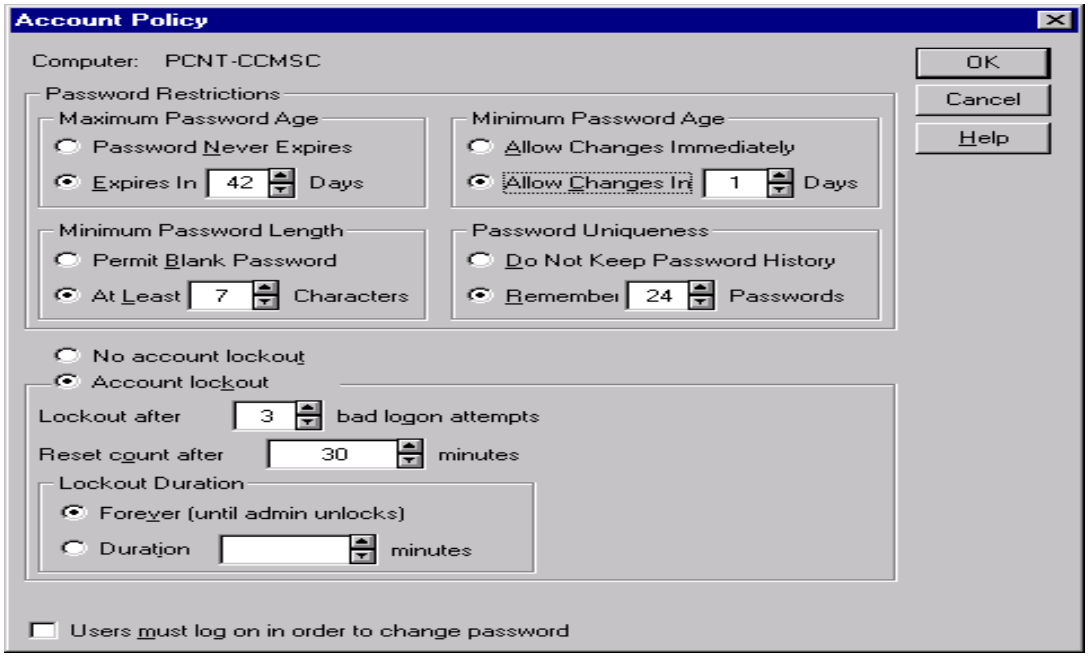

**Εικόνα 5-3: Το μενού Properties του σκληρού δίσκου φορμαρισμένου σε NTFS**

- **Μετονομασία του λογαριασμού του" administrator ".** Μια συνήθης επίθεση είναι αυτή των λεξικών και της ωμής βίας στον λογαριασμό του administrator ".

- **Δημιουργία ενός νέου λογαριασμού που ονομάζεται "administrator "** για την ανίχνευση των προσπαθειών παρείσφρησης.

- **Απενεργοποίηση του λογαριασμού "guest**". Μπορεί επίσης να θελήσετε να μετονομάσετε αυτόν τον λογαριασμό. Μόλις γίνει μετονομασία του λογαριασμού "guest", μπορεί να θελήσετε να δημιουργήσετε έναν νέο λογαριασμό που ονομάζεται "guest " για την ανίχνευση των προσπαθειών hacking.

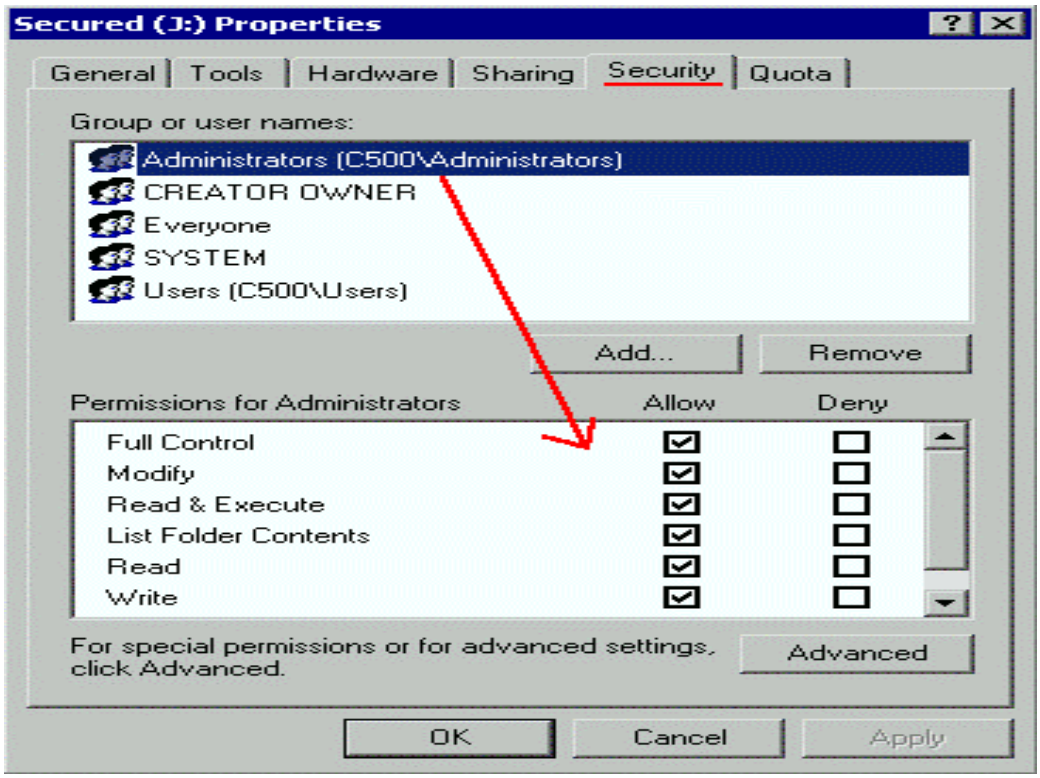
- **Επιβολή ορίου κλειδώματος του κωδικού πρόσβασης** ύστερα από έναν αποτυχημένο αριθμό προσπαθειών σύνδεσης με το σύστημα. Το κλείδωμα αυτό πρέπει να γίνεται μόνο από τον διαχειριστή.




**Εικόνα 5-4 Το μενού Account Policy που βρίσκεται στο User Manager**

- **Άδειες /δικαιώματα**:

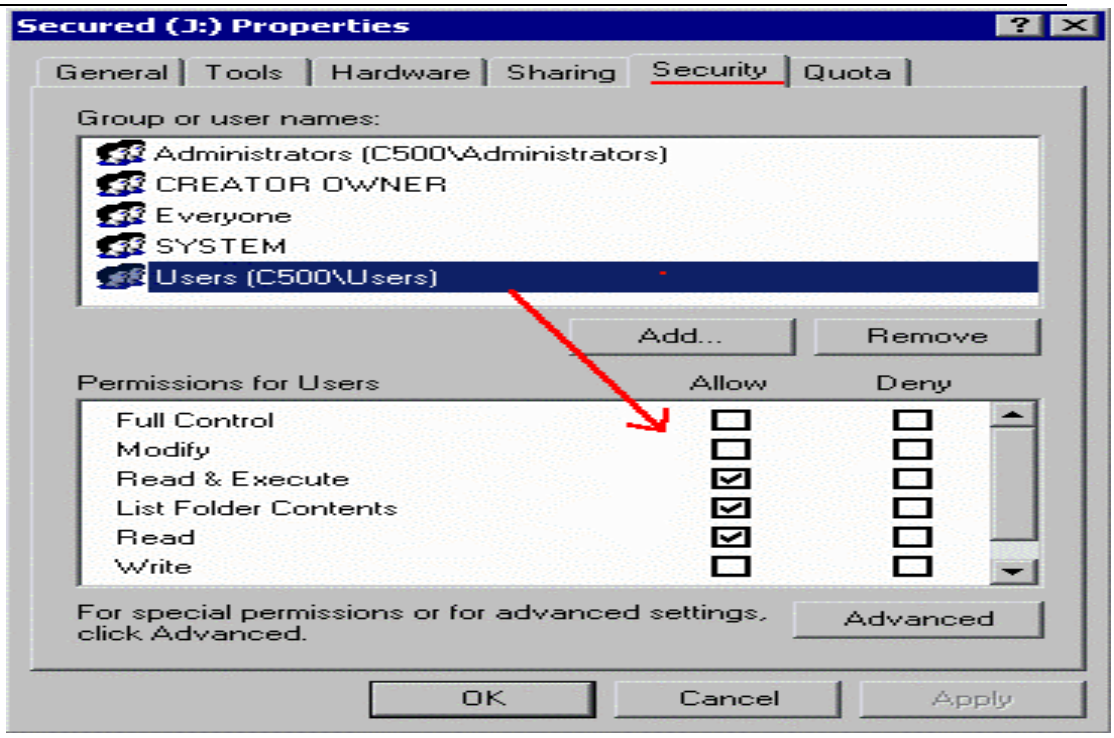
Εξ ορισμού, τα μέλη των administrators έχουν το "πλήρη έλεγχο", ο οποίος περιλαμβάνει όλες τις άδειες.




**Εικόνα 5-5: Το μενού Secured properties με τα δικαιώματα του Administrator**

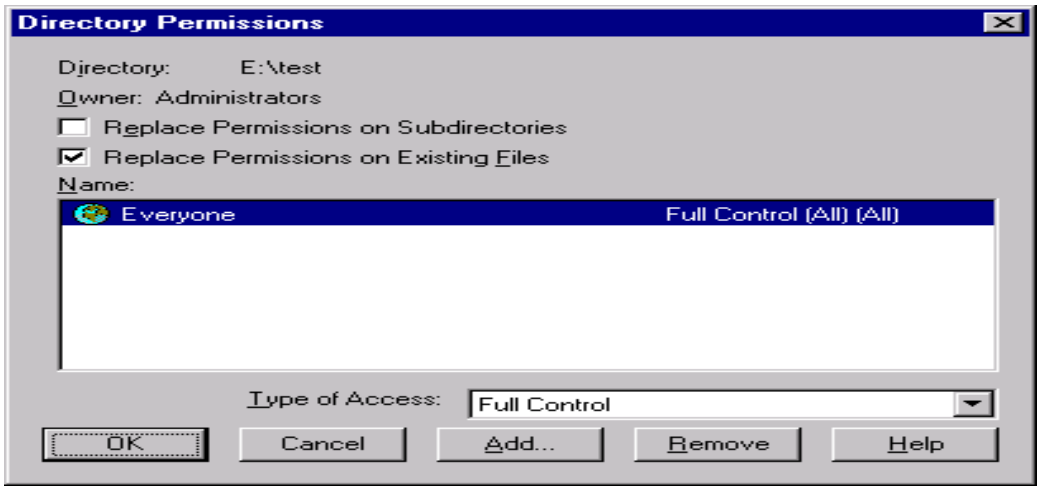
Τα μέλη άλλων ομάδων (όπως "οι χρήστες") έχουν περιορισμένη μόνο την άδεια πρόσβασης:

- μπορούν να διαβάσουν και να εκτελέσουν τα αρχεία
- δεν μπορούν να δημιουργήσουν / τροποποιήσουν / διαγράψουν τα αρχεία.




**Εικόνα 5-6 Το μενού Secured properties με τα δικαιώματα του χρήστη**

- **Αφαίρεση του 'Everyone Group'** και προσεκτική χρήση του 'special user' του συστήματος




**Εικόνα 5-7 Το μενού Directory Permissions με το Everyone Group**

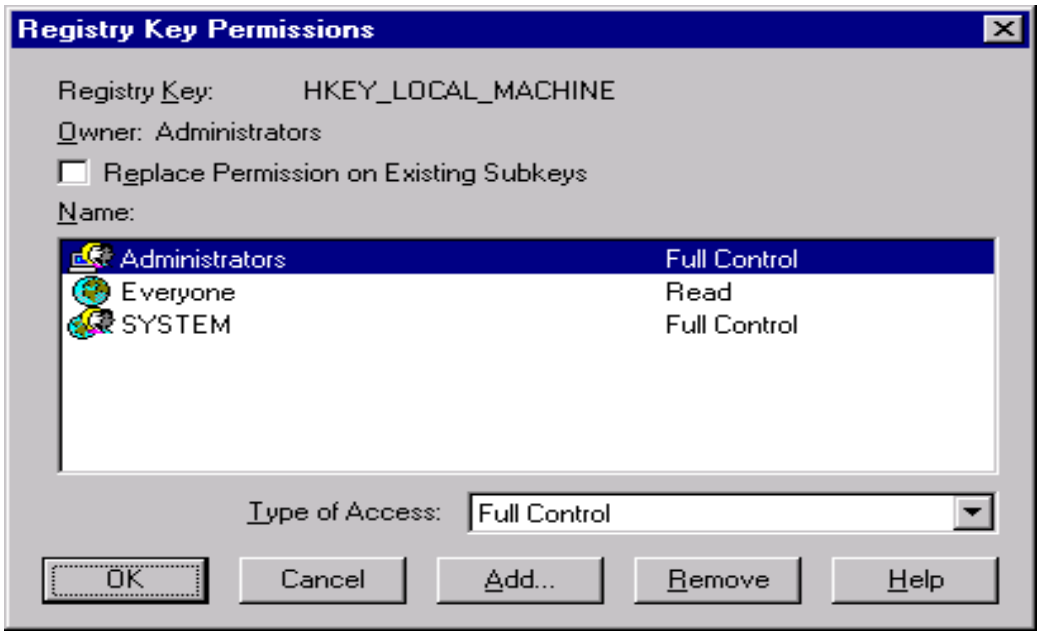
**Ρυθμίσεις ασφάλειας του διαμοιρασμού αρχείων (File Share)**

Η προεπιλεγμένη άδεια σε ένα διαμοιρασμό είναι να δοθεί στην ομάδα Everyone πλήρης έλεγχος

Εξασφάλιση ότι στην ομάδα Everyone δεν δίνεται ο πλήρης έλεγχος σε οποιεσδήποτε διαμοιράσεις

Απόδοση στους χρήστες (users) /τις ομάδες (groups) το ελάχιστο τών αδειών που απαιτούνται σε ένα διαμοιρασμό

- **Ασφάλεια του μητρώου**. Αλλαγή ρυθμίσεων για να μην υπάρχουν(όσο είναι αυτό δυνατόν) τρύπες ασφάλειας όπως η μηδενική επικύρωση κωδικού πρόσβασης




**Εικόνα 5-8 Το μενού Registry Key Permission**

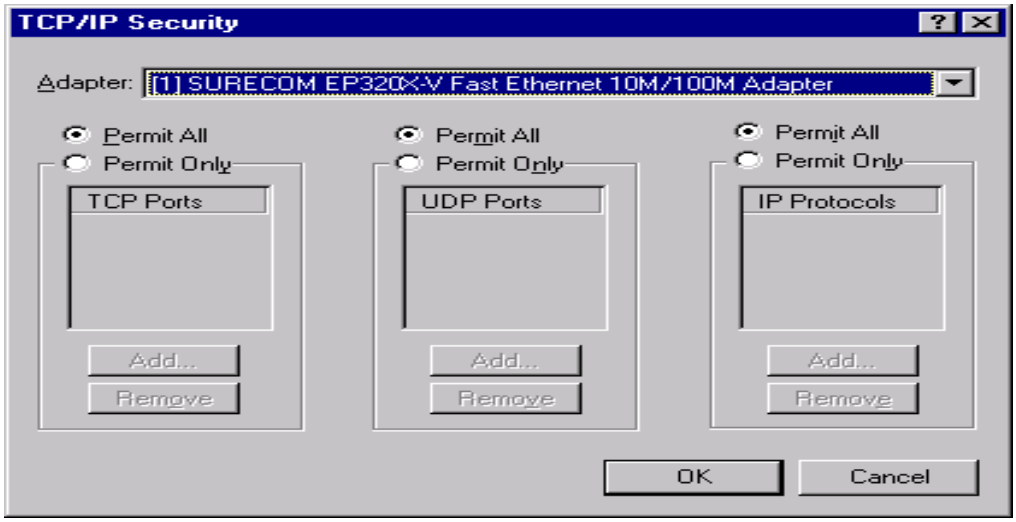
- ΄**Άνοιγμα του ελέγχου "HKEY_LOCAL_MACHINE\Security**" προκειμένου να ανιχνευθεί το κατευθυνόμενο browsing, από τυχών εισβολείς, του μητρώου.

- **Επιβολή "κωδικού πρόσβασης** που προστατεύεται /Password Protected " στο screensaver.

- **Κλείσιμο του αυτόματου sharing** του ADMIN$, C$ , D$, κ.λπ. μέσω της παραμέτρου "AutoShare" στο μητρώο. Αυτή η παράμετρος βρίσκεται στό "HKEY_LOCAL_MACHINE\ System\ CurrentControlSet \ Services\ LanmanServer \Parameters", και είναι "AutoShareServer" για

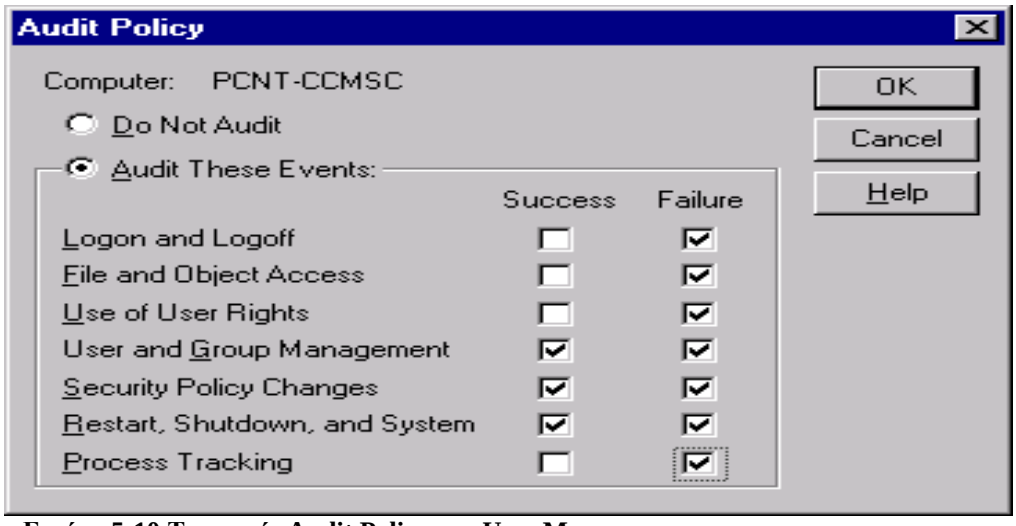
τον κεντρικό υπολογιστή/server WinNT ή "AutoShareWks" για τον τερματικό σταθμό WinNT. Αυτό είναι ένα DWORD, με τιμη "1" για επιτρεπόμενο (προεπιλογή), ή μια τιμή "0" για μη επιτρεπόμενο. Θα πρέπει να προσθέσει την τιμή ο ίδιος ο χρήστης επειδή δεν υπάρχει ήδη στο μητρώο.

- **Αφαίρεση όλων των περιττών υπηρεσιών**
- Αφαίρεση όλων των περιττών δικτυακών συνδέσεων και βασισμένο στην IP φιλτράρισμα πακέτων




**Εικόνα 5-9 Το μενού TCP/IP Security για τις δικτυακές ρυθμίσεις**

- **Χρησιμοποίηση λογισμικού άλλων εταιρειών** για ανάλυση του συστήματος για τρύπες ασφαλείας αλλά και ρύθμιση των επιλογών ελέγχου μέσα από τον User Manager




**Εικόνα 5-10 Το μενού Audit Policy του User Manager**

## 5.2. FIREWALLS

### 5.2.1. Τι είναι firewall και πότε χρειάζεται;

Ένα firewall μπορεί να είναι οποιαδήποτε συσκευή που χρησιμοποιείται ως ένας μηχανισμός ελέγχου της πρόσβασης σε επίπεδο δικτύου, για ένα συγκεκριμένο δίκτυο ή ομάδα δικτύων. Ένα firewall είναι ένα σύστημα ή μία ομάδα συστημάτων τα οποία επιβάλουν μία πολιτική ελέγχου πρόσβασης στην κυκλοφορία του δικτύου καθώς διέρχεται από συγκεκριμένα σημεία πρόσβασης.

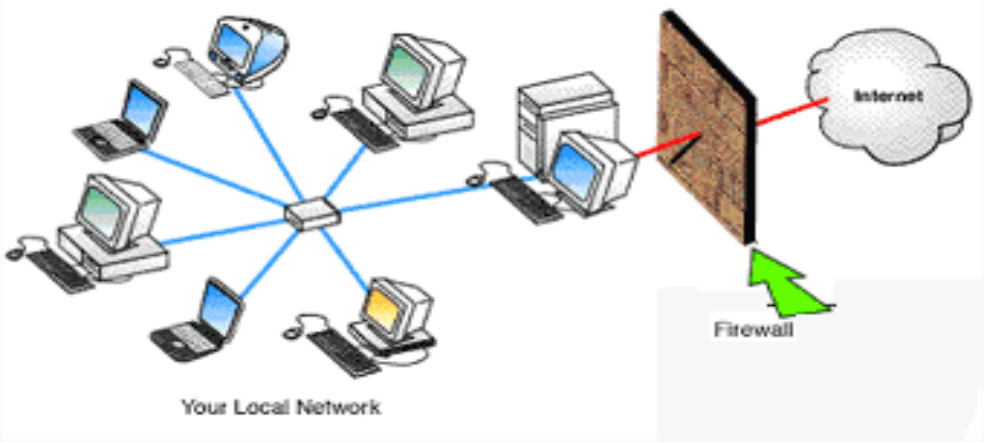
Οι ίδιες οι συσκευές firewalls είναι συνήθως αυτόνομοι υπολογιστές, routers ή «μέσα» firewall. Τα μέσα firewall είναι συνήθως εξειδικευμένες συσκευές υλικού, οι οποίες συχνά εκτελούν ένα προσαρμοσμένο ή ειδικό Λ.Σ.

Τα firewalls είναι σχεδιασμένα να λειτουργούν ως σημεία ελέγχου προς και από το δίκτυο και σκοπός τους είναι να ελέγχουν την ροή της κυκλοφορίας. Πρέπει να ελέγχει το firewall την κυκλοφορία λαμβάνοντας ταυτόχρονα υπόψη ότι τα πακέτα δεδομένων που βλέπει μπορεί να μην είναι αυτό που δείχνουν με την πρώτη ματιά.

Ένα firewall πρέπει να υποθέτει ότι μπορεί να υπάρχουν συστήματα τα οποία θα προσπαθήσουν να το ξεγελάσουν για να υποκλέψουν τις πληροφορίες που διέρχονται από αυτό.

Ένα firewall πρέπει να υποψιάζεται πάντα ότι οι κανόνες επικοινωνίας του δικτύου δεν τηρούνται πάντα. Αυτό κάνει την σχεδίασή τους δύσκολη

Παραδοσιακά τα firewalls χρησιμοποιούνται για τον έλεγχο της πρόσβασης μεταξύ του εσωτερικού δικτύου ενός οργανισμού και του internet, αλλά καθώς τα όρια των εσωτερικών δικτύων γίνονται ολοένα και πιο δυσδιάκριτα, τα firewalls έχουν αρχίσει πλέον να θεωρούνται σαν μία βασική λειτουργία η οποία προστίθεται σε κάθε υπολογιστή που συνδέεται σε δίκτυα.




**Εικόνα 5-11 Η λειτουργία του firewall μεταξύ Η/Υ& internet**

### 5.2.2. *Τεχνολογίες firewall*.

Τα περισσότερα firewall χρησιμοποιούν έναν συνδυασμό λειτουργιών για να την προστασία των δικτύων από την εχθρική κυκλοφορία. Οι πιο γνωστές τεχνολογίες είναι:

- Στατικό φιλτράρισμα πακέτων.
- Δυναμικό φιλτράρισμα πακέτων.
- Φιλτράρισμα βάση κατάστασης.
- Διακομιστές μεσολάβησης (proxy)

### *5.2.3. Στατικό φιλτράρισμα πακέτων*

Το στατικό φιλτράρισμα πακέτων ελέγχει την κυκλοφορία του δικτύου χρησιμοποιώντας τις πληροφορίες που είναι αποθηκευμένες στις κεφαλίδες των πακέτων.

