ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΧΗΜΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕ ΕΙΔΙΚΕΥΣΗ:
LOGISTICS (Εφοδιασμός και Διακίνηση Προϊόντων)

Διπλωματική Εργασία
Ασφάλεια Ηλεκτρονικών Συναλλαγών στο Διαδίκτυο

Μιχαήλ Χ. Μεταξάς (ΜΠL: 0215)

Επιβλέπων Καθηγητής: Γρηγόρης Χονδροκούκης

ΠΕΙΡΑΙΑΣ 2006

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Χονδροκούκη για τη βοήθειά και καθοδήγηση του τόσο στα μαθήματα κατά τη διάρκεια του μεταπτυχιακού προγράμματος αλλά και στην πορεία της παρούσας εργασίας.

Αφιερωμένο στη μνήμη του πατέρα μου που «έφυγε» τον Φεβρουάριο 2006.

ΠΡΟΛΟΓΟΣ

Στις μέρες μας η χρήση του διαδικτύου εξαπλώνεται ολοένα και περισσότερο στη ζωή μας επηρεάζοντας καθημερινές μας συναλλαγές. Η διείσδυση του internet στην Ελλάδα εκτιμάται στα 2,5 εκατομμύρια σύμφωνα με πρόσφατη έρευνα (περίπου 25% του συνολικού πληθυσμού) και οι χρήστες εκτελούν ένα ευρύ φάσμα ηλεκτρονικών συναλλαγών (από αγορές προϊόντων online μέχρι τραπεζικές συναλλαγές). Ολοένα και περισσότερες επιχειρήσεις δραστηριοποιούνται στο ηλεκτρονικό εμπόριο, περιλαμβάνοντας e-καταστήματα, B2B και B2C δραστηριότητες. Υπηρεσίες που έχουν σχέση με τη διανομή και την εφοδιαστική αλυσίδα (προμήθειες, αγορές, διανομές προϊόντων) γίνονται ηλεκτρονικά. Καθώς διευρύνεται όμως η χρήση του διαδικτύου και των ηλεκτρονικών συναλλαγών, τίθεται συνεχώς πιο επιτακτικά το θέμα της ασφάλειας των δικτύων, των ηλεκτρονικών συναλλαγών και γενικά των ανταλλασσόμενων δεδομένων.

Στις εικόνες που ακολουθούν (Εικόνα 2), φαίνονται τα αποτελέσματα της παραπάνω έρευνας.

Επίσης στο τεύχος του αμερικάνικου περιδικού «TIME» στις 25-12-2006, ως άνθρωπος της χρονιάς, το περιοδικό ανακυρρύσσει τον κάθε ένα χρήστη του διαδικτύου που διαμορφώνει την κοινωνία της πληροφορίας (είτε χρησιμοποιώντας υπηρεσίες ηλεκτρονικού εμπορίου είτε χρησιμοποιώντας το internet για προσωπική ψυχαγωγία (Εικόνα 1).

Μιχαήλ Χ. Μεταξάς

Χημικός Μηχανικός Ε.Μ.Π

Πειραιάς 17-12-2006

Person of the Year

Dec. 25, 2006

E-mail this «

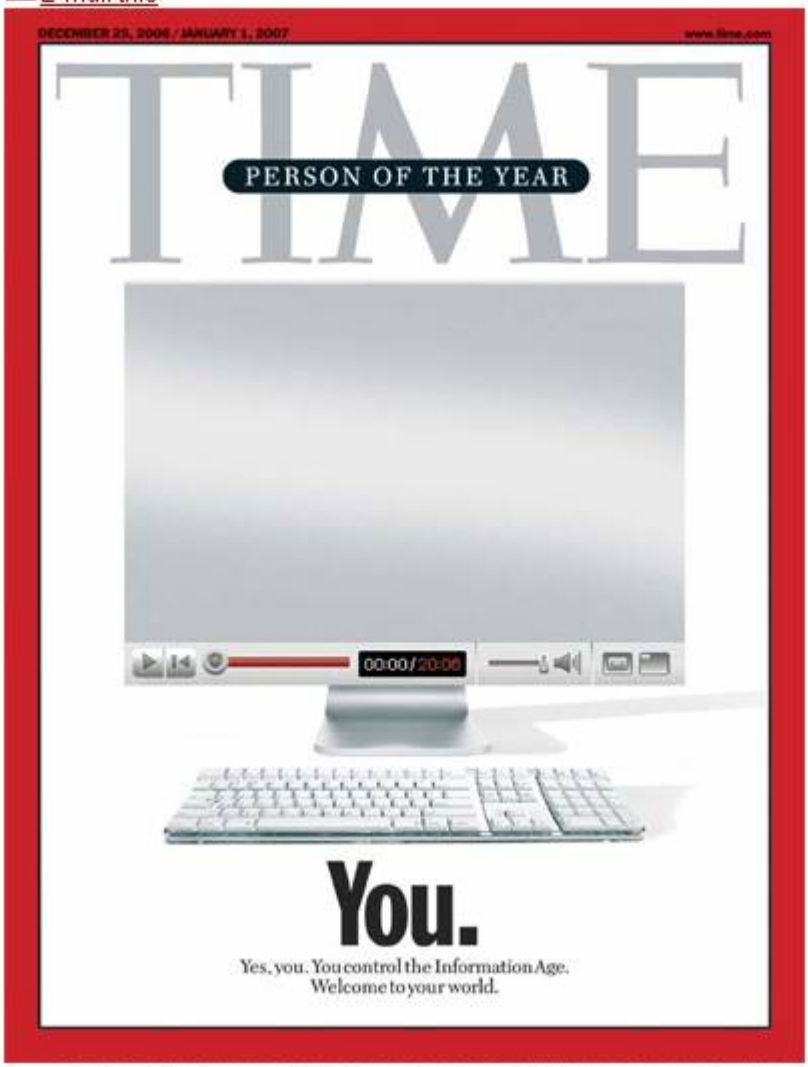
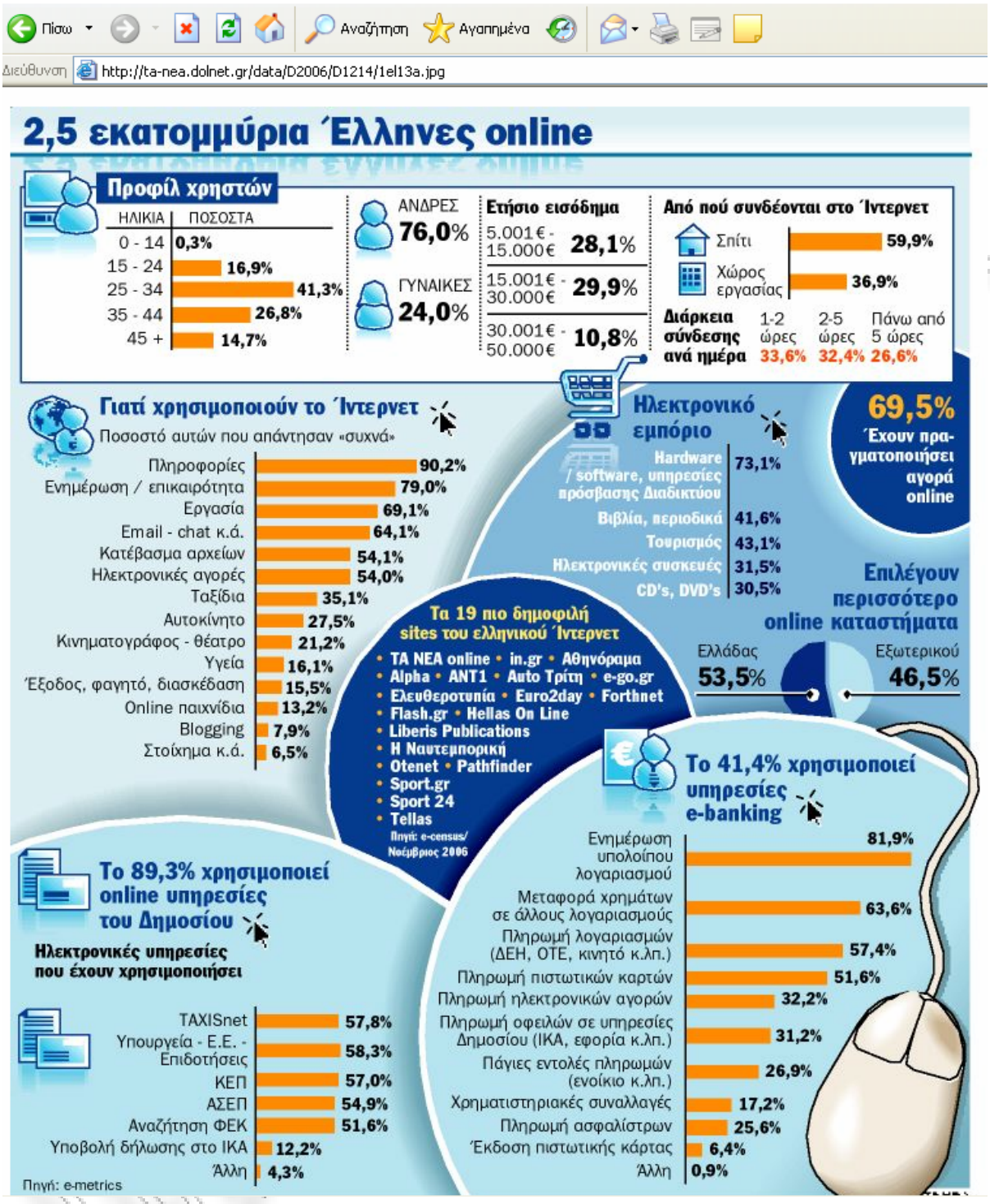


PHOTO-ILLUSTRATION FOR TIME BY ARTHUR HOCHSTEIN. WITH

Εικόνα 1: Time 25-12-2006

Πρόσωπο της χρονιάς: **ΕΣΥ** ο χρήστης του internet



Εικόνα 2: Έρευνα για τη διείσδυση του internet στην Ελλάδα

Περιεχόμενα

Κεφάλαιο 1

Ηλεκτρονικό Εμπόριο (E-commerce)

1.1 Ορισμός

Το ηλεκτρονικό εμπόριο είναι μια έννοια που περιγράφει τη διαδικασία αγοράς, πώλησης ή ανταλλαγής προϊόντων, υπηρεσιών και πληροφοριών μέσω δικτύων υπολογιστών, συμπεριλαμβανομένου και του διαδικτύου (Internet). Βασικός στόχος του δεν είναι απλά η χρήση υπολογιστών αλλά η τοποθέτηση του εμπορίου σε νέα βάση. Έτσι, μπορούμε να το ορίσουμε κάτω από διαφορετικές οπτικές γωνίες:

- Επικοινωνιακά: e-commerce είναι η μετάβαση των πληροφοριών, προϊόντων, υπηρεσιών, πληρωμών μέσω τηλεφωνικών γραμμών, δικτύων υπολογιστών και άλλων ηλεκτρονικών μέσων.
- Επιχειρησιακά: e-commerce είναι η αυτοματοποίηση των επιχειρησιακών συναλλαγών με την εφαρμογή της τεχνολογίας.
- Υπηρεσιακά: με το e-commerce μειώνεται το κόστος των υπηρεσιών από την πλευρά των εταιριών, ενώ παράλληλα βελτιώνεται η ποιότητα και η ταχύτητα των παρεχομένων υπηρεσιών.
- Online: e-commerce είναι η δυνατότητα online αγοράς και πώλησης προϊόντων, υπηρεσιών και πληροφοριών στο internet.

Πρέπει να αναφέρουμε ότι το ηλεκτρονικό εμπόριο (ΗΕ) είναι ένα μέρος του «ηλεκτρονικού επιχειρείν» (e-business). Με τον όρο αυτό, αναφερόμαστε όχι μόνο στις διαδικασίες αγοράς και πώλησης, αλλά και στην εξυπηρέτηση πελατών, στη συνεργασία με επιχειρηματικούς εταίρους, καθώς και στις συναλλαγές εντός της

επιχείρησης. Στη συνέχεια ο όρος e-commerce θα καλύπτει όλες της δραστηριότητες της ηλεκτρονικής επιχειρηματικότητας.

1.2 Μικρό Ιστορικό ΗΕ

Οι εφαρμογές του ΗΕ εμφανίστηκαν στις αρχλες της δεκαετίας του 70 με την ηλεκτρονική μεταφορά κεφαλαίων (Electronic Fund Transfer). Ωστόσο αυτές οι εφαρμογές χρησιμοποιήθηκαν από μεγάλους οργανισμούς και οικονομικά ιδρύματα περισσότερο και από λίγες μικρές επιχειρήσεις. Ακολούθησε η Ηλεκτρονική Μεταφορά Δεδομένων (Electronic Data Interchange, EDI), η οποία έδωσε τη δυνατότητα στις επιχειρήσεις να ανταλλάσουν τα έγγραφα και παραστατικά τους με ηλεκτρονικό τρόπο. Σαν αποτέλεσμα περισσότερες επιχειρήσεις συμμετείχαν στο ΗΕ καθώς επεκτάθηκε το είδος των συναλλαγών και αφορούσε επίσης κατασκευαστές , λιανικούς πωλητές, υπηρεσίες κλπ. Ακολούθησαν πολλές ακόμα εφαρμογές που κυμαίνονται από ανταλλαγή μετοχών σε σύστημα κράτησης ταξιδιωτικών θέσεων. Τέτοια συστήματα περιγράφηκαν ως συστήματα τηλεπικοινωνιών.

Με την εμπορευματοποίηση του Internet στις αρχές της δεκαετίας του 90 και την ταχεία εξέλιξη σε πολλούς δυνητικούς πελάτες, δημιουργήθηκε ο όρος *ηλεκτρονικό εμπόριο* και οι εφαρμογές του αυξήθηκαν γρήγορα. Η ταχεία εξάπλωση της τεχνολογίας οφείλεται σε δύο κυρίως παράγοντες:

- Ανάπτυξη δικτύων, πρωτοκόλλων, λογισμικού και προδιαγραφών
- Αύξηση του ανταγωνισμού και άλλων επιχειρησιακών πιέσεων.

Μετά το 1995 εμφανίζονται αρκετές καινοτόμες εφαρμογές που ποικίλουν από διαφημίσεις ως πλειστηριασμούς και εικονική πραγματικότητα. Μερικά στοιχεία:

1996: Το Forester Research Institute καταγράφει κύκλο εργασιών B2B 518 million USD και προβλέπει 6,6 billion USD για το 2000 (εκτίμηση που αναθεωρήθηκε στα 20 billion USD) .

3.000.000 χρήστες στις ΗΠΑ διαχειρίζονται ηλεκτρονικά τις μετοχές τους.

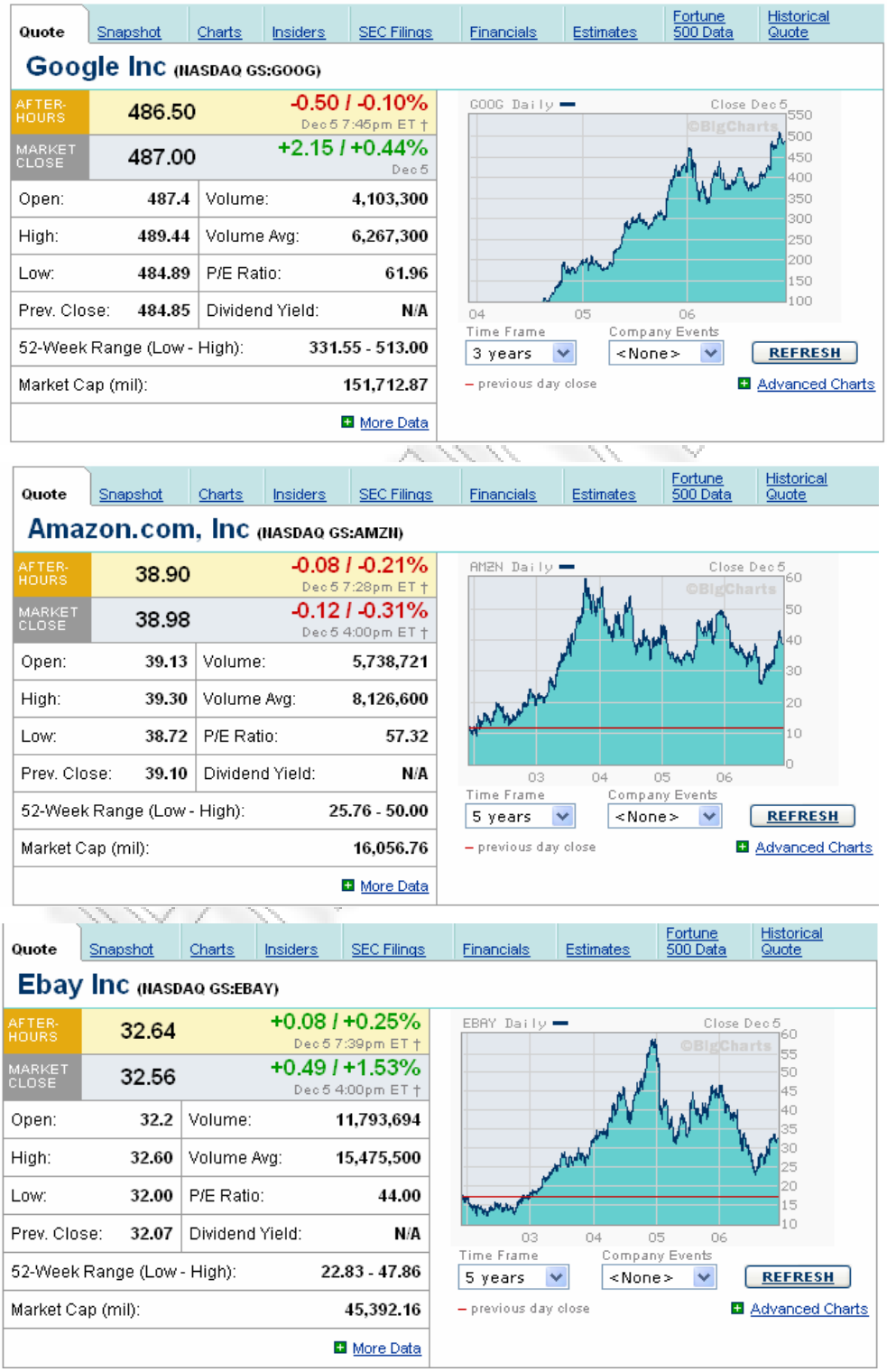
1997: Αξία συναλλαγών B2B στις ΗΠΑ 10 million USD μέσω Internet.Αξία συναλλαγών B2C 2 billion USD.

1998: 5.000.000 χρήστες στις ΗΠΑ διαχειρίζονται ηλεκτρονικά τις μετοχές τους.

2002: Οι περισσότερες εταιρίες ΗΕ αρχίζουν να έχουν μεγάλα κέρδη. Για παράδειγμα, αναφέρω την εξέλιξη των μετοχών εταιριών που δραστηριοποιούνται στο e-business

στο χρηματιστήριο της Νέας Υόρκης τα τελευταία χρόνια (Google, Amazon, EBay) (http://money.cnn.com)

2006: Η ΙΑΤΑ αποφασίζει την υποχρεωτική καθιέρωση του e-ticket στις αεροπορικές εταιρίες και την σταδιακή κατάργηση των χάρτινων εισητηρίων από το 2007.



Σχήμα 1: Εξέλιξη μετοχών εταιριών που δραστηριοποιούνται στο e-commerce (Google, Amazon, eBay) http://money.cnn.com

1.3 Φύση των συναλλαγών στο ΗΕ

Μια κοινή ταξινόμηση του ΗΕ είναι βάση της φύσης των συναλλαγών που πραγματοποιούνται και των συναλλασσομένων μερών. Διακρίνονται οι παρακάτω τύποι:

- **B2B (Business to Business)** Επιχείρηση προς επιχείρηση: είναι ο τύπος που χαρακτηρίζει σήμερα το ηλεκτρονικό εμπόριο. Περιλαμβάνει συναλλαγές μεταξύ οργανισμών (π.χ. χρήση ενδοεπιχειρισιακών ηλεκτρονικών εφαρμογών και πληροφοριακών συστημάτων για διάφορες λειτουργίες όπως παραγγελιοληψία και τιμολόγηση)
- **B2C (Business to Consumer)** Επιχείρηση προς καταναλωτή: πρόκειται για τις συναλλαγές λιανικής πώλησης με ανεξάρτητους αγοραστές. Παρουσιάζει αυξανόμενη χρήση σε διεθνές επίπεδο λόγω της χρήσης του internet σαν εργαλείο για την αποτελεσματική προώθηση προϊόντων και υπηρεσιών (π.χ. αγορά βιβλίων, μουσικής, αεροπορικών εισητηρίων, υπηρεσιών courier κλπ.)
- **C2C (Consumer to Consumer)** Καταναλωτής προς καταναλωτή: είναι η περίπτωση που ένας καταναλωτής πουλά απευθείας σε άλλους καταναλωτές (π.χ. μικρές αγγελίες για πώληση ακινήτων, αυτοκινήτων, υπηρεσιών κ.ά., δημοπρασίες και διαφημίσεις).
- **C2B (Consumer to Business)** Καταναλωτής προς επιχείρηση: είναι άτομα που πωλούν προϊόντα ή υπηρεσίες σε οργανισμούς καθώς και άτομα που ψάχνουν για αγοραστές, αλληλεπιδρούν με αυτούς και ολοκληρώνουν μια συναλλαγή.
- **Non Business EC**. Μη επιχειρησιακό ΗΕ: αφορά σε μη επιχειρησιακά ιδρύματα, π.χ. ακαδημαϊκά ιδρύματα, μη κερδοσκοπικούς οργανισμούς, κοινωνικές και μη κυνερνητικές οργανώσεις χρησιμοποιούν το ΗΕ για να μειώσουν τα έξοδά τους αφενός και για να βελτιώσουν τις λειτουργίες και την εξυπηρέτηση των πελατών τους. (π.χ. ηλεκτρονικές βιβλιοθήκες πανεπιστημίων)

- **Intra-business EC.** Ενδοεπιχειρησιακό ΗΕ: περιλαμβάνονται οι ενδοεπιχειρησιακές δραστηριότητες, οι οποίες πραγματοποιούνται σε intranets, και περιλαμβάνουν ανταλλαγή προϊόντων, υπηρεσιών ή πληροφοριών. Τέτοιες είναι για παράδειγμα, ενδοεταιρικές ανακοινώσεις για το προσωπικό που αφορούν σε αποτελέσματα της εταιρίας, εταιρικές παροχές, δυνατότητες εξέλιξης ή εκπαίδευσης των εργαζομένων.

1.4 Αλληλεπιδράσεις με διάφορα επιστημονικά πεδία

Το ΗΕ θεμελιώνεται και εξαρτάται από πολλά επιστημονικά πεδία και αρχές, οι κυριότερες από τις οιποίες είναι:

Marketing: Πολλά ζητήματα του ΗΕ αφορούν στο marketing, πχ προώθηση προϊόντων, στρατηγικές διαφήμισης και η σχέση κόστους – αποδοτικότητας των διαφημίσεων. Έτσι πολλές επιχειρήσεις διαφημίζουν στο Internet μέσω των ιστοσελίδων τους τα προϊόντα και τις υπηρεσίες που παρέχουν.

Computer Science: Το ΗΕ εξαρτάται και επηρεάζεται άμεσα από γλώσσες προγραμματισμού, πολυμέσα και δίκτυα ΗΥ.

Consumer Behavior and Psychology: Η επιτυχία του ΗΕ βασίζεται στη γνώση της συμπεριφοράς των πελατών αλλά και των πωλητών των επιχειρήσεων.

Finance: Οι οικονομικές αγορές και οι τράπεζες συμμετέχουν στο ΗΕ, καθώς πολλές συναλλαγές γίνονται βάση οικονομικών διακανονισμών (π.χ. αγορές μέσω πιστωτικής κάρτας), αλλά και διαδικασίες ΗΕ αφορούν σε αγοραπωλησίες μετοχών ή άλλες χρηματιστηριακές πράξεις. Επίσης, εμπλέκονται στο θέμα της ασφάλειας στις ηλεκτρονικές συναλλαγές μέσω πιστωτικών καρτών και της καταπολέμησης της απάτης στις online συναλλαγές.

Economics: Οι οικονομικές δυνάμεις και οι εξελίξεις στην παγκόσμια οικονομία επηρρεάζουν και αυτές το ΗΕ, καθώς οι εταιρίες που δραστηριοποιούνται στο ΗΕ θα πρέπει να λάβουν σοβαρά υπόψη τους τις μικροοικομικές θεωρίες και την επίδραση της πορείας της οικονομίας.

MIS systems: Μέσω των πληροφοριακών συστημάτων αναπτύσσεται το ΗΕ. Σχεδιάζονται τα συστήματα που υποστηρίζουν τις συναλλαγές ΗΕ, μέσω του

σχεδιασμού, ανάλυσης και ολοκλήρωσης των συστημάτων, αλλά και της ασφάλειας των ηλεκτρονικών συναλλαγών.

Accounting and auditing: Αναφέρεται στον έλεγχο και την παρακολούθηση των ηλεκτρονικών συναλλαγών από τη λογιστική πλευρά καθώς και στη σχέση κόστους αποτελεσματικότητας τους.

Management: Οι εταιρίες ΗΕ ακολουθούν και εκείνες τις αρχές Διοίκησης Επιχειρήσεων και χαράζουν στρατηγικές όπως όλες οι επιχειρήσεις.

Business Law and Ethics: Ζητήματα νομικά και ηθικά προκύπτουν και είναι πολύ σημαντικά για την εξέλιξη του ΗΕ. Αυτά αντομετωπίζονται μέσω της νομοθεσίας και αφορούν θέματα όπως π.χ η πνευματική ιδιοκτησία και η προστασία προσωπικών δεδομένων.

Άλλα πεδία: Τέλος, άλλα επιστημονικά πεδία και αρχές εμπλέκονται με το ΗΕ, όπως η γλωσσολογία (μια εταιρία που απευθύνεται σε περισσότερες χώρες πρέπει να διαθέτει τις υπηρεσίες ΗΕ σε διαφορετικές γλώσσες), η ρομποτική, επιχειρησιακή έρευνα, στατιστική και δημόσια διοίκηση (για την παροχή υπηρεσιών της δημόσιας διοίκησης στους πολίτες). Επίσης το ΗΕ ενδιαφέρει τομείς όπως μηχανική, υγεία, επικοινωνίες, εκδόσεις, και διασκέδαση.

1.5 Πλεονεκτήματα και οφέλη του ΗΕ

Α. Επιχειρήσεις

Η χρήση του ΗΕ είναι από τη φύση της μια έννοια δι-επιχειρησιακή. Παρόλο που το ΗΕ μπορεί να εφαρμοστεί και μέσα σε μια επιχείρηση, τα πραγματικά οφέλη εμφανίζονται όταν εφαρμόζεται μεταξύ επιχειρήσεων, κυρίως μεταξύ επιχειρήσεων που λειτουργούν με σχέσεις προμηθευτή - πελάτη (με την ευρύτερη δυνατή έννοια του όρου). Για το λόγο αυτό και τα οφέλη που αποκομίζουν οι χρήστες είναι σχεδόν πάντα παράλληλα. Κάθε επιχειρηματική ευκαιρία που παρέχει η χρήση ΗΕ σε έναν προμηθευτή, μπορεί στις περισσότερες περιπτώσεις να μεταφραστεί και σε ένα αντίστοιχο όφελος για τους πελάτες του. Με την έννοια αυτή, το ΗΕ είναι μια επαναστατική επιχειρηματική καινοτομία, αφού για να αποδώσει καρπούς δεν στηρίζεται στον ανταγωνισμό, αλλά στη συνεργασία μεταξύ των εμπλεκομένων για το αμοιβαίο τους κέρδος (win-win σχέσεις).

Παρακάτω αναφέρονται μερικά μόνο από τα οφέλη και τις ευκαιρίες που μπορεί να δημιουργήσει το Η.Ε., τόσο για τους προμηθευτές όσο και για τους αγοραστές προϊόντων και υπηρεσιών.

Παγκόσμια παρουσία / Παγκόσμια επιλογή

Το ΗΕ δίνει (για πρώτη φορά στην παγκόσμια ιστορία του εμπορίου) σε όλους τη δυνατότητα να δραστηριοποιηθούν στην παγκόσμια αγορά, ανεξάρτητα από μέγεθος και τις οικονομικές τους δυνατότητες. Μέχρι σήμερα κάτι τέτοιο ήταν εφικτό μόνο για τις μεγάλες πολυεθνικές επιχειρήσεις, ενώ οι μικρότερες επιχειρηματικές μονάδες ήταν υποχρεωμένες να κινούνται σε μικρές τοπικές αγορές που προσδιορίζονταν από γεωγραφικούς, εθνικούς, χρηματοοικονομικούς ή άλλους περιορισμούς. Σήμερα (και ολοένα και περισσότερο στο μέλλον) η αγορά-στόχος μιας επιχείρησης που συναλλάσσεται ηλεκτρονικά με τους εταίρους της περιορίζεται μόνο από την ύπαρξη τηλεπικοινωνιακών δικτύων. Με τη συνεχώς αυξανόμενη κάλυψη όλου του πλανήτη με τέτοια δίκτυα, το ΗΕ δίνει για πρώτη φορά ακόμα και σε μικρού μεγέθους επιχειρήσεις τη δυνατότητα να επιτύχουν την παρουσία τους στην «παγκόσμια» αγορά. Από την άλλη πλευρά, αυτή ακριβώς η δυνατότητα δίνει απεριόριστες δυνατότητες επιλογών στους πελάτες που δεν είναι πλέον υποχρεωμένοι να επιλέξουν προϊόντα και υπηρεσίες μόνο από τους προμηθευτές εκείνους που μπορούν να έρθουν σε φυσική επαφή.

Βελτιωμένη ανταγωνιστικότητα/ ποιότητα υπηρεσιών

Η ηλεκτρονική επικοινωνία επιτρέπει στους προμηθευτές προϊόντων και υπηρεσιών να γίνουν πιο ανταγωνιστικοί, κυρίως προσφέροντας προς τους πελάτες τους υπηρεσίες που πριν ήταν αδύνατο ή πολύ δύσκολο να προσφερθούν. Για παράδειγμα, η υποστήριξη του πελάτη πριν και μετά την αγορά ήταν αντιοικονομική για πολλές επιχειρήσεις. Αντίθετα, με τη χρήση μεθόδων ηλεκτρονικής επικοινωνίας, ο προμηθευτής έρχεται «κοντά» στον πελάτη του (χωρίς στις περισσότερες περιπτώσεις να χρειαστεί να μετακινηθεί πραγματικά, προσφέροντας του έτσι υπηρεσίες υψηλής ποιότητας με πολύ μικρό επιπλέον κόστος.

Παροχή και λήψη εξειδικευμένων υπηρεσιών

Με τη χρήση του ΗΕ, οι προμηθευτές μπορούν να παρακολουθούν πιο αποτελεσματικά το προφίλ του αγοραστικού κοινού τους. Με τον τρόπο αυτό, μπορούν να σχεδιάζουν και να προσφέρουν προϊόντα που απευθύνονται στους

μεμονομένους πελάτες τους, αλλά σε τιμές της μαζικής αγοράς. Ένα απλό παράδειγμα μπορεί να είναι ένα ηλεκτρονικό περιοδικό που προσφέρει τα άρθρα του στο Internet με τέτοιο τρόπο που να δίνει έμφαση στα συγκεκριμένα ενδιαφέροντα κάθε ενός συνδρομητή, προτείνοντας του συγκεκριμένες πηγές αναζήτησης πληροφοριών στο δίκτυο.

Μείωση απογραφών και εξόδων διαχείρησης της εφοδιαστικής αλυσίδας

Με ένα σύστημα ΗΕ, η ανάγκη για καταγραφή φυσικών αποθεμάτων μειώνεται καθώς μπορεί να εφαρμοστεί διαχείρηση των προμηθευτικών αναγκών "pull-type". Τότε οι ανάγκες ξεκινούν από τις εντολές των πελατών και γίνεται εφαρμογή του μοντέλου JIT (just in time), ώστε να μειώνονται τα ποθέματα και το κόστος διατήρησής τους.

Σμίκρυνση προμηθευτικής αλυσίδας/Άμεση κάλυψη αναγκών

Ένα από τα πλέον αναφερόμενα οφέλη του ΗΕ είναι η συμβολή του στην εξάλειψη των μη απαραίτητων μεσαζόντων στις εμπορικές συναλλαγές. Κάτι τέτοιο συνεπάγεται αυτόματα τη σμίκρυνση της προμηθευτικής αλυσίδας με τρόπο που ο προμηθευτής έρχεται σε απευθείας επικοινωνία με τον πελάτη χωρίς την παρεμβολή τρίτων (π.χ. αποστολή προϊόντων χωρίς τη χρήση διαμεταφορέων, ενδιάμεσων αποθηκών, κ.α.). Το αντίστοιχο όφελος για τον πελάτη είναι φυσικά η άμεση κάλυψη των αναγκών του, καθώς μπορεί να παραλάβει το προϊόν/ υπηρεσία που επιθυμεί χωρίς τις χρονικές καθυστερήσεις που αναπόφευκτα εισάγουν στον κύκλο διανομής τα ενδιάμεσα μέρη. Η πλέον ακραία περίπτωση σμίκρυνσης της προμηθευτικής αλυσίδας επέρχεται στην περίπτωοη που το ίδιο το προϊόν έχει τέτοια φύση που μπορεί να μεταφερθεί ηλεκτρονικά. Στην περίπτωση αυτή μιλάμε για για πλήρη εξάλειψη της προμηθευτικής αλυσίδας, καθώς δεν χρειάζεται καμία φυσική επαφή για να πραγματοποιηθεί η εμπορική πράξη. Τέτοια παραδείγματα έχουν αρχίσει να εμφανίζονται σε αγορές όπως η βιομηχανία παραγωγής λογισμικού (υπάρχουν οίκοι λογισμικού που δεν έχουν καν γραφεία, αλλά συναλλάσσονται αποκλειστικά μέσω δικτύου), οι τομείς ψυχαγωγίας και ενημέρωσης (π.χ. βίντεο, μουσική, περιοδικά, εφημερίδες) και η εκδοτική βιομηχανία (οι περισσότερες εγκυκλοπαίδειες που πωλήθηκαν στις ΗΠΑ το 1995 ήταν σε ηλεκτρονική μορφή παρά σε έντυπη).