Όταν τα πακέτα φτάνουν στη συσκευή φιλτραρίσματος οι παράμετροι που περιέχονται στις κεφαλίδες των πακέτων συγκρίνονται με την πολιτική ελέγχου πρόσβασης δηλαδή την λίστα ελέγχου πρόσβασης ACL(Access control list).

Μόλις γίνει η σύγκριση η συσκευή φιλτραρίσματος επιτρέπει ή απαγορεύει την κυκλοφορία.

Ένα στατικό φίλτρο πακέτων για τον έλεγχο της ροής της κυκλοφορίας μπορεί να χρησιμοποιεί διάφορες μεταβλητές όπως:

- Διεύθυνση προορισμού
- Διεύθυνση προέλευσης
- Θύρα υπηρεσίας στον προορισμό
- Θύρα υπηρεσίας στην προέλευση
- Πρωτόκολλο

Οι συσκευές που χρησιμοποιούνται για στατικό φιλτράρισμα πακέτων δεν είναι έξυπνες, παρέχουν ελάχιστη προστασία έναντι προχωρημένων μορφών επιθέσεων. Εξετάζουν το ελάχιστο δυνατό ποσό πληροφοριών για να εξακριβώσουν ποια είδη κυκλοφορίας θα επιτρέπουν και ποια θα μπλοκάρουν. Πολλοί routers έχουν τη δυνατότητα στατικού φιλτραρίσματος πακέτων.

### *5.2.4. Δυναμικό φιλτράρισμα πακέτων*

Το δυναμικό φιλτράρισμα προάγει το στατικό φιλτράρισμα πακέτων σε άλλο επίπεδο, διατηρώντας έναν πίνακα συνδέσεων για την παρακολούθηση της κατάστασης μιας συνόδου επικοινωνίας. Δεν βασίζεται μόνο στις τιμές των σημάνσεων. Αυτή είναι μία ισχυρή λειτουργία, η οποία μπορεί να χρησιμοποιηθεί για τον καλύτερο έλεγχο ροής της κυκλοφορίας.

Ας υποθέσουμε ότι ένας εισβολέας στέλνει ένα πακέτο δεδομένων στο σύστημα με περιεχόμενο ικανό και ειδικά σχεδιασμένο για την κατάρρευση του. Ο εισβολέας έχει κάνει αυτό το πακέτο να φαίνεται σαν απάντηση σε προηγούμενη αίτηση για δεδομένα. Ένα απλό φίλτρο πακέτων θα ανέλυε το συγκεκριμένο πακέτο, θα έβλεπε ότι το bit ACK έχει τιμή 1και θα πίστευε ότι είναι απάντηση προς μία αίτηση για δεδομένα. Έτσι θα περνούσε η πληροφορία στο εσωτερικό σύστημα.

Ένα δυναμικό φίλτρο πακέτων δεν ξεγελιέται. Μόλις λαμβάνει μία πληροφορία συμβουλεύεται τον πίνακα συνδέσεων του. Εξετάζοντας τον πίνακα, το δυναμικό φίλτρο πακέτων αντιλαμβάνεται ότι το εσωτερικό σύστημα δεν συνδέθηκε ποτέ με το αυτό το εξωτερικό σύστημα οπότε δεν έκανε ποτέ αίτηση για δεδομένα. Επομένως εφόσον η πληροφορία δεν ζητήθηκε το δυναμικό φίλτρο πακέτων θα απορρίψει το πακέτο.

### *5.2.5. Φιλτράρισμα βασιζόμενο σε πληροφορίες κατάστασης*

Το φιλτράρισμα πακέτων με έλεγχο κατάστασης βασίζεται στην ιδέα του φιλτραρίσματος πακέτων και προχωρεί μερικά βήματα πιο πέρα. Τα firewalls που δομούνται με αυτό το μοντέλο παρακολουθούν συνεδρίες και συνδέσεις σε εσωτερικούς πίνακες κατάστασης και έτσι μπορούν να αντιδράσουν ανάλογα. Για αυτό τα προϊόντα φιλτραρίσματος πακέτων με έλεγχο κατάστασης είναι πιο ευέλικτα από τα απλά προϊόντα φιλτραρίσματος πακέτων.

Το μεγαλύτερο πλεονέκτημα του βασιζόμενου σε πληροφορίες κατάστασης φιλτραρίσματος έναντι του απλού φιλτραρίσματος πακέτων είναι η δυνατότητα που έχει να διατηρεί πληροφορίες για τη κατάσταση εφαρμογών και όχι μόνο για την κατάσταση της σύνδεσης. Οι πληροφορίες για την κατάσταση εφαρμογών επιτρέπει σε έναν ήδη πιστοποιημένο χρήστη να δημιουργεί συνδέσεις χωρίς να απαιτείται μία καινούρια πιστοποίηση, σε αντίθεση με τις πληροφορίες της κατάστασης σύνδεσης, οι οποίες διατηρούν την πιστοποίηση του χρήστη μόνο κατά τη διάρκεια μιας συνόδου επικοινωνίας.

Πρωτοπόρος στη τεχνική «stateful Multilevel Inspection» είναι η checkpoint που κάνει το φιλτράρισμα πακέτων με έλεγχο κατάστασης με ένα βήμα. Δίνει τη δυνατότητα οι διαχειριστές να δομούν κανόνες για τα firewalls, για να εξετάζουν το πραγματικά «ωφέλιμο φορτίο» δεδομένων και όχι μόνο τις διευθύνσεις και τις θύρες.

### *5.2.6. Τύποι firewall*

Τα firewalls μπορούν να χωριστούν σε τέσσερις κατηγορίες :

- Ενσωματωμένα σε συσκευές
- Υλοποιημένα με λογισμικό
- Υλοποιημένα με hardware
- Επιπέδου εφαρμογής

**Firewalls ενσωματωμένα σε Συσκευές**

Όταν οι λειτουργίες firewall περιέχονται σε ένα router ή σε ένα switch, το firewall ονομάζεται ενσωμετωμένο. Τα ενσωματωμένα firewalls εκτελούν συνήθως έλεγχο των πακέτων στο επίπεδο του IP χωρίς να εξετάζουν την κατάσταση της σύνδεσης, πράγμα το οποίο έχει σαν αποτέλεσμα μεγαλύτερη απόδοση αλλά αυξημένη ευπάθεια σε εχθρικό κώδικα

**Firewalls Υλοποιημένα με Λογισμικό**

Τα υλοποιημένα με λογισμικό firewalls χωρίζονται σε δύο τύπους: για μεγάλες επιχειρήσεις και οργανισμούς, τα οποία απευθύνονται σε μεγάλα δίκτυα, και για μικρά γραφεία και οικιακές εφαρμογές. Παρέχουν συνήθως όλη την γκάμα των λειτουργιών firewall και εγκαθίστανται σε συστήματα επιπέδου server με αντίστοιχο λειτουργικό σύστημα (Windows 2000)

**Firewalls Υλοποιημένα με Hardware**

Τα firewalls αυτής της κατηγορίας σχεδιάζονται σαν ολοκληρωμένα συστήματα “με το κλειδί στο χέρι”. Αυτό σημαίνει ότι δεν απαιτούν εκτεταμένες και πολύπλοκες εργασίες εγκατάστασης ή διαμόρφωσης για να ξεκινήσουν να παρέχουν υπηρεσίες firewall. Τα firewalls που είναι υλοποιημένα με hardware, όμοια με τα υλοποιημένα με λογισμικό firewalls, μπορεί να στοχεύουν είτε σε μεγάλους οργανισμούς, είτε σε μικρές επιχειρήσεις.

**Firewalls Επιπέδου Εφαρμογής**

Τα firewalls επιπέδου εφαρμογής αποτελούν συνήθως πρόσθετα συστατικά υπαρχόντων firewalls υλοποιημένων με hardware ή λογισμικό. Ο βασικός τους στόχος είναι να παρέχουν προηγμένο φιλτράρισμα περιεχομένου για τα δεδομένα που διακινούνται στο επίπεδο εφαρμογής. Καθώς οι δυνατότητες των firewalls αυξάνονται και το φιλτράρισμα επικεντρώνεται όλο και περισσότερο στα δεδομένα του επιπέδου εφαρμογής, αυτά τα firewalls γίνονται όλο και πιο εξειδικευμένα.

## *5.3. Διακομιστές μεσολάβησης (proxy-servers)*

### *5.3.1. Τι είναι ένας proxy server;*

**Proxy** (=πληρεξούσιος) **server** λέγεται ένας server που παρεμβάλλεται μεταξύ του υπολογιστή και της διεύθυνσης του διαδικτύου που θέλει να πάει ο χρήστης (web σελίδα η ftp server) δρώντας σαν ενδιάμεσος. Κάθε αίτημα για σύνδεση που στέλνει ο υπολογιστής πηγαίνει πρώτα στον proxy server ο οποίος και το προωθεί στην τελική διεύθυνση εμφανιζόμενος αυτός σαν αποστολέας αντί για το χρήστη. Στη συνέχεια τα δεδομένα που ζητούνται φτάνουν στον proxy server και αυτός τα προωθεί στον υπολογιστή του χρήστη .
Οι διάφοροι τύποι proxy είναι:

- **HTTP/HTTPS** server με πρόσβαση στα ports 80, 8080 κτλ
- **Proxy** Server με πρόσβαση στα ports 80, 8080, 3128 κτλ
- **FTP** servers με πρόσβαση στο port 21
- **SMTP** servers με πρόσβαση στο 25
- **NNTP** servers με πρόσβαση στο 119
- **PopD** servers με πρόσβαση στο 110
- **TelNet/Wingate** servers με πρόσβαση στο port 23
- **Socks** servers με πρόσβαση στο port 1080

Τα νούμερα των βασικών ports είναι σημαντικό να είναι γνωστά στο χρήστη έτσι ώστε όταν κάνει ένα port scanning] σε ένα server να μπορεί να δει ποια είναι ανοιχτά για το σκοπό που το θέλει.

### *5.3.2. Τι προσφέρει ένας proxy server;*

Συνήθως ένας proxy server χρησιμοποιείται για να **αυξήσει την ταχύτητα της σύνδεσης**. Ένας proxy server διατηρεί αντίγραφα των σελίδων που επισκέπτεται σε μία βάση δεδομένων που λέγεται **"cache"**. Το cache κάθε proxy server είναι συνήθως τεράστιο σε μέγεθος και περιλαμβάνει τα αρχεία που έχουν ζητήσει εκατοντάδες, η και χιλιάδες χρήστες του διαδικτύου. Αυτό έχει σαν αποτέλεσμα τα δεδομένα που ζητάει ο χρήστης να βρίσκονται, πολλές φορές, ήδη στο cache δίνοντας τη δυνατότητα στον proxy να τα στείλει αμέσως (χωρίς να απαιτηθεί σύνδεση του με την πηγή των δεδομένων εκ νέου). Συχνά, η αύξηση της ταχύτητας είναι εντυπωσιακή. Μερικές φορές χρειάζεται να γίνει **RELOAD** η **REFRESH** στη web σελίδα για να φανεί μια πρόσφατη έκδοση μια και το αντίγραφο στο cache του proxy server μπορεί να είναι παλαιότερο.

Πολλές φορές, οι ιδιοκτήτες συγκεκριμένων τόπων του διαδικτυου θέτουν **γεωγραφικούς περιορισμούς** στη σύνδεση. Για παράδειγμα, ο server μιας ελληνικής web σελίδας μπορεί να είναι προγραμματισμένος να δέχεται συνδέσεις μόνο από το domain**.gr**. Σε αυτή την περίπτωση, βρισκόμενος σε κάποια άλλη χώρα, μπορεί ο χρήστης να χρησιμοποιήσει ένα ελληνικό proxy server και να συνδεθεί παρουσιαζόμενος σαν να είναι από την Ελλάδα.

Ακόμα υπάρχουν χώρες όπου **η κυβέρνηση λογοκρίνει** τους διαδικτυακούς τόπους στους οποίους οι πολίτες της χώρας μπορούν να συνδεθούν. Συνδεόμενοι με ένα proxy server μπορούν να ξεγελάσουν τους λογοκριτές και να αποκτήσουν πρόσβαση σε "απαγορευμένους τόπους" εμφανιζόμενοι ότι συνδέονται με τη διεύθυνση του proxy server και όχι την πραγματική τους.

Τέλος, χρησιμοποιώντας ορισμένους proxy servers μπορεί να **προστατευτεί η ανωνυμία** του χρήστη.

### *5.3.3. Τι είναι ο ανώνυμος proxy server;*

Κάθε web σελίδα, σε όλο τον κόσμο, μπορεί να καταγράψει τις κινήσεις κάποιου χρήστη και να παρακολουθήσει τα ενδιαφέροντα του χρησιμοποιώντας την διεύθυνσή IP του, που είναι μοναδική. Ανάλογα με την πολιτική του κάθε διαδικτυακού τόπου, ενδέχεται ο χρήστης να μη μπορέσει να έχει πρόσβαση σε αυτό που θέλει. Ακόμα, τα στοιχεία της επίσκεψης του καταγράφονται και μπορεί να χρησιμοποιηθούν αργότερα.

Είναι ευρέως γνωστό ότι διάφορες κυβερνήσεις και οργανισμοί στήνουν **web σελίδες δολώματα** που αναφέρονται σε αμφισβητούμενα θέματα με στόχο την παρακολούθηση των ενδιαφερομένων. Επιπρόσθετα αυτές οι πληροφορίες σε συνδυασμό με την διεύθυνση e-mail του, μπορούν να χρησιμοποιηθούν για να τον βομβαρδίσουν με κατευθυνόμενη διαφήμιση.
Με τη χρήση και μόνο της διεύθυνσης IP και τις πληροφορίες γύρω από το λειτουργικό σύστημα του υπολογιστή, μια web σελίδα μπορεί αυτόματα να εκμεταλλευτεί κάποια κενά ασφαλείας (security holes) του συστήματος με τη βοήθεια απλών προγραμμάτων που κυκλοφορούν έτοιμα και δωρεάν στο διαδίκτυο. Τα πιο απλά από αυτά απλά θα παγώσουν τον υπολογιστή. Όμως υπάρχουν άλλα ισχυρότερα που μπορούν να αποκτήσουν πρόσβαση στα στοιχεία που είναι αποθηκευμένα είτε στο σκληρό δίσκο είτε στη μνήμη RAM του υπολογιστή. Ένας ανώνυμος proxy server προστατεύει αποκρύπτοντας την διεύθυνση IP (σημ. δεν την στέλνει μέσω HTTP), αποκλείοντας έτσι την πρόσβαση κάποιου τρίτου στον υπολογιστή. Συνήθως όμως, οι proxy servers ενημερώνουν με άλλο, παράλληλο τρόπο τον server-στόχο σχετικά με την διεύθυνση IP.
ΜΟΝΟ οι πραγματικά ανώνυμοι proxy servers δεν στέλνουν μέσω HTTP την διεύθυνση IP του χρηστη και αποκρύπτουν αποτελεσματικά τις πληροφορίες γύρω από αυτόν και τις συνήθειές του. Κάποιοι από αυτούς έχουν την δυνατότητα να αποκρύπτουν ακόμα και το γεγονός ότι χρησιμοποιείται ένα proxy server! Τέλος, οι ανώνυμοι proxy servers μπορούν να χρησιμοποιηθούν για διάφορες υπηρεσίες του διαδικτύου όπως Web-Mail (MSN Hot Mail, Yahoo mail), Web-chatrooms, αρχεία FTP, κτλ.

### *5.3.4. Ο proxy server είναι αληθινά ανώνυμος;*

Υπάρχουν χιλιάδες "δημόσιοι" (=public) proxy servers σε πολλές χώρες που επιτρέπουν τη σύνδεση δωρεάν, όμως η πλειονότητα δεν είναι ανώνυμοι.
Στις διάφορες λίστες υπάρχουν πολλοί που χαρακτηρίζονται σαν ανώνυμοι, μια και δεν ανακοινώνουν την διεύθυνση IP του χρήστη με τον συνήθη τρόπο (HTML), **αλλά στην πραγματικότητα δεν είναι**, μια και κοινοποιούν τα στοιχεία με άλλο τρόπο. Επιπλέον έχει παρατηρηθεί ότι ακόμα και ανώνυμοι proxy servers, κάποιες φορές κοινοποιούν τα στοιχεία. Ποτέ δεν θα πρέπει να θεωρείται ένα proxy server ανώνυμος χωρίς να τον τσεκάρεται πρώτα από τον ίδιο τον χρήστη!
Ο απλούστερος τρόπος για να ελεγχθεί ο βαθμός ανωνυμίας ένος proxy server είναι η σύνδεση μέσω **telnet** αλλιώς υπάρχει και μια δεύτερη λύση.
Γίνεται η υπόθεση ότι το proxy που είναι για να τεστάρισμα είναι το **proxyx.com** και το port **8080**:

telnet proxyx.com 8080 η

telnet proxyx.com:8080 (ανάλογα με το σύστημα)

GET http://smartsearch.hypermart.net/cgi-bin/chkip/senv2.cgi

ENTER (2 φορές)

1. Αν η απάντηση είναι **connection refused** τότε ο proxy server δεν είναι διαθέσιμος-ανοικτός. Σε αντίθετη περίπτωση θα φανούν όλα τα

στοιχεία που στέλνει ο browser προς τα έξω. Βέβαια αντί του **http://smartsearch.hypermart.net/cgi-bin/chkip/senv2.cgi** μπορεί να χρησιμοποιηθεί οποιαδήποτε άλλη διεύθυνση.

2. Αν δεν θέλει ο χρήστης να ασχοληθεί με το **telnet** τότε μπορεί να χρησιμοποιήσει απ΄ ευθείας τα διάφορα cgi η java scripts που είναι διαθέσιμα στο διαδίκτυο για αυτή τη δουλειά.

Και στις δύο περιπτώσεις πρέπει να εξεταστεί με προσοχή το αποτέλεσμα. Πρέπει να γίνει έρευνα αν η διεύθυνση IP του χρήστη παρουσιάζεται κάπου στα αποτελέσματα. Αν την δει, τότε ο proxy server που τσεκάρει **δεν είναι ανώνυμος** (παράδειγμα 2).
Ακολουθούν τρία παραδείγματα που θα βοηθήσουν να γίνει κατανοητό το θέμα.

HTTP_USER_AGENT=Opera/6.05 (Windows 2000; U)[en]

PATH=/usr/local/bin:/usr/bin:/bin

PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi

REMOTE_ADDR=200.203.2x.xxx

REMOTE_HOST=200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br

REMOTE_PORT=65080

#### 5.3.4.1. Παράδειγμα 1 **(απ΄ ευθείας σύνδεση)**

Σε αυτό το παράδειγμα η σύνδεση έγινε χωρίς την μεσολάβηση κάποιου proxy server ούτε άλλου φίλτρου. Βλέπουμε καθαρά όχι μόνο **τον browser** που χρησιμοποιήσαμε (Opera), **το λειτουργικό σύστημα** (Windows 2000) αλλά και **την διεύθυνση IP** (200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br)

HTTP_CLIENT_IP=200.203.2x.xxx

HTTP_CONNECTION=keep-alive

HTTP_HOST=smartsearch.hypermart.net

HTTP_PRAGMA=no-cache

HTTP_USER_AGENT=Opera/6.05 (Windows 2000; U) [en]

HTTP_X_FORWARDED_FOR=148.233.111.232

PATH=/usr/local/bin:/usr/bin:/bin

PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi

REMOTE_ADDR=200.64.191.50

REMOTE_HOST=dup-200-64-191-50.prodigy.net.mx

REMOTE_PORT=50323

#### 5.3.4.2. Παράδειγμα 2 **(transparent (=διαφανής) proxy)**

Εδώ η σύνδεση έγινε μέσω ενός διαφανούς proxy server. Βλέπουμε πάλι **τον browser** (Opera) και **το λειτουργικό σύστημα** (Windows 2000), αφού δεν

χρησιμοποιήσαμε κάποιο φίλτρο. Αυτή τη φορά όμως **η διεύθυνση IP** εμφανίζεται σαν **HTTP_CLIENT_IP** (που δείχνει ότι η εντολή HTTP προήλθε από τη διεύθυνση 200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br) μέσω των proxy servers 148.233.111.232 και dup-200-64-191-50.prodigy.net.mx (με αυτή ακριβώς τη σειρά).

HTTP_USER_AGENT=bobb 4.78

PATH=/usr/local/bin:/usr/bin:/bin

PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi

REMOTE_ADDR=200.41.230.99

REMOTE_HOST=server.hcdiputados-ba.gov.ar

REMOTE_PORT=3769

5.3.4.3. Παράδειγμα 3 **(ανώνυμος proxy+proxomitron 4.4)**

Εδώ η σύνδεση έγινε μέσω ενός ανώνυμου proxy server. Το μόνο που βλέπουμε είναι η διεύθυνση του proxy server **server.hcdiputados-ba.gov.ar** χωρίς άλλα ίχνη προέλευσης. Αυτή τη φορά ο **browser** παρουσιάζεται σαν **bobb 4.78** ενώ το **το λειτουργικό σύστημα** είναι άφαντο. Για το φιλτράρισμα έχουμε χρησιμοποιήσει το Proxomitron

## *5.4. IDS*

### *5.4.1. Τι είναι ένα "σύστημα ανίχνευσης παρείσφρησης (intrusion detection system IDS)";*

Μια **παρείσφρηση** γίνεται από κάποιον που προσπαθεί να διεισδύσει και να κάνει χρήση(με κακό σκοπό τις περισσότερες φορές εάν όχι πάντα) των συστημάτων των ηλεκτρονικών υπολογιστών προς όφελος του. Αυτό μπορεί να είναι πολύ οδυνηρό διότι μπορεί να κλαπούν εμπιστευτικά στοιχεία, με ότι συνέπειες μπορεί να έχει αυτό για το νόμιμο χρήστη. Ένα **IDS** χρησιμοποιείται για να ανιχνεύει τέτοιες παρεισφρήσεις. Γενικά υπάρχουν 2 τύποι συστημάτων ανίχνευσης παρείσφρησης:

**Συστήματα ανίχνευσης παρείσφρησης δικτύων (NIDS/ Network intrusion detection systems)** παρακολουθεί την κίνηση των πακέτων στο δίκτυο και προσπαθεί να ανακαλύψει έναν εισβολέα με το να συγκρίνει και να ταιριάζει το σχέδιο επίθεσης ψάχνοντας σε μια βάση δεδομένων πού περιέχει τα γνωστά σχέδια επίθεσης. Ένα χαρακτηριστικό παράδειγμα είναι το ψάξιμο για ένα μεγάλο αριθμό αιτημάτων σύνδεσης TCP (TCP connection requests) σε πολλές διαφορετικές πύλες (ports) σε έναν υπολογιστή στόχο, ανακαλύπτοντας κατά συνέπεια εάν κάποιος προσπαθεί να κάνει μια ανίχνευση θυρών TCP. Ένα σύστημα ανίχνευσης παρείσφρησης δικτύων οσμίζεται (sniffs) την κυκλοφορία του δικτύου.