Ελαχιστοποίηση κόστους παραγωγής/Ελαχιστοποίηση τιμών

Φυσικά η πρώτη ίσως συνεισφορά που θα μπορούσε να αποδώσει κανείς στο ΗΕ θα ήταν η μείωση του λειτουργικού κόστους για τους προμηθευτές, με τα αντίστοιχα οφέλη και για τους πελάτες (μείωση του δικού τους κόστους και δυνατότητα απολαβής καλύτερων τιμών). Κάθε φυσική επικοινωνία που ήταν απαραίτητη για μια εμπορική συναλλαγή κοστίζει λιγότερο αν πραγματοποιηθεί ηλεκτρονικά (π.χ. ηλεκτρονικό ταχυδρομείο αντί για τηλέφωνο ή συναντήσεις) και μπορεί να λάβει χώρα σε μικρότερο συνήθως χρόνο. Με την ωρίμανση της τεχνολογίας των δικτύων υπολογιστών, η διαφορά κόστους μεταξύ φυσικής και ηλεκτρονικής επικοινωνίας θα γίνεται ολοένα και πιο εμφανής.

Νέες επιχειρηματικές ευκαιρίες/Νέα προϊόντα και υπηρεσίες

Τέλος, καθώς το ΗΕ ανοίγει μια τελείως νέα εποχή στις εμπορικές συναλλαγές, προσφέρει παράλληλα την ευκαιρία δημιουργίας εντελώς νέων προϊόντων και υπηρεσιών και μια σειρά από επιχειρηματικές ευκαιρίες στους πρωτοπόρους. Τέτοιες υπηρεσίες περιλαμβάνουν την παροχή δικτύων και δικτυακών υπηρεσιών (π.χ. παροχείς πρόσβασης στο Internet), υπηρεσίες ηλεκτρονικών καταλόγων, συμβουλευτικές υπηρεσίες σε επιχειρήσεις για υιοθέτηση του ΗΕ κα.

Β. Καταναλωτές

Βασικά πλεονεκτήματα για τους καταναλωτές είναι τα παρακάτω:

Εξυπηρέτηση 24/7

Το ΗΕ επιτρέπει στους καταναλωτές να μπορούν να κάνουν τις αγορές τους και τις συναλλαγές τους 24/7 (καθημερινά σε 24ωρη βάση), από όποα τοποθεσία και αν βρίσκονται.

Πληθώρα επιλογών

Οι καταναλωτές μπορούν να επιλέξουν από μεγάλο αριθμό επιχειρήσεων, προϊόντων από περισσότερες χώρες και όχι αναγκαστικά από τον τόπο διαμονής τους.

Λειτουργία Ανταγωνισμού

Ο καταναλωτής έχοντας τη δυνατότητα να επιλέξει από μεγάλη ποικιλία προϊόντων και υπηρεσιών μπορεί εύκολα να συγκρίνει τιμές για να επιλέξει την πιο συμφέρουσα επιλογή, αλλά και οι επιχειρήσεις προσφέρουν τα προϊόντα σε καλύτερες τιμές. Δημιουργείται έτσι ένα ανταγωνιστικό περιβάλλον προς όφελος του καταναλωτή.

Ταχύτητα

Σε πολλές περιπτώσεις ο χρόνος παράδοσης μηδενίζεται. Αυτό ισχύει για τα ψηφικής μορφής προϊόντα (πχ μουσική, εκδόσεις, ταινίες, λογισμικό κά). Αλλά και οποιαδήποτε πληροφορία σχετικά με το προϊόν (π.χ. τεχνικά χαρακτηριστικά ή οδηγίες χρήσης) είναι άμεσα προσβάσιμα.

Γ. Κοινωνία

Το ΗΕ έχει και κοινωνικά οφέλη, μερικά από τα οποία είναι:

Εξοικονόμηση χρόνου

Μπορεί να γίνει εξοικονόμηση του χρόνου που αφιερώνει ένας εργαζόμενος για τις αγορές του καθώς αυτές μπορούν να γίνουν χωρίς να μετακινηθεί. Έτσι, δυνητικά μπορεί να υπάρχει θετική επίδραση στη μείωση της κυκλοφορίας στους δρόμους, άρα βελτίωση κυκλοφοριακών συνθηκών και μείωση ρύπανσης. Ο χρόνος που εξοικονομείται μπορεί να αφιερωθεί σε άλλες ατομικές δραστηριότητες (hobby) ή να αφιερωθεί στην οικογένεια.

Βελτίωση βιωτικού επιπέδου

Περισσότερα προϊόντα είναι διαθέσιμα σε περισσότερο κόσμο. Έτσι μπορεί να βελτιωθεί το βιωτικό επίπεδο ατόμων που μπορούν πλέον να προμηθευτούν αγαθά τα οποία δεν είναι ακόμα διαθέσιμα στην τοπική αγορά, αλλά και λόγω του ανταγωνισμού τα ακριβά προϊόντα είναι διαθέσιμα σε πιο προσιτές τιμές, άρα μπορούν να αγοραστούν από άτομα με χαμηλότερα εισοδήματα.

Συνεχιζόμενη Εκπαίδευση

Είναι δυνατό άτομα σε απομακρυσμένες περιοχές να παρακολουθούν προγράμματα εξειδίκευσης (π.χ. σεμινάρια e-learning ή προγράμματα σπουδών στο Ανοικτό Πανεπιστήμιο) και να αποκτήσουν κάποιο πτυχίο ή εξειδικευμένες γνώσεις σε κάποιο τομέα ή να μάθουν κάποια ξένη γλώσσα.

Δημόσιες Υπηρεσίες

Διευκολύνεται η μεταφορά δημοσίων υπηρεσιών, όπως για παράδειγμα οι υπηρεσίες υγείας σε αραιοκατοικημένες ή δυσπρόσιτες περιοχές μέσω πογραμμάτων τηλε-

ιατρικής, ή άλλων υπηρεσιών όπως πληροφόρηση των πολιτών (πχ www.e-gov.gr, www.kep.gov.gr) ή ακόμα συναλλαγές με υπηρεσίες (π.χ. Taxisnet για συναλλαγές με εφορία στο www.gsis.gr, ΙΚΑ για υποβολή δήλωσης εργοδότη στο www.ika.gr κ.ά)

1.6 Περιορισμοί του ΗΕ

Οι περιορισμοί του ΗΕ μπορούν να κατηγοριοποιηθούν σε τεχνικούς και μη τεχνικούς περιορισμούς.

Α. Τεχνικοί Περιορισμοί

Θέμα έλλειψης ασφάλειας του συστήματος, αξιοπιστίας και κατάλληλων πρωτοκόλλων επικοικωνίας.

Ανεπαρκές τηλεπικοικωνιακό εύρος μηκών κύματος

Ραγδαία εξέλιξη και ανάπτυξη και μεταβολές στο λογισμικό

Δυσκολία στην ολοκλήρωση του λογισμικού στο Internet με τις υπάρχουσες εφαρμογές και βάσεις δεδομένων

Οι εταιρίες μπορεί να χρειάζονται και ειδικούς web hosts και άλλες υποδομές εκτός από εξυπηρετητές δικτύου

Ασυμβατότητα ορισμένου μέρους λογισμικού του ΗΕ με κάποια λειτουργικά συστήματα υπολογιστών

Οι παραπάνω τεχνικοί περιορισμοί με την εξέλιξη του ΗΕ αναμένεται να μειωθούν ή και να απαλοιφθούν τελείως. Προς το παρόν, για την αποφυγή τους χρειάζεται σωστός σχεδιασμός και προγραμματισμός.

Β. Μη τεχνικοί Περιορισμοί

Σύμφωνα με έρευνα του Internetweek, οι κύριοι μη τεχνικοί περιορισμοί που επιβραδύνουν την εξάπλωση του ΗΕ είναι:

Κόστος και Δικαιολόγηση Χρήσης

Το κόστος ανάπτυξης εφαρμογών ΗΕ μπορεί να είναι ιδιαίτερα υψηλό, λόγω κακού σχεδιασμού και έλλειψης εμπειρίας που μπορεί να οδηγήσει σε καθυστερήσεις. Επίσης η δικαιολόγηση της χρήσης εμπεριέχει και ρίσκο καθώς κάποια ζητήματα

όπως η αναμενόμενη αποδοτικότητα ή η βελτίωση της εξυπηρέτησης των πελατών δύσκολα ποσοτικοποιούνται.

Ασφάλεια και Ιδιωτικότητα

Το ζήτημα της ασφάλειας είναι ιδιαίτερα σημαντικό ιδίως στις B2B συναλλαγές. Συνεχώς βελτιώνονται τα μέτρα που λαμβάνονται για την προστασία της ιδιωτικότητας των συναλλαγών αλλά οι πελάτες δύσκολα πείθονται αν είναι πράγματικά αποτελεσματικά.

Έλλειψη εμπιστοσύνης και αντίσταση του χρήστη

Δύσκολα αντικαθίστανται η αμεσότητα της προσωπικής επικοινωνίας με ένα απρόσωπο περιβάλλον και ορισμένοι «παραδοσικοί» πελάτες βλέπουν με σκεπτικισμό τις συναλλαγές χωρίς χαρτί ή τις αγορές από ηλεκτρονικά καταστήματα.

Άλλοι περιοριστικοί παράγοντες

Έλλειψη της αίσθησης όταν βλέπεις ένα προϊόν στην πραγματικότητα. Αρκετές φορές επηρεαζόμαστε από την εμφάνιση ενός προϊόντος ή την αίσθηση όταν το αγγίζουμε ή το επεξεργαζόμαστε φυσικά.

Επίσης διάφορα νομικά θέματα που δεν έχουν διευθετηθεί επειδή κυνερνητικοί οργανισμοί δεν είναι κατάλληλα προετοιμασμένοι και δεν έχουν επεξεργαστεί κατάλληλα πρότυπα.

Κάποιοι περιμένουν να εξελιχθεί και εξαπλωθεί περισσότερο το ΗΕ ώστε να είναι πιο σταθερές οι συνθήκες λειτουργίας του.

Έλλειψη συστημάτων υποστήριξης

Ορισμένες εφαρμογές δεν είναι ακόμα επικερδείς καθώς δεν υπάρχει ακόμα το απαιτούμενο ενδιαφέρον.

Η πρόσβαση στο internet παρά τον ανταγωνισμό είναι ακόμα ακριβή (μικρή σχετικά διείσδυση του ADSL)

Παρά όμως τους περιορισμούς αυτούς το ΗΕ εξελίσσεται με αλματώδεις ρυθμούς και υπάρχει η τάση όλο και περισσότερες εταιρίες να υιοθετούν εφαρμογές ΗΕ.

Κεφάλαιο 2

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 Γενικά

Το Διαδίκτυο έχει αποκτήσει πλέον σαφέστατα πολυδιάστατο χαρακτήρα, και η ανάπτυξη και ευρεία αποδοχή του σε παγκόσμια κλίμακα συνιστούν ένα ανοιχτό περιβάλλον, όπου δεν μπορεί να υπάρχει εμπιστοσύνη μεταξύ των χρηστών και συνεπώς δε μπορεί να χαρακτηριστεί καθόλου ασφαλές. Αξιοποιώντας το internet μπορούν να διακηνιθούν προσωπικά δεδομένα, ενώ υπάρχου κακόβουλοι χρήστες που έχουν σκοπό τους να εξαπατήσουν και να προκαλέσουν φθορές σε συστήματα με στόχο είτε το κέρδος είτε την προσωπική τους ικανοποίηση. Η σημασία αυτού του ζητήματος εντείνεται ακόμα περισσότερο αν ληφθεί υπόψη το συνεχώς αυξανόμενο εμπορικό ενδιαφέρον από τη χρήση του internet.

Έτσι λοιπόν, η ασφάλεια θεωρείται ως ένας από τους πιο σημαντικούς σκοπέλους για το Ηλεκτρονικό Εμπόριο και γενικά για την επικοινωνία μέσω του διαδικτύου. Στην ουσία θα το χαρακτηρίζαμε περισσότερο εμπορικό παρά τεχνολογικό πρόβλημα, αφού η επίλυση του επηρεάζει κυρίως την ανάπτυξη και εξέλιξη των εμπορικών συναλλαγών. Η τεχνολογία από την πλευρά της προσφέρει σημαντικά όπλα για μία γενική αντιμετώπιση του προβλήματος.

Οι κυριότεροι λόγοι για τους οποίους η ασφάλεια οφείλει να μας προβληματίζει είναι οι ακόλουθοι:

Οι υπολογιστές είναι συνδεδεμένοι.

Μέχρι την ανάπτυξη του internet το πρόβλημα της ασφάλειας περιοριζόταν στο χρήστη του υπολογιστή. Από τη στιγμή που χρήστες των βάσεων δεδομένων ήταν άτομα εξουσιοδοτημένα τότε δεν υπήρχε κανένας κίνδυνος για την ασφάλεια των δεδομένων. Στο internet όμως δίνεται η δυνατότητα σε οποιονδήποτε να εισέρχεται σε κάθε υπολογιστή που είναι συνδεδεμένος.

Το δίκτυο είναι ψηφιακό.

Το να αποκτήσει κάποιος πρόσβαση στο τηλεφωνικό δίκτυο για να παρακολουθεί τις τηλεφωνικές συνδιαλέξεις είναι μεν εφικτό, αλλά δεν εγγυάται ευκολία στην απόκτηση πληροφοριών. Αυτό διότι δεν είναι δυνατή η ταυτόχρονη παρακολούθηση διάφορων τηλεφωνικών αριθμών και επίσης απαιτείται χρόνος μέχρι να "ακούσει" την πληροφορία που αναζητά. Μέσα όμως στο δίκτυο των υπολογιστών έχει τη δυνατότητα να παρακολουθεί ταυτόχρονα ένα μεγάλο πλήθος συνομιλιών και το σημαντικότερο ο υπολογιστής μπορεί να αναζητά με μεγάλη ταχύτητα συγκεκριμένες πληροφορίες, χωρίς ο εισβολέας στην ουσία να κάνει τίποτα.

Οι υπολογιστές συλλέγουν δεδομένα.

Η ίδια η λειτουργία των υπολογιστών είναι τέτοια που καθιστά εφικτά συγκεκριμένα είδη επιθέσεων. Τα πληροφοριακά συστήματα είναι έτσι χτισμένα ώστε τα επιθυμητά -και ταυτόχρονα άκρως σημαντικά- δεδομένα να είναι εύκολα προσβάσιμα. Συνεπώς αν κάποιος εισέλθει εντός του συστήματος δεν θα δυσκολευτεί να αναζητήσει και να συλλέξει τα δεδομένα που επιθυμεί.

Οι υπολογιστές μπορούν να προγραμματιστούν.

Ένας εισβολέας είδαμε πως μπορεί να χρησιμοποιήσει τον υπολογιστή προκειμένου να ψάξει ανάμεσα στα δεδομένα για αυτά που τον ενδιαφέρουν. Ταυτόχρονα μπορεί να τον προγραμματίσει ώστε να αναζητά τρόπους για να αποκτήσει πρόσβαση στο σύστημα. Τέλος υπάρχει η δυνατότητα να κατασκευασθούν προγράμματα εισβολών σε συστήματα από ικανούς εισβολείς που θα μετατρέψουν και τους πιο άπειρους σε επικίνδυνους. Αν για παράδειγμα, υπάρχει, απλή σε λειτουργία, συσκευή που να ξεκλειδώνει κλειδαριές τότε δεν απαιτείται έμπειρος κλειδαράς για την ανοίξει.

Η εισβολή σε πληροφορικά συστήματα μένει ανεξακρίβωτη.

Ένα ανοχύρωτο πληροφοριακό σύστημα δεν διατηρεί πειστήρια παραβίασης του. Τα εγκλήματα στο φυσικό κόσμο συνοδεύονται πάντα από αποδεικτικά: Αποτυπώματα, αυτόπτες μάρτυρες, καταγραφή εικόνας σε κάμερα ασφαλείας, -παραβιασμένες πόρτες κλπ. Η ύπαρξη συστήματος ασφαλείας μας παρέχει ίχνη του τι συνέβει και από ποιόν.

Υπάρχουν εμπειρίες επιθέσεων.

Πλείστα καθημερινά παραδείγματα έρχονται να επιβεβαιώσουν με τον πιο τρανταχτό τρόπο την ανάγκη θωράκισης των δεδομένων μας. Ακόμη και βάσεις δεδομένων, ιστοσελίδες και πληροφοριακά συστήματα μεγάλων οργανισμών και κυβερνήσεων έπεσαν θύματα εισβολών.

Όταν συνδεόμαστε στο internet αυτόματα θέτουμε σε κίνδυνο:

- Τα δεδομένα, δηλαδή τις ανταλσσόμενες πληροφορίες αλλά και όλα τα στοιχεία που φυλάσσονται σε βάσεις δεδομένων.
- Τα πληροφοριακά συστήματα που χρησιμοποιούμε
- Τη φήμη της επιχείρησης.

2.1.1 Τα Δεδομένα

Τα δεδομένα έχουν τρία κρίσιμα χαρακτηριστικά που πρέπει να προστατευθούν και να εξασφαλιστούν για να μπορεί, το διαδίκτυο να είναι αξιόπιστο μέσο:

Μυστικότητα (Privacy): Να μην διαβάζονται από τρίτους

Ακεραιότητα (Integrity): Να μην παραποιούνται

Διαθεσιμότητα (Availability): Να είναι ανά πάσα στιγμή προσβάσιμα.

Οι περισσότεροι επικεντρώνουν την προσοχή τους στους κινδύνους που αφορούν τη μυστικότητα των δεδομένων. Σε μεγάλο βαθμό το γεγονός αυτό είναι απόλυτα φυσιολογικό, καθώς πολλές εταιρείες διατηρούν στους υπολογιστές τα σημαντικότερα δεδομένα τους, όπως για παράδειγμα: Τα σχέδια των προϊόντων τους, οικονομικά αρχεία, αριθμούς πιστωτικών καρτών, πελατολόγιο, προσφορές. Η λύση στο πρόβλημα της μυστικότητας δείχνει απλή ειδικά για τις επιχειρήσεις που δεν απαιτείται να ανταλλάσσουν δεδομένα τους με άλλες επιχειρήσεις ή πελάτες μέσω internet. Απομονώνουν τα μηχανήματα που περιέχουν τα «κρίσιμα» δεδομένα από εκείνα που συνδέονται με το διαδίκτυο. Επομένως για αυτούς το πρόβλημα της ασφάλειας των βάσεων δεδομένων λύθηκε; Η απάντηση είναι όχι διότι δεν έχει αποκλειστεί ο κίνδυνος για τη διαθεσιμότητα και ακεραιότητα των δεδομένων. Ακόμη και αν τα δεδομένα μιας εταιρείας δεν είναι μυστικά είναι βέβαιο πως το πλήγμα της

παραποίησης ή της καταστροφής τους, θα έχει σημαντικό κόστος τόσο οικονομικό όσο και γοήτρου.

Τα περιστατικά που αφορούν την ασφάλεια των βάσεων δεδομένων διαφέρουν από τα τυπικά εγκλήματα γιατί η ανίχνευση τους είναι δύσκολη. Σε πολλές περιπτώσεις μια βίαιη είσοδος στο πληροφοριακό σύστημα μπορεί να είναι προτιμότερη από μία εισβολή που δεν αφήνει ίχνη και επομένως δεν γνωρίζουμε τι ακριβώς "διαβάστηκε" ή "πειράχτηκε".

2.1.2 Το Πληροφοριακό Σύστημα (hardware-software)

Ένας εισβολέας εκτός από την κλοπή, παραποίηση ή καταστροφή των δεδομένων έχει τη δυνατότητα να χρησιμοποιήσει το συγκεκριμένο σύστημα και να εμφανιστεί στο διαδίκτυο με τη δική μας ταυτότητα, να χρησιμοποιήσει το λογισμικό μας ή ακόμη και να καταστρέψει ολόκληρο ή μέρος του συστήματος μας. Πέρα από την πιθανότητα καταστροφής που η σημασία της είναι προφανής, η ενδεχόμενη χρήση του συστήματος μας κρύβει εξίσου σημαντικούς κινδύνους. Από το να μην μπορούμε να χρησιμοποιήσουμε το σύστημα, μέχρι το να θεωρηθούμε υπεύθυνοι για τις πράξεις που γίνονται με δική μας ταυτότητα.

2.1.3 Η Φήμη της επιχείρησης

Η φήμη και το γόητρο της εταιρίας μπορεί να πληγούν ανεπανόρθωτα αν δεν αξιολογηθεί σωστά ο κίνδυνος από τους επίδοξους εισβολείς και αν δε ληφθούν τα κατάλληλα μέτρα προστασίας. Η χρήση του εταιρικού σήματος ή του ονόματος της εταιρίας από κάποιον τρίτο στο internet μπορεί να βλάψει σοβαρά την επιχείρηση και να τη διασύρει και δυσφημήσει με τις ενέργειές του. Αλλά και μόνο το γεγονός ότι χτυπήθηκε η ιστοσελίδα της εταιρίας και κλάπηκαν ή παραποιήθηκαν δεδομένα, είναι λόγοι να μειωθεί σημαντικά το κύρος και η αξιοπιστία της απέναντι στους πελάτες και τους συνεργάτες της.

2.2 Απειλές και Τύποι επιθέσεων

Βασικό τμήμα στο σχεδιασμό ενός συστήματος ασφαλείας είναι να εξακριβώσουμε τι επίπεδο ασφαλείας απαιτείται και ποιες απειλές θα κληθεί να αντιμετωπίσει. Οπότε το πρώτο βήμα είναι να αναγνωρίσουμε τους κινδύνους. Οι σημαντικότεροι τύποι επιθέσεων στο internet περιλαβάνουν:

- *Μη εξουσιοδοτημένη χρήση (Masquerade)*
  Χαρακτηρίζονται οι επιθέσεις κατά τις οποίες ένας μη εξουσιοδοτημένος χρήστης προσπαθεί να αποκτήσει πρόσβαση σε προστατευόμενους πόρους, στην απλοϊκότερη περίπτωση μέσω της υποκλοπής κάποιου συνθηματικού.
- *Μη ενεργός ή παθητική παρακολούθηση (Passive tapping)*
  Επιθέσεις τέτοιου είδους περιλαμβάνουν την παρακολούθηση των δεδομένων που διακινούνται μεταξύ των χρηστών ενός δικτύου. Σε αυτού του είδους την επίθεση, ο επιτιθέμενος δεν τροποποιεί τα δεδομένα.
- *Ενεργός παρακολούθηση (Active tapping)*
  Σε αντίθεση με το προηγούμενο είδος επίθεσης, στην περίπτωση αυτή τα δεδομένα που μεταδίδονται τροποποιούνται. Το είδος αυτών των επιθέσεων εντοπίζεται ευκολότερα σε σχέση με το προηγούμενο, αλλά η επικινδυνότητα των επιθέσεων είναι μεγαλύτερη.
- *Αποποίηση (Repudiation)*
  Στην κατηγορία αυτή εμπίπτουν οι περιπτώσεις που κάποια οντότητα αποποιείται τη συμμετοχή της σε μία επικοινωνία.
- *Άρνηση Παροχής Υπηρεσίας (Denial of Service)*
  Αυτού του είδους η επίθεση έχει ως στόχο την παρεμπόδιση της ομαλής λειτουργίας ενός δικτύου. Το αποτέλεσμα μπορεί να είναι είτε απώλεια των μηνυμάτων που μεταδίδονται, είτε καθυστέρηση στην εξυπηρέτηση, είτε πλήρης άρνηση παροχής υπηρεσιών.
- *Επανεκπομπή μηνυμάτων (Replay)*

Στις επιθέσεις τέτοιου είδους ένας ενεργός εισβολέας παρεμβαίνει στην επικοινωνία μεταξύ δύο οντοτήτων, καταγράφει έγκυρα μηνύματα που μεταδίδονται από τη μία οντότητα στην άλλη, ακολούθως τα αναπαράγει και τα αποστέλλει σε μεταγενέστερο χρόνο στην άλλη. Στόχος του ενεργού εισβολέα είναι να προσποιηθεί ότι είναι ένας εξουσιοδοτημένος χρήστης ή να δημιουργήσει τις προϋποθέσεις για επίθεση τύπου άρνησης παροχής υπηρεσίας.

- *Ανάλυση επικοινωνίας (Traffic Analysis)*

  Οι επιθέσεις τέτοιου είδους αφορούν την παρακολούθηση της ροής των δεδομένων που ανταλλάσσονται από τους χρήστες ενός δικτύου. Σε τέτοιες επιθέσεις, στόχος δεν είναι η υποκλοπή της πληροφορίας που διακινείται, αλλά η έμμεση εξαγωγή συμπερασμάτων με βάση την ταυτότητα των επικοινωνούντων, το χρόνο και την ποσότητα των δεδομένων.
- *Κακόβουλο Λογισμικό (Viruses, Trojan Horses, Worms)*

  Ο αρχικός στόχος του κακόβουλου λογισμικού ήταν οι αυτόνομοι υπολογιστές, επομένως η αντιμετώπιση του αφορούσε την ασφάλεια τους. Παρόλα αυτά, νέες μορφές κακόβουλου λογισμικού έχουν ως στόχο την προσβολή δικτυακών περιβαλλόντων. Για παράδειγμα, ένας δούρειος ίππος είναι δυνατόν, αφού εγκατασταθεί σε ένα σύστημα, να υποκλέψει δεδομένα ή να δημιουργήσει προϋποθέσεις για καλυμμένες επιθέσεις τύπου άρνησης παροχής υπηρεσιών.

Στην ορολογία της γνωστικής περιοχής της ασφάλειας στην τεχνολογία της πληροφορίας, περιλαμβάνονται οι ακόλουθοι συχνά χρησιμοποιούμενοι όροι:

- *Αδυναμία (Vulnerability):* αναφέρεται ως ένα ελάττωμα στο σχεδιασμό ή την υλοποίηση ενός πρωτοκόλλου, μιας υπηρεσίας, ή ενός συστήματος το οποίο μπορεί να εκμεταλλευτεί ένας εισβολέας (intruder) για να παραβιάσει ένα σύστημα ενδεχομένως για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή πόρους. Για παράδειγμα, η δυνατότητα των περισσοτέρων διεπαφών δικτύου (network interfaces) να λειτουργούν σε μία κατάσταση (promiscuous mode) όπου λαμβάνουν όλα τα πλαίσια (frames) ενός τοπικού δικτύου, αποτελεί μία αδυναμία του σχεδιασμού των τοπικών δικτύων γιατί επιτρέπει σε εισβολείς να συλλέξουν σημαντικές πληροφορίες, όπως διακινούμενα συνθηματικά.

- *Απειλή (Threat):* είναι η οντότητα που μπορεί να προκαλέσει την παραβίαση της ασφάλειας ενός συστήματος, είτε μεμονωμένου τμήματος είτε ολόκληρου του δικτύου, ή τη ζημιά σε κάποιους πόρους του.
- *Επίθεση (Attack):* είναι η εκμετάλλευση μιας αδυναμίας από έναν εισβολέα για την πραγματοποίηση μιας απειλής. Σε περιβάλλοντα δικτύου οι επιθέσεις μπορεί να προέρχονται από ενεργούς (active) εισβολείς ή από μη-ενεργούς (passive).
- *Αντίμετρα (Countermeasures):* είναι ένας μηχανισμός ή μία διαδικασία με στόχο τον περιορισμό ή την εξάλειψη των επιπτώσεων μιας απειλής. Για παράδειγμα, η χρήση αποτελεσματικών μηχανισμών κρυπτογραφίας κατά την αποστολή δεδομένων σε ένα δίκτυο μπορεί να διαφυλάξει την εμπιστευτικότητα των διακινούμενων πληροφοριών.

2.2.1 Άρνηση Παροχής Υπηρεσίας (Denial of Service)

Μία από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι crackers για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές είναι οι επιθέσεις DoS (Denial of Service). Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων (bogus requests) που δέχεται από τον επιτιθέμενο. Υπάρχουν διάφορα είδη επιθέσεων DoS, πολλά από τα οποία εκμεταλλεύονται αδυναμίες του ζεύγους πρωτοκόλλων TCP/IP. Για τα περισσότερα από αυτά είναι ήδη γνωστά τα αντίστοιχα μέτρα προστασίας. Συγκεκριμένα, οι διαχειριστές συστημάτων μπορούν να εγκαθιστούν patches σε λειτουργικά συστήματα και προγράμματα-διακομιστές, ώστε να αποτρέπουν επιθέσεις DoS ή να ελαχιστοποιούν τις συνέπειες τους. Όπως, όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων DoS. Σε γενικές γραμμές είναι επιθέσεις που έχουν σκοπό να αποτρέψουν τη χρήση ενός συστήματος από όλους (δηλαδή τους νόμιμους χρήστες του). Δεν γίνονται προσπάθειες παραβίασης ή κλοπής στοιχείων, είναι όμως δυνατός ο συνδυασμός τους με άλλες επιθέσεις που

γίνονται παράλληλα με σκοπό να "παραπλάνήσουν" τα συστήματα ανίνχνευσης (Intrusion Detection Systems) και τους διαχειριστές από την πραγματική απειλή.

Για τις απειλές αυτές δεν υπάρχει η "Εύκολη Λύση". Οι επιθέσεις DoS/DDoS είναι ακόμα σε μεγάλο βαθμό σε πεδίο έρευνας. Δυνητικός στόχος είναι οποιοδήποτε σύστημα στο Διαδίκτυο από απλά υπολογιστικά συστήματα (hosts) μέχρι ολόκληρα δίκτυα (domains). Ιδιαίτερα σημαντικό πρέπει να επισημανθεί ότι ακόμα και ενεργά στοιχεία δικτύου (π.χ. routers) είναι ευάλωτα και αποτελούν πιθανούς στόχους. Οι επιθέσεις αυτές ποικίλουν από απλά «παιχνίδια» μεταξύ hackers μέχρι και πιθανό «όπλο» από ανταγωνιστές και επιθέσεις σε σημαντικούς επιχειρηματικούς και πολιτικούς στόχους, αλλά και δυνητικά μπορεί να αποτελέσσουν μέσο για ένας κυβερνοπόλεμο, τρομοκρατικού τύπου.

Η εξέλιξη των DoS επιθέσεων μπορεί να διακριθεί σε τρεις φάσεις:

Πρώτη Φάση (αρχές δεκαετίας 90)

DoS–Επιθέσεις Άρνησης Υπηρεσίας. Αρχικά εκμετάλευση προβλημάτων (bugs) ή αδυναμιών λογισμικού. Οι πρώτοι στόχοι ήταν Single hosts -single services. Σε κάποιες περιπτώσεις αρκούσε ένα μοναδικό, κατάλληλα κατασκευασμένο, πακέτο.

Δεύτερη Φάση (1996-2000)

Κλήσεις εξυπηρέτησης από πολλές πηγές για κατανάλωση υπολογιστικών πόρων. Οι υποδομές του Internet χρησιμοποιούνται για "ενίσχυση" της έντασης των επιθέσεων.

Τρίτη Φάση (μετά το 2000)

Distributed DoS–Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας. Στόχο αποτελεί το δικτυακό εύρος (Bandwidth). Χρήση πολλαπλών ελεγχόμενων υπολογιστών, σε πολλαπλά στάδια επίθεσης με κλιμάκωση της επίθεσης.

Για να γίνει αντιληπτό το μέγεθος του προβλήματος αναφέρονται μερικά μεγάλα περιστατικά:

2000: Θύματα τέτοιων επιθέσεων έπεσαν μεγάλες εταιρίες που δραστηριοποιούνται στο internet, όπως CNN, Amazon, Yahoo, eBay κ.λπ.

2002: Ο ISP Cloud Nine αναγκάζεται να διακόψει την επιχειρηματική του δραστηριότητα. Προσπάθεια προσβολής των Route Name Servers.

Το 2004 το Computer Security Institute εκτιμά το κόστος από τις επιθέσεις DoS/DDoS σε 26 million USD. Αναφέρονται σε παρατηρήσεις κάποια αριθμητικά

μεγέθη επιθέσεων 12.000 περιστατικά σε τρεις εβδομάδες (Moore at al, 2001), και τουλάχιστον 10.000 περιστατικά ανά μήνα (Hussain et al, 2003).

Οι μεθοδολογίες που χρησιμοποιούνται είναι παρόμοιες με αυτές της παράνομης πρόσβασης. "Buffer overflows" σε κακώς σχεδιασμένα σημεία εισόδου στοιχείων είναι δυνατό να οδηγήσουν σε εγγραφές τμημάτων της μνήμης του συστήματος. Το αποτέλεσμα είναι άνοιγμα «διόδων πρόσβασης» ή η πλήρης αστοχία του συστήματος. Επίσης, κάποιες «αοριστίες» σε ορισμένες προδιαγραφές δικτυακών πρωτοκόλλων μπορούν να οδηγήσουν σε προβλήματα κατά την υλοποίησή τους. Υπάρχουν και ειδικά σχεδιασμένα κακόβουλα πακέτα που στοχεύουν σε αυτές τις αδυναμίες και μπορούν να προκαλέσουν σημαντικά προβλήματα. Για παράδειγμα, τα Land IP DoS attack: ειδικά πακέτα TCP/SYN με την ίδια διεύθυνση προέλευσης και προορισμού. Επίσης το φαινόμενο **Teardrop attack**: αποστολή κατακερματισμένων (fragmented) πακέτων IP σε συστήματα συνδεμένα στο δίκτυο. Εδώ ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση πακέτων IP. Κάθε πακέτο περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου εκεί περιγράφεται η θέση του στο αρχικό πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, "Teardrop", το οποίο τεμαχίζει πακέτα IP σε μικρότερα με λανθασμένες πληροφορίες στο αναφερόμενο πεδίο. Όταν ο υπολογιστής-στόχος προσπαθήσει να συναρμολογήσει τα τμήματα αυτά, θα κολλήσει ή θα κάνει επανεκκίνηση, εκτός και ο διαχειριστής του συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch.

Αυτό που επιτυγχάνεται είναι η εξάντληση των υπολογιστικών πόρων με τη συνεχή αποστολή μεγάλου αριθμού «νόμιμων» αιτημάτων εξυπηρέτησης. Όμως, τότε ο στόχος αναλλώνεται με αυτή τη διαδικασία χωρίς να προσφέρει καμμιά χρήσιμη υπηρεσία.

SYN Flooding attack

Πριν τη συνεδρία μεταξύ ενός πελάτη και ενός διακομιστή, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και σαν «ακολουθία χειραψίας» (handshake sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize ACKnowledge) του διακομιστή, ο τελευταίος θα επιμείνει για προκαθορισμένο χρονικό διάστημα. Ένας cracker, εκμεταλλευόμενος αυτή τη συμπεριφορά, μπορεί να υπερφορτώσει το διακομιστή-θύμα ή να τον κρεμάσει. Κατά τη διάρκεια μιας τέτοιας

επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση IP, κρύβοντας με τον τρόπο αυτό τα ίχνη του.

Ping Flooding attack

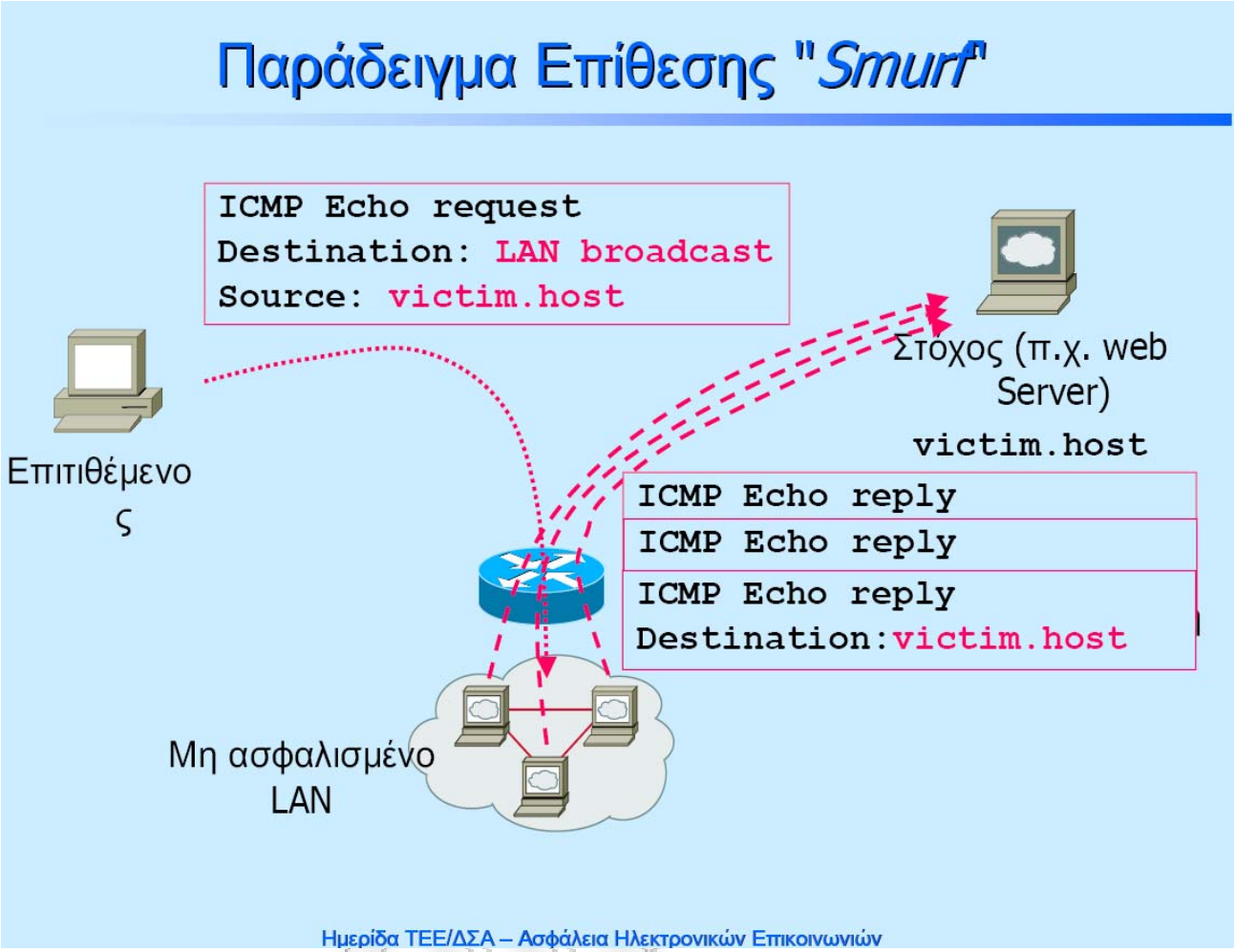
Αίτημα PING[1] (ή αλλιώς αίτηση ICMP[2]), προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (>64 Kb). Τέτοια παράτυπα πακέτα μπορούν να κρεμάσουν υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

Smurf attack

Επιτυγχάνεται αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής (broadcast address) στο υπό επίθεση δίκτυο ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP πλαστογραφείται, ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου, λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με αυτό τον τρόπο πληροφορικό «μποτιλιάρισμα». Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε 255 μηχανήματα (στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης Smurf, από κάθε αίτηση PING μπορούν να παραχθούν μέχρι και 255 απαντήσεις. Έτσι, μπορεί κανείς να αντιληφθεί τον υπέρογκο αριθμό των άχρηστων πακέτων που δημιουργούνται, όταν ο επιτιθέμενος στέλνει εκατοντάδες ή και χιλιάδες πακέτα ICMP.

[1] Εργαλείο για να διαπιστώνεται αν μια δεδομένη IP διεύθυνση είναι προσβάσιμη. Το πρόγραμμα στέλνει ένα πακέτο σε μια διεύθυνση και στη συνέχεια αναμένει μια απάντηση από τον υπολογιστή στον οποίο αντιστοιχεί.

[2] Επέκταση του πρωτοκόλλου IP για την αποστολή μυνημάτων λαθών και ελέγχου. Χρησιμοποιείται από την εντολή PING για να διαπιστώνεται αν ένα μηχάνημα είναι on-line, από δρομολογητές (routers), κάθε φορά που ειδοποιούν ένα μηχάνημα για τη διαθεσιμότητα ενός κόμβου στον οποίο απευθύνονται κλπ.



Σχήμα 2: Παράδειγμα επίθεσης Smurf
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

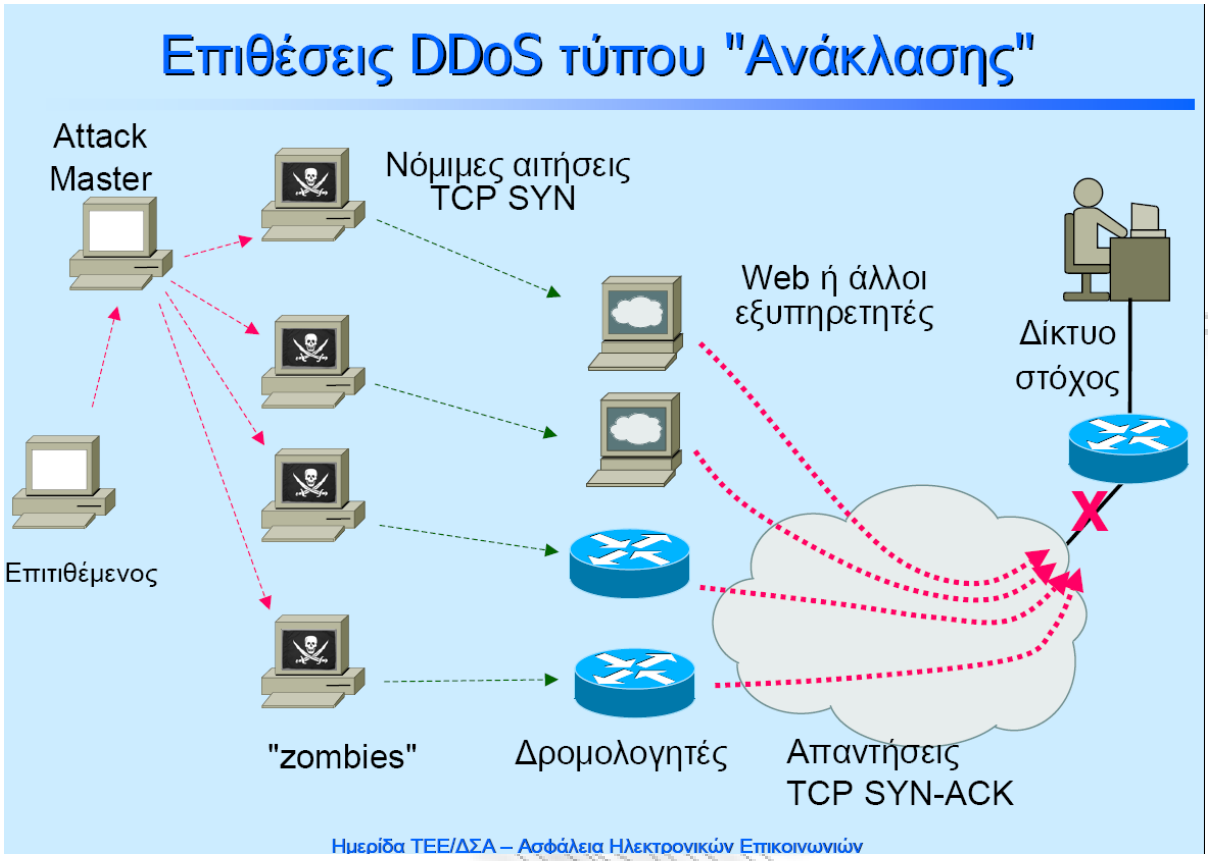
Μερικές εκατοντάδες συνεχείς ροές κίνησης (flows) αρκούν να επηρρεάσουν σημαντικά ακόμα και ένα μεγάλο δίκτυο. Η εισερχόμενη κίνηση μπορεί να ελεγχθεί μόνον πριν από το δίκτυο του τελικού στόχου, στους παρόχους δικτυακής διασύνδεσης (upstream providers). Συνήθως οι διευθύνσεις προέλευσης στα πακέτα επίθεσης είναι παραποιημένες (spoofing[3]). Σημαντικό είναι να επισημανθεί πως τα συστήματα που λαμβάνουν μέρος στην επίθεση μπορεί να ελέγχονται χωρίς γνώση των χρηστών τους (ακόμα και μέσω του προσωπικού υπολογιστή στο σπίτι). Υπάρχουν πολλά εργαλεία διαθέσιμα για τέτοιου είδους "χτίσιμο" επιθετικών δικτύων (rootkits).

[3] Τεχνική για την απόκτηση εξουσιοδοτημένης πρόσβασης σε δικτυωμένα μηχανήματα. Ο εισβολέας αποστέλλει μυνήματα με IP διεθύνσεις που δείχνουν ότι προέρχονατι από «έμπιστο» port. Ο επίδοξος cracker αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια σιεύθυνση που αντιστοιχεί σε ένα τέτοιο port. Στη συνέχεια, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλλει, ώστε να φαίνεται ότι προέρχονατι από ένα έμπιστο port. Η κατάλληλη ρύθμιση δρομολογητών και firewalls μπορεί να αποτρέψει τέτοιου είδους επιθέσεις.

Όταν σε μια επίθεση DoS συμμετέχουν περισσότερα από ένα μηχάνημα, έχουμε το φαινόμενο των κατανεμημένων επιθέσεων DoS (Distributed Denial of Service attacks). Στις επιθέσεις του είδους είναι δυνατό να συμμετέχουν και προσωπικοί υπολογιστές. Ο επιτιθέμενος cracker κατορθώνει με κάποιο τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία τους στην επίθεση. Τη στιγμή που θα την εξαπολύσει στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής DDoS-attack master). Τότε εκείνο ειδοποιεί μια ορισμένη χρονική στιγμή καθένα από τους υπόλοιπους υπολογιστές (πελάτες DDoS) και όλοι μαζί αρχίζουν να βάλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να «πλημμυρίσει» και να μη μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών.

Αν και ένα μηχάνημα που έχει πέσει θύμα επίθεσης DoS ή DDoS μπορεί να επανέλθει σε ομαλή λειτουργία σχετικά εύκολα, υπάρχουν έμμεσες αρνητικές συνέπειες. Τέτοιες είναι οι οικονομικές ζημιές που οφείλονται στο χρόνο που ένας κεντρικός διακομιστής είναι εξουδετερωμένος, καθώς και στο πλήγμα στο κύρος της εταιρίας στην οποία ανήκει ο διακομιστής-θύμα. Είναι γνωστό εξάλλου, ότι ο ανταγωνισμός πλέον είναι πολύ έντονος μεταξύ των παροχέων internet.

Στο παρακάτω σχήμα 3 απεικονίζεται επίθεση τύπου DDoS



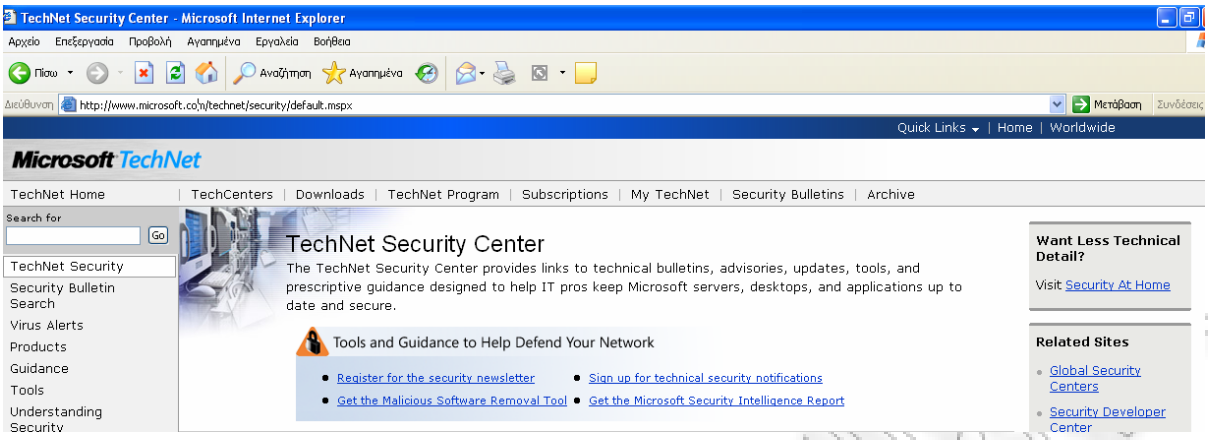
Σχήμα 3: Παράδειγμα επίθεσης DDoS
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικών επικοινωνιών, Αθήνα 01.06.2006)

2.2.2 Ιοί (Viruses)

Το internet έδωσε τη δυνατότητα για την ταχεία και ευρεία εξάπλωση των ιών. Στην προ-internet εποχή ο μόνος τρόπος να μολυνθεί με ιό ένας υπολογιστής ήταν να χρησιμοποιηθούν μολυσμένες δισκέτες. Τότε η μόλυνση με ιό ήταν κάτι όχι ασυνήθιστο ώσπου ανακάλυπταν ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του internet στη ζωή μας, και συγκεκριμένα με το email. Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το email όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντας τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται.

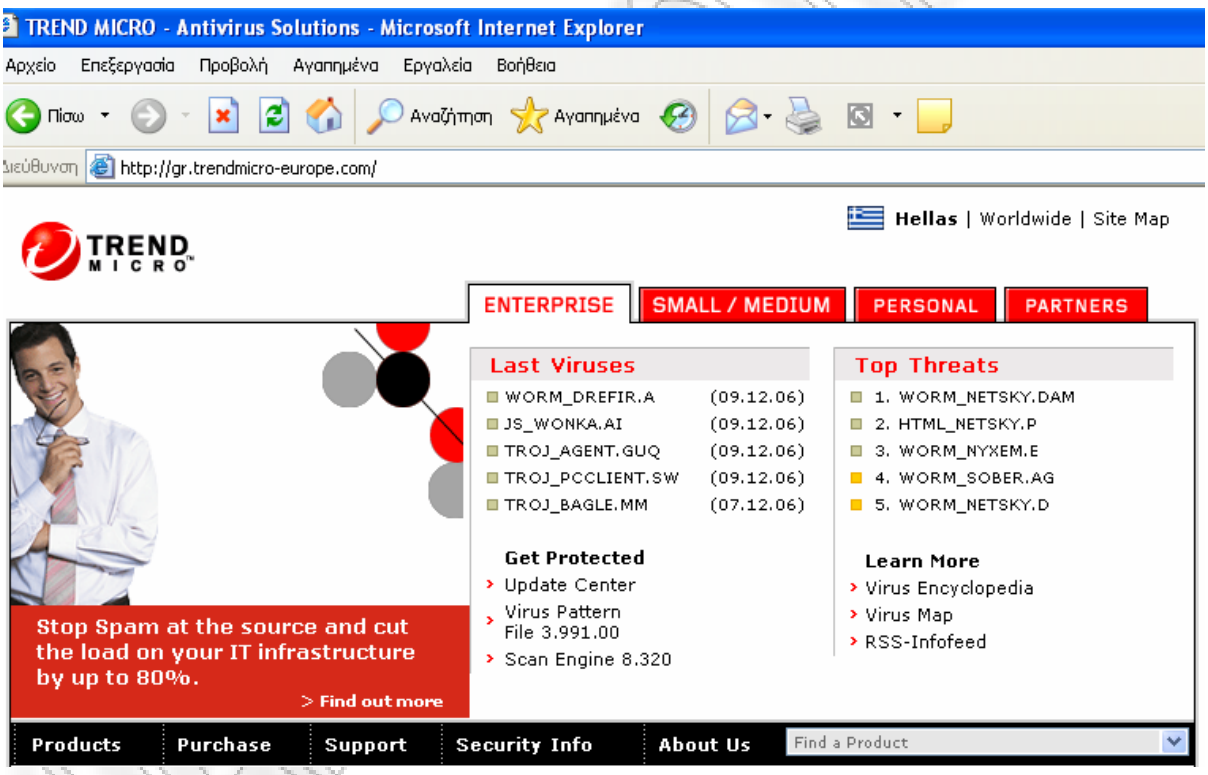
Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία/script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου Word, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Ας πάρουμε όμως τα πράγματα από την αρχή.

Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκριση μας και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο internet. Υπάρχουν αρκετά ήδη ιών: α) αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα, β) αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses), γ) αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως, π.χ., του Word και του Excel (Macro viruses), και δ) οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μία ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό email κειμένου να μπορεί να κάνει ζημιά. Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί μας προτρέπουν να αναβαθμίζουμε στη νεότερη έκδοση όλες τις εφαρμογές μας, ειδικά αυτές που σχετίζονται με το internet. Με αυτό τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης. (π.χ. μέσω updates για τις διάφορες εφαρμογές http://www.microsoft.com/technet/security ή προγραμμάτων προστασίας, π.χ. http://gr.trendmicro-europe.com)



Εικόνα 3: MICROSOFT **http://www.microsoft.com/technet/security**

Updates για εφαρμογές Microsoft



Εικόνα 4: TREND MICRO http://gr.trendmicro-europe.com

Updates για προστασία από Ιούς, Trojans, Worms

2.2.3 Δούριοι Ίπποι (Trojan Horses)

Δεν θα ήταν υπερβολή, εάν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών internet προέρχεται από τους δούρειους ίππους (Trojan Horses). Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το internet, το trojan-διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το trojan-πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο cracker αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως, π.χ./ να του διαγράψει το BI0S ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου.

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Πώς όμως μπορεί να «μπεί» ένα Trojan σε έναν υπολογιστή; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο email ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λπ. Υπάρχουν δύο τρόποι για να αποφεύγουμε τα Trojan. Ο πρώτος είναι να χρησιμοποιούμε ένα πρόγραμμα «Antivirus» ή «Anti-Trojan». Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν τα κατεβάζουμε ακόμα και στην περίπτωση που είναι ήδη

εγκατεστημένα στο PC και να τα διαγράφουν. Ο άλλος τρόπος είναι να χρησιμοποιούμε ένα προσωπικό firewall[4]. Κάθε φορά που ένα Trojan-διακομιστής θα προσπαθεί να «βγει» στο internet, το firewall θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος, καλό είναι να κατεβάζουμε στον υπολογιστή μας μόνο «έμπιστα» προγράμματα, από γνωστούς, επίσημους δικτυακούς τόπους.

2.2.4 Σκουλήκια (Worms)

Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το Melissa worm έχει αρχίσει ένα νέο γύρο καλυμμένο αυτήν τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα email σε όλη τη λίστα επαφών του Outlook. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα email από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Η μαζική αποστολή email, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

[4] Ένας από τους ρόλους του firewall είναι ο διαχωρισμός δύο δικτων. Η μέθοδός του βασίζεται σε επίπεδο υλικού ή/και λογισμικού και χρησιμοποιείται για να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Συχνά τα firewall χρησιμοποιούνται για να εμποδίζουν χρήστες του διαδικτύου να εισέρχονται σε ιδωτικά δίκτυα, τα οποία είναι και αυτά συνδεμένα με το internet. Γενικά μπορούμε να πούμε ότι ένα firewall διαχωρίζει ένα δίκτυο από κάποιο άλλο.

2.2.5 Ανεπιθύμητη Αλλογραφία (SPAM email)

Ένα φαινόμενο που ολοένα γίνεται πιο έντονο είναι το φαινόμενο της ενοχλητικής αλληλογραφίας. Ο χρήστης λαμβάνει στη διεύθυνση ηλεκτρονικής αλληλογραφίας του πληθώρα μηνυμάτων από άγνωστες διευθύνσεις, τα οποία συνήθως έχουν σαν θέμα κάποια διαφήμιση. Οι πληροφορίες που περιέχουν είναι άχρηστες για τον παραλήπτη αλλά γεμίζουν το χώρο της ηλεκτρονικής αλληλογραφίας. Πολλές φορές περιέχουν links που παραπέμπουν σε ιστοσελίδες πορνογραφικού περιεχομένου, διαφημίσεις για αγορά φαρμάκων (μη νόμιμης φυσικά), τραπεζικά προϊόντα κλπ. Είναι ιδιαίτερα χρονοβόρα διαδικασία να σβήνονται αυτά τα μηνύματα καθώς μπορεί σε μια μέρα να λάβει κανείς ίσως και πάνω από εκατό τέτοια email. Επιπλέον, εάν απαντήσει στις συνδέσεις που ρωτούν αν «ο χρήστης δεν επιθυμεί να συνεχίσει να λαμβάνει μηνύματα από τη συγκεκριμένη εταιρία», είναι ένα τέχνασμα για να επιβεβαιώνεται η ηλεκτρονική του διεύθυνση και να λάβει περισσότερα μηνύματα από διαφορετικούς φαινομενικά αποστολείς. Επίσης υπάρχει ο κίνδυνος, πχ σε τέτοια emails να ζητούνται προσωπικά δεδομένα (πχ τραπεζικοί λογαριασμοί ή αριθμοί πιστωτικών καρτών) και ο λήπτης να πέσει θύμα οργανωμένης απάτης. Για αυτό το λόγο, τα προγράμματα antivirus αλλά και οι παροχείς λογαριασμών ηλεκτρονικού ταχυδρομείου χρησιμοποιούν anti-spam φίλτρα για να περιοριστεί το φαινόμενο. Όμως η τακτική των ελέγχων που πραγματοποιούν τα φίλτρα αυτά (ύποπτος αποστολέας, αναζήτηση ύποπτων λέξεων στο κείμενο και ύποπτων Links στο email) δε φαίνεται να είναι αποτελεσματική. Τα spam emails περιέχουν εικόνες ώστε να μη μπορούν να εντοπιστούν λέξεις κλειδιά, και οι αποστολείς συγκεντρώνονται σε χώρες όπου δεν ισχύει κάποιος σχετικός νόμος (πχ Ρωσία, Ανατολική Ευρώπη, Ασία). Χαρακτηριστικό είναι ότι ο Bill Gates (πρόεδρος της Microsoft) είχε δηλώσει πριν τρία χρόνια ότι το 2006 το φαινόμενο του Spam θα είχε εξαλειφθεί. Αντίθετα όμως έχει διπλασιαστεί βρίσκοντας νέους τρόπους να εξαπλώνεται (New York Times, 6-12-2006, http://www.nytimes.com/2006/12/06/technology/06spam.html)

2.2.6 Dialers

Οι dialers είναι Προγράμματα που εγκαθίστανται στον υπολογιστή του χρήστη μέσω διαδικτύου και πραγματοποιούν μέσω του modem του ακούσια κλήσεις υψηλής χρέωσης. Τα προγράμματα dialer είναι λογισμικό το οποίο μπορεί να μεταδοθεί μέσω διαδικτύου και να εγκατασταθεί στον ηλεκτρονικό υπολογιστή. Αυτό που κάνουν οι dialers, αφού εγκατασταθούν στον υπολογιστή του χρήστη είναι να αλλάξουν τις ρυθμίσεις (settings) του modem από μία συγκεκριμένη σύνδεση στο διαδίκτυο σε μία άλλη. Συνήθως η αλλαγή είναι από το συνήθη αριθμό του παροχέα Internet (ISP) που χρησιμοποιείται, σε έναν αριθμό αυξημένης χρέωσης, είτε αυτός είναι της σειράς 90XXXXXXXX είτε αριθμός στο εξωτερικό (00XXXXXXXXX).

Οι dialers μπορεί να είναι ένας νόμιμος και βολικός τρόπος για να πληρώσει ο χρήστης πρόσβαση σε ειδικό περιεχόμενο μέσω του διαδικτύου (π.χ. λογισμικό, παιχνίδια, SMS logos, ερωτικό περιεχόμενο), αντί χρήσης πιστωτικής κάρτας.

Στην περίπτωση αυτή, ο χρήστης αντί να χρησιμοποιήσει πιστωτική κάρτα για τη χρέωσή του ειδικού περιεχομένου κάποιου διαδικτυακού τόπου, χρεώνεται για το περιεχόμενο αυτό στο λογαριασμό του τηλεφώνου του, μέσω των αριθμών αυξημένης χρέωσης, όπως ακριβώς συμβαίνει και με τις υπηρεσίες προστιθέμενης αξίας αυξημένης τιμολόγησης που καλεί από το τηλέφωνό του (π.χ. Audiotex).

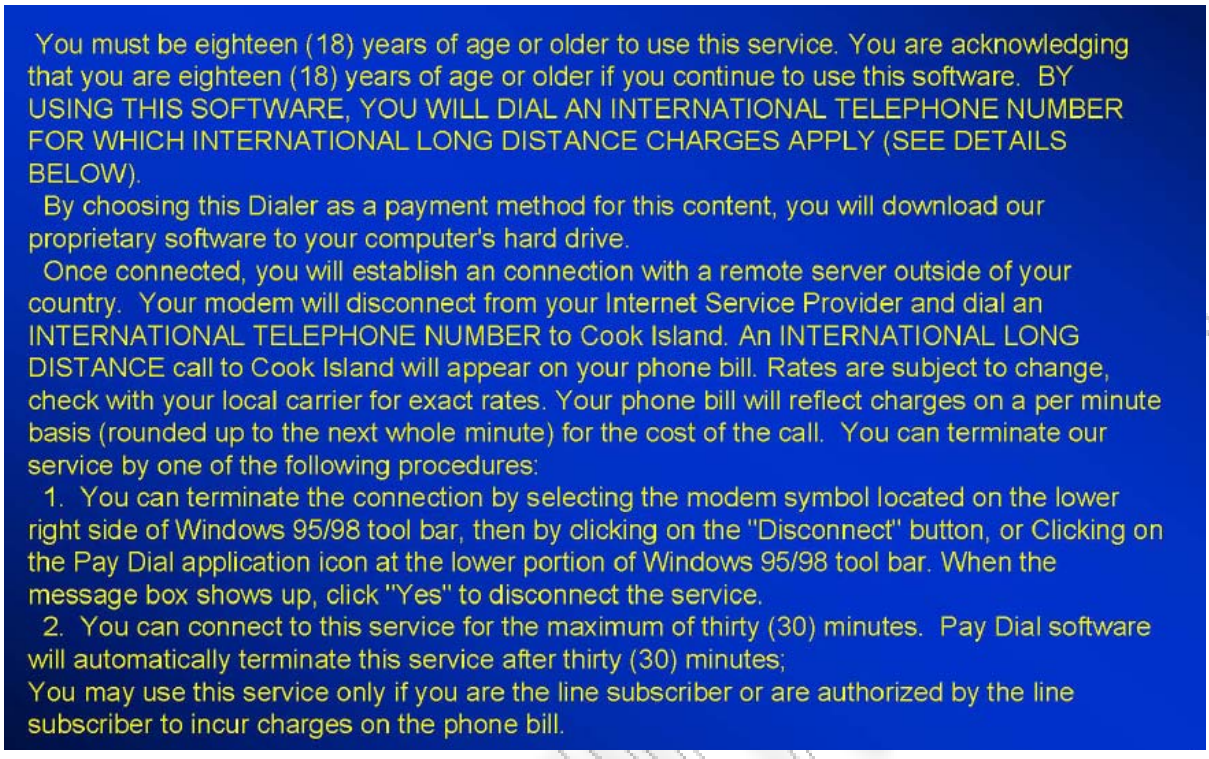
Ο τρόπος με τον οποίο οφείλουν να λειτουργούν οι νόμιμοι dialerdialers, προστατεύοντας τον καταναλωτή, είναι ο ακόλουθος: αν προσπαθήσετε να επισκεφτείτε μία ιστοσελίδα η οποία προσφέρει ειδικό περιεχόμενο με αυτόν τον τρόπο, θα εμφανιστεί στην οθόνη σας ένα παράθυρο διαλόγου το οποίο σας ρωτά αν θέλετε να κατεβάσετε το συγκεκριμένο πρόγραμμα dialer. Επίσης ενημερώνει για το είδος της υπηρεσίας την οποία πρόκειται να χρησιμοποιήσετε και για τη χρέωσή της. Αν επιλέξετε "yes", το λογισμικό του dialer εγκαθίσταται στον υπολογιστή σας. Το λογισμικό αλλάζει τον αριθμό σύνδεσής σας στο διαδίκτυο με αυτόν της αυξημένης χρέωσης, ενώ εσείς έχετε τη δυνατότητα πρόσβασης στο ειδικό περιεχόμενο ενώ χρεώνεστε με αυξημένη τιμολόγηση. Καθόλη τη διάρκεια πρόσβασης στο ειδικό περιεχόμενο, υπάρχει στην οθόνη σας ένδειξη ότι χρησιμοποιείται σύνδεση στο

διαδίκτυο αυξημένης χρέωσης. Στη συνέχεια, μόλις αποσυνδεθείτε από τη συγκεκριμένηιστοσελίδα, ο dialer απεγκαθίσταται από τον υπολογιστή σας, και η σύνδεση του modem επιστρέφει στον αριθμό του παροχέα Internet (ISP) που χρησιμοποιείται.