**Βασισμένο στον οικοδεσπότη σύστημα ανίχνευσης παρείσφρυσης (Host based intrusion detection system-HIDS)** - ένα βασισμένο στον οικοδεσπότη σύστημα ανίχνευσης παρείσφρησης δεν ελέγχει την κυκλοφορία

του δικτύου, αλλά ελέγχει τι συμβαίνει στους πραγματικούς υπολογιστές-στόχους. Το πετυχαίνει αυτό με τον έλεγχο των event logs ασφαλείας ή τον έλεγχο για τις αλλαγές στο σύστημα, παραδείγματος χάριν αλλαγές στα κρίσιμα αρχεία συστήματος ή στο μητρώο των συστημάτων. Τα βασισμένα στον οικοδεσπότη συστήματα ανίχνευσης παρείσφρησης μπορούν να χωριστούν σε δύο κατηγορίες:

**Ελεγκτές ακεραιότητας συστημάτων (System integrity checkers**)- Ελέγχει τα αρχεία συστήματος καθώς και το μητρώο του συστήματος για τυχών αλλαγές που γίνονται από τους εισβολείς. Υπάρχουν διάφοροι ελεγκτές ακεραιότητας αρχείων / συστημάτων, όπως ο "Tripwire" ή "ο ελεγκτής ακεραιότητας αρχείων LANguard".

**Όργανα ελέγχου αρχείων Log** (**Log file monitors)**

Ελέγχει αρχεία log που παράγονται από τα συστήματα των ηλεκτρονικών υπολογιστών. Τα συστήματα Windows NT/2000 & XP παράγουν /δημιουργούν τα γεγονότα ασφάλειας για τα κρίσιμα ζητήματα ασφάλειας που συμβαίνουν στον υπολογιστή (παραδείγματος χάριν ένας χρήστης αποκτά τα προνόμια επιπέδων root/administrator ) Με την ανάκτηση & την ανάλυση αυτών των γεγονότων ασφάλειας μπορούν να ανιχνευθούν οι εισβολείς.

### *5.4.2. Γιατί χρειάζομαι IDS εάν έχω ήδη firewall*

Μια κοινή παρανόηση είναι ότι τα firewalls αναγνωρίζουν τις επιθέσεις και τις εμποδίζουν. Αυτό δεν ισχύει. Τα firewalls είναι απλά μια συσκευή που αρχικά τα αποκλείει όλα, και έπειτα επιτρέπει μόνο μερικά καλά επιλεγμένα στοιχεία. Σε έναν τέλειο κόσμο, τα συστήματα " θα κλειδώνονταν " και θα ασφαλιζόταν και τα firewalls θα ήταν αχρείαστα. Ο λόγος που έχουμε τα firewalls είναι ακριβώς επειδή οι τρύπες ασφάλειας αφήνονται ανοικτές τυχαία. Κατά συνέπεια, κατά την εγκατάσταση ενός firewall, το πρώτο πράγμα που κάνει αυτό είναι να σταματά ΟΛΗ την επικοινωνία. Ο διαχειριστής του firewall έπειτα προσεκτικά προσθέτει "τους κανόνες" που επιτρέπουν στους συγκεκριμένους τύπους κυκλοφοριών να περάσουν από τα firewall. Παραδείγματος χάριν, ένα χαρακτηριστικό firewall μίας εταιρίας, που επιτρέπει την πρόσβαση στο διαδίκτυο θα σταματούσε όλη την κυκλοφορία πακέτων δεδομένων UDP και ICMP, όπως επίσης και τις εισερχόμενες συνδέσεις TCP, αλλά θα επέτρεπε τις εξερχόμενες συνδέσεις TCP. Αυτό θα σταματούσε όλες τις εισερχόμενες συνδέσεις από τους χάκερ του διαδικτύου, αλλά ακόμα θα επέτρεπε στους εσωτερικούς χρήστες να συνδεθούν στην εξερχόμενη κατεύθυνση.

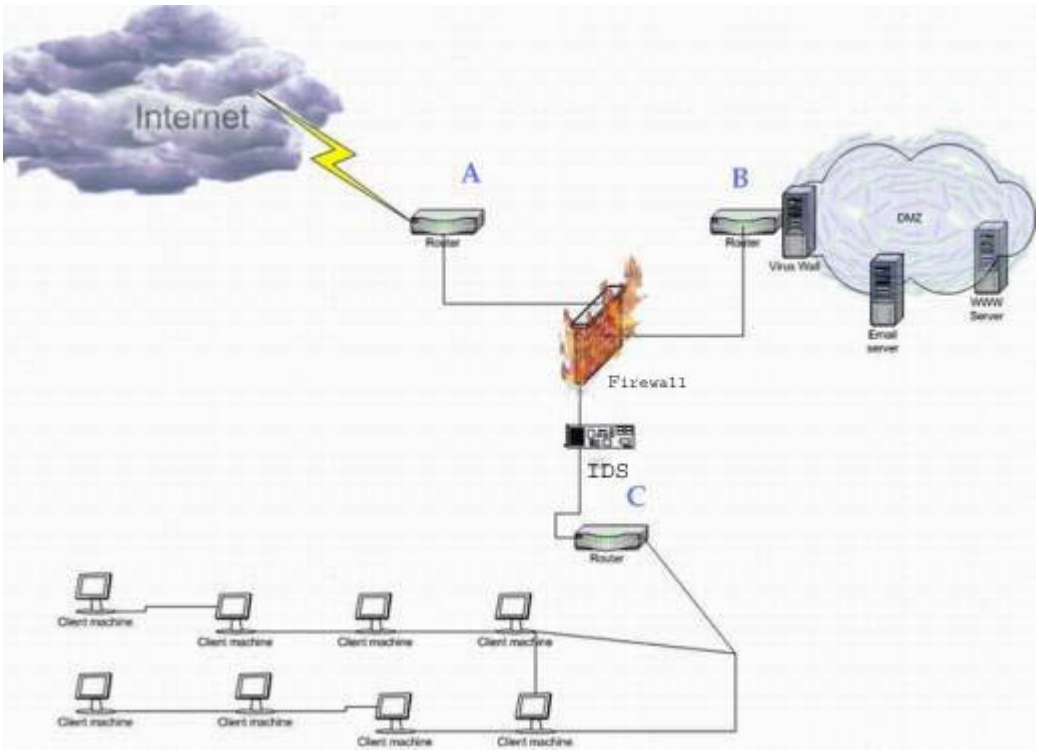
Ένα firewall είναι απλά ένας φράκτης γύρω από το δίκτυο, με μερικές καλά επιλεγμένες πύλες. Ένας φράκτης δεν έχει την ικανότητα της ανίχνευσης κάποιου που προσπαθεί να μπει μέσα, ούτε ξέρει εάν κάποιος που έρχεται μέσω της πύλης έχει την άδεια να μπει μέσα. Περιορίζει απλά την πρόσβαση στα οριζόμενα σημεία.

Εν περιλήψει, ένα firewall δεν είναι το δυναμικό αμυντικό σύστημα πού οι χρήστες φαντάζονται. Αντίθετα, ένα IDS είναι ένα δυναμικό αμυντικό σύστημα. Ένα IDS αναγνωρίζει επιθέσεις ενάντια στο δίκτυο πού τα firewalls δεν μπορούν να δουν. Ένα άλλο πρόβλημα με τα firewalls είναι ότι λειτουργεί μόνο στα όρια του δικτύου . Κατά προσέγγιση 80% όλων των οικονομικών απωλειών λόγω hacking έρχονται από μέσα από το δίκτυο. Τα firewalls στην περίμετρο του δικτύου δεν βλέπουν τι συμβαίνει στο εσωτερικό. Βλέπουν μόνο εκείνη την κυκλοφορία που γίνεται μεταξύ του εσωτερικού δικτύου και του διαδικτύου. Μερικοί λόγοι για να προσθέσει κάποιος IDS στο firewall του είναι:

- Εντοπίζει τις επιθέσεις που τα firewalls νόμιμα επιτρέπουν (όπως οι επιθέσεις ενάντια στους web servers).
- Εντοπίζει προσπάθειες hacking που αποτυγχάνουν.
- Εντοπίζει το εσωτερικό hacking.

Οι χάκερ είναι ικανότεροι από σκεφτόμαστε οπότε όσα περισσότερα συστήματα υπεράσπισης διαθέτουμε , τόσο το καλύτερο. Ακόμα και αυτά δεν θα μας προστατεύσουν από τον καθορισμένο χάκερ . Παρ' όλα αυτά, θα αυξήσουν το βαθμό δυσκολίας παραβίασης του συστήματος.

Στην παρακάτω φωτ. βλέπουμε ένα δίκτυο που διαθέτει firewall και IDS




**Εικόνα 5-12 Ταυτόχρονη χρήση firewall και IDS**

## 5.5. HONEYPOTS

### 5.5.1. Τι είναι τα honeypots

Ενώ δεν ακολουθούν αυστηρά τη λειτουργία των βασισμένων σε sniffer συστημάτων ανίχνευσης παρείσφρησης, τα honeypots επεξεργάζονται τα πρωτόκολλα δικτύων με τους ίδιους σχεδόν τρόπους. Ένα honeypot είναι ένα σύστημα που έχει σκοπό να μοιάσει με κάτι που ένας εισβολέας μπορεί να παραβιάσει π.χ να μιμηθεί γνωστές τρύπες στο λογισμικό προκειμένου να παραπλανηθούν οι χάκερ και να παγιδευτούν.

Τα παραδείγματα μπορούν να είναι τα εξής:

- Εγκατάσταση ενός υπολογιστή στο δίκτυο χωρίς ιδιαίτερο σκοπό εκτός από το να καταγράφει όλη την αποπειραθείσα πρόσβαση.
- Η εγκατάσταση έναν παλαιότερου λειτουργικού συστήματος χωρίς τα patches σε έναν υπολογιστή. Παραδείγματος χάριν, η εγκατάσταση default των WinNT 4 με IIS 4 Το σύστημα μπορεί να παραβιαστεί με διάφορες τεχνικές. Ένα τυποποιημένο σύστημα ανίχνευσης παρείσφρησης μπορεί έπειτα να χρησιμοποιηθεί για να καταγράψει τις παραβιάσεις που γίνονται ενάντια στον υπολογιστή και τον περαιτέρω εντοπισμό του σκοπού του εισβολέα μόλις το σύστημα εκτεθεί.
- Η εγκατάσταση του ειδικού λογισμικού που είναι σχεδιασμένο για αυτόν το λόγο. Έχει το πλεονέκτημα του να ξεγελά τον εισβολέα δήθεν ότι είναι επιτυχής η παρείσφρηση του χωρίς πραγματικά να του επιτρέπει την πρόσβαση.
- Σε οποιοδήποτε υπάρχον σύστημα μπορεί να υπάρξει honeypot Παραδείγματος χάριν, σε WinNT, είναι δυνατό να μετονομαστεί ο προεπιλεγμένος λογαριασμός "administrator", κατόπιν να δημιουργηθεί ένας πλαστός λογαριασμός αποκαλούμενος "administrator" χωρίς κωδικό πρόσβασης. Τα WinNT επιτρέπουν την εκτενή αναγραφή των δραστηριοτήτων ενός χρήστη, έτσι αυτό το honeypot θα εντοπίζει τους χρήστες που προσπαθούν να κερδίσουν την πρόσβαση administrator και να επομένως να εκμεταλλευτούν αυτή την πρόσβαση.

### 5.5.2. Ποια είναι τα πλεονεκτήματα ενός honeypot;

- Ένας πρόωρος-συναγερμός που θα χτυπήσει μόνο επάνω στην εχθρική δραστηριότητα. Τα συστήματα ανίχνευσης παρείσφρησης δικτύων έχουν πρόβλημα στο να διακρίνουν την εχθρική κυκλοφορία από την κυκλοφορία των νόμιμων χρηστών. Τα απομονωμένα honeypots έχουν πολύ ευκολότερο έργο επειδή είναι συστήματα που δεν πρέπει κανονικά να προσπελαστούν. Αυτό σημαίνει ότι όλη η κυκλοφορία σε ένα σύστημα honeypot είναι ήδη ύποπτη.
- Ένα εχθρικός-προσηλωμένο σύστημα καθορισμού. Τα Honeypots συχνά αυτοπαρουσιάζονται ως εύκολα συστήματα στο να παραβιαστούν .Ένα από τα πιό κοινά πράγματα που κάνουν οι χάκερ είναι η ανίχνευση(scan) στο διαδίκτυο κάνοντας "ελέγχους banner". Το honeypot μπορεί να ρυθμιστεί έτσι ώστε να παρέχει ένα banner που

μοιάζει με ένα σύστημα που μπορεί εύκολα να παραβιαστεί, κατόπιν να εντοπίσει εάν κάποιος κάνει πραγματικά την παραβίαση. Παραδείγματος χάριν, η POP3 υπηρεσία αναφέρει την έκδοση του λογισμικού. Διάφορες εκδόσεις των γνωστών πακέτων έχουν τρύπες υπερχείλισης απομονωτών (buffer-overflow holes). Ένας χάκερ συνδέεται με μια αφύλακτη πύλη και αποσπά τις πληροφορίες έκδοσης από το banner, κατόπιν ανατρέχει την έκδοση σε έναν πίνακα ο οποίος υποδεικνύει σε ποιο script μπορεί να χρησιμοποιηθεί για να εισβάλει στο σύστημα.

### *5.5.3. Ποια είναι τα μειονεκτήματα ενός honeypot;*

- Εάν το σύστημα πράγματι παραβιαστεί αυτό μπορεί να χρησιμοποιηθεί ως σκαλοπάτι στην περαιτέρω έκθεση και διακινδύνευση του δικτύου.
- Μερικοί άνθρωποι θεωρούν ότι αφού τα honeypots δελεάζουν τους χάκερ, τα νόμιμα δικαιώματα να διωχθούν ποινικός οι χάκερ μειώνονται. Αυτό είναι μια παρερμηνεία, επειδή τα honeypots δεν είναι ενεργά θέλγητρα -- δεν διαφημίζονται. Ένας χάκερ μπορεί μόνο να βρει ένα honeypot αρχικά με το τρέξιμο των προγραμμάτων αναζήτησης σε ένα δίκτυο.
- Τα Honeypots προσθέτουν πολυπλοκότητα στο σύστημα. Στην ασφάλεια, η πολυπλοκότητα είναι κακή.

## *5.6. SNIFFERS ~ Πώς μπορούν να προστατευθούν οι χρήστες;*

**Εργαλεία αντί- Sniffing**

Μια τρομακτική πτυχή αυτών των εργαλείων είναι ποιος μπορεί, και, ποιος θα τα χρησιμοποιήσει. Όπως αναφέρθηκε παραπάνω, τα sniffers μπορούν να χρησιμοποιηθούν και για νόμιμους και παράνομους λόγους. Παραδείγματος χάριν, ένας διαχειριστής δικτύων μπορεί να το χρησιμοποιήσει για να ελέγχει τη ροή της κυκλοφορίας στο δίκτυο και να εξασφαλίζει ότι το δίκτυο λειτουργεί αποτελεσματικά. Εντούτοις, τα sniffers μπορούν επίσης να χρησιμοποιηθούν από κακόβουλους χρήστες για να λάβουν πολύτιμες προσωπικές πληροφορίες. Είτε είναι κωδικοί πρόσβασης ή ιδιωτική επικοινωνία, και οι crackers και οι εργαζόμενοι-συνάδελφοι μπορούν να ωφεληθούν από την ανάγνωση των στοιχείων κάποιου χρήστη. Η υπεράσπιση ενάντια στα sniffers, όπως με οποιαδήποτε άλλη απειλή, πρέπει να αρχίσει από την κορυφή και να φτάνει στο χρήστη. Όπως σε οποιοδήποτε δίκτυο, οι διαχειριστές πρέπει να ασφαλίζουν τους ανεξάρτητους υπολογιστές και τους κεντρικούς υπολογιστές. Ένα sniffer είναι ένα από τα πρώτα πράγματα που ένας cracker θα φορτώσει για να δει τι πραγματοποιείται σε και γύρω από την πρόσφατα παραβιασμένο υπολογιστή.

Μια άλλη μέθοδος προστασίας περιλαμβάνει εργαλεία, όπως το antisniff, το οποίο ανιχνεύει τα δίκτυα για να καθορίσει εάν οποιαδήποτε κάρτα δικτύου είναι σε κατάσταση αδιακρισίας. Αυτά τα εργαλεία ανίχνευσης πρέπει να τρέχουν τακτικά, δεδομένου ότι ενεργούν ως συναγερμός.

### *5.6.1. Μεταστρεφόμενα δίκτυα*

Ένα μεταστρεφόμενο δίκτυο είναι επίσης ένας καλός αποτρεπτικός παράγοντας. Στο μη-μεταστρεφόμενο περιβάλλον, τα πακέτα είναι ορατά σε κάθε κόμβο στο δίκτυο, σε ένα μεταστρεφόμενο περιβάλλον, τα πακέτα παραδίδονται μόνο στη διεύθυνση-στόχο. Ενώ είναι ακριβότερα από τα hubs, το κόστος των switches έχει μειωθεί, καθιστώντας τα προσιτά στους περισσότερους προϋπολογισμούς. Αντίθετα από τα hubs, τα switches στέλνουν μόνο πλαίσια (frames) στον οριζόμενο παραλήπτη επομένως μία κάρτα δικτύου σε κατάσταση αδιακρισίας σε ένα μεταστρεφόμενο δίκτυο δεν θα συλλάμβάνει κάθε κομμάτι της τοπικής κυκλοφορίας. Αλλά προγράμματα όπως το dsniff, επιτρέπουν σε έναν επιτιθέμενο να ελέγχει και να παρακολουθεί ένα μεταστρεφόμενο δίκτυο με μια τεχνική γνωστή ως arp-spoofing. Αν και χρησιμοποιεί διαφορετικές μεθόδους, η τεχνική arp-spoofing μπορεί να παρέχει αποτελέσματα παρόμοια με το sniffing. Έτσι γεννάται η ερώτηση. Υπάρχει τίποτα που μπορεί αληθινά να προστατεύσει τα δεδομένα μόλις φθάσουν στο δίκτυο;

### *5.6.2. Κρυπτογράφηση*

Η κρυπτογράφηση είναι η καλύτερη προστασία ενάντια σε οποιαδήποτε μορφή παρεμπόδισης κυκλοφορίας .Είναι λογικό να υποτεθεί ότι σε κάποιο σημείο κατά μήκος μιας πορείας, τα στοιχεία μπορούν πάντα να εκτεθούν. Επομένως, η καλύτερη άμυνα είναι να εξασφαλιστεί ότι η κυκλοφορία είναι ουσιαστικά δυσανάγνωστη σε όλους εκτός του προοριζόμενου δέκτη. Αυτό δεν είναι δύσκολο να πραγματοποιηθεί, δεδομένου ότι πολλοί οργανισμοί έχουν επεκτείνει υπηρεσίες που χρησιμοποιούν τα Στρώματα Ασφαλών Υποδοχών (Secure Socket Layers -SSL), την Ασφάλεια Στρώματος Μεταφοράς (Transport Layer Security -TLS) και άλλες μεθόδους που παρέχουν ασφαλές ανταλλαγές μηνυμάτων, ασφαλή πλοήγηση στο web και πολλά ακόμα. Μόνο τα ωφέλιμα φορτία είναι ανακατεμένα, εξασφαλίζοντας ότι τα πακέτα φθάνουν στους σωστούς προορισμούς. Έτσι ένας επιτιθέμενος μπορεί να δει που κατευθύνθηκε η κυκλοφορία και από πού προήλθε, αλλά όχι τι φέρνει.

```
21:09:04.599289 192.168.1.3.32933 > opensource-01.ee.ethz.ch.https: . [tcp sum ok]
    793:793(0) ack 7011 win 20104        (DF) (ttl 64, id 12206, len 40)
    0x0000   4500 0028 2fae 4000 4006 c059 c0a8 0103   E.(/.@.@..Y....
    0x0010   8184 0799 80a5 01bb 19a2 0520 be10 d77f   ..............
    0x0020   5010 4e88 dfd0 0000                       P.N.....

21:09:04.599289 opensource-01.ee.ethz.ch.https > 192.168.1.3.32933: P [tcp sum ok]
```

```
7011:7135(124) ack 793 win 10052 (DF) (ttl 237, id 65192, len 164)
0x0000   4500 00a4 fea8 4000 ed06 43e2 8184 0799      E.....@...C.....
0x0010   c0a8 0103 01bb 80a5 be10 d77f 19a2 0520      ..............
0x0020   5018 2744 8303 0000 4d3a a587 805e e2bc      P.'D....M:...^..
0x0030   9a2a 8ff3 fe95 46d4 930e b2bc 74f0 a484      .*....F.....t...
0x0040   fcae 33ad 6d1f 0198 6020 aee5 0c26 908e      ..3.m...`....&..
0x0050   a1b5 17b4 84b7 44bc 1b0b 434e bbae a483      ......D...CN....
0x0060   1e23 38d3 520f 687e c5e3 b62e 5225 aa2f      .#8.R.h~....R%./
0x0070   f747 1a71 669c 8fd1 55bd 511c 4988 b78a      .G.qf...U.Q.I...
0x0080   a08d 554e a3fe bb7d 36ca e66b fb8b 0392      ..UN...}6..k....
0x0090   a3f3 4cef 7b04 af5a 7a94 cb4c a1e6 e7fa      ..L.{..Zz..L....
0x00a0   9610 a5ee                                    ....
```

Ας γίνει σύγκριση αυτού του ”οσμισμένου” δείγματος μιας συνόδου web με τον OpenSSL Web server με το παράδειγμα νωρίτερα. Παρατηρούμε ότι οι πληροφορίες επικεφαλίδας παραμένουν αναγνώσιμες, αλλά η ASCII αποκωδικοποίηση του ωφέλιμου φορτίου περιέχει φαινομενικά τυχαίους χαρακτήρες - χάρη στην κρυπτογράφηση. Οι δύο συμμετέχοντες σε αυτήν την ανταλλαγή, εντούτοις, μπορούν και οι δύο να αποκρυπτογραφήσουν και να επεξεργαστούν τα στοιχεία μόλις παραληφθούν. Αυτός ο τύπος προστασίας μπορεί να εφαρμοστεί σε ουσιαστικά οποιαδήποτε διαδικασία δικτύων και πρέπει να υιοθετείται όποτε είναι δυνατόν

## *5.7. PASSWORD*

### *5.7.1. Πώς λειτουργούν οι κωδικοί πρόσβασης*

Η βασική έννοια "του κλειδώματος" ένας λογαριασμού με έναν κωδικό πρόσβασης είναι απλή. Όταν ένας λογαριασμός χρήστη δημιουργείται, ένας κωδικός πρόσβασης ανατίθεται σε αυτόν, συνήθως από το διαχειριστή. Ο χρήστης χρησιμοποιεί αυτόν τον κωδικό πρόσβασης να συνδεθεί για πρώτη φορά. Στο χρήστη (αν και όχι πάντα) δίνεται η δυνατότητα να αλλάξει τον κωδικό πρόσβασης έτσι ώστε μόνο ο αυτός να τον ξέρει. Ανάλογα με τον τύπο του λογαριασμού, αποθηκεύεται σε μια βάση δεδομένων είτε σε τοπικό σκληρό δίσκο είτε σε έναν κεντρικό υπολογιστή (server) . Η βάση δεδομένων περιέχει έναν κατάλογο όλων των λογαριασμών των χρηστών και αντίστοιχων κωδικών πρόσβασής τους. Όταν ένας χρήστης συνδέεται και εισάγει τα πιστοποιητικά, ελέγχονται σε σχέση με αυτήν την βάση δεδομένων. Εάν ο κωδικός πρόσβασης ταιριάζει η πρόσβαση χορηγείται. Γενικά, οι κωδικοί πρόσβασης στη βάση δεδομένων θα κρυπτογραφηθούν για να προστατεύονται, χρησιμοποιώντας μια τεχνική αποκαλούμενη hashing. Είναι η hash αξία(value) σε σχέση με την οποία ελέγχεται ο κωδικός πρόσβασης, έτσι ώστε οι κωδικοί που αποθηκεύονται στη βάση δεδομένων να μην πρέπει ποτέ να αποκρυπτογραφηθούν (επομένως και να εκτίθονται στους πιθανούς χάκερ).