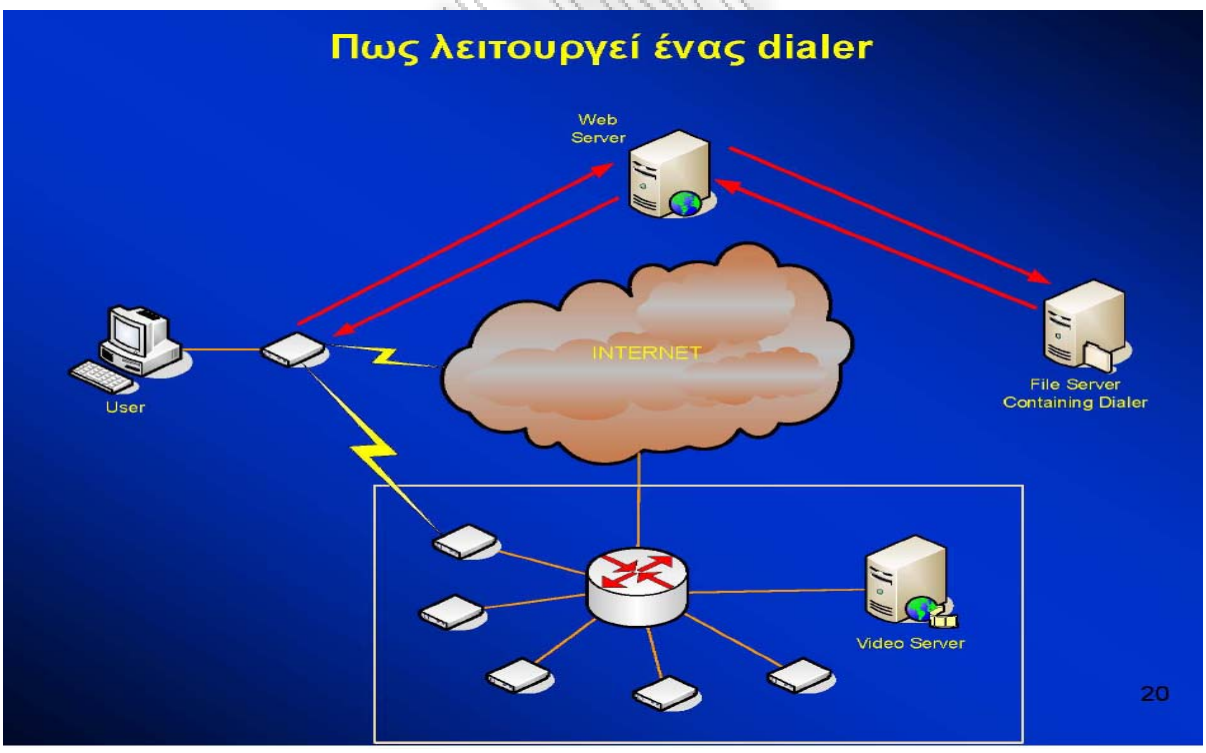
Το πρόβλημα ξεκινά όταν ο χρήστης δεν γνωρίζει ότι έχει «κατεβάσει» (download) έναν dialer από το διαδίκτυο ή όταν δεν γνωρίζει τι κάνει αυτός ο dialer τον οποίο έχει κατεβάσει. Η απάτη μέσω dialers συμβαίνει όταν ο διαδικτυακός τόπος δεν καθιστά σαφές για τον χρήστη ότι με τις ενέργειές του, οδηγείται στην εγκατάσταση λογισμικού στον ηλεκτρονικό του υπολογιστή ή ότι η σύνδεσή του στο διαδίκτυο θα αλλάξει, όχι μόνο για την πρόσβαση σε ειδικό περιεχόμενο, αλλά σε πιο συχνή ή και μόνιμη βάση. Οι dialers αυτοί μπορεί να πραγματοποιούν συνέχειακλήσεις προς έναν αριθμό αυξημένης χρέωσης, εις βάρος του χρήστη, κατά τη διάρκεια όλουτου εικοσιτετραώρου, ακόμα και κάθε λίγα λεπτά, αρκεί ο υπολογιστής να είναι αναμμένος. Υπάρχει ακόμα η πιθανότητα, κάποιοι dialers να φτάσουν στον χρήστη ως συνημμένα (attachment) σε κάποιο ηλεκτρονικό μήνυμα (email). Αυτοί δεν είναι εύκολο να ανιχνευθούν, και εγκαθίστανται χωρίς να ζητήσουν τη συγκατάθεση του χρήστη. Απάτες τέτοιου είδους μπορεί ακόμα να σιγήσουν τους ήχους κλήσης (dialing) στο διαδίκτυο που κάνει το modem για να αποκρύψουν το γεγονός ότι το modem πραγματοποιεί μία κλήση.

Πρόσφατα, το πρόβλημα με τις απάτες μέσω dialers έχει πάρει σημαντικές διαστάσεις και στην Ελλάδα. Ήδη, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχει λάβει μεγάλο αριθμό καταγγελιών από χρήστες διαδικτύου, οι οποίες αφορούν την υπέρογκη και εν αγνοία τους χρέωσή τους για κλήσεις σε αριθμούς της σειράς 90XXXXXXXX ή αριθμούς του εξωτερικού (00XXXXXXXXXXX), ενώ αυτές οι κλήσεις συνδέονται με την πρόσβασή τους στο διαδίκτυο. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, στην προσπάθειά της να αντιμετωπίσει το πρόβλημα αυτό στα πλαίσια των αρμοδιοτήτων της, εξετάζει την κατάρτιση Κώδικα Δεοντολογίας για τις Υπηρεσίες Προστιθέμενης Αξίας Αυξημένης Τιμολόγησης, στα πλαίσια του οποίου ρυθμίζονται και θέματα που αφορούν τους dialers και η θέσπιση κανόνων λειτουργίας οι οποίοι θα εξασφαλίσουν την προστασία των χρηστών από παράνομους dialers.

Στην επόμενη εικόνα φαίνεται παράδειγμα νόμιμου dialer:



Εικόνα 5: Παράδειγμα νόμιμου dialer
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)



Σχήμα 4: Σχηματική παράσταση λειτουργίας dialer
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

2.3 Wardriving

Ο όρος «Wardriving» χρησιμοποιείται για να περιγράψει την πρακτική εκείνη κατά την οποία ένας χρήστης του Διαδικτύου περιπλανιέται στους δρόμους συνοικιών εφοδιασμένος με συσκευή που έχει δυνατότητα ασύρματης πρόσβασης στο Διαδίκτυο με σκοπό να εντοπίσει ασύρματα δίκτυα πρόσβασης στο Διαδίκτυο, οικιακής ή επαγγελματικής χρήσης, και να χαρτογραφήσει την ύπαρξή τους για στατιστικούς ή άλλους λόγους, συνήθως με σκοπό το hacking.

Το Wardriving αναφέρθηκε για πρώτη φορά στις ΗΠΑ όταν οσύμβουλος ασφαλείας τηλεπικοινωνιακών δικτύων Peter M. Shipley έκανε, το 2000, έρευνα για τα ασύρματα δίκτυα στην πόλη Berkeley της California και δημοσιοποίησε τα αποτελέσματα των ερευνών του στο ετήσιο DefCon συνέδριο hackers τον Ιούλιο του 2001. Η έρευνα του Shipley αποσκοπούσε να δείξει τα κενά ασφαλείας των ασύρματων δικτύων που αναπτύσσονταν ραγδαία στο Berkeley, και να προκαλέσει την προσοχή των καθ' ύλη αρμοδίων φορέων για τη βελτίωση της ασύρματης τεχνολογίας δικτύων αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων. Με την έρευνά του ο Shipley απέδειξε ότι είναι δυνατή η πρόσβαση σε ασύρματο δίκτυο, κάνοντας χρήση απλών εργαλείων, ακόμη και από απόσταση σαράντα χιλιομέτρων μακριά από την κορυφή του κτιρίου όπου έχει τοποθετηθεί πομπός ασύρματης δικτύωσης.

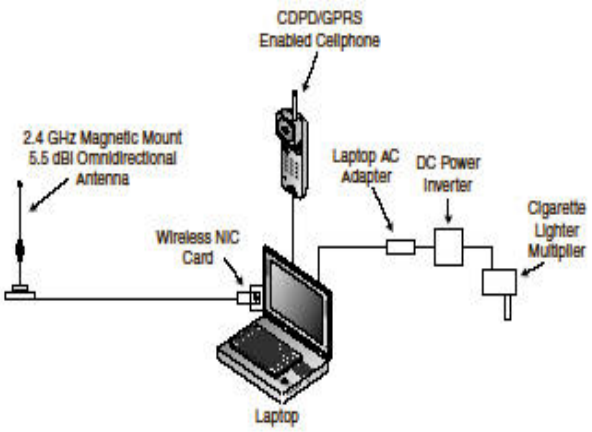
Το Wardriving δεν απαιτεί τη χρήση ακριβού ή δυσεύρετου εξοπλισμούγια την διενέργειά του. Μπορεί να γίνει με χρήση είτε φορητού ηλεκτρονικού υπολογιστή είτε προσωπικού ψηφιακού βοηθού (PDA). Στα παρακάτω σχήματα φαίνονται ο απαιτούμενος εξοπλισμός για Wardriving με laptop και με PDA αντίστοιχα. Στη συνδεσμολογία με laptop φαίνεται πως η παροχή ρεύματος γίνεται από τον αναπτήρα του αυτοκινήτου.

Εξοπλισμός Wardriving με laptop

- Για το Wardriving με laptop απαιτείται η χρήση του εξής εξοπλισμού:
  - laptop computer
  - ασύρματη NIC κάρτα
  - εξωτερική κεραία
  - συνδεσμολογία της εξωτερικής κεραίας με την NIC κάρτα
  - φορητή μονάδα GPS
  - καλωδίωση για GPS data
  - λογισμικό Wardriving
  - καλωδίωση για την παροχή ρεύματος στο laptop μέσω της μπαταρίας του αυτοκινήτου (για τον μετακινούμενο με αυτοκίνητο Wardriver).

    - Το λογισμικό Wardriving δεν απαιτεί τη χρήση laptop ιδιαιτέρων δυνατοτήτων. Άρα και ένα φτηνό laptop αρκεί. Το λογισμικό Wardriving μπορεί να είναι είτε συμβατό με το Linux λειτουργικό σύστημα, όπως είναι π.χ. το Kismet λογισμικό διαθέσιμο σε URL: http://www.kismetwireless.net/download.shtml είτε συμβατό με το λειτουργικό σύστημα των Windows MS, όπως είναι π.χ. το NetStumbler λογισμικό διαθέσιμο σε URL: http://www.netstumbler.com/downloads είτε συμβατο με Macintosh computer, όπως είναι π.χ. το MacStumbler λογισμικό διαθέσιμο σε URL: http://www.macstumbler.com.

Συνδεσμολογία Wardriving με laptop



Σχήμα 5: Εξοπλισμός και Συνδεσμολογία Wardriving με laptop

(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

Εξοπλισμός Wardriving με PDA

- Για το Wardriving με PDA απαιτείται η χρήση του εξής εξοπλισμού:
  - PDA με καλωδίωση για data
  - ασύρματη NIC κάρτα
  - εξωτερική κεραία
  - συνδεσμολογία της εξωτερικής κεραίας με την NIC κάρτα
  - φορητή μονάδα GPS
  - καλωδίωση για GPS data
  - συνδεσμολογία null modem
  - λογισμικό Wardriving.

    - Το λογισμικό Wardriving μπορεί να είναι είτε συμβατό με το Linux λειτουργικό σύστημα, όπως είναι π.χ. το Kismet λογισμικό είτε συμβατό με το λειτουργικό σύστημα των Windows MS, όπως είναι π.χ. το MiniStumbler λογισμικό διαθέσιμο σε URL: http://www.netstumbler.com/downloads.

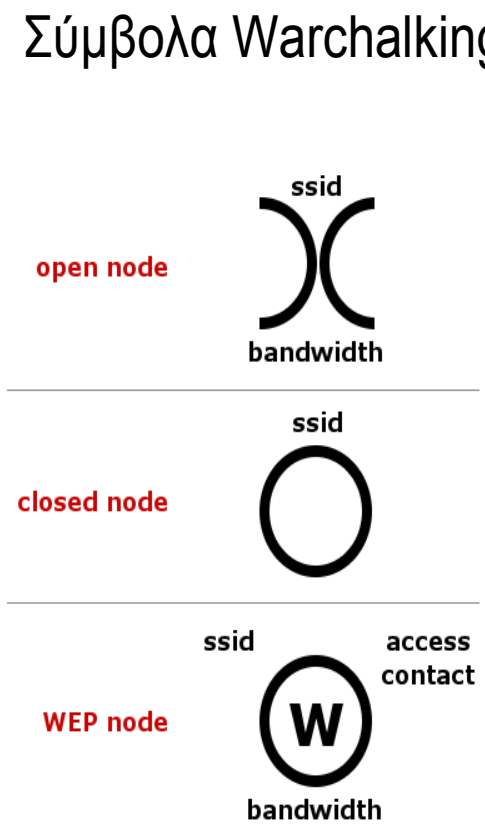
Σχήμα 6: Εξοπλισμός Wardriving με PDA

(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

Η διενέργεια του Wardriving έλαβε, σχεδόν αμέσως, διαστάσεις μαζικού, κινήματος και προβλήθηκε από τα αμερικανικά media ως λαμπρή ιδέα. Αλλά και στην Ευρώπη, το Wardriving εμφάνισε από νωρίς συμπτώματα μαζικού κινήματος. Σε σχετικές έρευνες της KPMG, ήδη από το 2003, καταγράφηκε ένα σημαντικό ποσοστό προσπαθειών hacking από τους Wardrivers του Λονδίνου. Σε μεταγενέστερη έρευνα του 2004 που έγινε στο Λονδίνο από την εταιρία RSA Security, βρέθηκε ότι μόνο το 66% των ιδιωτικών εταιρικών ασύρματων δικτύων χρησιμοποιούσαν στοιχειώδη συστήματα προστασίας από τους Wardrivers και hackers. Υπόψη, δε, του γεγονότος ότι κατά τη διάρκεια του 2004 στο Λονδίνο εμφανίστηκε αύξηση της χρήσης ασύρματων δικτύων κατά 235%, αντιλαμβάνεται κανείς ότι το 34% των μη φυλασσόμενων ή προστατευμένων ασύρματων δικτύων, βάσει τωνστοιχείων της έρευνας αυτής, αντιστοιχούσε σε εξαιρετικά μεγάλο αριθμό ασύρματων δικτύων.

2.4 *Warchalking*

Συχνά, οι Wardrivers, αφού εντοπίσουν ασύρματα δίκτυα, οικιακής ή επαγγελματικής χρήσης, για την πρόσβαση στο Διαδίκτυο δημοσιοποιούν κάθε σχετικό στοιχείο σε διαδικτυακούς τόπους μέσω των οποίων έρχονται σε επικοινωνία με ομοϊδεάτες τους. Για τη δημοσιοποίηση στοιχείων που αφορούν σε ασύρματα δίκτυα πρόσβασης στο Διαδίκτυο, χρησιμοποιείται ο όρος «Warchalking». Το Warchalking κυρίως περιγράφει τη σήμανση με σημειωτικούς χαρακτήρες συνήθως επί ακινήτων που βρίσκονται στην περιοχή στην οποία επιτυγχάνεται η κτήση πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο με σκοπό να επωφεληθούν και άλλοι που ενδεχόμενα θελήσουν να κάνουν χρήση της εντοπισμένης ασύρματης πρόσβασης στο δίκτυο ή Διαδίκτυο.



Σχήμα 7: Σύμβολα Warchalking
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

Οι Warchalkers χρησιμοποιούν τους σημειωτικούς χαρακτήρες που εμφανίζονται στο παραπάνω σχήμα 7, οι οποίοι έχουν ήδη γίνει κοινώς γνωστοί, για να γνωστοποιήσουν το είδος και την ευρυζωνικότητα του εντοπισμένου ασύρματου σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένο με το Διαδίκτυο. Από αυτά τα χρησιμοποιούμενα σύμβολα, το μεν πρώτο γνωστοποιεί την ύπαρξη ενός ανοιχτού σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο. Στο πάνω μέρος του συμβόλου σημειώνονται στοιχεία του Service Set Identifier (SSID)[5] ή το όνομα του δικτύου, ενώ στο κάτω μέρος σημειώνονται στοιχεία που αφορούν στην ευρυζωνικότητα του δικτύου. Στο δεύτερο από τα παραπάνω σύμβολα, που γνωστοποιεί την ύπαρξη μη προσβάσιμου σε τρίτους ασύρματου δικτύου, σημειώνεται στο πάνω μέρος του συμβόλου στοιχεία του Service Set Identifier (SSID), ενώ στο κάτω μέρος αυτού δεν γίνεται καμία αναγραφή. Στο τρίτο από τα παραπάνω σύμβολα, που γνωστοποιεί την ύπαρξη σημείου πρόσβασης σε ασύρματο τηλεπικοινωνιακό δίκτυο συνδεδεμένου στο Διαδίκτυο με WEP κρυπτογραφικό λογισμικό κώδικα, σημειώνονται στο πάνω αριστερό μέρος στοιχεία του Service Set Identifier (SSID), στο πάνω δεξιό μέρος στοιχεία επικοινωνίας για τη λήψη άδειας πρόσβασης στο εν λόγω δίκτυο, και στο κάτω μέρος στοιχεία που αφορούν στην ευρυζωνικότητα του δικτύου.

Οι παρακάτω φωτογραφίες είναι ενδεικτικές του συνήθους τρόπου χρήσης των Warchalking σημάνσεων για τους απανταχού Wardrivers και εν δυνάμει hackers.

[5] SSID είναι λογισμικός κώδικας 32 χαρακτήρων που υπάρχει στην προμετωπίδα (header) των στοιχείων που αποστέλλονται μέσω WAP, και ο οποίος περιέχει password για σύνδεση σε προστατευμένο ασύρματο δίκτυο. Όλες οι συσκευές ασύρματης δικτύωσης που επικοινωνούν μεταξύ τους ανταλλάσσουν το ίδιο SSID. Το SSID είναι στην πραγματικότητα η «ταυτότητα» του ασύρματου δικτύου. Περισσότερα για το SSID σε Wikipedia σε URL: http://en.wikipedia.org/wiki/SSID.

Εικόνες 6,7 : Σημάνσεις Warchalking
(Ημερίδα ΤΕΕ/ΔΣΑ Ασφάλεια Ηλεκτρονικων επικοινωνιών, Αθήνα 01.06.2006)

Μέχρι σήμερα, η επικαλούμενη νομιμότητα του Wardriving και του Warchalking δεν έχει επιβεβαιωθεί από οποιοδήποτε δικαστήριο, ούτε καν από τα αμερικανικά δικαστήρια με αφορμή την εισαγωγή σχετικής υπόθεσης ενώπιον της Δικαιοσύνης.

Αντίθετα, η Αμερικανική Κυβέρνηση έχει συμπεριλάβει το Wardriving ως απειλή κατά της ασφάλειας του κυβερνοχώρου στο σχέδιο εθνικής στρατηγικής για την ασφάλεια του κυβερνοχώρου που εξέδωσε το Φεβρουάριο του 2003. Ήδη, από το 2002 έχει προβληματίσει η νομιμότητα του Wardriving και Warchalking σε σχετικό σημείωμα που κυκλοφόρησε η ομοσπονδιακή υπηρεσία ασφαλείας FBI των Η.Π.Α.

Κεφάλαιο 3

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ – ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

3.1 Ασφάλεια Διαχείρησης Δικτύων Υπολογιστών

Η γενική αρχιτεκτονική ενός συστήματος διαχείρησης δικτύου βασίζεται στο μοντέλο εξυπηρετούμενου / εξυπηρετητή (client/server model), όπου ο εξυπηρετητής καλείται αντιπρόσωπος (agent) και ο εξυπηρετούμενος διαχειρηστής (manager). Ουσιαστικά ένα σύστημα διαχείρησης δικτύου περιλαμβάνει τρεις συνιστώσες:

- Ένα σύνολο διαχειρήσιμων πόρων, όπως ξενιστή υπολογιστή (host), πύλη (gateway) και γέφυρα (bridge), καθένας από τους οποίους περιέχει ένα αντιπρόσωπο.
- Τουλάχιστον ένα σταθμό διαχείρησης δικτύου, που συνήθως αποκαλείται διαχειρηστής.
- Ένα πρωτόκολλο διαχείρησης δικτύου, το οποίο χρησιμοποιείται από το σταθμό και τους αντιπροσώπους με σκοπό την ανταλλαγή πληροφοριών διαχείρησης.

Σε περιβάλλοντα διαχείρισης δικτύων χρησιμοποιείται ένα σύνολο λειτουργικών ενοτήτων διαχείρισης, το οποίο αφενός ομαδοποιεί τις διαφορετικές απαιτήσεις κάθε ιδιοκτήτη επιμέρους δικτύου, αφετέρου αποτελεί οδηγό για την καταγραφή των απαραίτητων λειτουργιών που πρέπει να υποστηρίζει το σύστημα διαχείρισης δικτύου. Το πλαίσιο αυτό είναι γνωστό ως FCAPS (Fault, Configuration, Accounting, Performance and Security Management).

Η συνοπτική περιγραφή της κάθε λειτουργικής ενότητας προσφέρει μία συνολική εικόνα για τις λειτουργίες που εκτελεί το σύστημα διαχείρισης δικτύου και τις δυνατότητες που αυτό έχει. Έτσι:

• η λειτουργική ενότητα της *διαχείρισης βλαβών* (fault management) περιλαμβάνει τα μέσα που παρέχουν στο διαχειριστή του δικτύου τη δυνατότητα αφενός να

εντοπίζει καταστάσεις βλάβης σε υποσυστήματα του υπό διαχείριση δικτύου, αφετέρου να τις διορθώνει, ώστε να επαναφέρει το δίκτυο στην πρότερη ομαλή λειτουργία του, λαμβάνοντας επιπλέον όλα τα απαιτούμενα μέτρα για να εξασφαλίσει την αποφυγή επανεμφάνισης της βλάβης

• η λειτουργική ενότητα της *διαχείρισης διάρθρωσης* (configuration management) παρέχει στο διαχειριστή τα απαιτούμενα μέσα για την αρχικοποίηση των ρυθμίσεων λειτουργίας του δικτύου, καθώς και για την τροποποίηση τους κατά τη λειτουργία του δικτύου (π.χ. σε περιπτώσεις υποστήριξης μιας νέας υπηρεσίας ή την προσθήκη νέας διαδρομής δρομολόγησης των δεδομένων)

• η λειτουργική ενότητα της *λογιστικής διαχείρισης* (accounting management) αναφέρεται στη διαχείριση από τον ιδιοκτήτη του κόστους κτήσης του δικτύου, των υπηρεσιών που αυτό υποστηρίζει και της χρέωσης των τελικών χρηστών

• η λειτουργική ενότητα της *διαχείρισης επιδόσεων* (performance management) αναφέρεται στις λειτουργίες που επιτρέπουν κατ' αρχήν τη μέτρηση της απόδοσης του υπό διαχείριση δικτύου με μεγέθη όπως ρυθμοαπόδοση (throughput), καθυστέρηση (latency) κλπ. και ακολούθως τη συσχέτιση των μετρούμενων στοιχείων με τις αναμενόμενες τιμές, ώστε να διαπιστωθεί αν το δίκτυο λειτουργεί εντός των αναμενόμενων επιπέδων απόδοσης ή αν πρέπει να διερευνηθεί το ενδεχόμενο βλάβης.

Σημειώνεται ότι σε ένα σύστημα διαχείρισης οι προαναφερθείσες λειτουργικές ενότητες δεν είναι ανεξάρτητες μεταξύ τους, αλλά συνδυάζονται για τη διεκπεραίωση της κάθε διαχειριστικής εργασίας. Για παράδειγμα, για να εκτελέσει η λειτουργική ενότητα λογιστικής διαχείρισης τις λειτουργίες χρέωσης για ένα χρήστη, θα πρέπει να διαθέτει στοιχεία για το είδος, την ποιότητα και το μέγεθος της υπηρεσίας που αυτός έλαβε από το δίκτυο, με όρους δεδομένων ή χρόνου ανάλογα με το υφιστάμενο μοντέλο χρέωσης. Κάποια από αυτά τα δεδομένα είναι αποθηκευμένα σε βάσεις δεδομένων που τηρεί και ενημερώνει η λειτουργική ενότητα διαχείρισης επιδόσεων, η οποία με τη σειρά της συνεργάζεται με τη λειτουργική ενότητα διαχείρισης βλαβών ώστε να ενημερώνεται ο διαχειριστής όταν εμφανίζονται ανεπιθύμητες καταστάσεις στη λειτουργία του δικτύου και να υποβοηθείται στη διαδικασία επίλυσης προβλημάτων.

• η λειτουργική ενότητα της διαχείρισης ασφάλειας (security management)

αναφέρεται σε θέματα ασφάλειας κατά την επικοινωνία μεταξύ συστημάτων και μεταξύ χρηστών και συστημάτων. Οι υπηρεσίες που παρέχονται από την ενότητα αυτή περιλαμβάνουν αυθεντικοποίηση και πιστοποίηση ταυτότητας οντοτήτων (authentication) έλεγχο προσπέλασης (access control), διασφάλιση εμπιστευτικότητας (confidentiality) και ακεραιότητας δεδομένων (data integrity). Συμπληρωματικές υπηρεσίες περιλαμβάνουν την ανίχνευση συμβάντων (event detection), τη διαχείριση ημερολογίων (audit trail logs) και τη διαχείριση συναγερμών (alarm management).

Αναλυτικότερα υπάρχουν οι ακόλουθες ομάδες υπηρεσιών ασφάλειας:

- *Αποτροπή* (prevention): περιλαμβάνει λειτουργίες πρόληψης φαινομένων προσπέλασης μη εξουσιοδοτημένων χρηστών καθώς και λειτουργίες ελέγχου προσπέλασης.
- *Ανίχνευση* (detection): πρόκειται για λειτουργία με προληπτικό αλλά και κατασταλτικό χαρακτήρα, η οποία περιλαμβάνει ενέργειες προφύλαξης έναντι πιθανής εισβολής με την ανίχνευση ασυνήθιστων δραστηριοτήτων και εισβολών στα υποσυστήματα ανίχνευσης και παρακολούθησης.
- *Αντιμετώπιση και επανάκαμψη* (containment and recovery): περιλαμβάνει λειτουργίες αντιμετώπισης εισβολής, επιδιόρθωσης βλαβών που οφείλονται σε εισβολές π.χ. από ιομορφικό λογισμικό (viral software) και επανάκαμψη μετά από εισβολές και παραβιάσεις ασφάλειας
- *Διαχείρηση ασφάλειας (security administration):* περιλαμβάνει λειτουργίες διαχείρησης, σχεδιασμού και συντήρησης των πολιτικών και των δεδομένων που σχετίζονται με θέματα ασφάλειας.

Οι σημαντικότερες απαιτήσεις ασφάλειας είναι οι παρακάτω:

3.1.1 Η πιστοποίηση και αυθεντικοποίηση (authentication)

Η επιβεβαίωση ταυτότητας σε ένα ηλεκτρονικό σύστημα είναι απαραίτητη, προκειμένου η πρόσβαση σε αυτό να επιτρέπεται μόνος σε όσους μπορούν να παράσχουν τα σχετικά διαπιστευτήρια. Στα περισσότερα συστήματα η επιβεβαίωση ταυτότητας διεκπεραιώνεται με τη χρήση ενός κωδικού χρήστη και ενός

συνθηματικού (password), τεχνική η οποία παρουσιάζει πλήθος αδυναμιών από πλευράς ασφάλειας. Σε άλλα περιβάλλοντα, για την επιβεβαίωση ταυτότητας χρησιμοποιούνται τα «ψηφιακά πιστοποιητικά» (ή ψηφιακές ταυτότητες). Τα συνηθέστερα σημεία αποθήκευσης ενός ψηφιακού πιστοποιητικού είναι είτε ο μαγνητικός δίσκος του υπολογιστή του χρήστη, είτε μια ειδική κάρτα (έξυπνη κάρτα) μικρού μεγέθους, που ο χρήστης έχει πάντα μαζί του. Με ψηφιακά πιστοποιητικά εξάλλου εφοδιάζονται όχι μόνο τα φυσικά πρόσωπα, αλλά και ορισμένα μηχανήματα, π.χ. ο web server μιας επιχείρησης, ώστε να μπορεί να "αποδείξει"» στον εν δυνάμει χρήστη που τον έχει επισκεφθεί μέσω του internet ότι πράγματι εκπροσωπεί μια συγκεκριμένη εταιρεία και έχει κατά συνέπεια το δικαίωμα να προβαίνει σε νόμιμες ηλεκτρονικές συναλλαγές (πωλήσεις κλπ.).

3.1.2 Η διασφάλιση της εμπιστευτικότητας (confidentiality)

Βασικό χαρακτηριστικό μιας ασφαλούς συναλλαγής μεταξύ δύο μερών είναι το περιεχόμενο της να παραμείνει μυστικό και απροσπέλαστο για οποιονδήποτε τρίτο. Τα προς προστασία δεδομένα μπορεί να αφορούν επιχειρηματικά σχέδια, οικονομικές συναλλαγές, πνευματική ιδιοκτησίας, εμπιστευτικές πληροφορίες σχετικές με το πρόσωπο κλπ. Κάποια συστήματα χρησιμοποιούν διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, στηριζόμενες σε κατάλληλα «κλειδιά», προκειμένου να κρατήσει τα ευαίσθητα δεδομένα προστατευμένα από κάθε ανεπιθύμητη πρόσβαση. Έτσι ακόμη και αν τα δεδομένα υποκλαπούν, θα είναι εξαιρετικά δύσκολο έως αδύνατο να αξιοποιηθούν, διότι θα πρέπει προηγουμένως να αποκρυπτογραφηθούν.

3.1.3 Η διασφάλιση της ακεραιότητας των δεδομένων (data integrity)

Η αρχή αυτή διασφαλίζει ότι τα δεδομένα που έφθασαν στον παραλήπτη ενός μηνύματος είναι τα ίδια με αυτά που απέστειλε ο αποστολέας και δεν έχουν αλλοιωθεί στην πορεία. Η σημασία της ακεραιότητας των δεδομένων μιας ηλεκτρονικής συναλλαγής γίνεται εύκολα αντιληπτή αν σκεφθεί κανείς το παράδειγμα μιας ηλεκτρονικά μεταδιδόμενης οικονομικής προσφοράς για 1.000 μονάδες ενός

συγκεκριμένου είδους, προς 5 ευρώ ανά μονάδα. Αν η τιμή μονάδας αλλοιωθεί σε 50 ευρώ, τότε αμφισβητείται η ίδια η υπόσταση της προσφοράς. Ένα σύστημα χρησιμοποιεί τους λεγόμενους αλγόριθμους κατατεμαχισμού και την έννοια του "αποτυπώματος" ενός μηνύματος, σε συνδυασμό με ψηφιακές υπογραφές, προκειμένου να επιτρέψει στον παραλήπτη να βεβαιωθεί ότι το μήνυμα δεν έχει αλλοιωθεί ούτε κατ' ελάχιστον σε σχέση με αυτό που πράγματι απέστειλε ο αποστολέας. Ακόμη και στην περίπτωση που δεν υφίσταται κίνδυνος κακόβουλης ενέργειας εκ μέρους τρίτων, η βεβαιότητα για την ακρίβεια και την πληρότητα ενός ηλεκτρονικού μηνύματος είναι σημαντική.

3.1.4 Η μη αποποίηση ευθήνης (non-repudation)

Η αρχή της μη αποκήρυξης σημαίνει ότι εάν προκύψει διαφωνία ή αμφισβήτηση σχετικά με τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής, υπάρχουν διαθέσιμα, αδιάψευστα αποδεικτικά στοιχεία, τα οποία μπορούν να χρησιμοποιηθούν από ένα τρίτο ουδέτερο μέρος, προκειμένου να διαπιστωθεί τι ακριβώς έχει συμβεί. Πρόκειται ουσιαστικά για το συνδυασμό "επιβεβαίωση ταυτότητας-ακεραιότητα δεδομένων", ο οποίος παρέχει στον παραλήπτη την βεβαιότητα ότι ο αποστολέας δεν θα μπορέσει να αρνηθεί (ψευδώς) ότι έχει δημιουργήσει, υπογράψει και αποστείλει ένα ηλεκτρονικό έγγραφο ή έχει συμμετάσχει σε μια συναλλαγή. Αυτό είναι ιδιαίτερα σημαντικό σε οικονομικές ιδίως συναλλαγές, όπου το ένα από τα δυο μέρη θα μπορούσε πιθανόν να αρνηθεί την πληρωμή π.χ. ενός λογαριασμού για παροχή υπηρεσιών, με τον ισχυρισμό ότι οι σχετικές υπηρεσίες δεν είχαν ποτέ ζητηθεί. Σε ένα διαδικτυακό περιβάλλον, η μη αποκήρυξη χρησιμοποιεί μεν την έννοια των ψηφιακών υπογραφών, προϋποθέτει όμως και ένα γενικότερο πλαίσιο λειτουργίας που καθορίζεται από συγκεκριμένες πολιτικές και διαδικασίες. Φυσικά, σημαντικό ρόλο παίζει στην περίπτωση αυτή και το ισχύον κάθε φορά νομικό πλαίσιο, το οποίο θα πρέπει να ληφθεί σοβαρά υπ' όψη.

3.2 Κρυπτογραφία

3.2.1 Συμμετρική Κρυπτογραφία

Η συμβατική κρυπτογραφία (conventional cryptography) αναφέρεται στη βιβλιογραφία και ως συμμετρική κρυπτογραφία (symmetric cryptography) ή κρυπτογραφία μυστικού κλειδιού (secret key cryptography).

Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες:

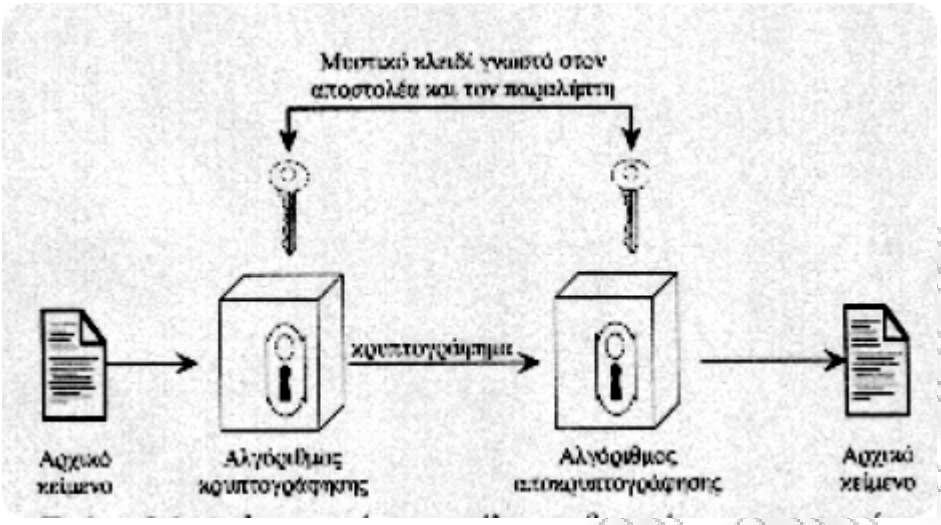
• *Αρχικό κείμενο (plaintext):* Αποτελεί το αρχικό μήνυμα ή τα αρχικά δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.

• *Αλγόριθμος κρυπτογράφησης (encryption algorithm):* Πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.

• *Μυστικό κλειδί (secret key):* Αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.

• *Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext):* Είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης. Το κρυπτογράφημα αυτό εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.

• *Αλγόριθμος αποκρυπτογράφησης (decryption algorithm):* Πρόκειται για έναν αλγόριθμο που πραγματοποιεί την αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.



Σχήμα 8: Απλοποιημένο μοντέλο συνβατικής κρυπτογραφίας

Για την ασφαλή χρήση της συμβατικής κρυπτογραφίας πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

• Απαιτείται η ύπαρξη ενός ισχυρού (strong) αλγορίθμου κρυπτογράφησης. Ως ελάχιστη απαίτηση αναφέρεται η ύπαρξη αλγορίθμου για τον οποίο ακόμη κι εάν αυτός είναι γνωστός στο δυνητικό επιτιθέμενο και υπάρχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφήματα, αυτός δε δύναται ούτε να υπολογίσει το μυστικό κλειδί, ούτε να συμπεράνει το αρχικό κείμενο, δηλαδή δε δύναται να κρυπταναλύσει το κρυπτογράφημα. Αυτή η απαίτηση δηλώνεται αυστηρότερα ως ακολούθως: ο επιτιθέμενος πρέπει να είναι αδύνατο να κρυπταναλύσει το κρυπτογράφημα ή να ανακαλύψει το κλειδί, ακόμη και αν κατέχει κάποια κρυπτογραφήματα μαζί με τα αντίστοιχα αρχικά μηνύματα, από τα οποία παράχθηκε καθένα από αυτά τα κρυπτογραφήματα.

• Ο πομπός και ο δέκτης πρέπει να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να διαφυλάσσουν αυτό το μυστικό κλειδί σε ασφαλές μέρος. Εάν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη, συνεπώς παραβιάζεται η εμπιστευτικότητα.

Σημειώνεται ότι αδύναμο κρίκο στην ασφάλεια της συμβατικής κρυπτογραφίας αποτελεί μόνον η μυστικότητα του κλειδιού και όχι η μυστικότητα του αλγορίθμου που χρησιμοποιείται. Αυτό θεωρείται δεδομένο εάν υποτεθεί ότι για τον επιλεγέντα αλγόριθμο ισχύει η προφανής σχεδιαστική απαίτηση να είναι αδύνατο να

αποκρυπτογραφηθεί ένα μήνυμα μόνο με γνώση του κρυπτογραφήματος και του αλγορίθμου κρυπτογράφησης. Συνεπώς, δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος, αλλά μόνο το μυστικό κλειδί. Το χαρακτηριστικό αυτό γνώρισμα της συμβατικής κρυπτογραφίας την καθιστά κατάλληλη για ευρεία χρήση. Το γεγονός ότι δε χρειάζεται να παραμένει μυστικός ο αλγόριθμος επιτρέπει στους κατασκευαστές να αναπτύσσουν χαμηλού κόστους υλοποιήσεις, τόσο σε λογισμικό όσο και σε υλικό, για εφαρμογές κρυπτογράφησης δεδομένων.

3.2.2 Κρυπτογράφηση

Τα κρυπτογραφικά συστήματα ταξινομούνται, γενικά, με βάση τρία ανεξάρτητα κριτήρια.

• Τον τύπο των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό τον αρχικού κειμένου σε ένα κρυπτογράφημα

Το σύνολο των αλγορίθμων κρυπτογράφησης στηρίζεται σε δύο γενικές αρχές: στην αντικατάσταση (substitution) σύμφωνα με την οποία κάθε στοιχείο του αρχικού κειμένου, είτε είναι δυαδικό ψηφίο, είτε χαρακτήρας, είτε ομάδα δυαδικών ψηφίων ή χαρακτήρων, αντικαθίσταται από άλλο στοιχείο και στη μετάθεση (transposition) στην οποία τα στοιχεία του αρχικού κειμένου αναδιατάσσονται. Βασική προϋπόθεση αποτελεί η μη απώλεια οποιασδήποτε πληροφορίας, ώστε όλες οι διαδικασίες να είναι αντιστρέψιμες. Τα περισσότερα συστήματα, που είναι γνωστά ως συστήματα παραγωγής (product systems), περιλαμβάνουν πληθώρα σταδίων αντικαταστάσεων και μεταθέσεων.

• Τον αριθμό των κλειδιών που χρησιμοποιούνται. Εάν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί, τότε το σύστημα αναφέρεται ως συμμετρικό ή μοναδικού κλειδιού ή μυστικού κλειδιού ή συμβατικής κρυπτογραφίας. Εάν, όμως, ο πομπός και ο δέκτης χρησιμοποιούν διαφορετικά κλειδιά, τότε το σύστημα αναφέρεται ως ασύμμετρο, ή σύστημα ζεύγους κλειδιών, ή κρυπτογραφίας δημοσίου κλειδιού.

• Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο. Ένας κωδικοποιητής τμημάτων (block cipher) επεξεργάζεται την είσοδο ενός τμήματος στοιχείων κάθε

φορά, παράγοντας ένα τμήμα εξόδου για κάθε συγκεκριμένο τμήμα εισόδου. Αντίθετα, ένας κωδικοποιητής ροής (stream cipher) επεξεργάζεται κατά συνεχή τρόπο τα στοιχεία εισόδου και κάθε φορά παράγεται ως έξοδος ένα στοιχείο, με τη σειρά που καταφθάνουν τα δεδομένα.

3.2.3 Κρυπτανάλυση

Η διαδικασία της προσπάθειας αποκάλυψης του αρχικού κειμένου ή του κλειδιού από μη εξουσιοδοτημένες οντότητες - δυνητικούς επιτιθέμενους, είναι γνωστή ως κρυπτανάλυση (cryptanalysis). Η στρατηγική που χρησιμοποιείται από τον κρυπταναλυτή εξαρτάται από τη φύση της κρυπτογράφησης και από τις πληροφορίες που είναι διαθέσιμες σε αυτόν.

Στον Πίνακα 1 παρουσιάζονται συνοπτικά διάφοροι τύποι επιθέσεων κρυπτανάλυσης, οι οποίοι διαφοροποιούνται, μεταξύ άλλων, με βάση την ποσότητα και το είδος της πληροφορίας που είναι γνωστή στον κρυπταναλυτή. Το πρόβλημα της κρυπτανάλυσης παρουσιάζει σημαντικές δυσκολίες όταν είναι γνωστό στον επιτιθέμενο μόνον το κρυπτογράφημα. Σε μερικές περιπτώσεις δεν είναι γνωστός ούτε ο αλγόριθμος κρυπτογράφησης, αλλά στη γενική περίπτωση μπορεί να υποτεθεί ότι ο αντίπαλος γνωρίζει τον αλγόριθμο που χρησιμοποιείται.

Μία κλασική επίθεση υπό αυτές τις περιστάσεις αποτελεί η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών(brute force attack), όπου ο επιτιθέμενος δοκιμάζει διαδοχικά όλα τα στοιχεία από το πεδίο όλων των πιθανών κλειδιών. Εάν το μέγεθος του κλειδιού είναι μεγάλο, η επίθεση αυτού του είδους θεωρείται πρακτικά ατελέσφορη. Κατά συνέπεια, ένας επιτιθέμενος για να είναι αποτελεσματικός θα πρέπει να αξιοποιήσει ανάλυση του κρυπτογραφήματος εφαρμόζοντας διάφορες στατιστικές δοκιμές σε αυτό. Ο επιτιθέμενος για να χρησιμοποιήσει αυτή την προσέγγιση θα πρέπει να γνωρίζει τον τύπο του αρχικού κειμένου που χρησιμοποιείται, π.χ. ένα απλό κείμενο σε συγκεκριμένη γλώσσα, ένα εκτελέσιμο αρχείο σε περιβάλλον συγκεκριμένου λειτουργικού συστήματος, ένα αρχείο με πηγαίο κώδικα σε συγκεκριμένη γλώσσα προγραμματισμού κλπ.

Τύπος Επίθεσης	Στοιχεία γνωστά στον κρυπταναλυτή
Επίθεση κρυπτογραφήματος (ciphertext – only attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα
Επίθεση γνωστού αρχικού κειμένου (known – plaintext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Ένα ή περισσότερα ζεύγη (αρχικού κειμένου, κρυπτογραφήματος), παραγόμενα από το μυστικό κλειδί
Επίθεση επιλεγμένου αρχικού κειμένου (chosen – plaintext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Αρχικό κείμενο επιλεγμένο από τον κρυπταναλυτή, σε συνδυασμό με το αντίστοιχο κρυπτογράφημα που παράγεται με το μυστικό κλειδί
Επίθεση επιλεγμένου κρυπτογραφήματος (chosen – ciphertext attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Επιλεγμένο απ' τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί
Επίθεση επιλεγμένου κειμένου (chosen – text attack)	Αλγόριθμος κρυπτογράφησης Κρυπτογράφημα Επιλεγμένο από τον κρυπταναλυτή μήνυμα αρχικού κειμένου, μαζί με το αντίστοιχο κρυπτογράφημα, που παράχθηκε με το μυστικό κλειδί Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο, που παράχθηκε με το μυστικό κλειδί

Πίνακας 1: Τύποι επιθέσεων σε κρυπτογραφημένα έντυπα

Η άμυνα σε επίθεση κρυπτογραφήματος (ciphertext only attack) αποτελεί γενικά εύκολη υπόθεση, επειδή ο αντίπαλος διατηρεί μικρή ποσότητα πληροφοριών με την οποία μπορεί να ασχοληθεί. Παρόλα αυτά, σε πολλές περιπτώσεις ο κρυπταναλυτής μπορεί να διαθέτει και περισσότερες πληροφορίες. Ο κρυπταναλυτής μπορεί να έχει

τη δυνατότητα να καταγράψει ένα ή περισσότερα μηνύματα αρχικού κειμένου, καθώς επίσης και τα αντίστοιχα κρυπτογραφήματα. Σε άλλη περίπτωση, μπορεί να γνωρίζει ότι συγκεκριμένα πρότυπα αρχικού κειμένου θα εμφανιστούν σε ένα μήνυμα. Για παράδειγμα, ένα αρχείο σε μορφή postscript αρχίζει πάντοτε με το ίδιο πρότυπο, ή μπορεί να υπάρξει μία τυποποιημένη επικεφαλίδα ή ένα λογότυπο σε ένα ηλεκτρονικό μήνυμα μεταφοράς κεφαλαίων. Τα προαναφερόμενα παραδείγματα αποτελούν επιθέσεις γνωστών μηνυμάτων. Με αυτή τη γνώση ο αναλυτής μπορεί να είναι σε θέση να συμπεράνει το κλειδί, με βάση τον τρόπο που μετασχηματίστηκε το γνωστό αρχικό κείμενο.

Αντίστοιχη με την επίθεση γνωστών μηνυμάτων (known plaintext attack) είναι η επίθεση πιθανής-λέξης (probable word attack). Εάν ο επιτιθέμενος ασχολείται με την κρυπτανάλυση κάποιου μηνύματος αγνώστου περιεχομένου μπορεί να μην κατανοεί επακριβώς το περιεχόμενο του μηνύματος. Παρόλα αυτά, εάν ο επιτιθέμενος αναζητά συγκεκριμένες πληροφορίες, τότε κάποια τμήματα του μηνύματος μπορούν να θεωρηθούν γνωστά. Για παράδειγμα, εάν διαβιβάζεται ολόκληρο λογιστικό αρχείο, ο επιτιθέμενος μπορεί να είναι σε θέση να γνωρίζει τη θέση κάποιων λέξεων-κλειδιών στην επικεφαλίδα του αρχείου. Άλλο παράδειγμα αποτελεί ο πηγαίος κώδικας ενός προγράμματος που αναπτύχθηκε από κάποια εταιρεία και ο οποίος μπορεί να περιλαμβάνει δήλωση πνευματικών δικαιωμάτων σε κάποια συγκεκριμένη θέση.

Εάν ο κρυπταναλυτής μπορεί με κάποιο τρόπο να παραπλανήσει το πηγαίο σύστημα ώστε να παρεμβάλλει ένα μήνυμα που έχει επιλέξει ο ίδιος, τότε είναι πιθανή μία επίθεση επιλεγμένων μηνυμάτων. Γενικά, εάν ο κρυπταναλυτής είναι σε θέση να επιλέγει τα μηνύματα για κρυπτογράφηση τότε μπορεί σκόπιμα να επιλέγει πρότυπα που αναμένεται να τον υποβοηθήσουν στην αποκάλυψη της δομής του κλειδιού.

Στον Πίνακα 1 εμφανίζονται και άλλοι δύο τύποι επίθεσης, η επίθεση επιλεγμένου κρυπτογραφήματος (chosen ciphertext attack) και η επίθεση επιλεγμένου κειμένου (chosen text attack), επιθέσεις οι οποίες δεν επιχειρούνται συχνά ως τεχνικές κρυπτανάλυσης, μπορούν όμως να αποτελέσουν δυνητικούς τρόπους επίθεσης.

Ένα σχήμα κρυπτογράφησης θεωρείται υπολογιστικά ασφαλές (computationally secure) εφόσον το κρυπτογράφημα που παράγεται πληροί ένα τουλάχιστον από τα ακόλουθα κριτήρια:

• Το κόστος της παραβίασης του κρυπτομηνύματος να υπερβαίνει την αξία των τελικά λαμβανομένων πληροφοριών από τη διαδικασία της κρυπτανάλυσης.

• Ο χρόνος που απαιτείται για τη διάσπαση του κρυπτομηνύματος πρέπει να υπερβαίνει την ωφέλιμη διάρκεια ζωής των λαμβανομένων πληροφοριών.

Ο υπολογισμός της απαιτούμενης προσπάθειας για την επιτυχή κρυπτανάλυση ενός κρυπτογραφήματος θεωρείται ιδιαίτερα δύσκολη διαδικασία. Παρόλα αυτά, θεωρώντας ότι δεν υπάρχει μαθηματική σχεδιαστική αδυναμία στον αλγόριθμο κρυπτογράφησης, προτείνεται η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών και είναι δυνατόν να πραγματοποιηθούν κάποιες ρεαλιστικές εκτιμήσεις όσον αφορά το κόστος και τον απαιτούμενο χρόνο. Η εξαντλητική αναζήτηση περιλαμβάνει την εξαντλητική (exhaustive) δοκιμή κάθε πιθανού κλειδιού μέχρις ότου υπάρξει μία κατανοητή απόδοση του κρυπτογραφήματος στο αρχικό κείμενο. Στατιστικά πρέπει να δοκιμαστούν τα μισά κλειδιά -στοιχεία από το πεδίο των πιθανών κλειδιών ώστε να επιτευχθεί κρυπτανάλυση. Στον Πίνακα 2 καταγράφεται ο χρόνος που αντιστοιχεί σε διαφορετικά μεγέθη κλειδιών. Το μέγεθος κλειδιού των 56-bit χρησιμοποιείται στον αλγόριθμο DES (Data Encryption Standard). Στα αποτελέσματα που εμφανίζονται για κάθε μέγεθος κλειδιού, θεωρήθηκε ότι χρειάζεται χρόνος 1μs για να εκτελεστεί μία μόνο αποκρυπτογράφηση, χρόνος ο οποίος αντιστοιχεί σε μία λογική τάξη μεγέθους ισχύος των σημερινών επεξεργαστών. Με μαζική χρήση παράλληλων μικροεπεξεργαστών είναι δυνατό να επιτευχθούν ρυθμοί επεξεργασίας οι οποίοι είναι κατά πολλές τάξεις μεγέθους μεγαλύτεροι. Παράλληλα, η αξιοποίηση κβαντικών υπολογιστών (quantum computers) στην κατεύθυνση της επέκτασης των παράλληλων υπολογισμών με αξιοποίηση του φαινομένου της κβαντικής επαλληλίας (quantum superposition), μπορεί θεωρητικά να απειλήσει τη ρωμαλεότητα των σύγχρονων κρυπτογραφικών συστημάτων, αλλά αυτό με τη σειρά του θα μπορούσε, απλώς, να οδηγήσει σε απαίτηση για διπλασιασμό του μεγέθους των κρυπτογραφικών κλειδιών. Στον Πίνακα παρατίθενται τα αποτελέσματα για ένα σύστημα που μπορεί να επεξεργαστεί 10^6 κλειδιά ανά μs. Με τη συγκεκριμένη απόδοση ο αλγόριθμος Data Encryption Standard -DES ουσιαστικά δεν μπορεί να θεωρηθεί υπολογιστικά ασφαλής.

Μήκος κλειδιού (bits)	Αριθμός των πιθανών κλειδιών	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 1 αποκρυπτογράφηση/μs	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 10^6 αποκρυπτογραφήσεις/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 λεπτά	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 χρόνια	10 ώρες
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4 × 1024 χρόνια	5.4×10^{18} χρόνια
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9 × 1036 χρόνια	5.9×10^{30} χρόνια

Πίνακας 2: Μέσος χρόνος για εξαντλητική αναζήτηση κλειδιών

3.3 Ασύμμετρη Κρυπτογραφία ή κρυπτογράφηση δημοσίου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό ενώ το άλλο είναι ιδιωτικό. Στην κρυπτογράφηση αυτή οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί. Για την παραγωγή ενός εμπιστευτικού μηνύματος, λοιπόν, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη (που του έχει πρωτύτερα μεταφερθεί) για να κρυπτογραφήσει το μήνυμα, έτσι ώστε να παραμείνει απόρρητο έως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη. Ο πιο ευρέως αποδεκτός αλγόριθμος είναι ο RSA (Rivest, Shamir and Adelman)

Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημοσίου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει, θεωρείται κατάλληλη για το ΗΕ επειδή εξασφαλίζει την εμπιστευτικότητα του μηνύματος και παρέχει πιο ευέλικτα μέσα αυθεντικοποίησης των χρηστών. Επίσης, υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος).

3.3.1 Αλγόριθμοι κρυπτογράφησης

Οι πιο γνωστοί αλγόριθμοι κρυπτογράφησης είναι συνοπτικά οι εξής:

- *DES-Data Encryption Standard.* Είναι ένα σώμα κρυπτογραφικών εντολών που δημιουργήθηκε από την IBM και πήρε έγκριση από την αμερικανική κυβέρνηση το

1977. Χρησιμοποιεί ένα 56-bit κλειδί και μια ομάδα από 64 bits. Είναι σχετικά γρήγορος αλγόριθμος για την κρυπτογράφηση μεγάλου όγκου δεδομένων ταυτόχρονα. Ορισμένοι πιστεύουν ότι ο αλγόριθμος δεν είναι ασφαλής. Ωστόσο, άλλοι γνωρίζουν ότι απαιτούνται πολλά χρόνια και χρήματα για την παραχάραξη του.

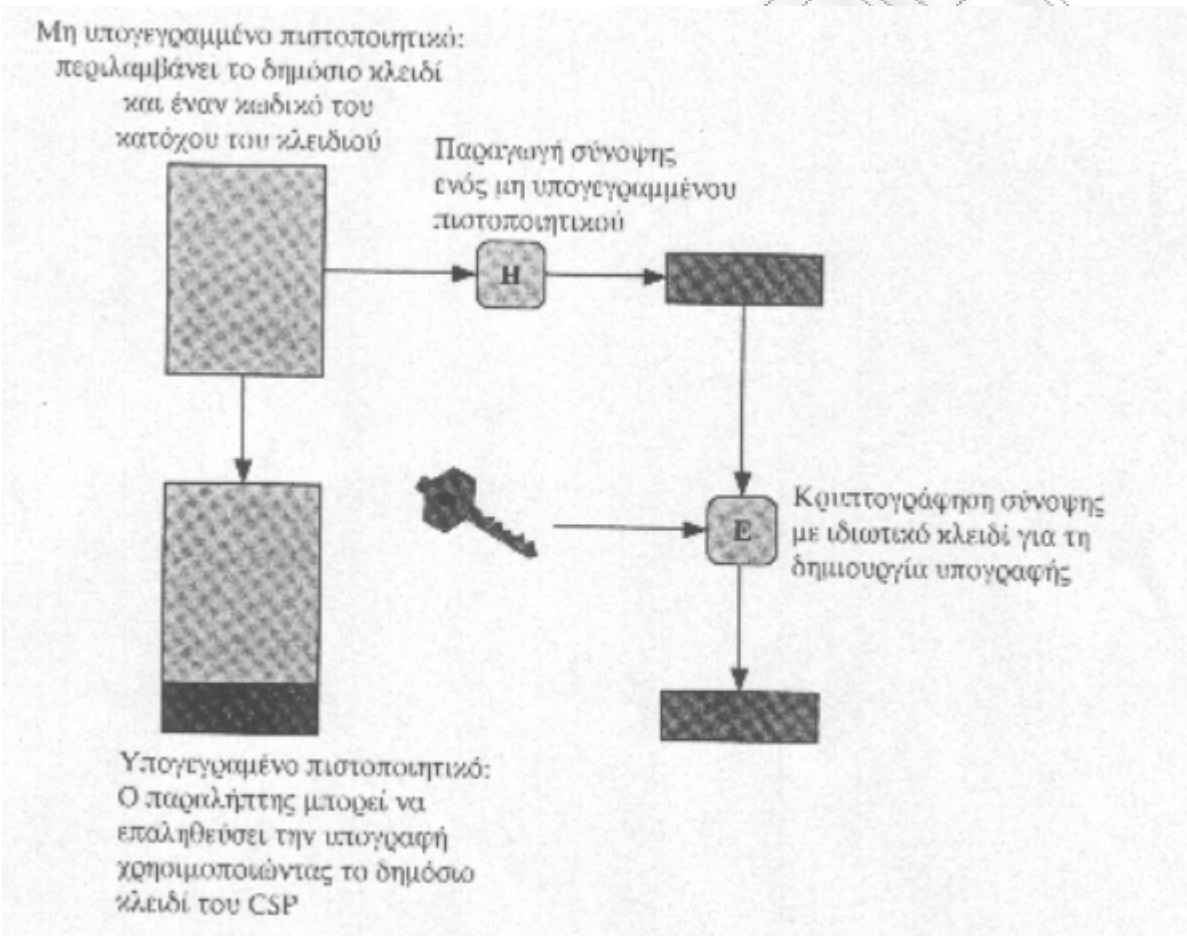
- *Triple DES.* Βασίζεται στον DES αλγόριθμο κι έχει προταθεί σαν εναλλακτική του λύση. Κρυπτογραφεί μια ομάδα δεδομένων τρεις φορές, με τρία διαφορετικά κλειδιά.
- *RC2, RC4.* Σχεδιάστηκαν από τον Ron Rivest. Παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού κρυπτογράφησης, για πολύ γρήγορη και μεγάλου όγκου κρυπτογράφηση. Οι δύο αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DES και μπορούν να γίνουν ακόμα πιο ασφαλείς αν επιλεχθεί μεγαλύτερο μήκος κλειδιού.
- *IDEA.* Ο International Data Encryption Algorithm δημιουργήθηκε το 1991 και σχεδιάστηκε για να είναι ικανός για πραγματοποίηση υπολογισμών στο λογισμικό. Προσφέρει πολύ δυνατή κρυπτογράφηση, χρησιμοποιώντας ένα 128-bit κλειδί.
- *RSA.* Ονομάστηκε έτσι από τους σχεδιαστές του, Rivest, Shamir και Adelman. Είναι ένας αλγόριθμος «δημοσίου κλειδιού» ο οποίος υποστηρίζει μια ποικιλία μήκους κλειδιών, καθώς επίσης ποικιλία όσον αφορά στο μέγεθος του κειμένου προς κρυπτογράφηση. Το συνηθισμένο μήκος κλειδιού είναι 512-1024 bits. θεωρείται ως σήμερα η ασφαλέστερη μέθοδος κρυπτογράφησης εφόσον ουδέποτε έχει προσβληθεί από «χάκερ». Ο RSA συνήθως χρησιμοποιείται για τη μετάδοση του ιδιωτικού κλειδιού του DES αλγορίθμου.
- *Diffie-Hellman.* Αποτελεί το παλαιότερο σύστημα κρυπτογραφίας δημοσίου κλειδιού που ακόμα χρησιμοποιείται. Δεν υποστηρίζει κρυπτογράφηση ή ψηφιακές υπογραφές. Το σύστημα έχει σχεδιαστεί για να επιτρέπει και στις δύο πλευρές να συμφωνούν με τη χρήση ενός κατανεμημένου κλειδιού (shared key), ακόμα και αν το μόνο που κάνουν είναι να ανταλλάσσουν μηνύματα δημοσίως.
- *DSA.* Ο Digital Signature Algorithm σχεδιάστηκε από την Nist. Το σχήμα των υπογραφών χρησιμοποιεί το ίδιο είδος κλειδιών που χρησιμοποιεί και ο Diffie-Hellman αλγόριθμος και μπορεί να δημιουργήσει υπογραφές πιο γρήγορα από τον RSA. Παρόλη την αποδοχή του όμως, απέχει ακόμα πολύ από το να παρέχει σιγουριά.

3.4 Ψηφιακές Υπογραφές

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας είναι προφανή, ωστόσο υπάρχει ένα σοβαρό ζήτημα που χρήζει ιδιαίτερης αντιμετώπισης. Ας υποτεθεί ότι παραλαμβάνουμε ένα μήνυμα ή αρχείο από το χρήστη με ηλεκτρονική διεύθυνση name@company.com. Υπό φυσιολογικές συνθήκες δεν έχουμε λόγο να πιστέψουμε ότι ο αποστολέας δεν είναι πράγματι ο αληθινός κάτοχος της συγκεκριμένης διεύθυνσης. Ωστόσο, ένας άλλος, κακόβουλος χρήστης, μπορεί, εάν θέλει, να χρησιμοποιήσει ένα κατάλληλο πρόγραμμα (email faker), για να στείλει αυτό το μήνυμα με διεύθυνση αποστολέα name@company.com. Με άλλα λόγια, έχει τη δυνατότητα να προβεί σε ηλεκτρονική πλαστοπροσωπία, για λόγους που μάλλον δεν θα είναι προς το συμφέρον μας (π.χ., μπορεί να είναι ανταγωνιστής και να προσπαθεί να αποσπάσει επιχειρηματικά μυστικά). Πώς μπορούμε να είμαστε βέβαιοι ότι το email που λάβαμε το έχει στείλει ο νόμιμος κάτοχος της διεύθυνσης και όχι κάποιος άλλος;

Η αδυναμία που μόλις περιγράψαμε ξεπερνιέται με τη βοήθεια των ψηφιακών υπογραφών (digital signatures), τις οποίες μπορούμε να σκεπτόμαστε ως το ηλεκτρονικό ισοδύναμο των χειρόγραφων υπογραφών. Οι ψηφιακές υπογραφές προσδιορίζουν τον υπογράφοντα και δηλώνουν μια σχέση ανάμεσα σε αυτόν και το υπογεγραμμένο έγγραφο. Ουσιαστικά, μια ψηφιακή υπογραφή είναι ορισμένα δεδομένα που συνοδεύουν ή συσχετίζονται λογικά με ένα ψηφιακά κωδικοποιημένο μήνυμα και τα οποία δεδομένα μπορούν να χρησιμοποιηθούν για να εξακριβωθεί, τόσο ο αποστολέας του μηνύματος, όσο και το ότι το μήνυμα δεν έχει κατά οποιονδήποτε τρόπο αλλοιωθεί, αφ' ότου έπαυσε να είναι υπό τον έλεγχο του αποστολέα. Όπως έχει ήδη προαναφερθεί, μια τέτοια υπογραφή είναι στην ουσία το αποτέλεσμα που παράγεται από μία μαθηματική διαδικασία που έχει κάποια ιδιαίτερα χαρακτηριστικά. Η ασφάλεια της στηρίζεται στη χρήση της ασύμμετρης κρυπτογραφίας, όπου η κρυπτογράφηση και η αποκρυπτογράφηση χρησιμοποιούν διαφορετικά κλειδιά η κάθε μία. Εδώ εφαρμόζεται η κρυπογραφία δημοσίου κλειδιού αντίστροφα. Στην περίπτωση αυτή, ο αποστολέας κωδικοποιεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Οποιοδήποτε χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει το μήνυμα μπορεί να είναι

σίγουρος για την ταυτότητα του πρώτου. Έτσι μια ψηφιακή υπογραφή παρέχει ισχυρή απόδειξη στον παραλήπτη ενός ψηφιακά υπογεγραμμένου μηνύματος ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί. Συνήθως προστίθεται σε ένα μήνυμα όπως προστίθεται και η υπογραφή σε κάποιο έγγραφο και επιβεβαιώνει την αυθεντικότητα και τη μη αποποίηση ευθύνης του αποστολέα.



Σχήμα 9: Σχηματική παράσταση λειτουργίας ψηφιακής υπογραφής

3.5 Διαχείρηση Δημοσίων Κλειδιών

Η διανομή των δημοσίων κλειδιών αποτελεί ένα από τα σημαντικότερα προβλήματα του ασύμμετρου κρυπτοσυστήματος. Υπάρχουν δύο διαφορετικές περιπτώσεις στη διανομή των κλειδιών που παρουσιάζουν ιδιαίτερο ενδιαφέρον:

- Η διανομή δημοσίων κλειδιών
- Η χρήση του ασύμμετρου κρυπτοσυστήματος για τη διανομή μυστικών κλειδιών, δηλαδή των κλειδιών που χρησιμοποιούνται στο συμμετρικό κρυπτοσύστημα.

Ψηφιακά Πιστοποιητικά

Για την αποτελεσματική λειτουργία του ασύμμετρου κρυπτοσυστήματος, το δημόσιο κλειδί πρέπει να μπορεί να είναι γνωστό σε όσους δυνητικά ενδιαφέρονται. Έτσι, υποθέτοντας ότι υπάρχει ένας ευρέως αποδεκτός αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης όπως ο RSA, οποιοσδήποτε μπορεί να αποστείλει το δημόσιο κλειδί του σε κάποιον άλλο ή να το μεταδώσει προς όλους. Η μέθοδος αυτή είναι αρκετά χρήσιμη, αλλά έχει μία σημαντική αδυναμία: την αδυναμία διασφάλισης της ακεραιότητας και της αυθεντικοποίησης του αποστολέα κατά την αποστολή του μηνύματος που περιέχει το δημόσιο κλειδί. Οποιοσδήποτε μπορεί να πραγματοποιήσει μία τέτοια μετάδοση. Με τον τρόπο αυτό, κάποιος Χ μπορεί να προσποιηθεί ότι είναι ο Α και να στείλει ένα δημόσιο κλειδί σε τρίτον ή να το μεταδώσει προς περισσότερες οντότητες. Μέχρι τη στιγμή που ο Α θα αντιληφθεί ότι βρίσκεται σε εξέλιξη μία απάτη, ο Χ θα έχει διαβάσει όλα τα κρυπτογραφημένα μηνύματα που προορίζονταν για τον Α, ενώ έχει τη δυνατότητα να υπογράφει και να αυθεντικοποιείται ως Α.

Λύση σε αυτό το πρόβλημα αποτελεί η χρήση του ψηφιακού πιστοποιητικού (digital certificate) ή απλώς πιστοποιητικού (certificate) δημοσίου κλειδιού. Συγκεκριμένα, ένα πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη και έναν κωδικό (user_ID) του κατόχου του κλειδιού, υπογεγραμμένα ψηφιακά από μία Έμπιστη Τρίτη Οντότητα (Trusted Third Party - TTP), η οποία συνήθως αποκαλείται Πάροχος Υπηρεσιών Πιστοποίησης (Certification Service Provider - CSP). Ο χρήστης παρουσιάζει το δημόσιο κλειδί του στον CSP με έναν αξιόπιστο τρόπο και λαμβάνει

ένα πιστοποιητικό που το περιέχει ή, στη γενική περίπτωση, ο CSP παράγει, αποθηκεύει, διανέμει και ανακαλεί, όταν απαιτείται, τα πιστοποιητικά. Οποιοσδήποτε επιθυμεί να χρησιμοποιήσει το δημόσιο κλειδί του χρήστη μπορεί να λάβει το πιστοποιητικό και να είναι σίγουρος για την ορθότητα του δημόσιου κλειδιού. Η διαδικασία αναπαρίσταται στο Σχήμα 9 (ψηφιακές υπογραφές). Παράδειγματα TTP είναι η Verisign (www.verisign.com), Thawte (www.thawte.com), SecureNet (www.securenet.com).

Το πιο διαδεδομένο σύστημα πιστοποιητικού είναι το πρότυπο ISO/ITU-T X.509, το οποίο χρησιμοποιείται σε πολλές περιπτώσεις, όπως στην ασφάλεια IP, στο TLS/SSL, στο SET, στο S/MIME κλπ.

Διανομή Μυστικών Κλειδιών με Ασύμμετρο Κρυπτοσύσιημα

Όπως αναφέρθηκε σε προηγούμενες παραγράφους, σε ένα συμμετρικό κρυπτοσύστημα προκειμένου να επικοινωνήσουν δύο χρήστες πρέπει να μοιράζονται τη γνώση ενός μυστικού κλειδιού. Για παράδειγμα, έστω τι ο Β θέλει να δημιουργήσει μία εφαρμογή που θα του παρέχει τη δυνατότητα να ανταλλάσσει μηνύματα με χρήση υπηρεσίας ηλεκτρονικού ταχυδρομείου με τον Α, χρησιμοποιώντας συμμετρικό κρυπτοσύστημα. Θα πρέπει να βρεθεί ένας τρόπος να αποστείλει ο Β στον Α ένα μυστικό κλειδί.