Η πληκτρολόγηση του ονόματος και του προσωπικού κωδικού κάθε φορά που θέλει να έχει πρόσβαση ένας χρήστης σε έναν διαφορετικό πόρο στον υπολογιστή ή το δίκτυο θα ήταν αργή διαδικασία, έτσι η διαδικασία επικύρωσης γίνεται διαφανής στο χρήστη μετά από την αρχική σύνδεση. Αυτό είναι καταλληλότερο, αλλά σημαίνει ότι εάν συνδεθεί κάποιος και αφήσει έπειτα τον υπολογιστή του χωρίς να τον κλειδώσει (παραδείγματος χάριν, με ένα προστατευόμενο από κωδικό screensaver), καθένας που κάθεται σε αυτόν θα είναι σε θέση να έχει πρόσβαση σε οποιουσδήποτε πόρους για τους οποίους ο λογαριασμός του έχει την άδεια, επειδή έχει ξεκλειδώσει ουσιαστικά την πόρτα και την άφησε ανοικτή.

Ακόμα κι αν κάποιος είναι επιμελείς για αυτό, εντούτοις, υπάρχουν πολλοί τρόποι με τους οποίους το σύστημα επικύρωσης κωδικού πρόσβασης (password authentication system) μπορεί να παραβιαστεί

### *5.7.2. Αδυναμίες κωδικών πρόσβασης*

Η μεγάλη αδυναμία των κωδικών πρόσβασης βρίσκεται στη φύση τους. Υπάρχουν αρκετοί διαφορετικοί τρόποι με τους οποίους ένα πρόσωπο μπορεί "να αποδείξει" την ταυτότητά του / της:

- Παρέχοντας κάτι πού ξέρει ( κωδικό πρόσβασης)
- Παρέχοντας κάτι πού έχει στην κατοχή του (όπως μια κάρτα)
- Παρέχοντας κάτι φυσικό (ένα φυσιολογικό χαρακτηριστικό όπως ένα δακτυλικό αποτύπωμα)
- Παρέχοντας κάτι που κάνει (όπως η ομιλία για την ανάλυση φωνής)

Επειδή ο κωδικός πρόσβασης είναι κάτι που ξέρετε, αυτή η γνώση μπορεί να αποκτηθεί με διαφορετικούς τρόπους. Αντίθετα στη λογική ότι ένα κλειδί (που είναι ένα φυσικό αντικείμενο) αντιστοιχεί σε μια κλειδαριά, ένας εισβολέας δεν είναι απαραίτητο να πάρει τον κωδικό πρόσβασης από τον ιδιοκτήτη του προκειμένου να τον έχει ο ίδιος. Αντ' αυτού, μπορεί να τον πάρει με διάφορους τρόπους (χωρίς ο ιδιοκτήτης του να ξέρει). Παραδείγματος χάριν:

**Εκμετάλλευση των αδύνατων κωδικών πρόσβασης:**

Οι χρήστες επιλέγουν συχνά "εύκολους" κωδικούς πρόσβασης που μπορούν να θυμηθούν χωρίς πρόβλημα. Αυτό σημαίνει ότι χρησιμοποιούν μια λέξη, μια φράση ή έναν αριθμό που έχει ειδική σημασία για αυτούς, όπως π.χ το όνομα του συζύγου τους, τα γενέθλια ή ο αριθμός κοινωνικής ασφάλισής τους. Ένας εισβολέας που ξέρει κάτι για το χρήστη μπορεί να είναι σε θέση να υποθέσει τον κωδικό πρόσβασης. Η χρήση οποιασδήποτε λέξης που είναι στο λεξικό δημιουργεί την αδυναμία, εξαιτίας επιθέσεων με τη μέθοδο **"ωμής βίας"** (που δοκιμάζουν τον έναν κωδικό πρόσβασης μετά τον άλλο έως ότου πετυχαίνουν το σωστό) και "**λεξικών**" οι οποίες μπορούν να σπάσουν τον κωδικό.

**Εκμετάλλευση της συμπεριφοράς χρηστών:**

Εάν ο κωδικός πρόσβασης είναι πιο σύνθετος και μη-διαισθητικός (ένας τυχαίος συνδυασμός γραμμάτων και αριθμών), ο χρήστης μπορεί να έχει το πρόβλημα στο να τον θυμάται και αυτό μπορεί να οδηγήσει στο να τον γράψει κάπου –συχνά σε μια προεξέχουσα θέση όπως το πρώτο συρτάρι του γραφείου ή ακόμα και σε μια σημείωση κολλημένη πάνω στην οθόνη. Οι χρήστες μπορούν επίσης να μοιραστούν τους κωδικούς πρόσβασής τους με άλλους χρήστες στο περιβάλλον εργασίας τους.

**Σύλληψη των πιστοποιητικών κατά τη μεταφορά:**

Ακόμα και όταν χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης και οι χρήστες τους κρατούν μυστικούς, οι εισβολείς μπορούν να είναι σε θέση να συλλάβουν τα πιστοποιητικά όταν στέλνονται μέσω τού δικτύου εάν ικανοποιητικά μέτρα ασφάλειας δεν είναι σε θέση να αποτρέψουν αυτό το γεγονός.

Επειδή υπάρχουν τόσοι πολλοί τρόποι για ένα αναρμόδιο πρόσωπο με λίγες τεχνικές γνώσεις και η ικανότητα να μάθει τους κωδικούς πρόσβασης των νόμιμων χρηστών, είναι πολύ σημαντικό οι οργανισμοί / εταιρείες να προωθούν μια πολύπλευρη πολιτική ενάντια στην παραβίαση κωδικών πρόσβασης. Αυτή αρχίζει με την έρευνα και την εξουσιοδότηση ότι μόνο οι ασφαλείς κωδικοί πρόσβασης χρησιμοποιούνται.

### *5.7.3. Δημιουργία ασφαλών κωδικών πρόσβασης*

Η δημιουργία των κωδικών πρόσβασης που είναι σχετικά ασφαλείς περιλαμβάνει την εξουσιοδότηση του μήκος και της πολυπλοκότητας τους (όσο μεγαλύτερος ο κωδικός πρόσβασης, και όσο πιό διαφορετικοί τύποι γραμμάτων – χαρακτήρων, αριθμών, συμβόλων, κεφαλαίων και μικρών – τόσο το καλύτερο). Μια άλλη εκτίμηση εξουσιοδοτεί / αναγκάζει τους κωδικούς πρόσβασης να αλλάζουν τακτικά. Όσο παλαιότερος είναι ένας κωδικός πρόσβασης, τόσο μεγαλύτερη πιθανότητα να έχει γίνει γνωστός σε κάποιο άλλον εκτός από του κατόχου του.

Γενικά, οι ακόλουθες οδηγίες πρέπει να τηρούνται στη δημιουργία των κωδικών πρόσβασης:

- Καταστήστε τον κωδικό πρόσβασης αρκετά μεγάλο σε μήκος έτσι ώστε να είναι δύσκολο να τον μαντέψει κάποιος , αλλά αρκετά σύντομα έτσι ώστε ο κάτοχος του να μπορεί να τον θυμηθεί (8-10 χαρακτήρες για τους απλούς χρήστες, με πιό μεγάλους σε μήκος κωδικούς πρόσβασης για τους διαχειριστές)
- Μην χρησιμοποιείτε τις λέξεις που είναι στο λεξικό.
- Αναμίξτε στον κωδικό τους κεφαλαίους και τους μικρούς αλφαβητικούς χαρακτήρες, τους αριθμούς, και τα σύμβολα.

- Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης ή τους ίδιους δύο ή τρεις κωδικούς επανειλημμένως όταν είναι ο καιρός να αλλαχτούν οι κωδικοί .

### *5.7.4. Προστασία των κωδικών πρόσβασης*

Η δημιουργία των ασφαλών κωδικών πρόσβασης είναι μόνο το πρώτο βήμα. Οι πολιτικές (από μέρος του κάθε οργανισμού / εταιρείας) πρέπει να τίθονται σε ισχύ για να ελέγχουν την συμπεριφορά των χρηστών, όπως π.χ την απαγόρευση του μοιρασμού των κωδικών ενός χρήστη με οποιονδήποτε άλλο χρήστη. Οι πολιτικές, είναι επιτακτικό να μην μένουν στα χαρτιά, αλλά να διαδίδονται σε όλους εκείνους που θα χρησιμοποιήσουν το δίκτυο. Οι χρήστες πρέπει για να υπογράψουν ένα έγγραφο / βεβαίωση, επιβεβαιώνοντας ότι έλαβαν και διάβασαν τις πολιτικές, και ότι αυτές είναι επιβεβλημένες.

### *5.7.5. Πολιτικές των διαχειριστών εναντίον των πολιτικών των χρηστών*

Μερικές από τις πολιτικές που αναπτύσσονται μπορούν να επιβληθούν μέσω των λειτουργικών συστημάτων ή τρίτων λογισμικών. Παραδείγματος χάριν, σε ένα δίκτυο windows 2000 μπορεί ο administrator να θέσει την πολιτική ομάδας (στο group policy editor για GPO, επιλογή Computer Configuration | Windows Settings | Security Settings | Account Policies | Password Policies) για να επιτρέψει μόνο τους κωδικούς πρόσβασης ενός συγκεκριμένου ελάχιστου μήκους ή για να αναγκάσει το λειτουργικό σύστημα να θυμηθεί το ιστορικό κωδικού του χρήστη και να μην επιτρέψει έναν κωδικό που έχει ήδη χρησιμοποιηθεί στο πρόσφατο παρελθόν. Αυτό σημαίνει ότι δεν είναι απαραίτητο να για τον διαχειριστή να στηριχθεί στους χρήστες να συμμορφωθούν με τους κανόνες – εάν προσπαθήσουν να θέσουν έναν κωδικό που δεν καλύπτει τις απαιτήσεις του διαχειριστή, το σύστημα θα τους απορρίψει.

Οι διαχειριστές μπορούν επίσης να αυξήσουν την ασφάλεια που παρέχεται από την επικύρωση κωδικού με τον καθορισμό του συστήματος να κλειδώνει έναν λογαριασμό ενός χρήστη μετά από ένα συγκεκριμένο αριθμό αποτυχημένων προσπαθειών σύνδεσης με το δίκτυο. Επειδή είναι απίθανο ότι ένας νόμιμος χρήστης θα αποτύχαινε αρκετές φορές στη σειρά να πληκτρολογήσει τον κωδικό του σωστά, οι πολλαπλές αποτυχημένες προσπάθειες συχνά δείχνουν ότι κάποιος προσπαθεί να υποθέσει τον κωδικό πρόσβασης.

Είναι επίσης χρήσιμο να επιτραπεί ο έλεγχος ασφάλειας και το σύστημα να καταγράφει τα γεγονότα στο Security log. Με αυτόν τον τρόπο, μπορεί να καθοριστεί πότε εμφανίζονται οι αποτυχημένες προσπάθειες σύνδεσης

### *5.7.6. Εναλλακτικές και πρόσθετες μέθοδοι επικύρωσης*

Όταν οι καλές πολιτικές είναι σε ισχύ, η επικύρωση κωδικού πρόσβασης μπορεί να παρέχει μια επαρκή προστασία των πόρων σε ένα χαμηλό ή μέσο περιβάλλον ασφάλειας. Εντούτοις, εάν τα στοιχεία στον υπολογιστή ή το δίκτυό είναι ιδιαίτερα ευαίσθητα, θα πρέπει να γίνεται η επικύρωση του κωδικού πρόσβασης με κάποια άλλη μέθοδο επικύρωσης.

**Η επικύρωση έξυπνων καρτών(smartcards)** υποστηρίζεται από τα Windows 2000/XP και παρέχει ένα πρόσθετο στρώμα ασφάλειας επειδή όχι μόνο πρέπει ο χρήστης να παρέχει κάτι που ξέρει για να συνδεθεί στο σύστημα (σε αυτήν την περίπτωση, ένας προσωπικός αριθμός αναγνώρισης -- Personal Identification Number ή PIN) αλλά πρέπει επίσης να παρέχει ένα φυσικό αντικείμενο – την ίδια την κάρτα. Μια έξυπνη κάρτα είναι μια πλαστική κάρτα τύπου πιστωτικής κάρτας με ένα ενσωματωμένο τσιπ που μπορεί να κρατήσει αποθηκευμένο ένα ψηφιακό πιστοποιητικό. Έτσι η επικύρωση των χρηστών επιτυγχάνεται μέσω μιας υποδομής δημοσίου κλειδιού. Ένας αναγνώστης έξυπνων καρτών/smartcard reader (μια συσκευή υλικού) απαιτείται, μέσω του οποίου η κάρτα επικυρώνεται. Παρακάτω θα αναφερθούμε εκτενέστερα στο θέμα αυτό (smartcard).

Μια άλλη και ασφαλέστερη επιλογή είναι να χρησιμοποιηθεί ***η βιομετρική επικύρωση***. Αυτό απαιτεί υλικό και λογισμικό ικανά να σκανάρουν ένα δακτυλικό αποτύπωμα, το αποτύπωμα της παλάμης, ακόμα και την αμφιβληστροειδή εικόνα του ματιού. Αν και ο εξοπλισμός είναι κάπως ακριβός και το λογισμικό δεν είναι τελειοποιημένο ακόμα, η βιομετρική επικύρωση έχει τη δυνατότητα να καταστεί ο ασφαλέστερος τρόπος επικύρωσης της ταυτότητας ενός χρήστη.

# ΚΕΦΑΛΑΙΟ 5Ο

## 6. SMARTCARDS

### 6.1. Τι είναι μια Smart Card

Κατά έναν γενικό ορισμό, μια Smart Card (ευφυής κάρτα) είναι μια πλαστική κάρτα όμοια σε σχήμα και μέγεθος με μια συνήθη πιστωτική κάρτα, η οποία όμως αντί να διατηρεί τα δεδομένα της σε μια μαγνητική ταινία, τα συγκρατεί σε ένα μικρό κύκλωμα από σιλικόνη (silicone chip), το οποίο βρίσκεται ενσωματωμένο στη κάρτα. Σε κάθε κάρτα υπάρχει μια επίχρυση ή ασημένια πλακέτα επαφής (contact plate), η οποία είναι ορατή στην επιφάνεια της κάρτας . Η πλακέτα επαφής επικοινωνεί με το chip της κάρτας και αποτελεί την μοναδική συσκευή εισόδου/εξόδου του chip της Smart Card, η οποία απαιτεί επιπρόσθετα επίπεδα υλικού και λογισμικού, ώστε να γίνεται σωστά η αλληλεπίδραση με το χρήστη.

Κατά έναν πιο τεχνικό και λεπτομερή ορισμό, μια Smart Card είναι μια κάρτα με ενσωματωμένο είτε έναν μικροεπεξεργαστή (microprocessor) και ένα κύκλωμα μνήμης (memory chip) ή ένα κύκλωμα μνήμης με μη-προγραμματίσιμη λογική (non-programmable logic) – υπάρχουν κι άλλοι τύποι Smart Cards, ωστόσο αναφέρονται οι παραπάνω ως οι πλέον διαδεδομένοι. Οι Smart Cards ανάλογα με τον τύπο τους, μπορούν να προσθέτουν, να αφαιρούν και γενικότερα να χειρίζονται συγκεκριμένες πληροφορίες ή να αναλαμβάνουν τη διεκπεραίωση μιας προκαθορισμένης λειτουργίας. Μία Smart Card μπορεί να μεταφέρει όλες τις απαραίτητες λειτουργίες και πληροφορίες πάνω της. Γι’ αυτό, και σε συναλλαγές με Smart Cards δεν απαιτείται πρόσβαση σε απομακρυσμένες βάσεις δεδομένων (remote databases access).

Λέγεται ότι οι Smart Cards κάποτε στο μέλλον θα είναι τόσο σημαντικές όσο είναι και οι Η/Υ στις μέρες μας. Ωστόσο, και οι Smart Cards στην ουσία είναι μικροσκοπικοί Η/Υ. Λόγω της παραπάνω ιδιότητάς τους, είναι δύσκολο να προβλέψουμε το φάσμα των μελλοντικών τους εφαρμογών. Το πιο πιθανό είναι να ακολουθήσουν τους ταχύτατους ρυθμούς ανάπτυξης των Η/Υ. Οι Smart Cards έχουν αποδειχθεί ιδιαιτέρως χρήσιμες σε περιπτώσεις συναλλαγών, εξακρίβωσης προσωπικών στοιχείων και εξουσιοδότησης πελατών σε πολλές Ευρωπαϊκές χώρες. Όσο οι δυνατότητές τους επεκτείνονται, θα μπορούσαν να εξελιχθούν σε μίνι – χαρτοφύλακες (thin client), αντικαθιστώντας τα πορτοφόλια και όλα όσα περιέχουν (πιστωτικές κάρτες, άδειες , μετρητά, ακόμη και προσωπικές φωτογραφίες). Περιέχοντας πολυπληθή πιστοποιητικά αναγνώρισης, οι Smart Cards θα μπορούσαν να χρησιμοποιηθούν για την αναγνώριση προσωπικών μας στοιχείων, ανεξάρτητα από το πού είμαστε ή σε ποιο δίκτυο Η/Υ είμαστε συνδεδεμένοι.

### 6.2. Ιστορική αναδρομή

Η πρώτη μορφή Smart Card υπήρξε το 1914 (!!), όπου ο Wells Fargo χρησιμοποίησε κάρτες αναγνώρισης από χαρτί ή χαρτόνι ως μέσο

ταχυδρομικών παραγγελιών. Αργότερα, μετά το 1960, το χαρτόνι αντικαταστάθηκε από πλαστικό και οι κάρτες αυτές χρησιμοποιήθηκαν σε τράπεζες (τραπεζικές κάρτες) .

Πρόγονος των Smart Cards, ήταν οι κάρτες με μαγνητική ταινία που παρουσιάστηκαν στα μέσα της δεκαετίας του 1960, αλλά χρειάστηκαν περίπου 15 χρόνια για να γίνουν αποδεκτές από τις μεγάλες εταιρίες πιστωτικών καρτών. Από το 1980 ως το 1990 κυκλοφόρησαν 1δις περίπου τέτοιες κάρτες. Οι Smart Cards εφευρέθηκαν σε διάφορες χώρες, διαφορετικές χρονικές στιγμές – Γερμανία 1967, Ιαπωνία 1970, Η.Π.Α. 1972 και Γαλλία 1974.

Ουσιαστικά, οι Smart Cards εφευρέθηκαν για πρώτη φορά στη Γαλλία. Παρόλο που οι εφευρέτες σε Η.Π.Α. και Ιαπωνία προηγούνται χρονικά του Γάλλου Roland Moreno – γνωστός κι ως «πατέρας των Smart Cards» – οι Γάλλοι ήταν οι πρώτοι που επένδυσαν μεγάλο κεφάλαιο για την προώθηση της συγκεκριμένης τεχνολογίας. Κι αυτό έγινε μετά το 1970 , κατά τη διάρκεια μιας περιόδου σημαντικών επενδύσεων, στη προσπάθεια του κράτους για αναβάθμιση της τεχνολογικής υποδομής του . Η πρώτη εταιρεία που ξεχώρισε ήταν η Bull , η οποία σήμερα αριθμεί πάνω από 700 τύπους καρτών με τεχνολογία μικροοεπεξεργαστή. Οι κάρτες αυτές έγιναν γνωστές αρχικά ως κάρτες μνήμης (memory cards). Το 1980, όταν η Γαλλία ξεκίνησε μια καμπάνια για την προώθηση της τεχνολογίας των Smart Cards , ο Roy Bright, στέλεχος της Intelimatique (οργανισμός μάρκετινγκ της κυβέρνησης) αναφέρθηκε για πρώτη φορά στη φράση Smart Card .

Μέσα στη δεκαετία του 1980 βελτιώθηκαν και δοκιμάστηκαν σε πολλές διαφορετικές συνθήκες χρήσης από τις εταιρίες πιστωτικών καρτών και τις τράπεζες. Στα τέλη της ίδιας δεκαετίας, οι Smart Cards χρησιμοποιούνταν στην Ιαπωνία ως δώρα – τα σούπερ μάρκετ χάριζαν τηλεφωνικές κάρτες για αγορές πάνω από ένα όριο. Το 1991, η Argos, μια βρετανική εταιρία φθηνών αγορών , παρουσίασε το «Premier Points», ένα πρόγραμμα με Smart Card στα πρατήρια της Mobil . Οι πελάτες είχαν τη δυνατότητα να συλλέγουν βαθμούς στη κάρτα τους με κάθε αγορά βενζίνης και στη συνέχεια τους εξαργύρωναν με προιόντα στα καταστήματα της Argos .

## *6.3. Τεχνικά χαρακτηριστικά και δομή*

Υπάρχουν Smart Cards πολλών και διαφορετικών τύπων – ακόμη και όταν προέρχονται από τον ίδιο κατασκευαστή – έχοντας η κάθε μία τη δικιά της αρχιτεκτονική (chip architecture) . Κάποιες αποτελούνται μόνο από μνήμη , κάποιες άλλες έχουν έναν ή και περισσότερους επεξεργαστές . Το καθένα από αυτά , ρυθμίζεται με απλές εφαρμογές ή μέσα από εφαρμογές λειτουργικών συστημάτων ικανών να χειρίζονται on-chip εφαρμογές , αλλά όλες οι Smart Cards είναι «άχρηστες» χωρίς την υποστήριξη μιας υποδομής τέτοιας ώστε να φέρουν εις πέρας τον σκοπό τους .

### *6.3.1. Τύποι μιας Smart Card*

Η πορεία εξέλιξης των Smart Cards , με βάση τα εκάστοτε χαρακτηριστικά τους , πέρασε από τα εξής στάδια :

- **Magnetic Stripe Cards** . Οι κάρτες της συγκεκριμένης κατηγορίας αποτελούνται από μία μαγνητική ταινία (magnetic stripe) . Η δυνατότητα

αποθήκευσης στη μαγνητική ταινία ανέρχεται σε περίπου 1000 bits και με χρήση της κατάλληλης συσκευής ο καθένας μπορεί να δει ή και να αλλάξει τα δεδομένα της κάρτας . Η μαγνητική ταινία βρίσκεται στην «πίσω» πλευρά της κάρτας , ενώ κάρτες αυτής της κατηγορίας χρησιμοποιούνται κυρίως με σκοπό την αναγνώριση και πιστοποίηση του χρήστη από Αυτόματες Ταμειακές Μηχανές (A.T.M.'s-Automated Teller Machines) , ως πιστωτικές κάρτες , κ.ά. .

• **Integrated Circuit (IC) Memory Cards .** Οι κάρτες αυτές μπορούν να αντέξουν 1-4 KB δεδομένων , αλλά δεν έχουν επεξεργαστή έτσι ώστε να χειρίζονται τα δεδομένα αυτά . Συνεπώς , εξαρτώνται από το σύστημα ανάγνωσης καρτών και είναι κατάλληλες για χρήσεις όπου η κάρτα εκτελεί μια καθορισμένη λειτουργία . Αυτές οι κάρτες μνήμης , αντιπροσωπεύουν το σύνολο των εκατομμυρίων καρτών που έχουν πωληθεί τα τελευταία χρόνια σε εφαρμογές όπως οι τηλεκάρτες . Τέλος , είναι γνωστές ως κάρτες υψηλής ασφάλειας .

• **Integrated Circuit (IC) Microprocessor Cards** . Οι κάρτες αυτές (γνωστές στη βιομηχανία και ως chip cards) προσφέρουν μεγαλύτερο χώρο μνήμης και μεγαλύτερη προστασία των δεδομένων σε σύγκριση με κάρτες παλαιότερης τεχνολογίας . Επίσης , οι συγκεκριμένες κάρτες μπορούν να επεξεργαστούν δεδομένα της κάρτας . Η σημερινή γενιά των chip cards αποτελείται από έναν επεξεργαστή 8 bits , 16KB ROM και 512 bytes RAM . Τα παραπάνω χαρακτηριστικά καθιστούν τις κάρτες αυτές ισοδύναμες με έναν αυθεντικό IBM-XT υπολογιστή , παρότι έχουν ελάχιστα μικρότερη χωρητικότητα μνήμης.

Αυτές οι κάρτες χρησιμοποιούνται για μια πληθώρα εφαρμογών , κυρίως γι' αυτές που περιλαμβάνουν κρυπτογράφηση , κάτι το οποίο απαιτεί πολύπλοκους υπολογισμούς . Έτσι , οι κάρτες αυτού του τύπου αποτελούν τη κύρια πλατφόρμα για κάρτες που φέρουν ασφαλή ψηφιακή ταυτότητα . Παραδείγματα τέτοιων καρτών είναι οι πιστωτικές κάρτες νέας τεχνολογίας , οι κάρτες ασφαλούς πρόσβασης σε δίκτυα , κάρτες προστασίας κινητών τηλεφώνων από υποκλοπές , κ.ά. .

• **Cryptographic Coprocessor Cards** . Αν και οι κάρτες αυτές έχουν πολλά κοινά με τις κάρτες της παραπάνω κατηγορίας , διαφέρουν από αυτές ως προς το κόστος και τη λειτουργικότητά τους . Οι περισσότεροι σύγχρονοι , ασύμμετροι αλγόριθμοι κρυπτογράφησης απαιτούν ιδιαίτερα πολύπλοκους μαθηματικούς υπολογισμούς . Με την προσθήκη ενός επιπλέον επεξεργαστή (coprocessor) , οι χρόνοι εκτέλεσης όλων των υπολογισμών και των διεργασιών μειώνονται σημαντικά . Ωστόσο , το κόστος για τη προσθήκη ενός τέτοιου μικροεπεξεργαστή μπορεί να αυξήσει την τιμή μιας Smart Card από 50% έως και 100% . Παρόλ' αυτά , τα οφέλη για την ασφάλεια υπολογιστών και δικτύων , με την προσθήκη επιπλέον μικροεπεξεργαστή , είναι μεγάλα , εφόσον το ιδιωτικό κλειδί από τη στιγμή που υπάρξει δεν θα μπορεί να διαγραφεί από τη κάρτα . Οι τεχνολογικές εξελίξεις προμηνύουν ότι η κατασκευή ισχυρότερων μικροεπεξεργαστών ή η εύρεση καλύτερων αλγορίθμων , αναμένεται να κάνει τη χρήση επιπλέον μικροεπεξεργαστή περιττή .

• **Contactless Smart Cards** . Οι κάρτες αυτής της κατηγορίας έρχονται να δώσουν λύση στα προβλήματα που έχουν μέχρι σήμερα παρουσιαστεί ,

σχετικά με την αξιοπιστία και την ανθεκτικότητα της επαφής (contact) της κάρτας στη φθορά , στις σκόνες , κ.τ.λ. . Παρέχει , επίσης , στον εκάστοτε χρήστη ένα φάσμα καινούριων δυνατοτήτων κατά τη διάρκεια χρήσης της κάρτας . Οι κάρτες δεν θα χρειάζονται πλέον να εισάγονται σε συσκευές ανάγνωσης , κάτι το οποίο θα διευκόλυνε την αποδοχή του τελικού χρήστη . Επιπλέον , δεν χρειάζεται το chip να είναι ορατό στην επιφάνεια της κάρτας , οπότε τα γραφικά και η εμφάνιση της κάρτας θα απεικονίζονται πιο ελεύθερα . Παρόλ'αυτά , οι κάρτες αυτής της κατηγορίας δεν έχουν την αναγνώριση που θα μπορούσαν να έχουν , διότι πρώτον το κόστος κατασκευής και αγοράς τους είναι υψηλό και δεύτερον δεν έχει αποκτηθεί αρκετή εμπειρία προκειμένου να υϊοθετηθεί η δεδομένη τεχνολογία . Οι εφαρμογές στις οποίες χρησιμοποιούνται οι κάρτες αυτής της κατηγορίας είναι ιδιαίτερα περιορισμένες , εφόσον οι πολύ μικροί χρόνοι συναλλαγής είναι καθοριστικοί για την ολοκλήρωσή της . Το πιο πιθανό πάντως είναι η συγκεκριμένη τεχνολογία να επεκταθεί σε πιο μελλοντικές εφαρμογές .

- **Optical Memory Cards** . Οι κάρτες αυτής της κατηγορίας μοιάζουν με κάρτες που έχουν πάνω τους κολλημένο ένα κομμάτι CD – στην ουσία αυτή είναι η μορφή τους . Μπορούν να αποθηκεύσουν μέχρι 4MB δεδομένων , τα οποία από τη στιγμή που γράφονται δεν μπορούν να αλλάξουν ή να διαγραφούν . Επομένως , αυτός ο τύπος καρτών είναι ιδανικός για εγγραφές – ιατρικά αρχεία , ιστορικό ατόμων , κ.ά. . Στις μέρες μας , οι κάρτες αυτές δεν έχουν επεξεργαστή (κάτι το οποίο αναμένεται στο προσεχές μέλλον) . Και παρότι είναι οικονομικά προσιτές όσο και οι IC κάρτες , οι συσκευές ανάγνωσής τους δεν χρησιμοποιούν συγκεκριμένα πρωτόκολλα και είναι υψηλού κόστους .

### *6.3.2. Προδιαγραφές*

Τα προβλήματα στην επιλογή και χρήση των Smart Cards δεν οφείλονται στην έλλειψη τεχνογνωσίας γύρω από τις προδιαγραφές που αυτές πρέπει κάθε φορά να καλύπτουν . Αντιθέτως , υπάρχει μια πληθώρα προδιαγραφών , καλύπτοντας τα πάντα από :

- Μέγεθος της κάρτας ,
- Θέση και διαστάσεις της πλακέτας επαφής του chip (chip contact plate) ,
- Αλληλεπίδραση μεταξύ των λειτουργιών της μαγνητικής ταινίας και της ακεραιότητας των δεδομένων του chip ,
- Πρωτόκολλα μεταφοράς δεδομένων ,
- κτλ. , κτλ. .

Οι οργανισμοί προδιαγραφών , που συνεργάζονται με σκοπό την παραγωγή και εξέλιξη των Smart Cards , παρουσιάζονται λεπτομερώς στην παρακάτω Internet διεύθυνση : www.cardeurope.demon.co.uk/stds.htm , όπου φιλοξενείται άρθρο του Δρ. J.M.Gill με τίτλο " Standards Committees and Standards related to Smart Cards ".

Η σειρά προδιαγραφών ISO 7816 , με βάση το ISO/IEC JTC1/SC17 , είναι ο βασικός τύπος προδιαγραφής για την κατασκευή του συνόλου των Smart Cards .

Ως γνωστόν , όπου υπάρχει ακμή , υπάρχουν και πολλές επιλογές . Οι κατασκευαστές καρτών έχουν επιλέξει να χρησιμοποιούν προδιαγραφές οι οποίες ταιριάζουν περισσότερο με τις απαιτήσεις τους , και σε ορισμένες περιπτώσεις έχουν αυξήσει τις προδιαγραφές προκειμένου να κάνουν τα προϊόντα τους πιο ανταγωνιστικά στην αγορά . Μάλιστα , οι προδιαγραφές πλέον δίνουν περισσότερη βαρύτητα στα πρωτόκολλα παρά στις διεπαφές (interfaces) – το IS 7816-4 (Interindustry Commands for Interchange) ορίζει την δομή και το περιεχόμενο των μηνυμάτων που εκτελούν τις διάφορες πράξεις στα δεδομένα του chip της Smart Card , αλλά δεν γνωστοποιεί τον τρόπο με τον οποίο λαμβάνονται τα μηνύματα αυτά . Αξιοσημείωτη , τόσο στο χώρο των Smart Cards όσο και στο τομέα υλικού και λογισμικού Η/Υ , παραμένει η έλλειψη κοινά αποδεκτών χαρακτηριστικών των διεπαφών , αποτελώντας στην ουσία εμπόδιο στην πιο επεκτεταμένη εκμετάλλευση των Smart Cards .

### *6.3.3. Αρχιτεκτονική μιας Smart Card*

Το chip μιας Hitachi 3112 Smart Card αποτελείται από επεξεργαστή 8 bits , σε σύγκριση με τους 32-bit επεξεργαστές της τρέχουσας γενιάς των Η/Υ , και περιέχει 24kb ROM (Read-Only Memory) για την ύπαρξη του λειτουργικού συστήματος , 8kb EEPROM (Electrically Erasable Programmable ROM) για τις εφαρμογές της κάρτας και 1056 bytes RAM (Random Access Memory) .

Σχηματικά και λειτουργικά , σε περιπτώσεις λογικών σφαλμάτων , η μνήμη μιας Smart Card προστατεύεται από την CPU (Central Processing Unit) , η οποία χειρίζεται όλες τις αιτήσεις συναλλαγών υπό τον έλεγχο του λειτουργικού συστήματος της κάρτας . Όταν η αίτηση γίνει αποδεκτή , είτε χειρίζεται απευθείας από το λειτουργικό σύστημα ή περνά στη διαχείριση μιας εφαρμογής της EEPROM . Και στις δύο περιπτώσεις χρησιμοποιούνται περιοχές της EEPROM για ημι-μόνιμα δεδομένα (semi-permanent data) και της RAM για την κάλυψη αναγκών κατά τη διάρκεια της λειτουργίας του chip . Τα περιεχόμενα της RAM χάνονται όταν η κάρτα πάψει να τροφοδοτείται . Αντιθέτως , οι ρυθμίσεις της EEPROM μπορούν να παραμείνουν αναλλοίωτες έως και 10 χρόνια .

Ο δευτερεύων επεξεργαστής (co-processor) της κάρτας είναι , κατά μεγάλο μέρος , υπεύθυνος για το επιπλέον κόστος των καρτών υψηλής ασφάλειας , ικανών να διεκπεραιώσουν χρηματικές συναλλαγές . Συγκεκριμένα , εκτελεί τη διαδικασία κρυπτογράφησης κι αποκρυπτογράφησης , διαδικασία απαραίτητη για ασφαλείς χρηματικές συναλλαγές .

Η FeRAM αναμένεται να αντικαταστήσει την EEPROM , ως η προτεινόμενη τεχνολογία μνήμης για την κατασκευή Smart Cards στο προσεχές μέλλον , προσφέροντας υψηλή ταχύτητα εγγραφής σε συνδυασμό με χαμηλή κατανάλωση ισχύος (100.000.000 κύκλους ανάγνωσης/εγγραφής σε σύγκριση με μερικές εκατοντάδες χιλιάδες για την EEPROM) .

Όσον αφορά στους προσωπικούς Η/Υ , η Smart Card είναι πολύ πιθανό να εφαρμόσει την RISC τεχνολογία επεξεργαστών . Η Hitachi ήδη προωθεί στην αγορά τον 32-bit SuperH RISC μικροεπεξεργαστή της , ο οποίος υϊοθετείται σε περιπτώσεις κατασκευής πολυμεσικών εφαρμογών και ψηφιακών κινητών

τηλεφώνων . Ο SuperH προσφέρει υψηλότερη απόδοση σε σύγκριση με την συμβατική CISC τεχνολογία . Όταν η νέα γενιά RISC συσκευών ενσωματωθεί σε Smart Cards , τότε οι τελευταίες θα αποκτήσουν μεγάλη επεξεργαστική ισχύ , σαφώς χρήσιμη για λειτουργικά συστήματα υψηλών απαιτήσεων , όπως αυτά της Java ή της Multos , καθώς και σε πολύπλοκες εφαρμογές όπως οι κάρτες κρυπτογράφησης .

Προς το παρόν ωστόσο , τα μεγέθη μνήμης των Smart Cards δεν αρκούν για τη κάλυψη των αναγκών σε σημαντικές πολλαπλές εφαρμογές .

### *6.3.4. Λειτουργικά Συστήματα για Smart Cards*

Παρότι ο προγραμματισμός του chip μιας Smart Card βασίζεται σε μερικές χιλιάδες bytes κώδικα , το λειτουργικό σύστημα που υποστηρίζει την κατασκευή του μικροεπεξεργαστή της κάρτας πρέπει να διαχειρίζεται εργασίες όπως :

- Μεταφορά δεδομένων στο «διπλής-κατεύθυνσης» (bi-directional) τερματικό διασύνδεσης χρήστη-κάρτας .
- Το «φόρτωμα» (loading) , η λειτουργία και η διαχείριση των εφαρμογών της κάρτας .
- Έλεγχος εκτέλεσης των εφαρμογών .
- Έλεγχος πρόσβασης στα δεδομένα .
- Διαχείριση μνήμης .
- Διαχείριση αρχείων .
- Διαχείριση κι εκτέλεση αλγόριθμων κρυπτογράφησης .

Σε αντίθεση με τα λειτουργικά συστήματα για Η/Υ όπως το Unix , το DOS και τα Windows , το λειτουργικό σύστημα για Smart Cards δεν υποστηρίζει περαιτέρω διασυνδέσεις χρήστη ή την ικανότητα πρόσβασης σε εξωτερικά περιφερειακά ή αποθηκευτικά μέσα . Το μέγεθός του κυμαίνεται από 3 έως 24 Kbytes και υποστηρίζει από ειδικές εφαρμογές έως και πολυεφαρμογές με άλλα λειτουργικά συστήματα .

Επιπλέον , η μνήμη μιας Smart Card είναι αυστηρά περιορισμένη , περιορίζοντας συγχρόνως και τα λειτουργικά συστήματα των Smart Cards στην υλοποίηση τυποποιημένων οδηγιών και δομών αρχείων . Για το λόγο αυτό , με τα πρότυπα ISO 7816-4 και EN 726-3 , παρουσιάστηκαν κάποιες προτάσεις (profiles) , σύμφωνα με τις οποίες ορίζονταν οι ελάχιστες απαιτήσεις για εντολές και δομές δεδομένων .

Στη σημερινή αγορά των Smart Cards , υπάρχουν διάφορα λειτουργικά συστήματα . Παρακάτω , παραθέτονται links και συνοπτική περιγραφή για δύο από τα γνωστότερα λειτουργικά συστήματα για Smart Cards .

### *6.3.5.* ***Multos***

Το Multos είναι ένα λειτουργικό σύστημα πολυεφαρμογών κατασκευασμένο από την Mondex . Η Mondex International είναι μια εταιρία που έχει αναπτύξει μια γλώσσα προγραμματισμού προορισμένη για Smart Cards , την MEL (Multos Enabling Language) . Εδώ και λίγα χρόνια , το Multos βρίσκεται υπό την εποπτεία της MAOSCO (Multi-Application Operating System Company) , μιας εταιρίας-κολοσσού που αποτελείται από εταιρίες όπως η Siemens , η Motorola , η Fujitsu , η Hitachi , η American Express , η Dai Nippon Printing, η Keycorp, η MasterCard International και η Mondex International .

### *6.3.6. Microsoft Smart Cards*

Το Microsoft Smart Cards αποτελεί κομμάτι της νέας γενιάς λειτουργικών συστημάτων της Microsoft . Με το συγκεκριμένο λειτουργικό σύστημα και με χρήση της Visual Basic , πραγματοποιείται η υλοποίηση εφαρμογών για Smart Cards . Η κάρτα επικοινωνεί με έναν Η/Υ – μέσω λειτουργικού συστήματος της Microsoft – βασισμένη σε οδηγίες του PC/SC Workgroup , ενός ομίλου εταιριών Η/Υ και κατασκευαστριών εταιριών Smart Cards . Ωστόσο , σημαντική είναι η αδυναμία του συγκεκριμένου λειτουργικού συστήματος να λειτουργεί με τη προϋπόθεση ότι υποστηρίζεται από λειτουργικό σύστημα της Microsoft .

### *6.3.7. Διαλειτουργικότητα*

Η διαλειτουργικότητα (interoperability) είναι η ικανότητα των συστατικών να επικοινωνούν ως συναρτήσεις υλικού και λογισμικού . Η χρησιμότητα μιας Smart Card – και των διαφόρων εφαρμογών της – καθορίζεται από την ευκολία με την οποία ενσωματώνεται στην υποδομή της κάρτας . Σκοπός κάθε φορά είναι οι συσκευές ανάγνωσης καρτών να δέχονται όλες τις κάρτες , ανεξάρτητα από τον κατασκευαστή τους , καθώς και η δυνατότητα της υποδομής για επικοινωνία μέσα από μια πολλαπλότητα συσκευών ανάγνωσης , με τις εκάστοτε εφαρμογές που εδρεύουν στην κάρτα .

Η διαλειτουργικότητα μιας Smart Card εφαρμόζεται σε διάφορα επίπεδα :

- **Φυσικό**

  ➢ Μηχανικό : Όλοι οι τύποι επαφής των καρτών έχουν τις ίδιες φυσικές διαστάσεις , όπως μια συνηθισμένη πιστωτική κάρτα , καθώς και την ίδια θέση για την πλακέτα επαφής (IS 7816) , κι έτσι μπορούν να εισαχθούν στην ίδια συσκευή ανάγνωσης .

  ➢ Ηλεκτρονικό : κάποιοι τύποι καρτών (contact-type cards) διαθέτουν μόνο μνήμη , άλλες διαθέτουν και μικροεπεξεργαστή . Αυτό συνιστά τις διάφορες παραλλαγές στην αρχιτεκτονική της πλατφόρμας της κάθε κάρτας , κάτι το οποίο παρεμποδίζει την διαλειτουργικότητα .

- **Πλατφόρμας** (Platform)

Οι κάρτες με μικροεπεξεργαστή έχουν συχνά ιδιόκτητα λειτουργικά συστήματα , παρέχοντας παραλλαγές για κάθε εσωτερική ή εξωτερική διασύνδεση . Τέτοιες κάρτες δεν προσφέρουν την ίδια πλατφόρμα εφαρμογής , περιορίζοντας την διαλειτουργικότητα σε αυτό το επίπεδο .

- **Εφαρμογής**

  - Inter-cards : οι κάρτες μπορεί να φέρουν τις ίδιες (ή συμβατές) εφαρμογές και γι'αυτό στο επίπεδο αυτό διαθέτουν διαλειτουργικότητα . Μια κάρτα που φέρει μια εφαρμογή Mondex δεν είναι δυνατό να «συνεργαστεί» με μία άλλη που δεν διαθέτει μια αντίστοιχη .

  - Intra-cards : Διαλειτουργικότητα μεταξύ εφαρμογών του ιδίου κυκλώματος (chip) είναι εφικτή μόνο στην περίπτωση που οι συγκεκριμένες εφαρμογές επιτρέπουν την δεδομένη λειτουργικότητα .

Το πρώτο μοντέλο ανάπτυξης μιας Smart Card βασίστηκε σε εμπορικά προϊόντα . Κατασκευάστριες εταιρίες όπως η Siemens ή η GemPlus , αγόραζαν μικροεπεξεργαστές , κατασκεύαζαν το λειτουργικό σύστημα του chip και στη συνέχεια τις αυστηρά σχεδιασμένες εφαρμογές που θα εξυπηρετούσαν έναν συγκεκριμένο σκοπό . Η κάρτα τότε πωλούνταν ως μέρος του προς κατανάλωση προϊόντος . Ωστόσο , τα λειτουργικά συστήματα καρτών σχεδιάστηκαν αρχικά διαθέτοντας συγκεκριμένες εφαρμογές εξυπηρετώντας η κάθε μία συγκεκριμένο σκοπό , και επακόλουθο ήταν να υπάρξει μια τεράστια γκάμα λειτουργικών συστημάτων προκειμένου να καλυφθούν οι κατά καιρούς απαιτήσεις από αυτά . Αυτή η έλλειψη διαλειτουργικότητας σε επίπεδο πλατφόρμας , σε συνδυασμό με την ανάπτυξη εφαρμογών σε περιβάλλοντα υψηλής εξάρτησης από τον κώδικα εκτέλεσης του μικροεπεξεργαστή , κατέστησε την δημιουργία μεταφέρσιμων on-chip εφαρμογών , ιδιαίτερα δύσκολη .

Οι κάρτες της Multos και της Java αποτελούν παραδείγματα πλατφόρμας μιας Smart Card ανεξάρτητης από το υλικό , προσφέροντας για πρώτη φορά τη δυνατότητα ύπαρξης διαλειτουργικότητας σε επίπεδο πλατφόρμας , για εφαρμογές που αφορούν τις Smart Cards . Τα συστήματα και των δύο (2) εταιριών παρέχουν ένα εικονικό περιβάλλον εφαρμογής καθώς και μια μηχανή μεταγλώττισης της ψευδογλώσσας , την οποία ο κατασκευαστής χρησιμοποιεί για την υλοποίηση της εφαρμογής – η MEL (Multos Executable Language) για την Multos Card , η Java για την Java Card .

Το Multos αποτελεί το πρώτο , ανοιχτό , υψηλής ασφάλειας , πολυ-εφαρμογών λειτουργικό σύστημα για Smart Cards , καθιστώντας δυνατή την ύπαρξη πολλών διαφορετικών εφαρμογών την ίδια στιγμή στην ίδια κάρτα .Όπως και η Java Card , ο στόχος του Multos είναι να ανοίξει νέους ορίζοντες στην αγορά των Smart Cards προσφέροντας ένα φάσμα οικονομικά προσιτών και πρωτότυπων εφαρμογών και να δημιουργήσει ευκολίες για τους χρήστες , δημιουργώντας οικονομικές ευκαιρίες για τις βιομηχανίες .

Η διαλειτουργικότητα μιας εφαρμογής απαιτεί μια κοινή διασύνδεση τόσο για τις συσκευές ανάγνωσης – ή το τερματικό – όσο και για την μέσω του λειτουργικού συστήματος της κάρτας on-card εφαρμογής . Τη λύση στο

παραπάνω πρόβλημα επιχειρούν να δώσουν δύο πηγές : τα PC/SC και OCF πρότυπα (*PC/SC & OCF Specifications*) .

Αναφορικά με το καθένα , με το PC/SC (Personal Computer/Smart Card) πρότυπο επιχειρείται η δημιουργία μιας διασύνδεσης κοινής για όλες τις συσκευές ανάγνωσης , ανεξάρτητα από την πηγή προέλευσής τους . Η όλη προσπάθεια επικεντρώνεται στην απαίτηση για διαλειτουργικότητα μεταξύ καρτών και συσκευών ανάγνωσης και την δυνατότητα ενσωμάτωσης των παραπάνω σε Η/Υ με λειτουργικό σύστημα τα Windows της Microsoft .

Απ'την άλλη μεριά , το OCF (OpenCard Framework) πρότυπο αποσκοπεί στη παροχή μιας κοινής διασύνδεσης και για τις συσκευές ανάγνωσης των Smart Cards και για τις εφαρμογές της κάρτας . Η αρχιτεκτονική του είναι βασισμένη στην τεχνολογία της Java η οποία προσφέρει αυξημένη δυνατότητα μεταφοράς και διαλειτουργικότητα , στόχοι-κλειδιά για την ευρεία εξάπλωση και χρήση των Smart Cards .

### *6.3.8. Υποδομή*

Όλες οι Smart Cards απαιτούν συγκεκριμένη υποδομή – υλικό και λογισμικό σχεδιασμένο για την αλληλεπίδραση με την Smart Card και την εκτέλεση των διαφόρων λειτουργιών – πριν χρησιμοποιηθούν σε οποιαδήποτε εφαρμογή . Η ανάγκη για διαλειτουργικότητα στις Smart Cards εξαπλώνεται πέρα από το σχήμα , τις διαστάσεις , την αρχιτεκτονική και τα πρωτόκολλα εφαρμογής , τα οποία βρίσκονται ενσωματωμένα στην ίδια την κάρτα , στις συσκευές που χρησιμοποιούνται για την αλληλεπίδραση με την κάρτα σε φυσικό επίπεδο – οι συσκευές ανάγνωσης των Smart Cards , οι διεπαφές τους και οι drivers (συχνά λογισμικού) που είναι απαραίτητα για την παροχή αυτής της λειτουργικότητας .