Ένας πολύ διαδεδομένος τρόπος είναι η αξιοποίηση ψηφιακού φακέλου (digital envelope), δηλαδή να χρησιμοποιήσει ο Β ασύμμετρο κρυπτοσύστημα για την αποστολή του μυστικού κλειδιού. Προφανώς απαιτείται η χρήση πιστοποιητικών και η λειτουργία PKI (Public Key Infrastructure), ώστε να εξασφαλίζεται η αυθεντικότητα του αποστολέα Α και η ακεραιότητα του μηνύματος. Τα γενικά βήματα που θα πρέπει να ακολουθηθούν σε μία τέτοια Περίπτωση είναι τα ακόλουθα:

Ο Β ετοιμάζει το προς αποστολή μήνυμα.

Ο Β κρυπτογραφεί το μήνυμα με συμβατικό κρυπτοσύστημα, χρησιμοποιώντας ένα μυστικό κλειδί που ο ίδιος δημιούργησε.

Ο Β κρυπτογραφεί το μυστικό κλειδί με το δημόσιο κλειδί του Α.

Ο Β επισυνάπτει το κρυπτογραφημένο μυστικό κλειδί στο μήνυμα και το αποστέλει στον Α.

Ο Α είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα και να διαβάσει το αρχικό κείμενο. Αν ο Β έχει ανακτήσει το δημόσιο κλειδί του Α μέσω πιστοποιητικών από κάποιο TTP, τότε ο Β είναι σίγουρος ότι το μυστικό κλειδί είναι σωστό.

3.6 Αναχώματα Ασφάλειας (Firewalls)

Πολλοί οργανισμοί και επιχειρήσεις έχουν συνδέσει τα εσωτερικά τους δίκτυα με το internet ενδιαφερόμενοι για λήψη χρήσιμων πληροφοριών από τον παγκόσμιο ιστό, αλλά και προσανατολισμένοι στις δυνατότητες του ηλεκτρονικού επιχειρείν και των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Με τον τρόπο αυτό, όμως, τα εσωτερικά τους συστήματα γίνονται ευπρόσβλητα σε κακόβουλη χρήση και επίθεση από εξωτερικούς χρήστες. Απαραίτητη φραγή της εισερχόμενης επιβουλής συνιστά ένα ανάχωμα ασφάλειας (firewall), δηλαδή μία διάταξη εξειδικευμένων μηχανισμών ασφάλειας που ελέγχει την πρόσβαση και τη μετακίνηση της πληροφορίας μεταξύ ενός δικτύου που εμπιστευόμαστε και ενός δικτύου που δεν εμπιστευόμαστε απαραίτητα. Το ανάχωμα ασφάλειας δεν είναι απλώς ένα σύνολο συνιστωσών λογισμικού ή υλικού, αλλά η τεχνική έκφραση μιας συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού.

Το ανάχωμα ασφάλειας μπορεί να οριστεί ως μία συλλογή από συστήματα τοποθετημένα στο σημείο σύνδεσης της υπό προστασία δικτυακής περιοχής με τα υπόλοιπα δίκτυα, που επιβάλλει μία προκαθορισμένη πολιτική ασφάλειας (security policy). Η εγκατάσταση ενός αναχώματος ασφάλειας στον οργανισμό γίνεται με σκοπό να βελτιωθεί το επίπεδο προστασίας των δεδομένων και των υπολογιστικών πόρων του οργανισμού από εισβολείς.

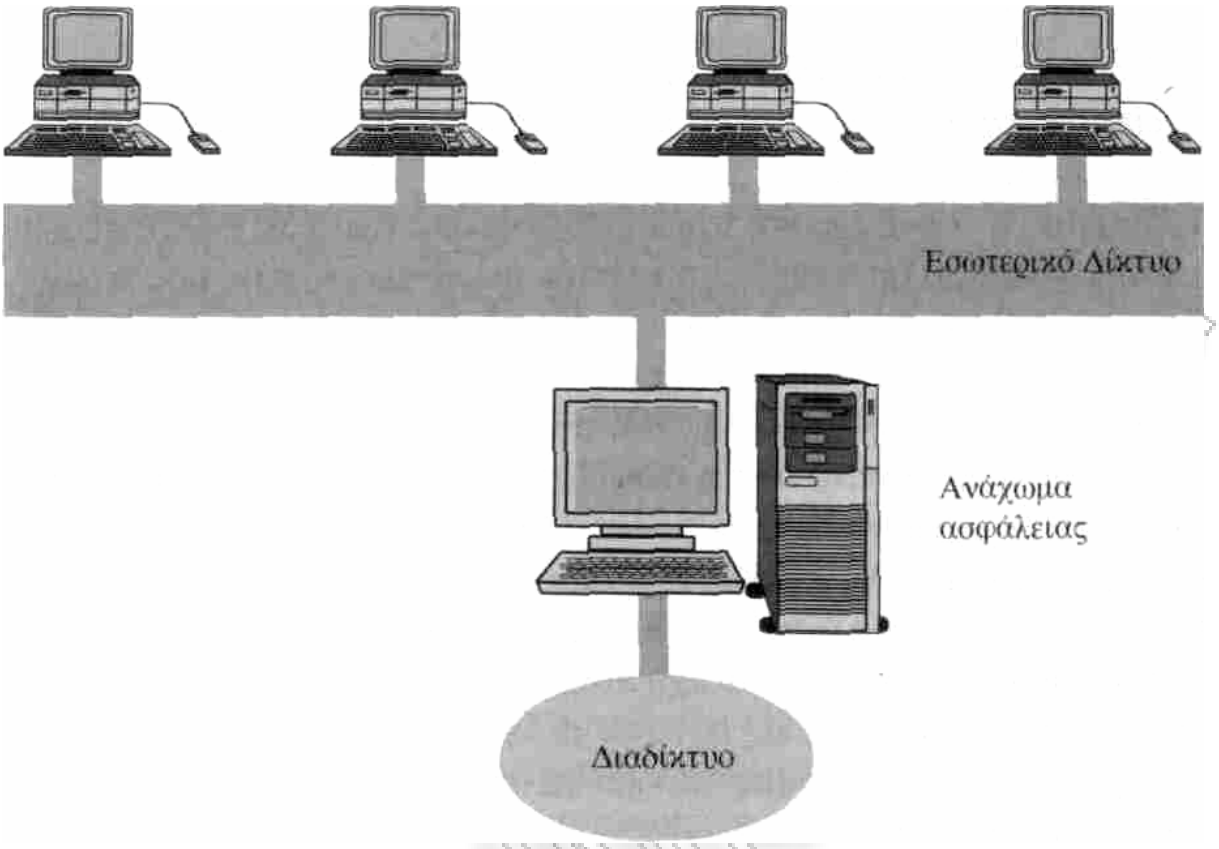
• Με τον όρο *ανάχωμα ασφάλειας (firewall)* εννοούμε συστήματα ή ομάδες συστημάτων τα οποία υλοποιούν τους κανόνες μιας πολιτικής ασφάλειας μεταξύ δύο δικτύων. Τις περισσότερες φορές (όπως φαίνεται στο ακόλυθο Σχήμα 10), το ένα από τα δύο δίκτυα είναι το internet, αλλά ένα ανάχωμα ασφάλειας, στη γενική περίπτωση, μπορεί να τοποθετηθεί και μεταξύ δύο τυχαίων δικτύων υπολογιστών.

Ο ρόλος του αναχώματος ασφάλειας μπορεί να είναι τόσο η αποτροπή μη εξουσιοδοτημένων προσβάσεων σε μία ασφαλή περιοχή, όσο και η αποτροπή μη

εξουσιοδοτημένης εξόδου πληροφορίας από μία περιοχή. Μπορεί δηλαδή να λειτουργήσει ως θύρα ελέγχου της κίνησης και προς τις δύο κατευθύνσεις.

Κρίσιμο σημείο το οποίο πρέπει να τονιστεί ιδιαιτέρως, είναι ότι ένα ανάχωμα ασφάλειας δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως από το πώς έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μία σαφής πολιτική ασφάλειας. Είναι δυνατόν ένα ανάχωμα ασφάλειας, το οποίο έχει εγκατασταθεί, διαμορφωθεί και λειτουργεί για να εξυπηρετήσει λανθασμένους σκοπούς, να δημιουργήσει σημαντικά προβλήματα. Το ανάχωμα ασφάλειας που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας που βρίσκεται κάθε φορά σε ισχύ και που πρέπει να είναι συγκεκριμένη και σαφής. Πρέπει, επίσης, να τονιστεί ότι το ανάχωμα ασφάλειας αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ τη μοναδική.

Μερικά από τα σύγχρονα εμπορικά προϊόντα για αναχώματα ασφάλειας επιχειρούν να τοποθετήσουν τα πάντα μέσα σε ένα απλό κουτί. Συνηθέστερα όμως ένα ανάχωμα ασφάλειας αποτελείται από πολλά μέρη, μερικά από τα οποία είναι δυνατό να αναλαμβάνουν και άλλες λειτουργίες εκτός από αυτές που επιτελούν ως μέρη του αναχώματος ασφάλειας. Για παράδειγμα, η σύνδεση με το internet αποτελεί σχεδόν πάντοτε μέρος του αναχώματος ασφάλειας. Επιπλέον, ακόμη και αν το ανάχωμα ασφάλειας βρίσκεται ολόκληρο μέσα σε ένα απλό κουτί, σίγουρα *δεν* πρέπει να το μελετήσουμε χωριστά από το website του οργανισμού που προστατεύει.



Σχήμα 10: Θέση ενός αναχώματος ασφαλείας (firewall)

3.6.1 Δυνατότητες ενός Αναχώματος Ασφάλειας

Τα αναχώματα ασφάλειας μπορούν να συνεισφέρουν σημαντικά στην ασφάλεια μιας ιστοθέσης. Μερικά, μάλιστα, από τα πλεονεκτήματα της χρήσης των αναχωμάτων ασφάλειας επεκτείνονται και πέρα από την ασφάλεια.

Η λειτουργικότητα των αναχωμάτων ασφάλειας εκτείνεται στα ακόλουθα:

• *Το ανάχωμα ασφαλείας αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφαλείας*

Το ανάχωμα ασφάλειας επιτρέπει στο διαχειριστή του δικτύου να ορίσει ένα κεντρικό σημείο ελέγχου (chock point), το οποίο αποτρέπει την προσπέλαση μη εξουσιοδοτημένων χρηστών στο προστατευμένο δίκτυο. Το ανάχωμα ασφάλειας απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο, το οποίο συνδέει τον οργανισμό με τον εξωτερικό κόσμο και όχι στον κάθε υπολογιστή χωριστά μέσα σε ολόκληρο το

δίκτυο. Η πρακτική αυτή είναι πολύ πιο αποτελεσματική από τη διάχυση σχετικών αποφάσεων ασφάλειας σε διάφορα σημεία.

• *Το ανάχωμα ασφάλειας εφαρμόζει έλεγχο προσπέλασης (access control) από και* προς *το δίκτνο, υλοποιώντας και υποστηρίζοντας την πολιτική ασφάλειας τον οργανισμού.*

Πρόκειται για την έκφραση του βασικού σκοποού ύπαρξης ενός αναχώματος ασφάλειας, ο οποίος επιτυγχάνεται συγκεντρώνοντας όσο το δυνατόν περισσότερη πληροφόρηση για την ταυτότητα τόσο των πακέτων (packets) όσο και των συνόδων (sessions) που διέρχονται μέσα από το ανάχωμα ασφάλειας. Με βάση αυτή την πληροφόρηση και μία ήδη καθορισμένη πολιτική ασφάλειας η οποία περιγράφει σε ποιά πακέτα και σε ποιές συνόδους επιτρέπεται η είσοδος ή η έξοδος, το ανάχωμα ασφάλειας αποφασίζει εάν θα επιτρέψει ή θα αρνηθεί την είσοδο ή έξοδο ενός πακέτου ή την έναρξη μιας συνόδου. Σε περίπτωση κατά την οποία απαγορευθεί η διέλευση, η αντίστοιχη σύνοδος στην οποία ανήκει το πακέτο αποτυγχάνει. Η μία από τις δυνατές πολιτικές ενός αναχώματος ασφάλειας βασίζεται ακριβώς στην άρνηση σε οποιαδήποτε πρόσβαση η οποία δεν έχει σαφώς επιτραπεί. Χωρίς το ανάχωμα ασφάλειας, κάθε υπολογιστής στο εσωτερικό δίκτυο ενός οργανισμού είναι εκτεθειμένος σε προσβολές από άλλους υπολογιστές του internet. Αυτό σημαίνει ότι η όλη ασφάλεια του εσωτερικού δικτύου εξαρτάται από το πόσο ισχυρά είναι τα χαρακτηριστικά ασφάλειας κάθε υπολογιστή του εσωτερικού δικτύου και άρα είναι τόσο ισχυρή όσο το πιο αδύνατο σύστημα.

• *Το ανάχωμα ασφάλειας* προσφέρει *αποτελεσματική καταγραφή τηςδραστηριότητας στο δίκτυο (network activity logging).*

Εφόσον όλη η κίνηση διέρχεται από το ανάχωμα ασφάλειας, αυτό μπορεί να αποτελέσει ένα καλό σημείο για τη συλλογή πληροφορίας σχετικά με τη χρήση τόσο των συστημάτων όσο και του δικτύου. Ένα αξιόπιστο ανάχωμα ασφάλειας καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων (activity log – audit log) το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου. Μερικά αναχώματα ασφάλειας, επίσης, προσφέρουν και μηχανισμούς συναγερμού (alarms) ώστε να βοηθήσουν στον έγκαιρο εντοπισμό μιας ύποπτης δραστηριότητας τη στιγμή που αυτή λαμβάνει χώρα και στην άμεση πληροφόρηση του διαχειριστή. Επίσης, η καταγραφή των συμβάντων από το ανάχωμα ασφάλειας επιτρέπει στο

διαχειριστή του δικτύου να εντοπίσει πιθανά σημεία συμφόρησης του διαθέσιμου εύρους ζώνης του οργανισμού (bandwidth bottlenecks).

• Το *ανάχωμα ασφάλειας προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού.*

Ένα ανάχωμα ασφάλειας μπορεί να χρησιμοποιηθεί για την προστασία ευαίσθητων σημείων του δικτύου απέναντι σε πρόσβαση από άλλα σημεία μέσα στο ίδιο δίκτυο. Μερικές φορές το ανάχωμα ασφάλειας μπορεί να χρησιμοποιηθεί για να διαχωρίσει ένα τμήμα του δικτύου από κάποιο άλλο. Με τον τρόπο αυτό μπορούμε να αποτρέψουμε την εξάπλωση σε ολόκληρο το δίκτυο ενδεχόμενων προβλημάτων που επηρεάζουν ένα συγκεκριμένο τμήμα. Σε μερικές περιπτώσεις αυτό μπορεί να συμβεί επειδή κάποιο τμήμα του δικτύου είναι πιο ευαίσθητο από κάποιο άλλο.

• *Το ανάχωμα ασφάλειας έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης*

Τα τελευταία χρόνια το internet αντιμετωπίζει πρόβλημα διαθέσιμων IP διευθύνσεων. Αυτό σημαίνει ότι οργανισμοί πού επιθυμούν να συνδεθούν με το internet είναι πιθανό να μην μπορούν να αποκτήσουν αρκετές πραγματικές IP διευθύνσεις ώστε να ικανοποιήσουν τις απαιτήσεις των χρηστών τους. Το ανάχωμα ασφάλειας έχει τη δυνατότητα να ενσωματώνει το NAT (Network Address Translator), το οποίο μεταφράζει τις εσωτερικές διευθύνσεις σε πραγματικές και να αντιμετωπίζει το πρόβλημα της έλλειψης ή της αλλαγής διευθύνσεων στην περίπτωση που ένας οργανισμός αλλάζει παροχέα υπηρεσιών internet.

Συνοπτικά σημειώνεται ότι τα αναχώματα ασφάλειας μπορούν να εμποδίσουν μη επιθυμητή κίνηση, να κατευθύνουν την εσωτερική κίνηση σε πιο αξιόπιστα εσωτερικά συστήματα, να αποκρύψουν ευαίσθητα ή ευπρόσβλητα συστήματα τα οποία δεν είναι εύκολο να αποκοπούν και να προστατευτούν από το internet, να αποκρύψουν ονόματα συστημάτων, τοπολογίες δικτύων και τύπους συσκευών δικτύων.

Πρέπει να σημειωθεί, όμως, ότι αν η σύνδεση στο internet αποτύχει, το εσωτερικό δίκτυο του οργανισμού θα συνεχίσει να λειτουργεί χωρίς προβλήματα και μόνον η πρόσβαση στο internet παύει να υφίσταται.

3.6.2 Περιορισμοί ενός Αναχώματος Ασφάλειας

Ένα ανάχωμα ασφάλειας προσφέρει εξαιρετική προστασία απέναντι σε απειλές κατά του δικτύου, αλλά δεν αποτελεί ολοκληρωμένη λύση ασφάλειας. Υπάρχουν συγκεκριμένες απειλές, οι οποίες βρίσκονται πέρα από τις δυνατότητες ελέγχου του αναχώματος ασφάλειας. Για αυτές τις απειλές απαιτούνται άλλες συμπληρωματικές ενέργειες, όπως μηχανισμοί φυσικής προστασίας (physical security), ενσωμάτωση ασφάλειας σε επίπεδο εξυπηρέτη (server security), εκπαίδευση των χρηστών (user education) στο πλαίσιο του συνολικού πλάνου ασφάλειας (security plan) και άλλες.
Οι αδυναμίες που παρουσιάζουν, γενικά, τα αναχώματα ασφάλειας συνοψίζονται στα ακόλουθα:

• *Το ανάχωμα ασφάλειας όεν μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό.*

Ένα ανάχωμα ασφάλειας παρέχει προστασία σε ένα περιβάλλον μόνον αν ελέγχει ολόκληρη την περίμετρο του περιβάλλοντος. Συνδέσεις που δε διέρχονται από το σημείο που βρίσκεται το ανάχωμα ασφάλειας, προφανώς δεν μπορούν να διασφαλισθούν από αυτό. Για παράδειγμα, αν επιτρέπεται στους χρήστες του εσωτερικού δικτύου να συνδέονται στο δίκτυο με απευθείας PPP συνδέσεις διαμέσου ενός παροχέα υπηρεσιών internet, τότε παρακάμπτονται οι μηχανισμοί ασφάλειας του αναχώματος ασφάλειας και δημιουργούνται ευπάθειες (vulnerabilities) στο δίκτυο, τις οποίες μπορεί να εκμεταλλευτούν ανεπιθύμητοι εισβολείς. Άλλο παράδειγμα αποτελεί μία ιστοθέση που επιτρέπει την πρόσβαση σε εσωτερικά συστήματα και βρίσκεται πίσω από τον ανάχωμα ασφάλειας, στο εσωτερικό του υπό προστασία δικτύου. Συνεπώς, ένα ανάχωμα ασφάλειας μπορεί να ελέγξει αποτελεσματικά την κίνηση που διέρχεται μέσα απ' αυτό, αλλά δεν μπορεί να αντιμετωπίσει επιθέσεις που δε σχετίζονται με αυτό.

• *Το ανάχωμα ασφάλειας δεν μπορεί να προστατεύσει από προγράμματα-ιούς*

Τα αναχώματα ασφάλειας δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Παρά το γεγονός ότι πολλά αναχώματα ασφάλειας ανιχνεύουν όλη την κίνηση για να καθορίσουν εάν επιτρέπεται η είσοδος στο εσωτερικό δίκτυο, η ανίχνευση αυτή αφορά στις διευθύνσεις και στις θύρες πηγής και προορισμού (source and destination addresses and port numbers) και όχι στις

λεπτομέρειες των δεδομένων. Έτσι, ανακριβή δεδομένα και ιομορφικό λογισμικό (viral software) δεν μπορούν να ελεγχθούν. Είναι λοιπόν απαραίτητο κάθε οργανισμός να χρησιμοποιεί λογισμικό αντιμετώπισης ιομορφών σε κάθε προσωπικό υπολογιστή και κυρίως στους εξυπηρέτες του, για την αντιμετώπιση σχετικών επιθέσεων από προγράμματα ιούς.

- *Το ανάχωμα ασφαλείας δεν μπορεί να προστατεύσει απέναντι στιςεπιθέσεις κακόβουλων χρηστών από το εσωτερικό τον οργανισμού.*

Οι εσωτερικοί χρήστες είναι σε θέση να υποκλέψουν δεδομένα, να καταστρέψουν υλικό και λογισμικό, να τροποποιήσουν προγράμματα και γενικότερα να παραβιάσουν την πολιτική ασφάλειας του οργανισμού χωρίς καν να έρθουν σε επαφή με το ανάχωμα ασφάλειας. Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή υπολογιστή (host security) και εκπαίδευση των χρηστών (user education). Επίσης, το ανάχωμα ασφάλειας δεν μπορεί να προστατέψει τον οργανισμό από επιθέσεις, στο πλαίσιο των οποίων κακόβουλα άτομα πείθουν υπαλλήλους της επιχείρησης να τους παραδώσουν άδεια εισόδου στο σύστημα προσποιούμενοι ίσως το διαχειριστή του δικτύου (social engineering attacks). Οι χρήστες πρέπει να ενημερωθούν σχετικά με τις διάφορες απειλές, τη σημασία της διατήρησης της μυστικότητας του συνθηματικού τους και της περιοδικής αλλαγής του, αφού όσο καλή και να είναι η ασφάλεια του συστήματος, η γνώση κάποιου συνθηματικού δίνει σε κακόβουλα άτομα εκτός ή ακόμη και εντός του οργανισμού εύκολη πρόσβαση στο σύστημα.

- *Το ανάχωμα ασφάλειας δεν μπορεί να προστατέψει τον οργανισμό απέναντι επιθέσεις συσχετιζόμενες με δεδομένα (data driven attacks)*

Τέτοιου είδους επιθέσεις συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρέτες του οργανισμού, είτε διαμέσου του ηλεκτρονικού ταχυδρομείου, είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος. Για παράδειγμα, μία επίθεση θα μπορούσε να οδηγήσει στη μεταβολή των αρχείων που σχετίζονται με τα προνόμια προσπέλασης ενός εξυπηρέτη, ώστε να διευκολύνει την πρόσβαση ενός μη εξουσιοδοτημένου χρήστη στο σύστημα.

- *Το ανάχωμα ασφάλειας δεν μπορεί να προστατεύσει τον οργανισμό από απειλές άγνωστου τύπου*

Το ανάχωμα ασφάλειας δεν έχει τη δυνατότητα να αμυνθεί αυτομάτως σε νέες απειλές οι οποίες προκύπτουν κατά καιρούς. Μπορεί να προστατεύσει το δίκτυο μόνον από γνωστές απειλές που έχουν αντιμετωπισθεί στο παρελθόν, εφόσον βεβαίως διαθέτει την απαιτούμενη τεχνολογία.

• *Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του αναχώματος ασφάλειας*

Είναι δυνατό ένα ανάχωμα ασφάλειας να ρυθμιστεί με πολύ αυστηρό τρόπο, με κίνδυνο να εμποδίσει τη διαδικτύωση ή να προκαλεί δυσαρέσκεια στους χρήστες, εξαιτίας των πολλών ελέγχων, των πολλαπλών επιπέδων ασφάλειας και κατά συνέπεια της συνολικής ελαττωμένης φιλικότητας και μειωμένης ευχρηστίας που εισάγει.

Γενικότερα πρέπει να αναφερθεί ότι τα αναχώματα ασφάλειας είναι τα πιο ευδιάκριτα σημεία μιας ιστοθέσης από την εξωτερική πλευρά και για αυτό το λόγο τα συστήματα στα οποία αυτά τοποθετούνται δέχονται τις περισσότερες επιθέσεις. Τα συστήματα αυτά στηρίζουν τη λειτουργικότητα τους στην ανθεκτικότητα και ρωμαλεότητα τους (robustness) απέναντι σε επιθέσεις. Η ανθεκτικότητα αυτή, τις περισσότερες φορές στηρίζεται στο γεγονός ότι τα συστήματα στα οποία έχει τοποθετηθεί ένα ανάχωμα ασφάλειας δεν παρέχουν πολλές λειτουργίες και εργαλεία για τους χρήστες (π.χ. μεταγλωττιστές, case-tools κλπ.). Για το λόγο αυτό, η σύνθεση των αναχωμάτων ασφάλειας πρέπει να γίνεται με προσοχή και ακρίβεια, ενώ παράλληλα πρέπει να ενημερώνεται τακτικά. Τα αρχεία ελέγχου πρέπει να παρακολουθούνται ανά τακτά χρονικά διαστήματα.

3.7 Passwords

Τα passwords είναι η πιο συνηθισμένη διαδικασία που χρησιμοποιείται σχεδόν παντού για να διασφαλίζει και να επιβεβαιώνει την ταυτότητα του χρήστη, επιτρέποντας του εν συνεχεία την είσοδο στο κάθε σύστημα. Η συγκεκριμένη μέθοδος εφαρμόζεται για κάθε είσοδο χρήστη σε ένα πληροφοριακό σύστημα ή στο δίκτυο. Από το χρήστη ζητούνται το user name και το password του, τα οποία εφόσον ταιριάζουν με αυτά που υπάρχουν στο password file, θεωρούνται από το σύστημα ως επιβεβαίωση της ταυτότητας του και έτσι ο χρήστης εισάγεται εντός του συστήματος ή του δικτύου. Τα passwords θεωρούνται ως αξιόπιστη και ασφαλής

διαδικασία ελέγχου ταυτότητας αλλά όπως σε όλα τα θέματα που αφορούν την ασφάλεια έτσι και εδώ ο κίνδυνος κρύβεται στις λεπτομέρειες.

- Η επιλογή του password είναι ίσως το κρισιμότερο σημείο και αυτό διότι οι επιλογές που κάνουν οι χρήστες συνήθως είναι προβλέψιμες. Αν από την άλλη τους δοθεί έτοιμο το password τότε επιλέγουν να το σημειώσουν παρά να το αποστηθίσουν. Στη χειρότερη περίπτωση θα ανακαλύψει κάποιος το password σε σημείωμα κολλημένο, στο πλάϊ της οθόνης του υπολογιστή του χρήστη. Η ορθότερη επιλογή είναι το password να αποτελείται από συνδυασμό γραμμάτων και αριθμών.
- Προκειμένου τα passwords να εξασφαλίζουν προστασία πρέπει τακτικά να αντικαθίστανται από νέες επιλογές. Οι χρήστες δυστυχώς αποφεύγουν αυτή την αλλαγή ή επιλέγουν να ανακυκλώνουν ένα μικρό αριθμό από passwords. Καλό θα ήταν η τακτική αλλαγή τους να επιβάλλεται από το ίδιο το λογισμικό.
- Εάν κάποιος έχει λογαριασμούς σε διαφορετικούς υπολογιστές ή sites στο internet θα πρέπει για λόγους ασφαλείας να χρησιμοποιεί διαφορετικά passwords για την είσοδο του σε κάθε σύστημα ή ιστοσελίδα. Ασφαλώς, κάτι τέτοιο είναι ιδαίτερα δύσκολο για τον χρήστη και το πιθανότερο είναι κάπου να τα σημειώσει προκειμένου να μην τα ξεχάσει. Από την άλλη μεριά η ύπαρξη ενός μόνο password αυξάνει την πιθανότητα από κάπου να αποκαλυφθεί. Σε κάθε περίπτωση η όσο το δυνατόν συχνότερη αντικατάσταση τους είναι μια καλή και ενδεδειγμένη πρόταση**.**
- Είναι προφανές πως το σημείο που το σύστημα ή το δίκτυο αποθηκεύει τα διάφορα passwords είναι σημείο που απαιτεί αυξημένη, ασφάλεια αφού αποτελεί βασικό στόχο για εισβολή. Ο συνηθισμένος τρόπος για να περιορίζεται ο κίνδυνος είναι να μην αποθηκεύονται ως κείμενο, ούτε ακόμη και με κρυπτογράφηση (encrypted), αλλά με τη μορφή που έχει το καθένα ως συνάρτηση hash. Η αντιστροφή της τιμής της συνάρτησης στο αντίστοιχο password είναι εξαιρετικά δύσκολη και έτσι τα passwords, ναι μεν δεν μπορούν να ανακτηθούν, αλλά εύκολα μπορεί να γίνεται ο έλεγχος ανάμεσα στο αποθηκευμένο password και σε αυτό που πληκτρολογείται κατά την είσοδο ενός χρήστη.

3.8 Smart Cards

Πρόκειται για μικρές κάρτες-αντίστοιχες με τις πιστωτικές- οι οποίες περιέχουν έναν επεξεργαστή, κάποια μνήμη και μια διασύνδεση με το εξωτερικό περιβάλλον. Χρησιμοποιούνται σε μία σειρά εφαρμογών συμπεριλαμβάνοντας και την ηλεκτρονική πληρωμή. Εκτελούν τρεις βασικές λειτουργίες: Αποθήκευση και διαχείριση πληροφοριών, επιβεβαίωση της ταυτότητας του χρήστη, καθώς και κρυπτογράφηση-αποκρυπτογράφηση. Το πλεονέκτημα της ως προς την ασφάλεια είναι ότι λειτουργεί σε ένα απομονωμένο περιβάλλον.

Σήμερα υπάρχει μία μεγάλη γκάμα από smart cards, οι οποίες μεταξύ τους διαφέρουν στην απόδοση και την ικανότητα του επεξεργαστή, το μέγεθος της μνήμης καθώς και την ταχύτητα διασύνδεσης με το εξωτερικό περιβάλλον. Για να λειτουργήσει απαιτείται η ύπαρξη της συσκευής που θα "διαβάσει" την smart card. Υπάρχουν διάφορες τέτοιες συσκευές (readers) ανάλογα με το τι είδους τεχνολογία διαθέτουν. Για παράδειγμα υπάρχουν συσκευές που διαβάζουν την κάρτα όταν αυτή τοποθετηθεί σε ειδική σχισμή και άλλες που τη διαβάζουν χωρίς επαφή με τη βοήθεια υπέρυθρων ακτίνων. Είτε με την πρώτη είτε με τη δεύτερη μέθοδο, επιτυγχάνεται η απαραίτητη ανταλλαγή δεδομένων ανάμεσα σε κάρτα και συσκευή ανάγνωσης και έτσι γίνεται ο έλεγχος της ταυτότητας του χρήστη.

3.9 Antivirus

Παρά την ύπαρξη περίπου αρκετών χιλιάδων ιών, εάν τηρηθούν μερικοί βασικοί κανόνες, ελαχιστοποιούμε τον κίνδυνο μόλυνσης. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το internet, είναι πλέον επιβεβλημένη η εγκατάσταση στο πληροφοριακό σύστημα κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται τακτική ενημέρωση από τους δημιουργούς του antivirus (μέσω internet κατά προτίμηση), ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών. Με την τεράστια εξάπλωση των ιών και των σκουληκιών που χρησιμοποιούν κυρίως το email για να εξαπλωθούν, θα

πρέπει το antivirus να είναι ικανό να ελέγχει και την εισερχόμενη αλληλογραφία της εταιρείας, προστατεύοντας έτσι το σύστημα από το βασικότερο τρόπο εγκατάστασης των ιών από το εξωτερικό περιβάλλον. Με αυτό τον τρόπο συλλαμβάνονται τα κακόβουλα προγράμματα, προτού φτάσουν στο ηλεκτρονικό γραμματοκιβώτιο της εταιρείας. Βέβαια, οι εφαρμογές προστασίας δεν λειτουργούν πάντα καλά, με συνέπεια να παρουσιάζονται περιστασιακά προβλήματα στη λήψη της αλληλογραφίας, αλλά μπροστά στον υπαρκτό κίνδυνο, τα συγκεκριμένα προβλήματα είναι αποδεκτά. Γενικά, δεν πρέπει να εκτελούνται επισυναπτόμενα αρχεία, εάν δεν υπάρχει βεβαιότητα για την καθαρότητα τους. Ακόμα και αν φαίνονται αθώα (μια εικόνα jpg, για παράδειγμα) ή προέρχονται από γνωστό αποστολέα, δεν αποκλείεται το αρχείο να είναι εκτελέσιμο και να έχει τη μορφή picture.jpg.exe. Πρέπει να επισημανθεί ότι ελάχιστες είναι οι πιθανότητες να μολυνθεί το σύστημα ανοίγοντας απλώς ένα email. Θα πρέπει να εκτελεστεί ο επισυναπτόμενος, καμουφλαρισμένος, κακόβουλος κώδικας. Προσοχή χρειάζεται και με τα αρχεία excel και word που λαμβάνονται, τα οποία καλό θα είναι να περνούν από έλεγχο για μακροϊούς. Επίσης, πρέπει να προσεχθούν και οι διάφορες εφαρμογές που εγκαθίστανται, ειδικά εάν προέρχονται οπό αμφιλεγόμενες πηγές.

Η παρουσία του antivirus προστατεύει επίσης το σύστημα και από τους εσωτερικούς κινδύνους για την περίπτωση που κάποιος χρήστης είτε εν αγνοία του, είτε εσκεμμένα προσπαθήσει να εγκαταστήσει έναν τέτοιο ιό. Άλλωστε ο κίνδυνος των δολιοφθορών εκ των έσω πρέπει να βρίσκεται ιδιαίτερα ψηλά στην ιεραρχία των κινδύνων, για το σχεδιαστή του συστήματος ασφαλείας. Αλλά και στην περίπτωση που το σύστημα μολυνθεί από κάποιον ιό, πρέπει αμέσως να ελεγχθεί από το antivirus και να εντοπιστεί ο ιός και καθαρίσει το σύστημα. Καλό είναι γενικά να δημιουργούνται backup files σε δισκέτες ή CD Roms ώστε να υπάρχει πάντα διαθέσιμο κάποιο αρχείο σε περίπτωση που μολυνθεί από ιό και να μη χαθεί, αλλά και να υπάρχουν δισκέτες εκκίνησης του συστήματος που να μπορούν να ξεκινήσουν το σύστημα σε περίπτωση που μολυνθεί ο boot sector.