Υπάρχουν τουλάχιστον τρεις (3) τομείς της βιομηχανίας που σχετίζονται με τη δημιουργία υποδομής τέτοιας που θα παρέχει στις Smart Cards το χαρακτηριστικό της διαλειτουργικότητας :

- **Κατασκευαστές Τερματικών Διασύνδεσης με την Κάρτα (Card Terminal Vendors)**

Παράγουν τις συσκευές ανάγνωσης (το πρώτο σημείο επαφής σε φυσικό επίπεδο) με την κάρτα . Κάθε vendor παράγει μια ποσότητα συσκευών ανάγνωσης από απλές συσκευές επαφής έως πιο πολύπλοκες συσκευές εξυπηρέτησης και προσφοράς λύσεων , συνδεδεμένες με την λειτουργικότητα της κάρτας . Οι Αυτόματες Ταμειακές Μηχανές (A.T.M.'s) αποτελούν ένα απλό παράδειγμα .

- **Παροχείς Λειτουργικών Συστημάτων Καρτών (Card Operating System Providers)**

Υπάρχουν πολλές εταιρίες που παράγουν λειτουργικά συστήματα και διασυνδέσεις χρήστη-εφαρμογών (A.P.I.'s) για Smart Cards . Μεταξύ αυτών προσφέρουν ένα ευρύ φάσμα από κώδικες με εντολές και αποκρίσεις έως και πιθανές εξωτερικές συσκευές .

• **Αντιπρόσωποι Καρτών (Card Issuers)**

Είναι οι υπεύθυνοι για την παραλαβή των Smart Cards από τους τελικούς χρήστες κι ελέγχουν τον τρόπο με τον οποίο γίνεται η τυποποίηση και η προσωποποίηση της κάθε κάρτας . Αυτό έχει πιθανή επίπτωση και στη λεπτομέρεια του τρόπου με τον οποίο τοποθετούνται και διευθυνσιοδοτούνται οι διάφορες εφαρμογές της κάρτας .

### *6.3.9. Συμβατότητα*

Η συμβατότητα των Smart Cards είναι πρακτικά ανεξάρτητη από τις φυσικές και ηλεκτρικές τους ομοιότητες . Πιο συγκεκριμένα , οι κάρτες με επαφή (contact-type cards) είτε είναι σύγχρονες (έχουν απλώς μνήμη) ή ασύγχρονες (έχουν και μνήμη και επεξεργαστή) , μπορεί να είναι ίδιες , αλλά δεν εκτελούν τις ίδιες λειτουργίες . Από τη στιγμή που ο κατασκευαστής της κάρτας προσθέσει ένα λειτουργικό σύστημα και μία επιπλέον εφαρμογή (σε μια ασύγχρονη κάρτα) , το προϊόν που παράγεται αφορά συγκεκριμένες εφαρμογές και περιορίζεται η δυνατότητα συμβατότητας – και διαλειτουργικότητας – με άλλα προϊόντα .

Με τα PC/SC και OCF πρότυπα επιχειρείται προσπάθεια μείωσης των επιδράσεων των παραπάνω θεμελιωδών διαφορών , προωθώντας μία κοινή πλατφόρμα μεταξύ των εφαρμογών χρήστη και των συσκευών ανάγνωσης και των συστημάτων Smart Cards στα οποία έχουν πρόσβαση . Ωστόσο , τα πρότυπα αυτά δεν εφαρμόζονται σε όλα τα επίπεδα της υποδομής μιας Smart Card . Προς το παρόν πάντως , η επιλογή μιας κάρτας θα καθορίζεται από την εφαρμογή για την οποία προορίζεται .

### *6.3.10. Φυσικά και ηλεκτρικά χαρακτηριστικά*

Το φυσικό μέγεθος μιας Smart Card χαρακτηρίζεται από τον τύπο ID-1 και περιγράφεται στο πρότυπο ISO 7810 . Οι διαστάσεις είναι 85.6 x 54 mm , με πάχος 0.76 mm και ακτίνα γωνίας 3.18 mm . Όταν δημιουργήθηκε το ISO 7810 το 1985 , δεν καθόριζε την θέση του chip αλλά αντί γι'αυτό καθόριζε χαρακτηριστικά για προγενέστερους τύπους καρτών (π.χ. *magnetic stripe cards* , κ.ά.) . Η δημιουργία του ISO 7816-2 το 1988 , ήρθε και κάλυψε τα παραπάνω κενά .Τα φυσικά χαρακτηριστικά μιας Smart Card απεικονίζονται στο σχήμα που ακολουθεί .

Οι ελάχιστες απαιτήσεις όσον αφορά στην ανθεκτικότητα της κάρτας , ορίζονται από το πρότυπα ISO 7810, 7813, και 7816 (μέρος $1^{o}$) . Στα συγκεκριμένα πρότυπα ορίζονται χαρακτηριστικά όπως η ποσότητα εκπομπής υπεριώδους ακτινοβολίας και ακτίνων X , το προφίλ της επιφάνειας της κάρτας , αντίσταση στις μεταβολές της θερμοκρασίας , κ.ά. . Το ISO/IEC

10373 ορίζει τις πειραματικές μεθόδους για πολλές από τις παραπάνω απαιτήσεις .

Τα ηλεκτρικά χαρακτηριστικά των Smart Cards ορίζονται στα πρότυπα ISO/IEC 7816 (μέρη 2 και 3) και GSM 11.11 . Οι περισσότερες Smart Cards αποτελούνται από οκτώ (8) πεδία επαφής στην μπροστινή τους πλευρά , ωστόσο δύο (2) από αυτά διατηρούνται για μελλοντική χρήση κι έτσι πολλοί κατασκευαστές παράγουν κάρτες με έξι (6) πεδία , κάτι το οποίο μειώνει ελάχιστα το κόστος παραγωγής . Οι ηλεκτρικές επαφές αριθμούνται από το C1 έως το C8 , ξεκινώντας από πάνω αριστερά και καταλήγωντας κάτω δεξιά

Ηλεκτρικές επαφές μιας Smart Card .

| ΘΕΣΗ | ΤΕΧΝΙΚΟΣ ΟΡΟΣ (ΣΥΝΤΟΜΟΓΡΑΦΙΑ) | ΛΕΙΤΟΥΡΓΙΑ |
|---|---|---|
| C1 | Vcc | Παροχή Τάσης |
| C2 | RST | Επαναφορά (RESET) |
| C3 | CLK | Συχνότητα Ρολογιού |
| C4 | RFU | Μελλοντική Χρήση |
| C5 | GND | Γείωση |
| C6 | Vpp | Εξωτερική Τάση |
| C7 | I/O | Σειριακές Επικοινωνίες Εισόδου/Εξόδου |
| C8 | RFU | Μελλοντική Χρήση |

Τα πεδία επαφής μιας Smart Card και οι λειτουργίες τους .

Η επαφή Vpp χρησιμοποιήθηκε αρκετά χρόνια πριν , για παροχή τάσης στις EEPROM για προγραμματισμό και διαγραφή . Ωστόσο , σήμερα η συγκεκριμένη επαφή χρησιμοποιείται ελάχιστα λόγω επινόησης νέων τεχνολογιών . Η παροχή τάσης για την Vcc ορίζεται σε 5V $\pm$ 10% . Υπάρχει μια σκέψη στη βιομηχανία των Smart Cards ώστε τα πρότυπα να υποστηρίζουν τεχνολογίες 3V , διότι όλα τα εξαρτήματα των κινητών

τηλεφώνων διατίθενται με τη συγκεκριμένη δυνατότητα ισχύος . Αυτό που προκύπτει , είναι ότι οι Smart Cards αποτελούν το μόνο εξάρτημα που απαιτεί από ένα κινητό τηλέφωνο να έχει και μετατροπέα τάσης . Παρόλ'αυτά , ένα ευρύτερο φάσμα για χειρισμό τάσεων 3–5V , πιθανόν στο μέλλον να αποτελεί επιτακτική ανάγκη .

### *6.3.11. Σετ οδηγιών κατασκευής μιας Smart Card*

Υπάρχουν τέσσερα διεθνή πρότυπα που ορίζουν τις στοιχειώδεις οδηγίες για την κατασκευή μιας Smart Card . Και παρότι οι οδηγίες αυτές αφορούν τέσσερα ξεχωριστά πρότυπα , παρουσιάζουν σε μεγάλο βαθμό συμβατότητα μεταξύ τους . Τα παραπάνω τέσσερα πρότυπα είναι τα GSM 11.11 (prETS 300608) , EN 726-3 , ISO/IEC 7816-4 , και το πρωταρχικό πρότυπο CEN (prEN 1546) . Οι οδηγίες με βάση τη λειτουργία τους, μπορούν να καταταχθούν συνοπτικά ως εξής :

| |
|---|
| Επιλογές αρχείου |
| Ανάγνωση κι εγγραφή σε αρχείο |
| Αναζήτηση σε αρχείο |
| Λειτουργίες του αρχείου |
| Αναγνώριση και ταυτοποίηση του κατόχου της κάρτας |
| Εξακρίβωση στοιχείων του κατόχου της κάρτας |
| Συναρτήσεις κρυπτογράφησης |
| Διαχείριση αρχείων |
| Οδηγίες για συναλλαγματικές εφαρμογές (πιστωτικές κάρτες) |
| Ολοκλήρωση λειτουργικού συστήματος |
| Δοκιμές υλικού (*hardware testing*) |
| Ειδικές οδηγίες για συγκεκριμένες εφαρμογές |
| Υποστήριξη πρωτοκόλλου μεταφοράς |

Τυπικά , για την κατασκευή μιας Smart Card , θα επιλέγεται η υλοποίηση κάποιων από τις παραπάνω οδηγίες , ανάλογα με την εφαρμογή της Smart Card . Κι αυτό λόγω των περιορισμών σε μνήμη ή σε κόστος .

### *6.3.12. Τρόπος Λειτουργίας μιας Smart Card*

Οι Smart Cards χρησιμοποιούνται γενικά ως υποκατάστατο στα συστήματα πιστοποίησης της ταυτότητας του κάθε χρήστη. Ένα πολύ πιο υψηλό επίπεδο ασφάλειας μπορεί να επιτευχθεί με ένα ασφαλές πρωτόκολλο επικοινωνίας μεταξύ της Smart Card και της συσκευής ανάγνωσης της κάρτας και μεταξύ της συσκευής ανάγνωσης και του Η/Υ. Το σύστημα λειτουργεί ως εξής:

**1** Η συσκευή ανάγνωσης και η Smart Card αυτοαναγνωρίζονται με την «επίδειξη» του ίδιου κλειδιού (κλειδί CK=Company Key ή CCK=Chipcard Communication Key). Με αυτόν τον τρόπο εξαιρείται η επεξεργασία καρτών άλλων, διαφορετικών κατασκευαστριών εταιριών. Στη συνέχεια, το CCK μπορεί να χρησιμοποιηθεί για να εξασφαλίσει την επικοινωνία μεταξύ της Smart Card και της συσκευής ανάγνωσης.

**2** Έχοντας ο χρήστης εισάγει την Smart Card στη συσκευή ανάγνωσης, πιστοποιείται η ταυτότητα του χρήστη με την ανάγνωση του PID (Personal Identification), πληροφορία μοναδική και μη μεταβλητή.

**3.** Το PIN που δίνει ο χρήστης ελέγχεται από την κάρτα. Το σκεπτικό είναι ότι κατά τη διαβίβαση του PIN δεν τίθεται θέμα υποκλοπής του από ειδικούς μηχανισμούς οι οποίοι αποσπούν το PIN που δίνει ο χρήστης κατά τη σύγκριση με το αντίστοιχο PIN της κάρτας.

**4.** Στο συγκεκριμένο σημείο, ξεκινά μια διαδικασία ελέγχου που εκτελείται στον φιλοξενητή υπολογιστή (host). Το PID του χρήστη στέλνεται στον host και αρχίζει μια διασύνδεση με την Smart Card, βασισμένη σε μία συγκεκριμένη για κάθε χρήστη τιμή (PK=Personal Key). Όταν η Smart Card «απαντήσει» θετικά, ο host έχει πλέον ολοκληρώσει την διαδικασία αναγνώρισης της κάρτας.

**5** Με την απάντηση επιβεβαίωσης της διαδικασίας αναγνώρισης από τον host προς την κάρτα, το chip της κάρτας μπορεί στη συνέχεια να περάσει σε επόμενα στάδια επεξεργασίας των δεδομένων της κάρτας.

#### 6.3.12.1. Δυνατότητες Κρυπτογράφησης των Smart Cards

Οι Smart Cards της τελευταίας τεχνολογίας έχουν επαρκείς ικανότητες κρυπτογράφησης, προκειμένου να υποστηρίξουν τις απαιτήσεις των περισσοτέρων εφαρμογών ασφάλειας και πρωτοκόλλων.

Οι υπογραφές και τα πιστοποιητικά του RSA (R.Rivest,A.Shamir & L.Adleman) αλγορίθμου υποστηρίζονται από «κλειδιά» μήκους 512, 768 και 1024 bits. Κατά ένα μεγάλο βαθμό, οι αλγόριθμοι αυτού του τύπου χρησιμοποιούν το θεώρημα CRT (Chinese Remainder Theorem – Κινέζικο Θεώρημα Υπολοίπου) ώστε να επιταχύνουν την όλη διαδικασία. Ακόμη και στην περίπτωση του κλειδιού των 1024 bits, ο απαιτούμενος χρόνος για την εκτέλεση μιας υπογραφής είναι περίπου λιγότερος από ένα (1) δευτερόλεπτο.

Συνήθως, το αρχείο της EEPROM που περιέχει το ιδιωτικό κλειδί, είναι σχεδιασμένο έτσι ώστε το ιδιαίτερα ευαίσθητο υλικό του κλειδιού να μην αφαιρείται ποτέ από το chip της κάρτας. Η χρήση του ιδιωτικού κλειδιού προστατεύεται από το PIN (Personal Identification Number) του κάθε χρήστη, έτσι ώστε να μην συνεπάγεται η δυνατότητα υπογραφής (ή πιστοποίησης) με την απλή κατοχή της κάρτας.

Παρότι οι Smart Cards έχουν την ικανότητα να παράγουν ζεύγη κλειδιών για τον αλγόριθμο RSA, η συγκεκριμένη διαδικασία είναι ιδιαίτερα χρονοβόρα (μέχρι και 10 δευτ/πτα). Επίσης, η ποιότητα των ζευγών κλειδιών πιθανόν να μην είναι η βέλτιστη. Η έλλειψη υπολογιστικής ισχύος συνεπάγεται μία σχετικά μικρής εμβέλειας πηγή τυχαίων αριθμών, καθώς και σχετικά ελλιπών αλγορίθμων για την επιλογή κυρίων αριθμών (prime numbers) .

Ο αλγόριθμος ψηφιακών υπογραφών (DSA-Digital Signature Algorithm) είναι λιγότερο εφαρμόσιμος από τον RSA. Κι όταν εφαρμόζεται, εφαρμόζεται μόνο σε «κλειδιά» μήκους 512 bits. Οι Smart Cards υποστηρίζουν τη δυνατότητα εφαρμογής πολλαπλών PIN, το καθένα από τα οποία χρησιμοποιείται για διαφορετικούς σκοπούς. Οι εφαρμογές μπορούν να ορίσουν ένα PIN ώστε να είναι PIN-υπεύθυνος ασφάλειας (Security Officer PIN), το οποίο θα χρησιμοποιείται για ξεκλείδωμα του κινητού μετά από μια σειρά απόδοσης λανθασμένων PIN ή για να επαναπροσδιορίσει τις λειτουργίες της κάρτας. Κάποια άλλα PIN μπορούν να οριστούν ώστε να ελέγχεται η πρόσβαση σε ευαίσθητα αρχεία ή σε διάφορες άλλες λειτουργίες ασφάλειας.

Οι DES και triple-DES (Data Encryption Standard) αλγόριθμοι κρυπτογράφησης, βρίσκονται στις περισσότερες Smart Cards. Συνήθως παρέχουν την επιλογή να χρησιμοποιηθούν σε μια λειτουργία MAC (Message Authentication Code Function). Εντούτοις, επειδή η σειριακή διασύνδεση μιας Smart Card έχει χαμηλό εύρος ζώνης, η μαζική συμμετρική κρυπτογράφηση είναι πολύ αργή. Λόγω του ότι είναι δύσκολο να εξαχθούν πληροφορίες για τα λειτουργικά συστήματα και τα αρχεία των chip, έχουν υπάρξει διάφορες μέθοδοι ελέγχου της ασφάλειας του υλικού (hardware security) στις περισσότερες Smart Cards. Οι κάρτες σχεδιάζονται με τρόπο τέτοιο ώστε να επανέρχονται σε μια συγκεκριμένη κατάσταση λειτουργίας εάν υπάρξουν απότομες διακυμάνσεις στην τάση, τη θερμοκρασία ή τη συχνότητα λειτουργίας του επεξεργαστή. Η ανάγνωση ή το γράψιμο της ROM συνήθως δεν υποστηρίζονται – εκ πρώτης όψεως. Ωστόσο, λόγω του ότι κάθε κατασκευαστής λειτουργεί με βάση τις δικές του προδιαγραφές, παροτρύνεται η έρευνα και αναζήτηση πληροφοριών από ανεξάρτητα εργαστήρια δοκιμών.

Οι λειτουργίες ηλεκτρονικών πορτοφολιών (electronic purse functions) συχνά υποστηρίζονται, αλλά βασίζονται σε τεχνολογίες συμμετρικού κλειδιού, όπως οι DES και triple-DES . Κατά συνέπεια, ένα κοινόχρηστο μυστικό κλειδί μπορεί κι επιβάλλει την ασφάλεια σε πολλά από αυτά τα πρότυπα.

Τις περισσότερες φορές, τα πρωτόκολλα επικοινωνιών των Smart Cards στο επίπεδο εντολών έχουν ενσωματωμένο πρωτόκολλο ασφάλειας. Αυτά κατά κύριο λόγο, βασίζονται στη τεχνολογία συμμετρικού κλειδιού και επιτρέπουν στην ίδια την κάρτα να επικυρώνει το τερματικό ανάγνωσης/εγγραφής ή και αντίστροφα. Εντούτοις, τα κρυπτογραφήματα και οι αλγόριθμοι για αυτά τα

πρωτόκολλα αφορούν συνήθως συγκεκριμένες εφαρμογές και δεδομένα σετ τερματικών.

## *6.4. Συσκευές ανάγνωσης Smart Cards (Smart Card Readers)*

Όλα τα τερματικά υποστήριξης Smart Cards – γνωστά και ως συσκευές ανάγνωσης ευφυών καρτών (Smart Card Readers) – έχουν εξ'ορισμού την δυνατότητα ανάγνωσης κι εγγραφής, όσο βέβαια το υποστηρίζουν και οι Smart Cards. Σε αντίθεση με τις Smart Cards, οι οποίες είναι σχεδόν κατασκευαστικά ίδιες, οι συσκευές ανάγνωσής τους ποικίλουν σε σχήμα και σε πολυπλοκότητα στο μηχανικό, στο λογικό και σε άλλα επίπεδα. Ορισμένα παραδείγματα συσκευών ανάγνωσης μιας Smart Card είναι: η συσκευή ανάγνωσης ενσωματωμένη στο εσωτερικό ενός αυτόματου πωλητή (vending machine), φορητή συσκευή ανάγνωσης υποστηριζόμενη από μπαταρία και οθόνη υγρών κρυστάλλων (LCD), συσκευή ανάγνωσης ενσωματωμένη σε κινητό τηλέφωνο, συσκευή ανάγνωσης συνδεδεμένη σε Η/Υ, κ.ά. .

Από μηχανικής πλευράς, οι συσκευές ανάγνωσης μπορούν να παρέχουν ένα πλήθος επιλογών. Κάποιες από αυτές: αν ο κάθε χρήστης πρέπει να εισάγει και να εξάγει την κάρτα ο ίδιος ή αν ο μηχανισμός αποδοχής και επιστροφής της κάρτας είναι αυτόματος, ευκολίες και δυνατότητες για την οθόνη διασύνδεσης χρήστη και δεδομένων της κάρτας, κ.ά. .

Όσο για τις ηλεκτρικές της προδιαγραφές, οι συσκευές ανάγνωσης οφείλουν να ακολουθούν τα όσα επιτάσσει το πρότυπο ISO/IEC 7816-3.

Μια αντιπροσωπευτική συσκευή ανάγνωσης Smart Card κοστίζει πάνω από 40.000 δρχ., ακριβότερη σε σύγκριση με τις συσκευές μέσω των οποίων γίνονται συναλλαγές με πιστωτικές κάρτες.

Οι επιλογές των συσκευών ανάγνωσης είναι πρακτικά απεριόριστες. Στη συνέχεια θα γίνει αναφορά σε συσκευές ανάγνωσης Smart Cards με δυνατότητα σύνδεσης σε Η/Υ, λόγω του ότι χρησιμοποιούνται ευρέως στην ασφάλεια υπολογιστών και δικτύων. Πολλοί τύποι συσκευών ανάγνωσης είναι διαθέσιμοι στη σημερινή αγορά. Στις Η.Π.Α. υπάρχουν πάνω από 14.000 συσκευές ανάγνωσης, σε αντίθεση με τις περισσότερες από 5.000.000 συσκευές, έχοντας τη δυνατότητα συναλλαγών με συμβατικές, πιστωτικές κάρτες.

Στο πίνακα που ακολουθεί περιγράφονται κάποιοι τύποι συσκευών ανάγνωσης Smart Cards, με τα βασικά πλεονεκτήματα και μειονεκτήματά τους.

| Τρόποι Σύνδεσης μιας συσκευής ανάγνωσης | Πλεονεκτήματα | Μειονεκτήματα |
|---|---|---|
| Σειριακή Θύρα | Οι πλέον διαδεδομένες . Ανθεκτικές και οικονομικές . Πλατφόρμα υποστήριξης για Windows , Mac και UNIX . | Πολλοί desktop υπολογιστές δεν έχουν ελεύθερες σειριακές θύρες . Απαιτείται μπαταρία ή διακόπτης εξωτερικής ισχύος . |
| PCMCIA | Ιδανικές για χρήστες που ενώ ταξιδεύουν , έχουν μαζί και φορητό Η/Υ . | Κοστίζουν περισσότερο . Πολλά συστήματα desktop δεν έχουν PCMCIA υποδοχές . |
| PS/2 (Θύρα Πληκτρολογίου) | Εύκολες στην εγκατάσταση με τη χρήση ειδικού προσαρμογέα . Παρέχουν προστασία στο PIN της κάρτας . | Χαμηλότερες ταχύτητες επικοινωνίας. |
| Floppy | Ιδιαίτερα εύκολες στην εγκατάσταση . | Απαιτείται μπαταρία . Αναξιόπιστες ως προς τις ταχύτητες επικοινωνίας . |
| USB | Ιδιαίτερα υψηλές ταχύτητες μεταφοράς δεδομένων . | Όχι ιδιαίτερα διαδεδομένες . Η χρήση κοινού διαύλου πιθανόν να προκαλεί θέματα ασφάλειας . |
| Ενσωματωμένη (Built-in) | Χωρίς απαίτηση εγκατάστασης υλικού ή λογισμικού . | Όχι ιδιαίτερα διαδεδομένες . |

**Πλεονεκτήματα και Μειονεκτήματα Τύπων Συσκευών Ανάγνωσης .**

Παγκοσμίως, υπάρχουν πάνω από 25 εταιρίες παραγωγής και προώθησης συσκευών ανάγνωσης για Smart Cards – Siemens, Fischer International, Utimaco , κ.ά. – και οι τιμές τους, αναμφίβολα, θα μειώνονται όσο αυξάνεται η ζήτηση τους. Κι αυτό είναι μια πραγματικότητα εφόσον εμπορικά καταστήματα, εστιατόρια και ένα πλήθος παροχέων κοινωνικών υπηρεσιών οφείλουν και θα αποκτήσουν μελλοντικά τέτοιες συσκευές.