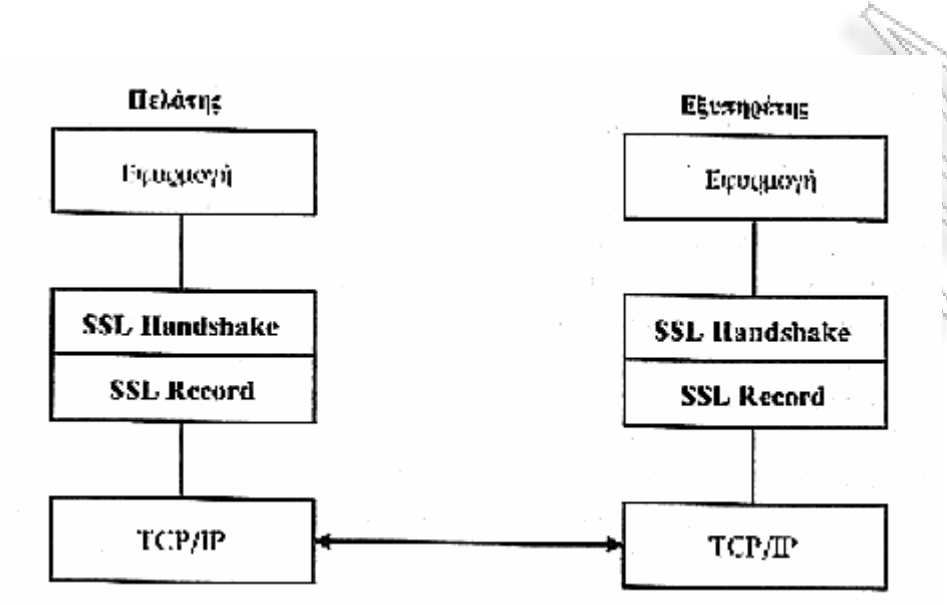
Εικόνα 8: Antivirus (Trend Micro)

3.10 Πρωτόκολλο Secure Sockets Layer – SSL

Στον προγραμματισμό εφαρμογών σε περιβάλλον internet είναι συνιθισμένο να χρησιμοποιείται μια γενικευμένη λειτουργία διαδιεργασιακής επικοινωνίας (Interprocess Communications – IPC) για την εργασία με διαφορετικά πρωτόκολλα επιπέδου μεταφοράς. Δυο δημοφιλείς διεπαφές IPC είναι τα BCD Sockets και Transport Layer Interface TLI, που συναντώνται στις διάφορες εκδοχές του Unix system. Μια ιδέα που μπορεί να σκεφτεί κάποιος όταν προσπαθεί να προσφέρει υπηρεσίες ασφάλειας για TCP/IP εφαρμογές είναι να βελτιώσει μια IPC διεπαφή, όπως το BCD Sockets, με τη δυνατότητα πλέον να αυθεντικοποιεί ομότιμες οντότητες, να ανταλλάσσει μυστικά κλειδιά και να τα χρησιμοποιεί για να αυθεντικοποιεί και κρυπτογραφεί τις ροές δεδομένων μεταξύ ομότιμων επικοινωνούντων οντοτήτων.

Η εταιρία Netscape Communications Corporation ακολούθησε αυτή την προσέγγιση όταν σχεδίασε για πρώτη φορά το πρωτόκολλο Secure Sockets Layer – SSL. Η

αρχική έκδοση χρησιμοποιήθηκε για τις εσωτερικές ανάγκες της εταιρίας. Στην επόμενη έκδοση καθιερώθηκε ως de facto πρώτυπο για την κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων.



Σχήμα 11: Αρχιτεκτονική τοποθέτηση του Πρωτοκόλλου SSL

Η αρχιτεκτονική τοποθέτηση του SSL απεικονίζεται στο Σχήμα 11. Το SSL στρωματοποιείται στην κορυφή μίας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που παρέχεται από το TCP/IP και είναι σε θέση να παρέχει υπηρεσίες ασφάλειας για αυθαίρετες TCP/IP εφαρμογές. Στην πραγματικότητα, ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείται στην κορυφή του.

Συνοπτικά, μπορεί να αναφερθεί ότι το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

• Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού.

• Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων, αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μία αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.

• Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα

αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

Κεφάλαιο 4

ΤΕΧΝΟΛΟΓΙΕΣ ΠΡΟΣΤΑΣΙΑΣ–ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

4.1 Ανίχνευση Εισβολέων

Στα πλαίσια των αρμοδιοτήτων των διαχειριστών συστημάτων περιλαμβάνεται και η προστασία των υπολογιστικών συστημάτων από ποικίλες επιθέσεις. Τα συστήματα πρέπει να παρακολουθούνται με σκοπό την ανίχνευση και καταγραφή όλων τω προσπαθειών για επιτυχή αλλά και ανεπιτυχή παραβίαση της ασφάλειας. Τα υπολογιστικά συστήματα που δέχονται επίθεση δεν πληρούν ένα από τα ακόλουθα χαρακτηριστικά:

1. Το σύνολο των ενεργειών των χρηστών και των διεργασιών ακολουθούν σε γενικές γραμμές, ένα στατιστικά προβλέψιμο τρόπο (pattern). Για παράδειγμα, ένας χρήστης που χρησιμοποιεί αποκλειστικά προγράμματα αυτοματισμού γραφείου θεωρείται απίθανο να προσπαθήσει να εκτελέσει λειτουργίες συντήρησης συστήματος.
2. Οι ενέργειες των χρηστών και των διεργασιών δεν περιλαμβάνουν ακολουθίες εντολών που να υπονομεύουν την πολιτική ασφαλείας του συστήματος. Θεωρητικά, κάθε τέτοια ακολουθία εντολών πρέπει να μη γίνει δεκτή. Στην πραγματικότητα όμως, μπορούν να ανιχνευθούν μόνο γνωστές ακολουθίες υπονόμευσης του συστήματος.
3. Οι ενέργεις των διεργασιών συμμορφώνονται με ένα σύνολο προδιαγραφών που περιγράφουν επιτρεπτές ενέργειες.

Τα συστήματα που πραγματοποιούν αυτόν τον έλεγχο αποκαλούνται *Συστήματα Ανίχνευσης Εισβολών* (Intrusion Detection Systems- IDS). Στη γενική περίπτωση, τα ανίχνευσης εισβολών θα μπορούσαν να καταγράφουν απλώς την κίνηση του δικτύου για μετέπειτα ανάλυση. Σε αυτή την περίπτωση, θα αποτελούσαν περισσότερο

μηχανές καταγραφής συμβάντων (logging engines), παρά μηχανισμούς εντοπισμού εισβολής.

Οι στόχοι των πραγματικών συστημάτων ανίχνευσης εισβολών αυτών είναι:

1. *Ανίχνευση μεγάλου εύρους εισβολών:* Οι εισβολές, τόσο αυτές που προέρχονται από το εσωτερικό του δικτύου, όσο και από το εξωτερικό, παρουσιάζουν ιδιαίτερο ενδιαφέρον. Με τα IDS μπορούν να εντοπιστούν γνωστές και άγνωστες επιθέσεις. Η δυνατότητα αυτή προϋποθέτει την ύπαρξη ενός μηχανισμού εκμάθησης ή προσαρμογής στους νέους τύπους επίθεσης και στις αλλαγές της συνήθους δραστηριότητας των χρηστών.

2. *Έγκαιρη ανίχνενση εισβολών:* Ο όρος *έγκαιρη* δεν αναφέρεται κυριολεκτικά σε πραγματικό χρόνο (real time), αφού η ανίχνευση της εισβολής σε πραγματικό χρόνο εισάγει σημαντικά ζητήματα ανταπόκρισης. Συχνά, όμως, απαιτείται η ανακάλυψη μίας εισβολής σε εύλογο χρονικό διάστημα. Και αυτό γιατί στις περισσότερες περιπτώσεις, ο προσδιορισμός μιας εισβολής που πραγματοποιήθηκε πριν από σημαντικό χρονικό διάστημα φαίνεται να μην παρουσιάζει ιδιαίτερη χρησιμότητα.

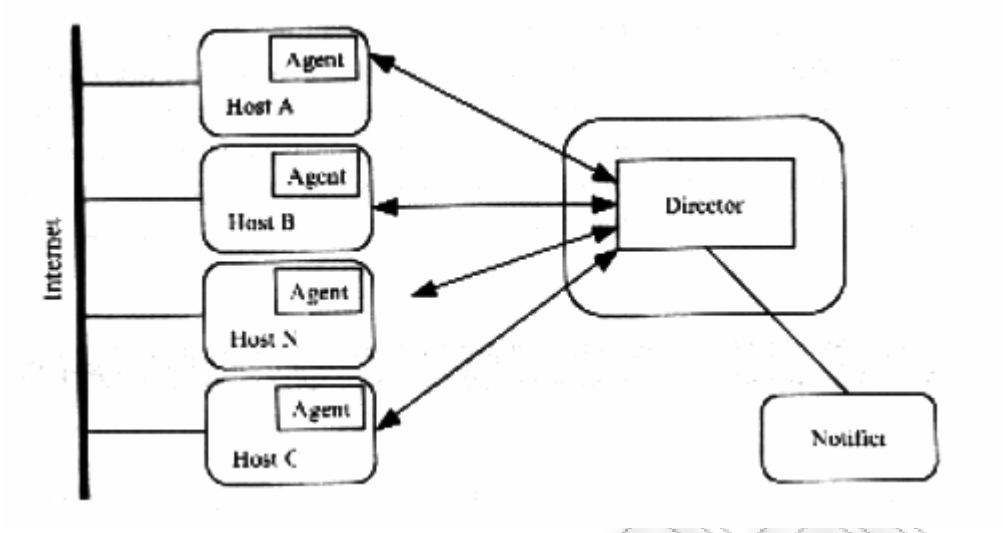
3. *Παρουσίαση της ανάλυσης με απλή και εύκολα αντιληπτή μορφή:* θα ήταν επιθυμητό τα αποτελέσματα ανίχνευσης μιας εισβολής να προκύπτουν, τελικά, από την τιμή μιας δίτιμης μεταβλητής. Συνήθως, όμως, αυτό δεν μπορεί να συμβεί αφού οι εισβολές δεν είναι λειτουργικά τόσο σαφείς. Για το λόγο αυτό, ο μηχανισμός ανίχνευσης εισβολών παρουσιάζει περισσότερο σύνθετα δεδομένα στον υπεύθυνο ασφάλειας του συστήματος. Εκείνος, με τη σειρά του, πρέπει να συνάγει αν πρέπει να ληφθούν κάποια μέτρα και ποια ακριβώς πρέπει να είναι αυτά. Επειδή οι μηχανισμοί ανίχνευσης εισβολών μπορεί να παρακολουθούν περισσότερα από ένα συστήματα, ιδιαίτερη κρισιμότητα παρουσιάζει η διεπαφή τους με το χρήστη.

4. *Να είναι ακριβή:* Ένα ψευδές θετικό σήμα (false positive) προκύπτει όταν ένα σύστημα εντοπισμού εισβολών αναφέρει μία επίθεση, ενώ στην πραγματικότητα δεν υπάρχει σχετική επίθεση σε εξέλιξη. Τα ψευδώς θετικά σήματα μειώνουν την αξιοπιστία του συστήματος και αυξάνουν αναιτίως την απαιτούμενη εργασία. Τα ψευδώς αρνητικά σήματα (false negative) παράγονται όταν ένα σύστημα ανίχνευσης εισβολών αποτυγχάνει να αναφέρει μία πραγματική επίθεση που βρίσκεται σε εξέλιξη. Αυτά είναι ιδιαίτερα αρνητικά, αφού ο σκοπός των συστημάτων εντοπισμού εισβολών είναι ακριβώς να αναφέρουν τις πραγματικές επιθέσεις. Γενικός σκοπός

ενός συστήματος ανίχνευσης εισβολών είναι να ελαχιστοποιήσει τις εσφαλμένες ενδείξεις από αμφότερες τις κατηγορίες σφαλμάτων.

Τα συστήματα ανίχνευσης εισβολών προσδιορίζουν εάν κάποιες ενέργειες αποτελούν εισβολές, με βάση ένα ή περισσότερα μοντέλα εισβολών (models of intrusion). Ένα μοντέλο ταξινομεί μία ακολουθία καταστάσεων ή ενεργειών, ή χαρακτηρίζει καταστάσεις ή ενέργειες ως «καλές» (δηλαδή δεν υπάρχει εισβολή) ή «κακές» (δηλαδή υπάρχουν πιθανές εισβολές). Τα μοντέλα ανίχνευσης διαταραχών (anomaly models) αποφαίνονται με βάση στατιστικά στοιχεία και ταξινομούν τις ενέργειες ή καταστάσεις που είναι στατιστικά ασυνήθιστες ως «κακές». Τέτοια είναι τα μοντέλα «τιμών κατωφλίου», «στατιστικών ροών» και «το μοντέλο του Markov». Τα μοντέλα κακής συμπεριφοράς (misuse models) συγκρίνουν ενέργειες ή καταστάσεις με ακολουθίες που είναι ήδη γνωστό ότι αποτελούν εισβολές, ή με ακολουθίες που θεωρείται ότι αποτελούν εισβολές και τις ταξινομούν ως «κακές». Τα μοντέλα που βασίζονται στις προδιαγραφές (specification-based models) ταξινομούν τις καταστάσεις που παραβιάζουν τις προδιαγραφές ως «κακές». Τα μοντέλα μπορεί να είναι είτε προσαρμοστικά (adaptive) δηλαδή μοντέλα που αλλάζουν τη συμπεριφορά τους με βάση τις καταστάσεις και τις ενέργειες των συστημάτων, είτε στατικά (static) δηλαδή μοντέλα που αρχικοποιούνται από δεδομένα που έχουν συλλέγει και δεν τροποποιούνται κατά τη διάρκεια εκτέλεσης του συστήματος.

Ένα σύστημα ανίχνευσης εισβολών αποτελεί ταυτόχρονα και ένα αυτοματοποιημένο μηχανισμό παρακολούθησης και ελέγχου (auditing). Όπως όλοι οι μηχανισμοί ελεγκτικής παρακολούθησης αποτελείται από τρία μέρη, όπως απεικονίζεται ατο παρακάτω Σχήμα 12. Ο αντιπρόσωπος (agent) αντιστιχεί στον logger: αποκτά πληροφορίες από ένα στόχο, όπως ένα υπολογιστικό σύστημα. Ο διευθυντής (director) αντιστοιχεί στον αναλυτή: αναλύει τα δεδομένα που προέρχονται από τους αντιπροσώπους όπως απαιτείται, με σκοπό να προσδιορίσει εάν μια επίθεση είναι σε εξέλιξη ή έχει ήδη συμβεί. Ο διευθυντής μεταδίδει την πληροφορία στον αγγελιοφόρο (notifier), ο οποίος αποφασίζει πότε και πώς να ειδοποιήσει την αναγκαία οντότητα. Ο αγγελιοφόρος μπορεί να επικοινωνήσει με τους αντιπροσώπους για να ρυθμίσει θέματα εισαγωγής στοιχείων, αν αυτό θεωρηθεί απαραίτητο.



Σχήμα 12: Αρχιτεκτονική ενός συστήματος ανίχνευσης εισβολών.

4.2 Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Η ανωνυμία (anonymity) και η ιδιωτικότητα (privacy) αποτελούν έννοιες ιδιαίτερης σημασίας για τις σύγχρονες κοινωνίες και πολιτισμούς. Η σημαντικότητα τους είναι ακόμη πιο υψηλή στα σύγχρονα ψηφιακά περιβάλλοντα.

Στη γενική περίπτωση, σε περιβάλλον απλής πλοήγησης στον ιστό, αλλά κυρίως σε υπηρεσίες ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης πρέπει να μπορεί να διασφαλιστεί η ανωνυμία, δηλαδή η δυνατότητα ενός χρήστη να μην αποκαλύπτεται η ταυτότητα του χωρίς τη σύμφωνη γνώμη του, εκτός βεβαίως από τις περιπτώσεις που αυτό απαιτηθεί ύστερα από σχετική δικαστική εντολή.

Η ιδιωτικότητα μπορεί να θεωρηθεί ως το δικαίωμα ελέγχου των τρόπων και των μεθόδων με τους οποίους μία πληροφορία που σχετίζεται με ένα φυσικό πρόσωπο αποκτάται, κατανέμεται, διαμοιράζεται και χρησιμοποιείται από άλλες οντότητες.

4.2.1 Cookies

Στο πρωτόκολλο HTTP που αποτελεί τη βάση για τον ιστό, δεν υπάρχει, γενικά, προφύλαξη από τη διάθεση μιας πληροφορίας σε διάφορες οντότητες. Αυτή η σχεδιαστική επιλογή παρουσιάζει κάποια πλεονεκτήματα. όπως η απλότητα και η

μείωση πρόσθετων ανταλλασσόμενων πληροφοριών κατά την αποστολή των μηνυμάτων. Ωστόσο υπάρχουν σημαντικά μειονεκτήματα, όπως το γεγονός ότι κάθε επικοινωνία μεταξύ ενός φυλλομετρητή και ενός εξυπηρέτη (server), στα πλαίσια εφαρμογών ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης, απαιτεί ολοκληρωμένες και σταθερές HTTP αιτήσεις και απαντήσεις για τη διασφάλιση της δυνατότητας χειρισμού σχετικών μηνυμάτων δοσοληψιών.

Τα cookies αποτελούν συνήθως αρχεία με αποθηκευμένη σε αυτά μικρή ποσότητα πληροφοριών. Σχεδιαστικός σκοπός των cookies είναι η απλοποίηση των διαδικασιών κατά την επικοινωνία εξυπηρετούμενου-εξυπηρέτη, επιτρέποντας στο φυλλομετρητή να καταχωρίσει συγκεκριμένες πληροφορίες. Ο φυλλομετρητής αποστέλλει στον εξυπηρέτη αυτές τις πληροφορίες κάθε φορά που επικοινωνεί με αυτόν. Αρχικά τα cookies χρησιμοποιούνταν κυρίως για την καταχώριση παραμέτρων χρήσης των εξυπηρετούμενων και για την υλοποίηση καρτών αγορών (shopping cards) σε περιβάλλον ηλεκτρονικού εμπορίου. Σήμερα πολλοί χρήστες θεωρούν -δικαιολογημένα- ότι με την ανίχνευση και καταγραφή των κινήσεων τους στο internet θίγεται η προσωπική τους ζωή. Και βεβαίως οι φόβοι για ανεπιθύμητη χρήση των πληροφοριών που συλλέγονται μέσω cookies σε πολλές περιπτώσεις έχουν αποδειχτεί βάσιμοι. Σχετικά πρόσφατο παράδειγμα απετέλεσε η εταιρεία DoubleClick, η οποία είχε δημιουργήσει την καταναλωτική κατατομή (profile) εκατοντάδων χιλιάδων χρηστών του internet χρησιμοποιώντας τις πληροφορίες που συγκέντρωνε από τα cookies. Χρησιμοποιώντας ένα προϊόν λογισμικού παρακολούθησης στο δίκτυο (packet sniffer), το οποίο μπορεί να αξιοποιηθεί για την ανίχνευση πληροφοριών που διακινούνται από τον υπολογιστή μέσω δικτύου, αποκαλύφθηκε ότι στους εξυπηρέτες της DoubleClick προωθούνταν τα ακόλουθα στοιχεία χρηστών: ηλεκτρονική διεύθυνση, τηλέφωνο, ταχυδρομική διεύθυνση και πλήρες όνομα. Τα δεδομένα που αποστέλλονταν στην εταιρεία DoubleClick μετά από συναλλαγές με αυτήν, περιλάμβαναν τίτλους βιντεοταινιών που ενδιαφέρθηκε να αγοράσει ο χρήστης, λεπτομέρειες αεροπορικών ταξιδιών, λέξεις-κλειδιά που χρησιμοποίησε σε μηχανές αναζήτησης στο internet, ακόμη και στοιχεία για την κατάσταση της υγείας των χρηστών, όπου αυτό ήταν κατορθωτό.

4.2.2 Ζητήματα από τη χρήση των cookies

Τα βασικά ζητήμτα κατά τη χρήση των cookies σχετίζονται ακριβώς με τηνιδιωτικότητα του χρήστη. Όπως προαναφέρθηκε, τα cookies επιτρέπουν στις ιστοθέσεις να καταγράψουν και να παρακολουθήσουν συνήθειες των χρηστών. Αυτά τα δεδομένα είναι ιδιαίτερα χρήσιμα και παρέχουν εκτενείς δυνατότητες αξιοποίησης, αφού οι προσωπικές πληροφορίες των χρηστών μπορούν δυνητικά να διαδίδονται σε ευρύτερη κοινότητα αποδεκτών και όχι μόνο στον προορισμό που αναφέρονται.
Πρόσθετες ανησυχίες σχετικά με τα cookies προέρχονται από συνήθεις υπερβολές σχετικά με τον τρόπο που υλοποιείται και λειτουργεί η τεχνολογία αυτή. Ένα cookie δε μπορεί να αποκτήσει κάθε πληροφορία για τον υπολογιστή ενός χρήστη. Δεν μπορεί να αποκτήσει αυτοβούλως, ως αποτέλεσμα διαδικασίας αναζήτησης στον υπολογιστή, στοιχεία για την ταυτότητα του χρήστη, τη διεύθυνση ή άλλα στοιχεία. Ο μόνος τρόπος με τον οποίο αυτές οι πληροφορίες μπορούν να καταλήξουν σε ένα cookie, είναι μόνον όταν ο ίδιος ο χρήστης θελήσει να τις παρέχει σε μία ιστοθέση. Σε αυτήν αυστηρά την περίπτωση οι πληροφορίες επιστρέφονται σε ένα cookie.
Συνήθως χρησιμοποιούνται cookies για να καταγράψουν τη συμπεριφορά των χρηστών και να δημιουργήσουν διαφημίσεις που θα έχουν μεγάλο βαθμό προσπελασιμότητας. Η DoubleClick εκμεταλλεύτηκε αυτή την τεχνική ένα βήμα παραπέρα, συγκεντρώνοντας τη δραστηριότητα των χρηστών διαμέσου άλλων ιστοθέσεων πελατών. Έτσι, ένας χρήστης όταν επισκεπτόταν μία αθλητική ιστοθέση και δεχόταν μία διαφήμιση από την DoubleClick, θα μπορούσε αργότερα να βρεθεί προ εκπλήξεως, αφού υπήρχε η δυνατότητα να του παρουσιάζονται τέτοιου είδους διαφημίσεις κατά την εισαγωγή του σε οποιαδήποτε άλλη ιστοθέση σχετικού περιεχομένου. Κάθε προσωπική πληροφορία που παρέχονταν από ένα χρήστη σε μία ιστοθέση που εξυπηρετούνταν από τη DoubleClick μπορούσε να καταλήξει να είναι διαμοιράσιμη με κάποιο διαφημιζόμενο φορέα. Επιπλέον, αξιοσημείωτο ήταν το γεγονός της απόκτησης από την DoubleClick του πρακτορείου της Abacus Direct, εταιρείας υπηρεσίας άμεσου marketing, που διαθέτει τεράστια βάση πληροφοριών για διάφορους χρήστες στο internet. Χρησιμοποιώντας αυτά τα δεδομένα, η

DoubleClick θα μπορούσε να συνδέσει μια οντότητα-χρήστη στο internet με την παρματική ταυτότητά της στο φυσικό κόσμο.

Άλλες αμφιλεγόμενες πρακτικές εμπλέκουν τη χρήση cookies σε μαζικά ηλεκτρονικά μηνύματα, τα οποία περιλαμβάνουν συνημμένα HTML αρχεία. Οι εικόνες σε αυτά τα HTML αρχεία αρχικοποιούν αιτήσεις, οι οποίες μπορούν να καταλήξουν σε τοποθέτηση και αργότερα ανάκτηση των cookies. Είναι επίσης δυνατό να συνδεθεί το ηλεκτρονικό ταχυδρομείο ενός χρήστη με ένα αποθηκευμένο ID που βρίσκεται σε ένα cookie της μηχανής του.

Η χρήση των cookies για την καταγραφή των ιχνών των χρηστών έχει δημιουργήσει εύλογη ανησυχία σε διεθνή κλίμακα. Ένας εξυπηρέτης πηγής, από τον οποίο μπορούν να ληφθούν cookies, πληροφορίες κλπ., μπορεί να δημιουργήσει μία επικεφαλίδα Set-cookie για να μπορεί να καταγράψει την πορεία ενός χρήστη μέσω του εξυπηρέτη.

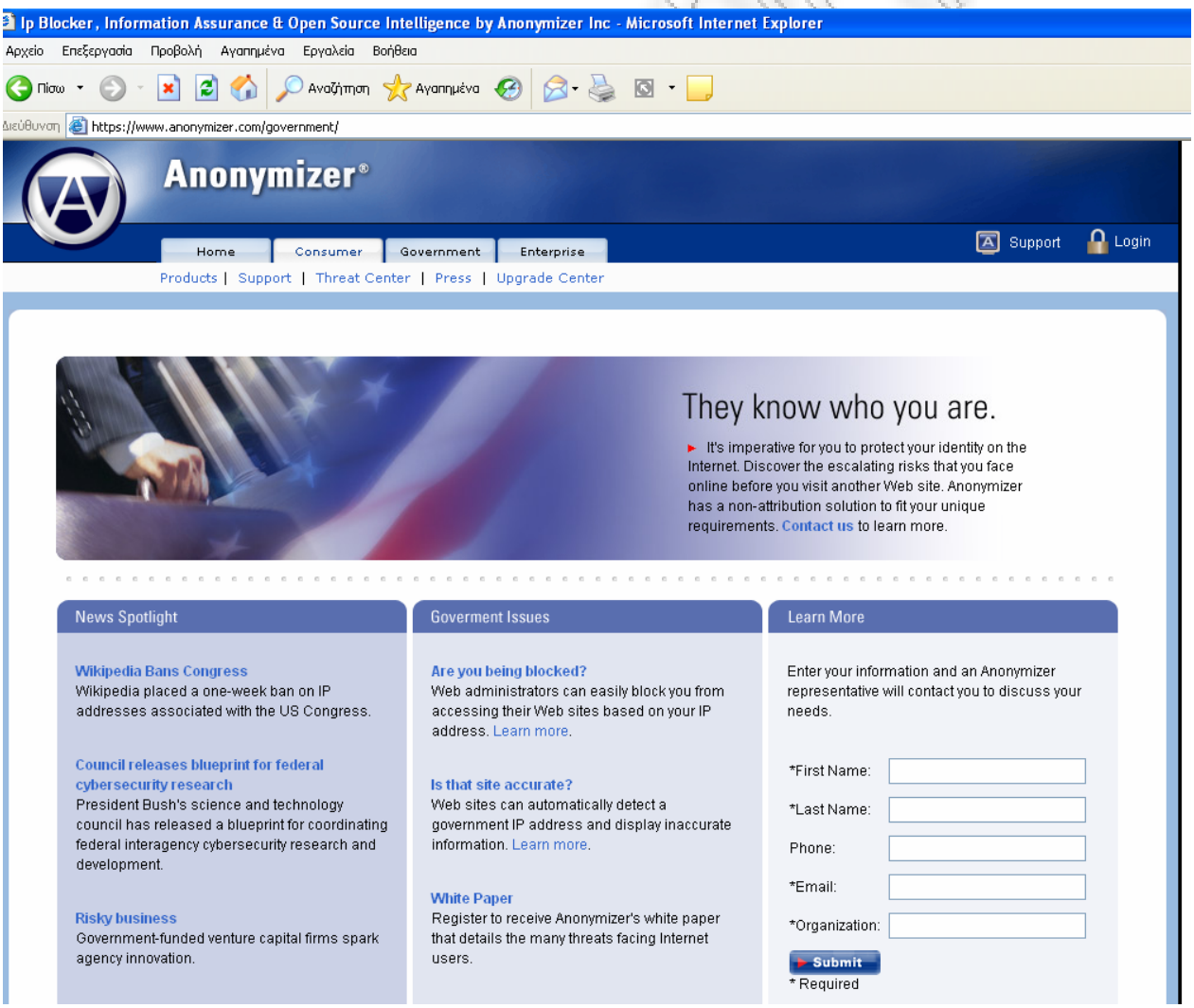
4.2.3 Ανώνυμη Φυλομέτρηση

Υπάρχουν αρκετά εργαλεία και υπηρεσίες που έχουν τη δυνατότητα να παρέχουν προστασία στην ανωνυμία και την ιδιωτικότητα των χρηστών του internet. Κατά καιρούς έχουν αναπτυχθεί αρκετά εργαλεία για την υποβοήθηση των χρηστών με σκοπό την ανώνυμη προσπέλαση σε ιστοσελίδες στο internet. Αυτοί οι αντιπρόσωποι ανωνυμίας (anonymity agents) βασίζουν τη λειτουργία τους στη διαβεβαίωση ότι οι αιτήσεις στις ιστοσελίδες δε θα συνδέονται με μία διεύθυνση IP από την οποία θα μπορεί ο χρήστης να αναγνωριστεί. Ένα από τα πιο γνωστά εργαλεία ανωνυμίας είναι ο Anonymizer, υπηρεσία που καταχωρίζει HTTP αιτήσεις σε ιστοθέσεις για λογαριασμό των χρηστών του.

Ο Anonymizer αποτελεί μία δημοφιλή υπηρεσία που σκοπό έχει τη διαφύλαξη της ανωνυμίας των επικοινωνιών στο internet. Αποτελεί ουσιαστικά μία ιστοσελίδα που λειτουργεί ως ένας πληρεξούσιος εξυπηρέτης (proxy server) για τις αιτήσεις στο internet, αντιπροσωπεύοντας τους χρήστες του. Με τον τρόπο αυτό, η μόνη IP διεύθυνση που αποκαλύπτεται στους εξυπηρέτες που φιλοξενούν την ιστοσελίδα και παρέχουν υπηρεσίες στους χρήστες είναι η διεύθυνση του anonymizer. Ο anonymizer παρέχεται από έναν HTTP πληρεξούσιο εξυπηρέτη που εκτελείται στη

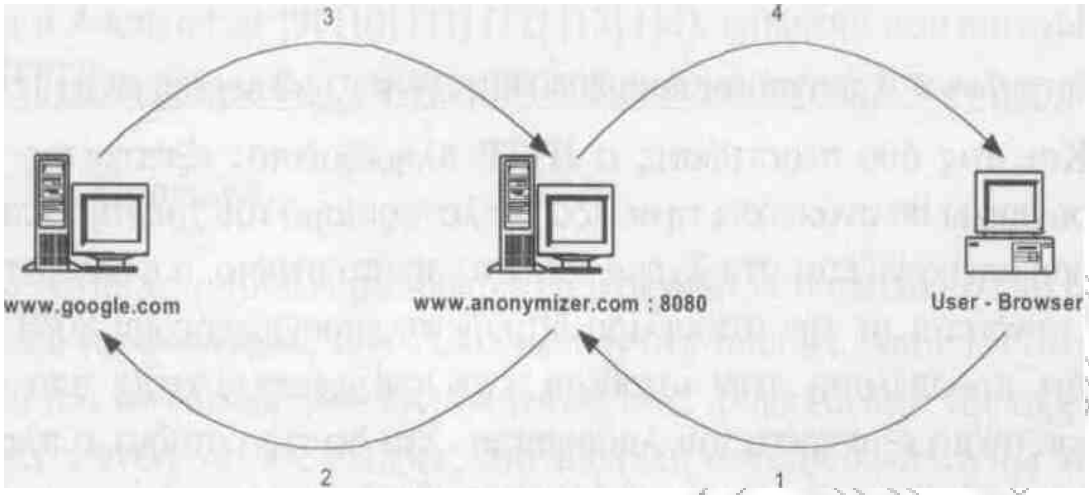
θύρα 8080 του εξυπηρέτη ο οποίος φιλοξενεί την anonymizer σελίδα, δηλαδή τη σελίδα που φιλοξενείται στη διεύθυνση www.Anonymizer.com.

Ένας χρήστης μπορεί είτε να καταγράψει το url του πληρεξούσιου εξυπηρέτη, είτε να παρακάμψει τον πληρεξούσιο εξυπηρέτη καταγράφοντας απευθείας το url του HTTP εξυπηρέτη. Η υπηρεσία ανωνυμίας είναι μία απλή στη χρήση υπηρεσία ανώνυμης προώθησης, η οποία μπορεί να χρησιμοποιηθεί δωρεάν και συνήθως είτε υπάρχει μία μικρή χρονική καθυστέρηση σε κάθε σελίδα για παρουσίαση διαφημίσεων, είτε πραγματοποιείται αγορά για έκδοση ενός λογαριασμού. Οι όροι συμφωνίας για το λογαριασμό αυτό βρίσκονται στην ιστοσελίδα του anonymizer.



Εικόνα 9: site www.Anonymizer.com

Η λειτουργία του Anonymizer μπορεί να διασαφηνιστεί από το παράδειγμα του επόμενου σχήματος 13:



Σχήμα 13: Παράδειγμα αίτησης επίσκεψης της σελίδας www.google.com με χρήση του Anonymizer.