## *6.5.* ***Εφαρμογές***

Στη σημερινή εποχή, οι Smart Cards καλύπτουν ένα ιδιαίτερα ευρύ φάσμα εφαρμογών. Πολλές από αυτές είναι η ασφάλεια των υπολογιστών, οι ασφαλείς ηλεκτρονικές συναλλαγές, οι τραπεζικές συναλλαγές, κ.ά.. Συγκεκριμένα, οι Smart Cards χρησιμοποιούνται ως τηλεφωνικές κάρτες, ως ηλεκτρονικά πορτοφόλια (electronic purses), ως κάρτες πρόσβασης σε ασφαλείς περιοχές, ως κάρτες SIM κινητών τηλεφώνων, ως κάρτες πληρωμής διοδίων και σε ένα σύνολο πολλών άλλων εξειδικευμένων εφαρμογών.

### *6.5.1. Η αξία των Smart Cards στην ασφάλεια των υπολογιστών*

Ζούμε σε μια ψηφιακή εποχή, στην οποία οι υπολογιστές και τα δίκτυα αποτελούν όλο και περισσότερο το κέντρο των εξελίξεων, με αποτέλεσμα η ανάγκη για ασφάλεια να γίνεται εντονότερη. Οι Smart Cards είναι η τεχνολογία μέσω της οποίας παρέχεται η προστασία και η ασφάλεια, την οποία δεν είναι σε θέση να παρέχουν άλλα μέσα επικοινωνίας και παροχής ασφάλειας.

Στο χώρο του Internet, με τις Smart Cards εξασφαλίζονται στο μέγιστο βαθμό η αυθεντικότητα, η πιστοποίηση, η ιδιωτικότητα, η ακεραιότητα και η διαθεσιμότητα. Κι αυτό διότι το ιδιωτικό κλειδί-πιστοποιητικό της κάρτας είναι αναπόσπαστο κομμάτι της και πολύ δύσκολα μπορεί να γνωστοποιηθεί σε χρήστες απλά συνδεδεμένους στο διαδίκτυο.

Σε περιπτώσεις όπου υπολογιστικά συστήματα διαφόρων τεχνολογιών ενσωματώνονται σε ένα ευρύτερο σύστημα, οι Smart Cards παρέχουν τη δυνατότητα εύκολης σχετικά σύνδεσης κι επικοινωνίας μεταξύ τους, αποθηκεύοντας πολλαπλά πιστοποιητικά και κωδικούς πρόσβασης σε μία μόνο κάρτα. Εφαρμογές όπως το e-mail, η πρόσβαση σε δίκτυα Intranet και σε dial-up συνδέσεις, η κρυπτογράφηση κι αποκρυπτογράφηση αρχείων και πολλές άλλες, βελτιώνονται αισθητά με τη χρήση των Smart Cards.

Σε περιπτώσεις Extranet δικτύων, όπου επιθυμείται από την εταιρία η ασφάλεια να διαχειρίζεται από τους επιχειρηματίες-συνεργάτες και τους προμηθευτές, οι δυνατότητες των Smart Cards μπορούν και «διανέμονται», παρέχοντας διάφορα δικαιώματα σε διάφορους φορείς. Η σημασία τους είναι προφανής λόγω του ότι απαιτείται η μέγιστη δυνατή ασφάλεια, όταν οποιοσδήποτε έχει τη δυνατότητα να ξεπεράσει τις αμυντικές τακτικές του Firewall και του Proxy. Διανέμοντας τις δυνατότητες μιας Smart Card, μια εταιρία εξασφαλίζει ότι οι παραπάνω δεν μπορούν να κοινοποιηθούν ή να αντιγραφούν.

Παρακάτω ακολουθούν κάποιοι λόγοι, στους οποίους έγκειται η αξία των Smart Cards στα σύγχρονα, σημερινά υπολογιστικά συστήματα:

- Η υποδομή δημοσίου κλειδιού (PKI-Public Key Infrastructure) παρέχει μεγαλύτερη ασφάλεια σε σύγκριση με τους απλούς κωδικούς πρόσβασης, διότι δεν υπάρχει δυνατότητα γνωστοποίησης του μυστικού κωδικού. Το ιδιωτικό κλειδί απαιτείται να είναι γνωστό σε ένα μόνο σημείο, ούτε καν δύο ή περισσότερα. Αν αυτό το ένα σημείο είναι πάνω σε μια Smart Card, το ιδιωτικό κλειδί δεν είναι δυνατό να χαθεί από τη κάρτα κι επομένως ο μυστικός κωδικός, για όποιο κι αν είναι το σύστημα, δεν είναι διαπραγματεύσιμος. Μια Smart Card επιτρέπει τη χρήση του ιδιωτικού κλειδιού, αλλά όχι τη γνωστοποίησή του σε ένα δίκτυο ή στον host computer ενός υπολογιστικού συστήματος.

- Παρότι οι Smart Cards έχουν προφανή πλεονεκτήματα στα συστήματα βασισμένα στο PKI, μπορούν επιπλέον να αυξήσουν την ασφάλεια σε συστήματα που στηρίζονται σε απλούς κωδικούς

πρόσβασης (passwords). Στα τελευταία από τα παραπάνω συστήματα, συνήθως οι χρήστες σημειώνουν πρόχειρα κάπου το password και το αφήνουν σε σημεία, στα οποία είναι εκτεθειμένο και σε άλλους χρήστες. Πολλές φορές μάλιστα, επιλέγουν «εύκολα» passwords, δίνοντάς τα σε άλλους. Χρησιμοποιώντας μια Smart Card η οποία συγκρατεί πολλαπλά passwords, απαιτείται η απομνημόνευση μόνο του κωδικού PIN της κάρτας προκειμένου ο χρήστης να έχει πρόσβαση σε όλους τους κωδικούς που φυλάσσονται στην κάρτα.

- Τα συστήματα ασφαλείας επωφελούνται περισσότερο όταν χρησιμοποιούνται πολλοί παράγοντες πιστοποίησης. Κοινά χρησιμοποιούμενοι παράγοντες είναι: Κάτι που ξέρεις, κάτι που έχεις, κάτι που είσαι και κάτι που κάνεις. Στα συστήματα βασισμένα σε passwords, χρησιμοποιείται συνήθως μόνο ο πρώτος παράγοντας. Οι Smart Cards χρησιμοποιούν και τον δεύτερο από τους παραπάνω παράγοντες, καθώς η πιστοποίηση με δύο παράγοντες έχει αποδειχθεί πιο αποτελεσματική. Κάποιες Smart Cards, μπορούν να έχουν τη δυνατότητα χρήσης και των τεσσάρων παραπάνω παραγόντων. Σε άλλες περιπτώσεις, τα δακτυλικά αποτυπώματα, το περίγραμμα του ανθρώπινου ματιού ή άλλα βιοχαρακτηριστικά, μπορούν να αποθηκεύονται ως πληροφορίες σε μια Smart Card, προκειμένου να συγκρίνονται με δεδομένα τα οποία εισέρχονται στην κάρτα μέσω μιας συσκευής ελέγχου βιοχαρακτηριστικών (biometrics input device). Παρομοίως, χαρακτηριστικά με χειρόγραφη υπογραφή ή περιγράμματα παραμορφωμένων ήχων, μπορούν να αποθηκευτούν στην κάρτα και να συγκριθούν με δεδομένα που μέσω εξωτερικών συσκευών εισόδου, γίνονται αποδεκτά από την κάρτα.

- Τα πιστοποιητικά δημοσίου κλειδιού και τα ιδιωτικά κλειδιά, μπορούν να χρησιμοποιηθούν από μηχανές πλοήγησης για το διαδίκτυο (web browsers) και από άλλα πακέτα λογισμικού, αλλά περισσότερο αναγνωρίζουν τον Η/Υ που βρίσκονται και όχι τους χρήστες του Η/Υ. Τα δεδομένα του κλειδιού και του πιστοποιητικού αποθηκεύονται σε κατάλληλο χώρο της μηχανής πλοήγησης και πρέπει να εισάγονται και να εξάγονται από τον ένα Η/Υ στον άλλο. Με τη χρήση των Smart Cards, το πιστοποιητικό και το ιδιωτικό κλειδί είναι μεταφέρσιμα, και μπορούν να χρησιμοποιηθούν σε πολλαπλά μηχανήματα, ανεξάρτητα από το αν αυτά είναι στο σπίτι, στη δουλειά ή στο δρόμο. Τέλος, όσο το λογισμικό το επιτρέπει, μπορούν να χρησιμοποιούνται από διαφορετικά προγράμματα, διαφορετικού κατασκευαστή και σε διαφορετική πλατφόρμα, όπως τα Windows, το Unix και το Mac.

- Όταν ένα ιδιωτικό κλειδί αποθηκεύεται σε ειδικά αρχεία μιας μηχανής πλοήγησης (browser) σε ένα σκληρό δίσκο, τυπικά προστατεύεται από έναν κωδικό πρόσβασης (password). Το συγκεκριμένο αρχείο όμως είναι δυνατόν να «δεχθεί επίθεση», δηλαδή χρησιμοποιώντας μία σειρά από passwords, αν βρεθεί το σωστό password, η τιμή του ιδιωτικού

κλειδιού μπορεί να γίνει γνωστή. Αντιθέτως, μια Smart Card, μετά από έναν μικρό σχετικά αριθμό αποτυχημένων προσπαθειών απόδοσης του σωστού PIN λειτουργίας της, «κλειδώνει». Για παράδειγμα, η ευφυής κάρτα GSM των κινητών τηλεφώνων, κλειδώνει μετά από τρεις (3) αποτυχημένες απόπειρες πληκτρολόγησης του σωστού PIN. Έτσι, η λήψη του ιδιωτικού κλειδιού, όταν αυτό βρίσκεται σε μια Smart Card, δεν θα είναι πλέον «αποδοτική».

- Η δυνατότητα κάποιος να αρνηθεί, εκ των υστέρων, ότι το ιδιωτικό του κλειδί εκτέλεσε μια ψηφιακή υπογραφή, λέγεται μη αποδοχή της πραγματικότητας (repudiation). Ωστόσο, αν το ιδιωτικό κλειδί ψηφιακών υπογραφών βρίσκεται σε μια Smart Card και ο κάτοχός της γνωρίζει απλώς το PIN της κάρτας, είναι πολύ δύσκολο για άλλους χρήστες προσποιούμενοι και χρησιμοποιώντας το ιδιωτικό του κλειδί, να οικειοποιηθούν την δική του ψηφιακή υπογραφή. Πιο ειδικά, οι Smart Cards παρέχουν τη δυνατότητα το ιδιωτικό κλειδί να φυλάσσεται σε συγκεκριμένη περιοχή ασφάλειας, η οποία προστατεύεται από ένα κουπόνι υλικού (hardware token) και να μη μπορεί να χρησιμοποιηθεί, χωρίς τη γνώση του κατάλληλου PIN.

- Σε πολλές από τις καθημερινές μας δραστηριότητες κι ενέργειες, βασιζόμαστε κι εξαρτόμαστε από το κύρος της χειρόγραφής μας υπογραφής. Οι ψηφιακές υπογραφές βασισμένες σε Smart Card υπερέχουν σε κύρος απέναντι στις κλασικές χειρόγραφες υπογραφές, διότι είναι αναμφίβολα πολύ δύσκολο να πλαστογραφηθούν και γενικότερα ενισχύουν την ακεραιότητα του εγγράφου απέναντι σε τεχνολογίες παραποίησης του. Επίσης, από τη στιγμή που η ψηφιακή υπογραφή βασίζεται ουσιαστικά σε έναν Η/Υ, μπορεί να γίνει προφανές ότι συνεπάγονται πολλά προνόμια. Για παράδειγμα, μια Smart Card θα μπορούσε να μετρήσει τις φορές που χρησιμοποιήθηκε το ιδιωτικό κλειδί, δίνοντας έτσι μια σαφή εικόνα χρήσης του ιδιωτικού κλειδιού για μία δεδομένη χρονική περίοδο.

### *6.5.2. Χρηματικές Συναλλαγές & Ηλεκτρονικό Εμπόριο*

Στις αρχές της δεκαετίας του 1980, κατασκευάστηκε για πρώτη φορά μια Smart Card προσανατολισμένη να εξυπηρετήσει τραπεζικούς σκοπούς, ως την πλέον ιδανική λύση απέναντι στο πρόβλημα της οικονομικής απάτης. Για παράδειγμα, σήμερα κυκλοφορούν πάνω από 30 εκατομμύρια τέτοιες κάρτες στη Γαλλία, ενώ και οι περισσότερες ευρωπαϊκές χώρες όλο και πιο πολύ υιοθετούν την τεχνολογία ασφάλειας των Smart Cards απέναντι στις κλασικές – και ίσως ξεπερασμένες – πλαστικές τραπεζικές κάρτες.

Μία άλλη καινοτομία στο χώρο των ηλεκτρονικών συναλλαγών αποτελούν τα ηλεκτρονικά πορτοφόλια . Ένα ηλεκτρονικό πορτοφόλι είναι μια Smart Card η οποία θα αντικαθιστά τα χρήματα τα οποία μέχρι σήμερα είχαμε στις τσέπες και τα πορτοφόλια μας και η οποία θα παρέχει έναν πολύ απλό τρόπο

πληρωμής μέσω της κάρτας . Ο κάτοχος της κάρτας θα μπορεί να «γεμίζει» την κάρτα του με χρήματα μέσω ενός Α.Τ.Μ. ή και μέσω τηλεφώνου.

Στον τομέα του ηλεκτρονικού εμπορίου, η Bull κατέχει την πρωτοπορία στο ότι βασισμένη σε Smart Cards καθιέρωσε ένα υψηλής ασφάλειας σύστημα ηλεκτρονικών πληρωμών για το Internet. Συγκεκριμένα, εξασφαλίζει την ακεραιότητα στη συναλλαγή μεταξύ του χρήστη και του παροχέα υπηρεσιών (user-server transaction) και προσαρμόζεται στις εκάστοτε συνθήκες πρόσβασης και πιστοποίησης (πρωτόκολλα πληρωμής, τύπος της κάρτας, κ.τ.λ.).

### *6.5.3. Παροχή Υπηρεσιών Υγείας*

Οι Smart Cards, πέρα από την χρήση τους σε εφαρμογές ασφάλειας και ηλεκτρονικού εμπορίου, χρησιμοποιούνται και για τη μεταφορά σημαντικών ιατρικών πληροφοριών. Πέρα από το να υποδεικνύουν απλώς ότι ένα άτομο είναι ιατρικώς ασφαλισμένο, μπορούν για παράδειγμα να περιέχουν λεπτομέρειες σχετικές με την ασφαλιστική κάλυψη του κάθε ατόμου. Μπορούν επίσης να παρέχουν κάποιες βασικές ιατρικές πληροφορίες για το άτομο, όπως ευαισθησίες και αντενδείξεις για συγκεκριμένα φάρμακα, το ιατρικό ιστορικό του ατόμου (εισαγωγές σε κλινικές, εγχειρήσεις, κ.ά.), τη διεύθυνση και το τηλέφωνο επικοινωνίας με τον προσωπικό γιατρό του κάθε ατόμου κι άλλες πληροφορίες άκρως σημαντικές σε περιπτώσεις ανάγκης. Αναμφίβολα, μια Smart Card μπορεί να διευκολύνει τον τρόπο με τον οποίο παρέχονται ιατρικές υπηρεσίες σε κάποιον, διατηρώντας παράλληλα την ιδιωτικότητα των δεδομένων που βρίσκονται στην κάρτα του κάθε ατόμου .

Αυτοματοποιώντας τη διαδικασία εισαγωγής του ονόματος του ασθενούς και ενός αριθμού (προσωπικός λογαριασμός του ασθενούς) σε ειδικές ιατρικές φόρμες, η όλη ασφαλιστική διαδικασία γίνεται πιο γρήγορα και πιο αποδοτικά. Ήδη, το συγκεκριμένο σύστημα εφαρμόζεται σε κάποιες χώρες της Ευρώπης (Γερμανία, Γαλλία, κ.ά.) .

Στη Γαλλία και την Ιαπωνία, οι νεφροπαθείς μεταφέρουν κάρτες οι οποίες περιέχουν πληροφορίες σχετικά με τη πορεία της πάθησής τους και τον τρόπο θεραπείας της πάθησης. Πιο συγκεκριμένα, με τη χρήση των Smart Cards, παρέχεται η δυνατότητα εξυπηρέτησης των ασθενών ανεξάρτητα από το ιατρικό κέντρο, κάτι το οποίο πριν την εξέλιξη των Smart Cards δεν ήταν δυνατό. Όσο για την ασφάλεια των δεδομένων της κάρτας, με κατάλληλο έλεγχο εξασφαλίζεται ότι μόνο γιατροί ή εξουσιοδοτημένα άτομα έχουν δυνατότητα ανάγνωσης κι ενημέρωσης των στοιχείων της κάρτας.

### *6.5.4. Άλλες Εφαρμογές των Smart Cards*

Το GSM (Global Standard for Mobile communications), τεχνολογία που χρησιμοποιείται από ευρωπαϊκές εταιρίες κατασκευής κινητών τηλεφώνων, χρησιμοποιεί Smart Card ως ταυτότητα χρήστη. Συγκεκριμένα, όλα τα GSM κινητά τηλέφωνα αποτελούνται από μια Smart Card, η οποία βασίζεται και υλοποιεί τις διαδικασίες του SIM (Subscriber Identity Module). Το SIM Tool Kit (STK) αποτελεί ένα σετ εργαλείων για ανάπτυξη εφαρμογών πάνω στην

κάρτα SIM, για κινητά της τεχνολογίας GSM. Τα εργαλεία αυτά ορίζουν τον τρόπο με τον οποίο οι εφαρμογές της κάρτας SIM επικοινωνούν με το πληκτρολόγιο και την οθόνη του κινητού τηλεφώνου, παρέχοντας ένα πλήθος δυνατοτήτων και υπηρεσιών. Παράδειγμα χρήσης του STK, αποτελεί το τηλέφωνο με κάρτα Barclay (Barclaycard phone) το οποίο χρησιμοποιείται ως τερματικό τραπεζικών συναλλαγών.

Επιπλέον, οι Smart Cards συνδέονται και με το WAP (Wireless Application Protocol). Το συγκεκριμένο πρωτόκολλο εμφανίστηκε για πρώτη φορά τον Απρίλιο του 1998 (WAP version 1.0). Ενσωματώνοντας το 1999 για πρώτη φορά Smart Cards στις εφαρμογές του WAP, παρέχονται στα κινητά με WAP, δυνατότητες για πληρωμές, διαχείριση ασφάλειας, κ.ά. .

Συμπερασματικά, οι Smart Cards αποτελούν και θα αποτελέσουν έναν από τους βασικότερους φορείς και παράγοντες για την διάδοση της τεχνολογίας και των υπηρεσιών των GSM κινητών τηλεφώνων.

## 6.6. *Ειδικές Εφαρμογές Ασφάλειας*

Στο συγκεκριμένο κομμάτι γίνεται αναφορά σε κάποια προϊόντα ασφάλειας κι εξηγείται το πώς οι Smart Cards, αν χρησιμοποιηθούν, συμβάλλουν στο να αυξηθεί η ασφάλεια των συγκεκριμένων προϊόντων.

- **Μηχανές Πλοήγησης Διαδικτύου (Web Browsers)**

Οι διάφορες Μηχανές Πλοήγησης Διαδικτύου χρησιμοποιούν τεχνολογίες όπως το SSL (Secure Socket Layer) και το TLS (Transport Layer Security) ώστε να παρέχεται ασφάλεια κατά την πλοήγηση στο Internet. Οι συγκεκριμένες τεχνολογίες μπορούν και πιστοποιούν την ταυτότητα μεταξύ πελάτη και παροχέα υπηρεσιών (client-server authentication) κι επιπλέον παρέχουν ένα κρυπτογραφημένο κανάλι για τη μεταφορά μηνυμάτων και αρχείων γενικότερα. Η σημασία των Smart Cards έγκειται στο ότι η πιστοποίηση ενισχύεται λόγω του ότι το ιδιωτικό κλειδί βρίσκεται αποθηκευμένο με ασφάλεια στην κάρτα. Το κρυπτογραφημένο κανάλι χρησιμοποιεί συνήθως έναν ειδικό αλγόριθμο κρυπτογράφησης, σύμφωνα με τον οποίο η κρυπτογράφηση εκτελείται στον host computer εξαιτίας των χαμηλών ταχυτήτων μεταφοράς δεδομένων από και προς την κάρτα. Παρόλ' αυτά, τα τυχαία παραγόμενα κλειδιά για την κρυπτογράφηση «κλειδώνουν» πάνω στο δημόσιο κλειδί του συνδιαλεγόμενου υπολογιστή (partner computer), κάτι που σημαίνει ότι το «ξεκλείδωμα» των κλειδιών και του δημοσίου κλειδιού γίνεται πάντα πάνω στην κάρτα. Με αυτόν τον τρόπο, καθίσταται ιδιαίτερα δύσκολο για κάποιον τρίτο υπολογιστή να επέμβει και να αποκτήσει γνώση των κλειδιών και των αρχείων που μεταφέρονται.

- **Ασφαλής Ηλεκτρονική Αλληλογραφία (Secure E-mail)**

Το S/MIME και το OpenPGP είναι δύο τεχνολογίες που παρέχουν στην ηλεκτρονική αλληλογραφία δυνατότητες κρυπτογράφησης κι επισύναψης ψηφιακής υπογραφής. Με τη χρήση των Smart Cards ενισχύεται η ασφάλεια των συγκεκριμένων λειτουργιών, προστατεύοντας τη μυστικότητα του

ιδιωτικού κλειδιού και περιορίζοντας το πεδίο δράσης των κλειδιών που απαιτούνται κατά την κρυπτογράφηση και αποκρυπτογράφηση.

- **Υπογραφή Ηλεκτρονικών Φορμών (Form Signing)**

Οι φόρμες της HTML (Hyper Text Mark-up Language – γλώσσα προγραμματισμού για σχεδίαση Internet σελίδων) μπορούν να υπογραφούν ψηφιακά από το ιδιωτικό κλειδί του κάθε χρήστη. Η συγκεκριμένη δυνατότητα αποτελεί σημαντικό πλεονέκτημα για εταιρίες και υπηρεσίες βασισμένες στο Internet, καθώς επιτρέπει σε ψηφιακά έγγραφα να παραμένουν και να διαχειρίζονται στους/από τους servers με σχετικά «εύκολο» τρόπο – για παράδειγμα, αιτήσεις ηλεκτρονικών αγορών και οι φόρμες αίτησης παροχής υπηρεσιών ηλεκτρονικού ταχυδρομείου (e-mail). Οι Smart Cards στη συγκεκριμένη περίπτωση, παρέχουν δυνατότητα μεταφοράς του ιδιωτικού κλειδιού και όσα αυτό συνεπάγεται για περιπτώσεις πιστοποίησης του χρήστη κι εφαρμογών ασφάλειας.

- **Ηλεκτρονική Πιστοποίηση Αντικειμένων (Object Signing)**

Όταν ένας οργανισμός γράφει κώδικα τον οποίο κάποιος μπορεί να «κατεβάσει» από το Internet και στη συνέχεια να τον εκτελέσει στον Η/Υ του, θα ήταν επιθυμητό αυτός ο κώδικας να έχει προηγουμένως πιστοποιηθεί, ώστε οι μελλοντικοί χρήστες του να είναι βέβαιοι ότι προέρχεται από ευυπόληπτη πηγή. Στην περίπτωση αυτή, οι Smart Cards θα μπορούσαν να χρησιμοποιηθούν από την φερόμενη εταιρία πιστοποίησης ώστε το ιδιωτικό κλειδί να μην αποτελέσει αντικείμενο προς συναλλαγή, με εταιρίες κακόβουλων προθέσεων.

- **Η/Υ & Ηλεκτρονικά Περίπτερα (Kiosk/Portable Preferences)**

Υπάρχει ένα πλήθος εφαρμογών, οι οποίες λειτουργούν καλύτερα όταν βρίσκονται σε περιβάλλον «ηλεκτρονικού περίπτερου» (kiosk mode), όπου πολλοί χρήστες χρησιμοποιούν τον ίδιο Η/Υ. Εισάγοντας ο κάθε χρήστης τη δική του Smart Card, έχει τη δυνατότητα να ρυθμίζει τον Η/Υ ανάλογα με τις δικές του προτιμήσεις. Το μηχάνημα στην περίπτωση αυτή, μπορεί να χρησιμοποιηθεί για εφαρμογές όπως το Secure E-mail, πλοήγηση στο διαδίκτυο, κ.ά., χωρίς ποτέ το ιδιωτικό κλειδί της κάρτας του κάθε χρήστη να γίνεται γνωστό σε χρήστες που χρησιμοποιούν τον ίδιο Η/Υ. Επιπλέον, το μηχάνημα μπορεί να ρυθμιστεί έτσι ώστε να μη γίνεται εισαγωγή δεδομένων από το πληκτρολόγιο ή το ποντίκι, ωσότου κάποιος εξουσιοδοτημένος χρήστης να εισάγει μια Smart Card και να πληκτρολογήσει το σωστό PIN.

- **Logon σε Η/Υ (Workstation Logon)**

Τα απαιτούμενα διαπιστευτήρια για τη διαδικασία του logon σε έναν Η/Υ θα μπορούν να αποθηκεύονται με ασφάλεια σε μια Smart Card. Ο συνήθης μηχανισμός, όπου σε μια γραμμή εντολών ζητείται το username και το

password του κάθε χρήστη, είναι δυνατόν να αντικαθίσταται από την απλή εισαγωγή της κάρτας στον Η/Υ.

- **Πρόσβαση μέσω τηλεφώνου (Dial-up Access)**

Πολλά από τα πρωτόκολλα απομακρυσμένης πρόσβασης μέσω τηλεφώνου (RAS, PPTP, RADIUS, TACACS), χρησιμοποιούν passwords ως μηχανισμό ασφάλειας. Όπως έχει ειπωθεί στις προηγούμενες σελίδες, οι Smart Cards είναι μια τεχνολογία η οποία ενισχύει την ασφάλεια των passwords. Επίσης, τα περισσότερα από τα παραπάνω πρωτόκολλα εξελίσσονται ώστε να υποστηρίζουν συστήματα βασισμένα στο δημόσιο κλειδί (PKI). Στην εξέλιξη αυτή, οι Smart Cards έχουν καταλυτική συνεισφορά διότι ενισχύουν την ασφάλεια και τη δυνατότητα μεταφοράς του ιδιωτικού κλειδιού κι άλλων πιστοποιητικών.

- **Πρωτόκολλα Ηλεκτρονικών Πληρωμών (Payment Protocols)**

Το SET (Secure Electronic Transactions) είναι πρωτόκολλο που παρέχει τη δυνατότητα ασφαλούς μεταφοράς των δεδομένων της πιστωτικής κάρτας , από τον κάτοχό της σε οικονομικούς φορείς και παροχείς υπηρεσιών του διαδικτύου . Λόγω του ότι το συγκεκριμένο πρωτόκολλο βασίζεται στην τεχνολογία του PKI , οι Smart Cards αποτελούν πολύ καλή επιλογή για την αποθήκευση και φύλαξη του ιδιωτικού κλειδιού και άλλων πιστοποιητικών .

- **«Ηλεκτρονικά Μετρητά» (Digital Cash)**

Για κάποια συστήματα, οι Smart Cards μπορούν να υλοποιήσουν πρωτόκολλα και συγχρόνως να αποτελούν τα «ηλεκτρονικά» μας πορτοφόλια. Σε τέτοιες περιπτώσεις, η αρχιτεκτονική των συστημάτων προστατεύεται από κλειδιά, τα οποία είναι περιορισμένα σε ένα χώρο εξ'αρχής ορισμένο από τις συσκευές υλικού. Τα Mondex, VisaCash, EMV (Europay-Mastercard-Visa) και Proton αποτελούν παραδείγματα πρωτοκόλλων για συναλλαγές με ηλεκτρονικά μετρητά που σχεδιάστηκαν να λειτουργούν βασισμένα στην τεχνολογία των Smart Cards.

- **Ασφαλή Πρόσβαση σε Κτιριακές Εγκαταστάσεις (Building Access)**

Παρότι ο χρόνος εισαγωγής, επεξεργασίας δεδομένων και αφαίρεσης μιας Smart Card μοιάζει μπελάς όταν πρόκειται να γίνει έλεγχος της εισόδου σε κτιριακές εγκαταστάσεις, η τεχνολογία της προσθήκης μιας μαγνητικής ταινίας ή ενός chip, παρέχει μέσω ενός απλού τεκμηρίου (token) ασφάλεια συστήματος και φυσικής πρόσβασης.

## 6.7. *«Επίθεση» σε Smart Cards*

Λέγοντας «επίθεση» σε Smart Cards – και σε υπολογιστικά συστήματα γενικότερα – εννοούμε κάθε απόπειρα από ανεπιθύμητους, «ξένους» χρήστες να αποκτήσουν πληροφορίες κρίσιμες για τη λειτουργία του υπολογιστικού συστήματος και για τη σωστή απόδοση υπηρεσιών από τον παροχεά υπηρεσιών του συστήματος. Συγκεκριμένα, οι επιθέσεις σε Smart Cards χωρίζονται σε τέσσερις (4) κατηγορίες:

- **Λογικές Επιθέσεις (Logical Attacks)**

Μια λογική επίθεση υφίσταται όταν μια Smart Card λειτουργεί υπό κανονικές συνθήκες, αλλά ευαίσθητες πληροφορίες απορρέουν από την κάρτα εξετάζοντας ένα-ένα τα bytes που έρχονται και φεύγουν στην και από την κάρτα. Παράδειγμα αυτής της επίθεσης, είναι η “timing attack”. Συγκεκριμένα, σύμφωνα με τον Paul Kocher, η επίθεση ξεκινά όταν διάφορα τμήματα από bytes στέλνονται στη κάρτα να υπογραφούν από το ιδιωτικό κλειδί. Πληροφορίες όπως ο απαιτούμενος χρόνος εκτέλεσης της λειτουργίας και τα ‘0’- ‘1’ των bytes εισόδου, χρησιμοποιούνται για την απόκτηση του ιδιωτικού κλειδιού. Υπάρχουν τρόποι αντιμετώπισης της συγκεκριμένης επίθεσης, ωστόσο λίγοι κατασκευαστές Smart Cards τους υλοποιούν.

- **Φυσικές Επιθέσεις (Physical Attacks)**

Μια φυσική επίθεση υφίσταται όταν φυσικοί παράγοντες, όπως η θερμοκρασία, η τάση του ρεύματος, κ.ά., μεταβάλλονται ώστε να επιτευχθεί πρόσβαση σε ευαίσθητες πληροφορίες της κάρτας. Τα περισσότερα λειτουργικά συστήματα για Smart Cards, γράφουν ευαίσθητα δεδομένα στην EEPROM κρυπτογραφημένα έτσι ώστε να είναι δύσκολο να αποκτηθούν λέξεις-κλειδιά με απευθείας εισβολή στην περιοχή της EEPROM. Φυσικές επιθέσεις που πραγματοποιούνται με επιτυχία είναι κι αυτές όπου παρεμβάλεται μια εντατική, φυσική διακύμανση στην ακριβή ώρα και τοποθεσία κατά την πιστοποίηση του PIN της κάρτας. Με αυτόν τον τρόπο, ευαίσθητες λειτουργίες εκτελούνται ακόμη κι όταν το PIN της κάρτας δεν είναι γνωστό. Ο συγκεκριμένος τύπος επίθεσης, σε συνδυασμό με τις λογικές επιθέσεις – όπως αναφέρθηκαν παραπάνω – είναι εφικτό να αποδώσει την τιμή του ιδιωτικού κλειδιού. Γενικά πάντως, οι περισσότερες φυσικές επιθέσεις απαιτούν ειδικό εξοπλισμό.

- **Επιθέσεις «Δούρειων Ίππων» (Trojan Horse Attacks)**

Ο συγκεκριμένος τύπος επίθεσης περιλαμβάνει μια «ύπουλη», εφαρμογή Δούρειου Ίππου, η οποία βρίσκεται εμφωλευμένη στον Η/Υ ενός ανυποψίαστου χρήστη. Ο Δούρειος Ίππος περιμένει μέχρι ο χρήστης να υποβάλλει ένα PIN από μια έμπιστη εφαρμογή – παρέχοντας τη δυνατότητα χρήσης του ιδιωτικού κλειδιού – και στη συνέχεια ζητά από την Smart Card να υπογράψει ψηφιακά κάποια «ύπουλα» δεδομένα. Η διαδικασία ολοκληρώνεται, αλλά ο χρήστης δεν πρόκειται να μάθει ότι το ιδιωτικό του κλειδί έχει χρησιμοποιηθεί χωρίς την έγκρισή του. Η αρχιτεκτονική

μονόδρομης πρόσβασης στον οδηγό μιας συσκευής (single-access device driver) αποτελεί ένα από τα αποτρεπτικά μέτρα για τον συγκεκριμένο τύπο επίθεσης. Με βάση την παραπάνω αρχιτεκτονική, το λειτουργικό σύστημα επιβάλλει ότι μόνο μία εφαρμογή μπορεί να έχει πρόσβαση σε μια σειριακά συνδεδεμένη συσκευή κι επομένως και για τις Smart Cards. Με αυτόν τον τρόπο, αποτρέπεται η επίθεση αλλά επιπλέον μειώνεται και η ευχρηστία της κάρτας, διότι πολλαπλές εφαρμογές δεν είναι δυνατόν να επωφεληθούν από την κάρτα την ίδια χρονική στιγμή. Ένας ακόμη τρόπος να αποτραπεί ο συγκεκριμένος τύπος επίθεσης είναι χρησιμοποιώντας μια Smart Card η οποία θα επιτρέπει τη χρήση ενός μόνο ιδιωτικού κλειδιού ανά μία εισαγωγή του PIN ("one private key usage per PIN entry" policy model). Με βάση το συγκεκριμένο μοντέλο, ο χρήστης πρέπει να εισάγει το PIN κάθε φορά που απαιτείται η λήψη του ιδιωτικού κλειδιού, οπότε ο Δούρειος Ίππος δεν θα έχει πρόσβαση στο κλειδί.

- **Επιθέσεις Εξαρτημένες από Ανθρώπινη Συμπεριφορά (Social Engineering Attacks)**

Οι επιθέσεις αυτού του είδους προκαλούνται, συνήθως, από ανθρώπινα λάθη. Για παράδειγμα, όταν ένας hacker προσποιείται τον τεχνικό υπηρεσιών δικτύου. Ο υποτιθέμενος τεχνικός προσεγγίζει με διπλωματικό τρόπο έναν χαμηλόβαθμο υπάλληλο και του ζητά κωδικούς πρόσβασης για σκοπούς επισκευής βλαβών του δικτύου. Απ' την άλλη πλευρά, χρησιμοποιώντας Smart Cards ο συγκεκριμένος τύπος επίθεσης δεν είναι πλέον «αποδοτικός», καθώς οι περισσότεροι κάτοχοι μιας Smart Card δεν θα εμπιστεύονταν εύκολα την κάρτα και το PIN της σε κάποιον, προσποιούμενο τον τεχνικό δικτύου.

Εν κατακλείδι, κανένα σύστημα ασφάλειας, συμπεριλαμβανομένων και των Smart Cards, δεν είναι ανίκητο. Ωστόσο, μπορεί συνήθως να γίνει μια εκτίμηση του κόστους που απαιτείται για την υπέρβαση της ασφάλειας και την εισβολή σε ένα σύστημα, σύμφωνα με την οποία το κόστος αυτό ξεπερνά κατά πολύ την αξία των δεδομένων που προστατεύονται από το σύστημα. Κάποια ανεξάρτητα εργαστήρια εξετάζουν την παρούσα χρονική στιγμή συνήθεις μεθόδους επίθεσης σε Smart Cards, παρέχοντας μια σχετική εκτίμηση για το κόστος και τις γνώσεις που απαιτούνται για μια «πετυχημένη» επίθεση.

### *6.7.1. Πλεονεκτήματα και Μειονεκτήματα των Smart Card*

Με βάση τα όσα έχουν προειπωθεί κι έχοντας μια σφαιρική άποψη της παγκόσμιας αγοράς των Η/Υ και των τεχνολογιών ασφάλειας, είναι δυνατό να διατυπωθούν με συνοπτικό τρόπο κάποια από τα πλεονεκτήματα και τα μειονεκτήματα της τεχνολογίας των Smart Cards.

6.7.1.1. Πλεονεκτήματα

- Μεγάλη ανθεκτικότητα της κάρτας και μικρότερη πιθανότητα καταστροφής του chip.
- Παρέχουν υψηλή ασφάλεια ως αποθηκευτικά μέσα ευαίσθητών δεδομένων.

- Παρέχουν υψηλή ασφάλεια κατά τη διάρκεια λειτουργιών κρυπτογράφησης.
- Γρήγορη αναγνώριση και πιστοποίηση χρήστη (απαιτείται μόνο το PIN).
- Βελτιστοποίηση της ασφάλειας των χρηστών (κλείδωμα με τη κατοχή και διατήρηση της κάρτας).
- Δυνατότητα για αυτόματη είσοδο σε servers και hosts.
- Δυνατότητα για χρήση σε πολυεφαρμογές (κάρτες πρόσβασης, χρονική καταγραφή , κ.ά.) .
- Όροι χρήσης , προσωπικές ρυθμίσεις (profiles), κλειδιά και άλλα πιστοποιητικά ασφάλειας συνοδεύουν πάντα τον χρήστη (καλύτερη υποστήριξη των χρηστών που ταξιδεύουν) .

6.7.1.2. Μειονεκτήματα

- Απαιτείται ειδικό υλικό για την ανάγνωση των καρτών.
- Υφίσταται η πιθανότητα απώλειας της κάρτας.
- Απαιτείται αρχιτεκτονική υψηλής ασφάλειας (υψηλό κόστος κατασκευής της κάρτας).
- Ενημέρωση της κάρτας μόνο σε ειδικά τεχνολογικά κέντρα, μέσω εξειδικευμένων διαδικασιών.
- Αδυναμία παροχής πρότυπης αρχιτεκτονικής και υποδομής για τις συσκευές ανάγνωσης των Smart Cards.
- Η κατασκευή συσκευών ανάγνωσης ενσωματωμένων σε Η/Υ συνεπάγεται μεγάλη οικονομική επιβάρυνση για τις κατασκευάστριες εταιρίες.
- Δεν έχει υιοθετηθεί κοινή βάση και κοινές προδιαγραφές από την παγκόσμια βιομηχανία των Η/Υ γύρω από την τεχνολογία των Smart Cards .

## *6.8. Περίπτωση χρήσης: Επιλέγοντας Smart Cards*

Στο συγκεκριμένο εδάφιο, παρουσιάζεται το εξής σενάριο: ως ειδικοί ασφάλειας υπολογιστών, αναλαμβάνουμε εκ μέρους μιας μεγάλης εταιρίας και με τη χρήση της τεχνολογίας των Smart Cards, να προστατεύσουμε το υπολογιστικό σύστημα – δίκτυο της εταιρίας.

Η χρήση των Smart Cards σε αυτή την περίπτωση, θα συνεπάγεται τα εξής:

Κάθε υπολογιστής του δικτύου της εταιρίας θα περιλαμβάνει εκτός των άλλων, έναν Smart Card Reader. Η συσκευή ανάγνωσης κάθε Η/Υ, θα οφείλει απλώς την αναγνώριση της κάρτας μέσω ενός κωδικού (PIN). Κάθε χρήστης-υπάλληλος της εταιρίας θα έχει την ξεχωριστή, δική του κάρτα, ενώ το PIN της κάθε κάρτας θα αποδίδεται με μοναδικό τρόπο, ώστε να μην υπάρχει άλλη με

το ίδιο PIN. Η έκδοση μιας κάρτας για κάποιο χρήστη, θα επιβάλλει αυτομάτως την ενημέρωση της συσκευής ανάγνωσης του Η/Υ του εκάστοτε χρήστη, προκειμένου η αντιστοιχία κάρτας – συσκευής ανάγνωσης να είναι μοναδική.

Επιπλέον, η κάρτα για κάθε χρήστη θα αποτελεί και μέσο πρόσβασης στα γραφεία της εταιρίας. Συγκεκριμένα, σε όλους τους χώρους εκτός των χώρων υποδοχής κοινού, θα επιτρέπεται πρόσβαση μόνο με την κατοχή της κάρτας. Μια συσκευή ανάγνωσης θα «διαβάζει» κάποιον κωδικό-PIN στη κάρτα, και σύμφωνα με την τιμή του θα επιτρέπεται η πρόσβαση. Επίσης, η κάρτα του κάθε χρήστη θα μπορεί να χρησιμοποιείται και ως «κλειδί» για το προσωπικό γραμματοκιβώτιο του κάθε υπαλλήλου ή και ως κάρτα ελεύθερης στάθμευσης στους χώρους στάθμευσης αυτοκινήτων της εταιρίας.

Η όλη διαδικασία θα ελέγχεται μέσω ενός κεντρικού Η/Υ, ο οποίος θα ανήκει στον διαχειριστή δικτύου της εταιρίας και ο οποίος με την κάρτα του θα έχει δικαίωμα πρόσβασης σε κάθε Η/Υ ή χώρο της εταιρίας . Η απώλεια της κάρτας του κάθε χρήστη θα επιβάλλει την αντικατάστασή της με μία νέα και ό,τι επιπλέον αυτό συνεπάγεται .

# 7. ΣΥΜΠΕΡΑΣΜΑΤΑ

**ΔΕΝ ΥΠΆΡΧΕΙ ΑΠΟΛΥΤΗ ΑΣΦΑΛΕΙΑ**

Κανένας κώδικας δεν μπορεί να χαρακτηριστεί απολύτως ασφαλείς και δεν υπάρχει πρόγραμμα που οι χρήστες θα έπρεπε να εμπιστεύονται 100%.Εχοντας ένα εκτελέσιμο ,μια ακολουθία από 0 και 1 δεν είναι γνωστό τι άλλο κάνει πέρα από αυτό που ισχυρίζονται τα έγγραφα που το συνοδεύουν. Ο κώδικας πιθανών να περιέχει μια κρυφή πίσω πόρτα, μια εντολή π.χ που όταν ο χρήστης κάνει login να στέλνει τα στοιχεία του λογαριασμού του σε έναν τρίτο. Έτσι ποια θα ήταν η λύση; Να φτιάξει ο χρήστης τον δικό του κώδικα από την αρχή, κάτι πάρα πολύ δύσκολο και ακραίο. Όμως ο χρήστης θα είναι σίγουρος ότι έχει γράψει σωστά τον κώδικα και χωρίς να αφήσει κάποια κενά που θα εκμεταλλευτεί κάποιος αργότερα; Η απάντηση είναι όχι!

Πάντα θα υπάρχει ο κίνδυνος παραβίασης του λειτουργικού συστήματος από κάποιους hackers που θα προσπαθούν να εκμεταλλευτούν το ‘αδύνατο σημείο του φράχτη’ και να παρεισφρήσουν στο σύστημα. Οι χρήστες το καλύτερο που έχουν να κάνουν είναι να κρατάνε άμυνα με τα μέσα ασφαλείας που διαθέτουν γιατί στην συντριπτική πλειοψηφία των περιπτώσεων οι επιτιθέμενοι είναι ένα βήμα μπροστά από τους αμυνόμενους.

Αυτό που περιγράφεται παραπάνω είναι μια κατάσταση πολιορκίας και μπορεί να φαντάζει υπερβολική όμως δυστυχώς τα πράγματα είναι έτσι. Είναι στο χέρι κάθε χρήστη να επιλέξει την ασφάλεια του ώστε να μην νοιώθει διαρκώς απειλημένος…μέχρι την επόμενη επίθεση που θα δεχθει!!!

# 8. ΒΙΒΛΙΟΓΡΑΦΙΑ


1)Δίκτυα Υπολογιστών, Tanenbaum, Παπασωτηρίου (Τρίτη έκδοση-2000)

2) Ασφάλεια Πληροφοριών,Ernst & Young (Πρώτη ¨Εκδοση-1995)

3) Maximum Security, Ανώνυμος,Μ.Γκιούρδας

4) Ασφάλεια Δικτύων, Michael A.Banks, -Μ.Γκιούρδας

5)Πώς να αισθάνονται οι χρήστες ασφαλείς,


## URLs


**1**.http://www.cert.org/homeusers/HomeComputerSecurity/#intro

**2**.http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html

**3.**http://socrates.berkeley.edu:4201/bcc/Winter2003/feat.windowssecurity.html

**4**.http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/smrtcard/default.asp

**5**.http://www.smartcard.co.uk/articles/intro2sc.html

**6**.http://java.sun.com/products/javacard/smartcards.html

**7**.http://www.usenix.org/publications/library/proceedings/smartcard99/full_papers/messerges/messerges_html/

**8**.http://www.ctst.com/smartcards.html

**9**.http://www.smartcard-solutions.com/pages/other/learn.html

**10**.http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smcdtech.asp

**11**.http://visaeu.com/smartcards/main.html

**12**.http://www.compinfo-center.com/tpsmrt-t.htm

**13**.http://www2.rad.com/networks/1998/proxy/proxy.htm

**14**.http://www.securityfocus.com/microsoft

## ΑΚΡΩΝΥΜΙΑ ΘΕΜΑΤΟΣ

**LAN**-Local Area Network (Τοπικό Δίκτυο)

**UDP**-User Datagram Protocol (Πρωτόκολλο Δεδομενογραφημάτων Χρήστη)

**TCP**-Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μεταφοράς)

**ICMP**-Internet Control Message Protocol (Πρωτόκολλο Μηνυμάτων Ελέγχου Internet)

**HTTP**-HyperText Transfer Protocol (Πρωτόκολλο Μεταφοράς)

**FTP**-File Transfer Protocol (Πρωτόκολλο Μεταφοράς Αρχείων)

**DDE**- Dynamic Data Exchange (Δυναμική Ανταλλαγή Δεδομένων)

**GUI** - graphical user interface (Γραφικό περιβάλλον Διεπαφής Με Το Χρήστη)

**SMB** -Server Message Block (Παροχέας Φραγμού Μηνυμάτων)

**RPC** -Remote Procedure Call (Απομακρυσμένη Κλήση Διαδικασίας)

**URL**-Uniform Recourse Locator (Ομοιόμορφος Εντοπιστής Πόρων)

**HTML**- HyperText Markup Language (Γλώσσα Σήμανσης Υπερ-κειμένου)

**IDS** -intrusion detection system (Σύστημα Ανίχνευσης Παρείσφρησης)

**PIN** -Personal Identification Number (Προσωπικό Νούμερο Αναγνώρισης)

**MEL**- Multos Executable Language (Εκτελέσιμη Γλώσσα Multos)

**DES** -Data Encryption Standard (Πρότυπο Κρυπτογράφησης Δεδομένων)

**MAC** -Message Authentication Code (Κώδικας Πιστοποίησης Μηνυμάτων)

**PKI** -Public Key Infrastructure (Υποδομή Δημοσίου Κλειδιού)

**GSM**- Global Standard for Mobile communications (Παγκόσμιο Σύστημα Για Κινητές Επικοινωνίες)

**A.T.M**- Asynchronous Transfer Mode (Ασύγχρονος Τρόπος Μεταφοράς)

**SIM**-Subscriber Identity Module (Διαμόρφωση Ταυτότητας Συνδρομητή)

**WAP** -Wireless Application Protocol (Πρωτόκολλο Ασύρματης Εφαρμογής)

**SSL** -Secure Socket Layer (Στρώμα Ασφαλούς Υποδοχής)

**TLS** -Transport Layer Security (Ασφάλεια Μεταφοράς Στρώματος)