Ο χρήστης επισκέπτεται την ιστοσελίδα του Anonymizer και ζητά μέσω αυτής να επισκεφτεί την ιστοσελίδα www.google.com. Ο Anonymizer λειτουργεί για το φυλλομετρητή του χρήστη ως πληρεξούσιος στη θύρα 8080 και ο φυλλομετρητής του χρήστη δείχνει στο πεδίο διευθύνσεων:

http://anon.free.Anonymiser.com/http://www.google.com

- Ο Anonymizer λαμβάνει την αίτηση του χρήστη και αποστέλλει αντίστοιχη αίτηση για την ιστοσελίδα www.google.com, παρέχοντας έτσι στοιχεία όχι για το χρήστη, αλλά για τον ίδιο τον Anonymizer.
- Ο δικτυακός τόπος του google μόλις δεχτεί την αίτηση, έχει τη δυνατότητα καταγραφής της και προσδιορίζει τον αιτούντα. Αυτός, όπως προαναφέρθηκε, είναι ο εξυπηρέτης Anonymizer. Στη συνέχεια, στέλνει τα αιτούμενα δεδομένα σε αυτόν που τα ζήτησε, δηλαδή στον Anonymizer.
- Ο Anonymizer λαμβάνοντας τα δεδομένα, τα προωθεί στον αρχικά αιτούντα.

4.3 Τεχνολογίες Λογοκρισίας

Η ευρεία αξιοποίηση του internet γενικότερα και του παγκόσμιου ιστού ειδικότερα, συχνά δέχεται έντονη κριτική ότι εκτός από μέσον αναζήτησης και παροχής πληροφόρησης ευρείας κλίμακας παρέχει την υποδομή κακής χρήσης και διανομής περιεχομένου το οποίο μπορεί να είναι επιθετικό, υβριστικό, χυδαίο και γενικώς παράνομο. Τυπικά παραδείγματα αποτελούν το υλικό που προάγει την παιδική πορνεία, οι οδηγίες για παρασκευή ναρκωτικών ουσιών, καθώς και προπαγανδιστικό υλικό από τρομοκρατικές οργανώσεις και καθεστώτα αυταρχικών αντιλήψεων. Για την επίτευξη λογοκρισίας, ακριβώς υπό την έννοια του ελέγχου προσπέλασης στον παγκόσμιο ιστό με βάση το περιεχόμενο, έχουν προταθεί συγκεκριμένες τεχνικές λύσεις.

Ως λογοκρισία (cencorship) χαρακτηρίζεται η καταστολή δημοσίευσης ιδεών, κειμένων, φωτογραφιών, ταινιών, ή άλλου είδους πληροφοριών. Οι τεχνικές λύσεις που έχουν μέχρι σήμερα προταθεί για τη λογοκρισία - έλεγχο προσπέλασης με βάση το περιεχόμενο - εντάσσονται σε δύο επιμέρους κατηγορίες: στη δέσμευση περιεχομένου (content blocking) και στη βαθμονόμηση περιεχομένου (content rating) από κοινού με την έννοια της αυτοοριοθέτησης (self-determination):

Η ιδέα της δέσμευσης περιεχομένου καθιστά τους παρόχους υπηρεσιών internet (ISPs-Internet Service Providers) υπεύθυνους να αποφασίζουν για το περιεχόμενο που δε θα παρέχουν στους συνδρομητές τους.

Η ιδέα της βαθμονόμησης περιεχομένου και της αυτοοριοθέτησης, αντιθέτως, καθιστά τους ίδιους τους συνδρομητές υπεύθυνους για το περιεχόμενο που προσπελαύνουν.

Στην περίπτωση της δέσμευσης περιεχομένου, οι ISPs οφείλουν να σχεδιάσουν και υλοποιήσουν τεχνολογικές λύσεις ώστε να καταστήσουν μη προσπελάσιμες τις ιστοσελίδες που παρέχουν, ή καθιστούν διαθέσιμο στους συνδρομητές, υλικό με αμφιλεγόμενο περιεχόμενο. Αντίθετα, οι ISPs δεν έχουν καμία σχετική υποχρέωση στην περίπτωση της βαθμονόμησης περιεχομένου και της αυτοοριοθέτησης, όπου αφενός οι ίδιοι οι πάροχοι του περιεχομένου οφείλουν να το αξιολογήσουν, αφε-

τέρου οι χρήστες του internet και συνδρομητές των ISPs οφείλουν να προστατευτούν ρυθμίζοντας τα προγράμματα πλοήγησης με τρόπον ώστε να μη λαμβάνεται το αμφιλεγόμενο υλικό. Κατά συνέπεια, η στρατηγική της δέσμευσης περιεχομένου χαράσσεται από τους ISPs, ενώ η στρατηγική βαθμονόμησης περιεχομένου και αυτοοριοθέτησης χαράσσεται από τους παρόχους του περιεχομένου και τους ίδιους τους συνδρομητές των ISPs.

4.3.1 Δέσμευση Περιεχομένου

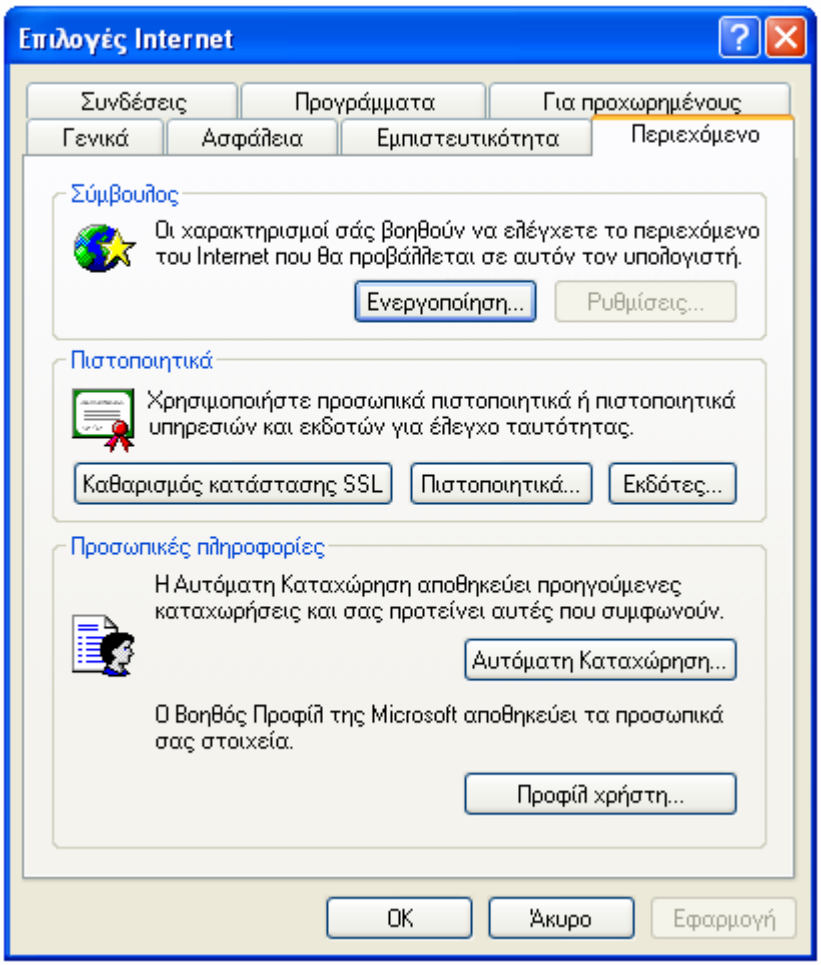
Η δέσμευση περιεχομένου στο επίπεδο μεταγωγής πακέτου απαιτεί δρομολογητές φιλτραρίσματος (screening routers), οι οποίοι εξετάζουν την IP διεύθυνση της πηγής του εισερχόμενου πακέτου, τη συγκρίνουν με μία *μαύρη λίστα* (black list) και είτε προωθούν το πακέτο αν η IP διεύθυνση δεν ανήκει στη μαύρη λίστα, είτε το απορ-ρίπτουν αν η IP διεύθυνση ανήκει στη μαύρη λίστα.

Η δέσμευση περιεχομένου στο επίπεδο εφαρμογών απαιτεί αναχώματα ασφάλειας επιπέδου εφαρμογής (application gateways) και πληρεξούσιους εξυπηρέτες (proxy servers) οι οποίοι εξετάζουν τους πόρους ή τις πληροφορίες για τους πόρους, προκειμένου να αποφασίσουν αν η αίτηση του αντίστοιχου πρωτοκόλλου εφαρμογών, όπως μία κλήση GET του HTTP, πρέπει να εξυπηρετηθεί ή όχι. Για παρά-δειγμα, μία συνήθης προσέγγιση στο επίπεδο εφαρμογής είναι ο καθορισμός των urls που δεν πρέπει να εξυπηρετούνται και η τοποθέτηση τους σε αντίστοιχες μαύρες λίστες που διατίθενται και εγκαθίστανται σε πληρεξούσιους εξυπηρέτες. Πριν εξυπηρετηθεί μία HTTP αίτηση, ένας πληρεξούσιος εξυπηρέτης θα πρέπει να βεβαιωθεί ότι το url δε βρίσκεται στη μαύρη λίστα.

Σύμφωνα με αυτή τη συνοπτική περιγραφή, η δέσμευση στο επίπεδο μεταγωγής πακέτου συχνά αναφέρεται ως *δέσμευση IP διευθύνσεων* (IP address blocking), ενώ η δέσμευση στο επίπεδο εφαρμογών καλείται *δέσμευση url.* (url blocking).

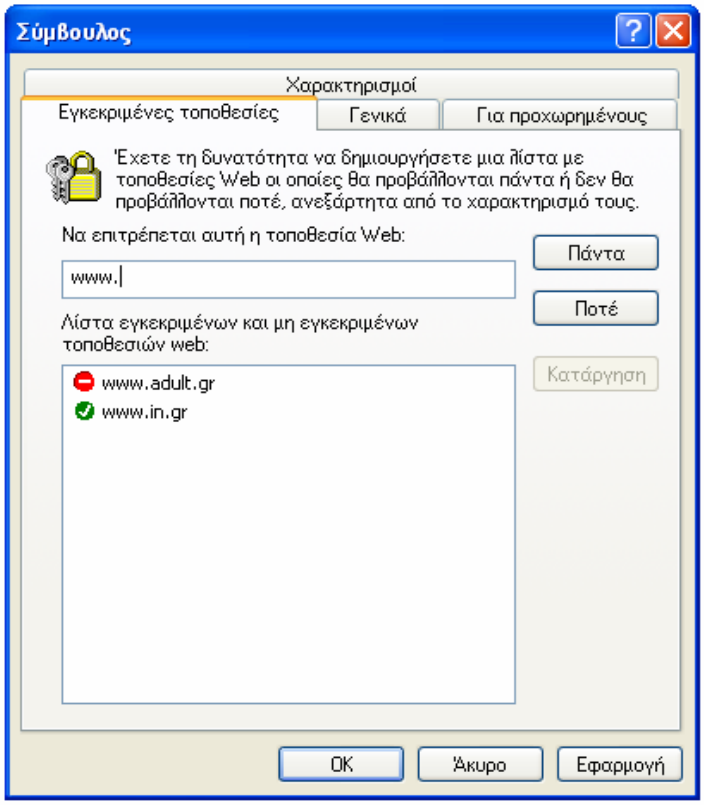
4.3.2 Βαθμονόμηση Περιεχομένου και Αυτοοριοθέτηση

Εναλλακτική λύση της επίτευξης λογοκρισίας και ελέγχου προσπέλασης του περιεχομένου που διατίθεται στο internet ως αποτέλεσμα δέσμευσης IP και URL διευθύνσεων και αξιοποίησης μαύρων λιστών, αποτελεί η ιδέα της βαθμονόμησης περιεχομένου (contenet rating) και της αυτοοριοθέτησης (self-determination). Σύμφωνα με αυτή την ιδέα, παρέχεται η δυνατότητα στους ίδιους τους χρήστες να κρίνουν το περιεχόμενο μιας ιστοσελίδας με βάση κάποια συγκεκριμένα κριτήρια. Αυτή η ιδέα στην πραγματικότητα συμβαδίζει με το γενικό επιχείρημα ότι οι χρήστες είναι τελικά υπεύθυνοι για τη δική τους συμπεριφορά και δραστηριότητα. Βεβαίως η πραγματικότητα είναι διαφορετική, αφού αναφερόμενοι στα σύγχρονα μέσα όπως εφημερίδες και τηλεοπτικά προγράμματα, μπορεί κανείς να ισχυριστεί ότι μόνον αυστηροί νομικοί περιορισμοί θα μπορούσαν να ελέγξουν την προσβλητικότητα κάποιου περιεχομένου. Το επιχείρημα αυτό είναι σύνηθες και χρησιμοποιείται εναντίον της αξιοποίησης της βαθμονόμησης περιεχομένου και της αυτοοριοθέτησης.
Σαν παράδειγμα, αναφέρεται ο Microsoft Internet Explorer, από το ακόλουθο μενού του οποίου μπορεί να ενεργοποιηθεί ο «Σύμβουλος». Εργαλεία -> Επιλογές Internet -> Φάκελος «Περιεχόμενο».

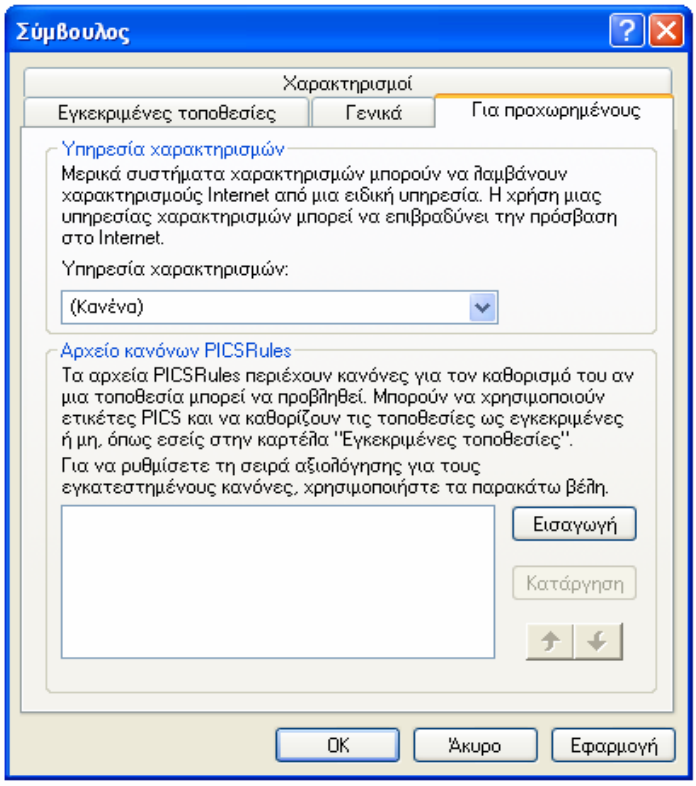


Εικόνα 10: Δυνατότητα ενεργοποίησης του «Σύμβουλου» στον IE 6.0

Από τα παράθυρα διαλόγου του Συμβούλου, μπορεί ο χρήστης να ορίσει ιστοσελίδες στις οποίες να έχει πάντοτε ή ποτέ πρόσβαση (Εικόνα 11) ή να μελετήσει και να αλλάξει τη λίστα των συστημάτων βαθμονόμησης περιεχομένου που υποστηρίζονται, καθώς και να καθορίσει τη χρήση ενός online γραφείου βαθμονόμησης (από την καρτέλλα «για προχωρημένους» Εικόνα 12).



Εικόνα 11: Δυνατότητα αποκλεισμού ή έγκρισης συγκεκριμένων ιστοσελίδων (IE 6.0)



Εικόνα 12: Διάλογος «Για προχωρημένους» στο Σύμβουλο του IE 6.0

4.4 Προστασία Δικαιωμάτων Πνευματικής Ιδιοκτησίας

Η ραγδαία αξιοποίηση των εφαρμογών της Πληροφορικής και των Επικοινωνιών σε διεθνή κλίμακα έχει διαμορφώσει ένα νέο έννομο αγαθό, την πληροφορία (information), η οποία έχει πλέον σημαντική κοινωνική, οικονομική, πολιτιστική αλλά και πολιτική σημασία. Στο σημερινό ψηφιακό κόσμο, η προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας αποτελεί ιδιαίτερα σημαντική παράμετρο.

Η αναγκαιότητα της προστασίας των δικαιωμάτων πνευματικής ιδιοκτησίας καθίσταται ιδιαίτερα σημαντική λόγω της ραγδαίας εξέλιξης των τεχνολογιών, οι οποίες επιτρέπουν να δημιουργούνται αντίγραφα συγκεκριμένου περιεχομένου. Το γεγονός αυτό αναδεικνύεται από διάφορα παραδείγματα.

Η αξιοποίηση των τεχνολογιών εγγραφής για ήχο και βίντεο ακολουθήθηκε από ιδιαίτερο σκεπτικισμό σχετικά με την ανάγκη ταυτόχρονης προστασίας των δικαιωμάτων πνευματικής ιδιοκτησίας. Στην περίπτωση εγγραφών σε δίσκο βινυλίου η δημιουργία αντιγράφων απαιτούσε ειδικό εξοπλισμό, ενώ τα αντίγραφα δεν ήταν της ίδιας ποιότητας με το δίσκο της πρωτογενούς εγγραφής. Ωστόσο, με την αξιοποίηση των μαγνητικών κασετών για εγγραφή ήχου και βίντεο η πειρατεία αυξήθηκε σε υψηλό βαθμό, κυρίως επειδή το κόστος για την αντιγραφή ήταν μικρό και ο σχετικός εξοπλισμός ευρύτατα διαδεδομένος. Ευτυχώς, σημαντικό εμπόδιο για περαιτέρω πειρατεία αποτελούσε η προοδευτική υποβάθμιση της ποιότητας του περιεχομένου για κάθε γενιά αντιγράφων: το αντίγραφο του αντιγράφου ενός πρωτότυπου αντικειμένου περιέχει όλο το θόρυβο και τις ατέλειες που παράγονταν και ενισχύονταν σε κάθε επιμέρους βήμα.

Στον ψηφιακό κόσμο, ένα πολυμεσικό έγγραφο (multimdedia document) περιέχει ψηφιακά δεδομένα, τα οποία μπορούν να κωδικοποιούν κείμενα, γραφικά, εικόνες, ήχο και βίντεο. Η ψηφιακή αναπαράσταση και διανομή πολυμεσικών εγγράφων έχει αυξήσει το ενδεχόμενο κλοπής και παράνομης αξιοποίησης, ενώ έχει επιτείνει σημαντικά τα προβλήματα που σχετίζονται με την προστασία δικαιωμάτων πνευματικής ιδιοκτησίας. Τα προβλήματα πηγάζουν από τα εγγενή χαρακτηριστικά των ψηφιακών δεδομένων με βάση τα οποία η δημιουργία και διανομή ενός αντιγράφου

αποτελεί διαδικασία ταχεία, εύκολη και με σχετικά χαμηλό κόστος, με αποτέλεσμα κάθε αντίγραφο να είναι όμοιο με το πρωτότυπο.

Οι φορείς δημιουργίας και διανομής πολυμεσικών εγγράφων δεν ενθαρρύνουν και σε αρκετές περιπτώσεις αποφεύγουν τις online υπηρεσίες, ενώ αναζητούν αποτελεσματικές τεχνικές λύσεις για την προστασία δικαιωμάτων πνευματικής ιδιοκτησίας. Στην πραγματικότητα η προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας αποτελεί διαρκώς ύψιστο ζήτημα στα πλαίσια των συναλλαγών ηλεκτρονικού εμπορίου στον παγκόσμιο ιστό.

Μία από τις κύριες προσεγγίσεις για την επίλυση προβλημάτων που σχετίζονται με την προστασία δικαιωμάτων πνευματικής ιδιοκτησίας και την ενίσχυση τους, επιτυγχάνεται με τον έλεγχο χρήσης (usage control). Σύμφωνα με αυτή την προσέγγιση, κάθε χρήση του προστατευμένου υλικού, όπως είναι η ανάγνωση, η εκτέλεση και η εκτύπωση, ελέγχεται από υλικό ή λογισμικό. Η βιομηχανία λογισμικού έχει μακρά παράδοση στις τεχνολογίες ελέγχου χρήσης. Στην πραγματικότητα αυτός ο τύπος τεχνολογίας έχει προταθεί από το 1995 στις ΗΠΑ από τη σχετική Ομάδα Εργασίας για την Προστασία Πνευματικής Ιδιοκτησίας (Working Group on Intellectual Property Rights for the US National Information Infastructure).

Αν και ο έλεγχος χρήσης βρίσκεται σε φάση ανάδειξης ως επικρατούσα τεχνολογία για ειδικές εφαρμογές, όπως συνδρομητική τηλεόραση (pay-TV) και βίντεο κατ' απαίτηση (video on demand), μάλλον είναι απίθανο να αποτελέσει τη μοναδική λύση για το εγγύς μέλλον. Εκτιμάται ότι μπορεί να υπάρξει ανάσχεση της ευρύτερης ανάπτυξης της τεχνολογίας του ελέγχου χρήσης, λόγω της ύπαρξης νομικών και πρακτικών προβλημάτων που σχετίζονται με την αυστηρά περιοριστική φύση της τεχνικής αυτής.

Εναλλακτική λύση στην προσπάθεια περιορισμού και ελέγχου χρήσης του προστατευόμενου υλικού, θα ήταν να επιτραπεί η χωρίς όρια αντιγραφή και χρήση, παρέχοντας όμως ταυτόχρονα τεκμήρια σε περίπτωση κακής χρήσης. Αυτή η λύση απαιτεί τεχνικές, γνωστές ως τεχνικές τοποθέτησης ετικετών digital copyright labelling techniques). Γενικά, οι τεχνικές τοποθέτησης ετικετών ενσωματώνουν ψηφιακά μοναδικά γνωρίσματα σε προστατευμένα υλικά για να καθορίσουν πληροφορίες που σχετίζονται με τα δικαιώματα πνευματικής ιδιοκτησίας, όπως προέλευση, ιδιοκτησία, περιεχόμενο ή νόμιμο παραλήπτη. Συνεπώς, η τοποθέτηση

των ετικετών, πρέπει να μπορεί: να παρέχει τεκμήρια για ενδεχόμενη παραβίαση δικαιώματος μετά το συμβάν και να αποτελεί αποτρεπτικό παράγοντα στην αθέμιτη αντιγραφή και διασπορά, κάνοντας την κακή χρήση του προστατευμένου υλικού εξιχνειάσιμη, παρέχοντας εκ των υστέρων τεκμήρια για αποκάλυψη παρανόμων ενεργειών.

Ας σημειωθεί πάντως, ότι η χρήση τεχνικών τοποθέτησης ετικετών προϋποθέτει την ύπαρξη ενός νομικού πλαισίου που να επιτρέπει στους δικαιούχους να ενάγουν τους παρανομούντες. Επίσης, θα πρέπει να γίνει κατανοητό ότι η χρήση τεχνικών τοποθέτησης ετικετών, δεν έρχεται σε αντίθεση με τον έλεγχο χρήσης.

Γενικώς, υπάρχουν δύο τύποι ετικετών για αναγνώριση και προστασία δικαιωμάτων πνευματικής ιδιοκτησίας, όσον αναφορά τα multimedia έγγραφα:

- ετικέτα ιδιοκτήτη (ownership labelling): ένα έγγραφο πρέπει να είναι σηματοδοτημένο με μία ετικέτα που να αναγνωρίζει μοναδικά τον κάτοχο των δικαιωμάτων πνευματικής ιδιοκτησίας
- ετικέτα παραλήπτη (recipient labelling): ένα έγγραφο πρέπει να είναι σηματοδοτημένο με τέτοιο τρόπο, ώστε ο παραλήπτης να είναι μοναδικά αναγνωρίσιμος.

Σε αντίθεση με τις τεχνικές ελέγχου χρήσης, η τοποθέτηση ετικετών ψηφιακών υδατογραφημάτων δεν περιορίζει τον επιτρεπτό αριθμό αντιγράφων, αλλά μπορεί να αποτρέψει την παράνομη αντιγραφή είτε επιτρέποντας την αναγνώριση του νόμιμου ιδιοκτήτη του προστατευόμενου υλικού και του αντίστοιχου δικαιώματος του δημιουργού, σε περίπτωση ετικέτας ιδιοκτήτη, είτε δίνοντας τη δυνατότητα αναγνώρισης από τον πραγματικό παραλήπτη μιας περιοριστικά αθέμιτης αντιγραφής, σε περίπτωση ετικέτας παραλήπτη.

Στο φυσικό κόσμο σε τυπικά περιβάλλοντα εκδοτικών οίκων, συχνά, οι ετικέτες ιδιοκτήτη αναφέρονται ως υδατογραφήματα (watermarks), ενώ οι ετικέτες παραλήπτη αναφέρονται ως μοναδικές σημάνσεις (fingerprints). Αυτοί οι όροι διατηρούνται αντίστοιχα και στον ψηφιακό κόσμο.

Αν και η τοποθέτηση ετικετών ψηφιακών υδατογραφημάτων συσχετίστηκε μόλις πριν από λίγο καιρό με την προστασία δικαιωμάτων πνευματικής ιδιοκτησίας, οι σχετικές θεωρίες και τεχνικές είχαν προταθεί για πρώτη φορά πριν από αρκετό καιρό.

Μερικές τεχνικές τοποθέτησης ετικετών μπορούν να υποστηρίξουν πολλαπλές ετικέτες, είτε υδατογραφήματα είτε μοναδικές σημάνσεις και να τα εξάγουν ξεχωριστά. Στην πράξη, αυτό το χαρακτηριστικό είναι απαραίτητο για να προσδιορίσει την ιδιοκτησία και άλλα πνευματικά δικαιώματα τα οποία συνθέτουν αγαθά σχετικών δικαιωμάτων.

4.5 Ασφάλεια Ηλεκτρονικών Πληρωμών

Στα πλαίσια επέκτασης και αξιοποίησης εφαρμογών ηλεκτρομικού εμπορίου, σημαντική δραστηριότητα υπάρχει στην ανάπτυξη συστημάτων ασφαλών ηλεκτρονικών πληρωμών. Η πρόοδος των συστημάτων μεταφοράς αξίας κορυφώθηκε με τα συστήματα ηλεκτρονικών πληρωμών (electronic payment systems). Στην πραγματικότητα, η σπουδαιότητα του ηλεκτρονικού εμπορίου και των αντίστοιχων εφαρμογών έχει ως αποτέλεσμα την εισαγωγή ποικιλίας διαφορετικών και ενδεχομένως ανταγωνιστικών συστημάτων ηλεκτρονικών πληρωμών. Στα τρέχοντα διαθέσιμα συστήματα ηλεκτρονικών πληρωμών οι πληρωμές πραγματοποιούνται ηλεκτρονικά, αλλά η σχεδίαση ανάμεσα στις ηλεκτρονικές πληρωμές και στη μεταφορά της «αληθινής αξίας» είναι ακόμη εγγυημένη από τις τράπεζες, μέσω καθαρά οικονομικών συστημάτων. Τα συστήματα αυτά οικοδομούνται αξιοποιώντας τα κλειστά δίκτυα των οικονομικών οργανισμών, τα οποία θεωρούνται ασφαλέστερα από τα ανοιχτά δίκτυα, όπως το internet**.**

Όλα τα υπάρχοντα συστήματα ηλεκτρονικών πληρωμών διαφέρουν στον τρόπο λειτουργίας και τις λεπτομέρειες υλοποίησης, αλλά έχουν ως κοινό βασικό σκοπό τη διευκόλυνση της μεταφοράς χρηματικής αξίας μεταξύ πολλαπλών μερών. Γενικά, οι ηλεκτρονικές πληρωμές εμπλέκουν έναν αγοραστή, την οντότητα που θέλει να αγοράσει αγαθά ή υπηρεσίες και έναν έμπορο που αποτελεί την οντότητα που θέλει να πουλήσει αγαθά ή υπηρεσίες. Στην ορολογία των συστημάτων ηλεκτρονικών πληρωμών, ο αγοραστής συχνά καλείται πληρωτής (payer) και ο έμπορος συχνά καλείται αποδέκτης πληρωμής (payee).

4.5.1 Πρωτόκολλο SET (Secure Electronic Transaction)

Το πρωτόκολλο SET σχεδιάστηκε αρχικά από τη Visa και τη Mastercard το 1997 και έχει έκτοτε εξελιχθεί. Το πρωτόκολλο αυτό συμφωνεί με τις απαιτήσεις σε ασφάλεια όπως το SSL. Επίσης ορίζει τη μορφή του μηνύματος και του ψηφιακού πιστοποιητικού , και τη διαδικασία που απαιτείται για την ολοκλήρωση της πληρωμής.

Συνοπτικά το SET αναφέρεται στις αλληλεπιδράσεις ανάμεσα στους κατόχους πιστωτικών καρτών, στους εμπόρους και τις τράπεζες εγγύησης. Όλα τα μέρη κατέχουν ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού και ένα αντίστοιχο πιστοποιητικό δημοσίου κλειδιού. Επιπλέον τα περισσότερα μέρη κατέχουν δύο ζεύγη κλειδιών:

Ένα ζεύγος κλειδιών για ανταλλαγή κλειδιών

Ένα ζεύγος κλειδιών για ψηφιακές υπογραφές

Ο κάτοχος της πιστω τικής κάρτας και ο έμπορος πρέπει να αποκτήσουν τα πιστοποιητικά των δημισίων κλειδιών τους όταν εγγράφονται, πρωτού συμμετάσχουν σε οποιαδήποτε συναλλαγή. Συνεπώς η χρήση του SET απαιτεί μια ικανοποιητικά λειτουργούσα υποδομή Δημόσιων Κλειδιών PKI βασισμένη σε ITU/ISO X.509 πιστοποιητικά, ενώ συμπεριλαμβάνονται και στοιχεία όπως μηχανισμοί ανάκλη-σης πιστοποιητικών CRLs.

Είναι ευρέως αποδεκτό, ότι ένα πρωτόκολλο ηλεκτρονικών πληρωμών μέσω πιστωτικών καρτών θα πρέπει να παρέχει στον έμπορο μόνο συγκεκριμένες πληροφορίες, όπως τα αγοραζόμενα είδη και οι αντίστοιχες τιμές συμφωνίας πώλησης τους και στον εγγυητή μόνο τις πληροφορίες των πιστωτικών καρτών. Συγκεκριμένα, ο έμπορος δε θα πρέπει να απαιτεί πρόσβαση στην πιστωτική κάρτα του πελάτη από τη στιγμή που ο εγγυητής εγκρίνει την πληρωμή. Ομοίως, ο εγγυητής δε χρειάζεται να γνωρίζει τις λεπτομέρειες των ειδών που αγοράστηκαν, εκτός από την περίπτωση ορισμένων πολύ ακριβών αγαθών. Σε μία τέτοια περίπτωση, ο εγγυητής ίσως θέλει να βεβαιωθεί ότι ο πελάτης έχει τη δυνατότητα να καταβάλει το ποσό της πληρωμής. Αυτός ο διαχωρισμός των διαθέσιμων πληροφοριών επιτυγχάνεται με ένα απλό και αποτελεσματικό μηχανισμό, γνωστό ως διπλή υπογραφή (dual signature): δύο μέρη ενός μηνύματος υπογράφονται διπλά με

χρήση συνάρτησης σύνοψης, συνενώνονται τα δύο αποτελέσματα της σύνοψης, επανυποβάλλεται το αποτέλεσμα στη συνάρτηση σύνοψης και υπογράφεται ψηφιακά το αποτέλεσμα. Ο ένας αποδέκτης παίρνει το αρχικό κείμενο του πρώτου μέρους του μηνύματος και το αποτέλεσμα της σύνοψης του δευτέρου και ο άλλος αποδέκτης παίρνει το αποτέλεσμα της σύνοψης του πρώτου μέρους του μηνύματος και το αρχικό κείμενο του δευτέρου μέρους. Με τον τρόπο αυτό, ο κάθε αποδέκτης μπορεί να επαληθεύσει την ακεραιότητα του συνολικού μηνύματος, αλλά μπορεί να διαβάσει μόνο το κείμενο του μέρους του μηνύματος που απευθύνεται ειδικά σε αυτόν. Το άλλο μέρος παραμένει ως τιμή σύνοψης οπότε αποκρύπτεται τεχνικά το πραγματικό του περιεχόμενο.

Ας υποτεθεί ότι ένας κάτοχος πιστωτικής κάρτας έχει επιλέξει να αγοράσει ορισμένα είδη και θέλει να εισάγει μία αντίστοιχη πληρωμή μέσω πιστωτικής κάρτας στον έμπορο. Ο κάτοχος της πιστωτικής κάρτας κατασκευάζει δύο πακέτα πληροφοριών:

• τις πληροφορίες της εντολής (OM (Order Message)

• τις οδηγίες της πληρωμής (PM) (Payment Message)

Το OI περιλαμβάνει μερικές πληροφορίες που σχετίζονται με τα αγοραζόμενα είδη, όπως τα αγαθά ή τις υπηρεσίες και τις τιμές πώλησης τους, ενώ το PI περιλαμβάνει πληροφορίες που σχετίζονται με την πληρωμή μέσω πιστωτικής κάρτας, όπως τον αριθμό της πιστωτικής κάρτας και την ημερομηνία λήξης της. Ακολουθεί διαδικασία δημιουργίας κλειδιών σύνοψης για κάθε ένα από τα παραπάνω, και η συνένωσή τους με διπλή υπογραφή. Λόγω της χρήσης διπλών υπογραφών, ο έμπορος δε μαθαίνει τις πληροφορίες της πιστωτικής κάρτας του πελάτη του. Για πρακτικούς λόγους αυτό είναι πολύ σημαντικό εφόσον απαλλάσσει τους πελάτες από την αμφισβήτηση που γεννάται σχετικά με την ασφάλεια των στοιχείων στην ιστοθέση του εμπόρου.

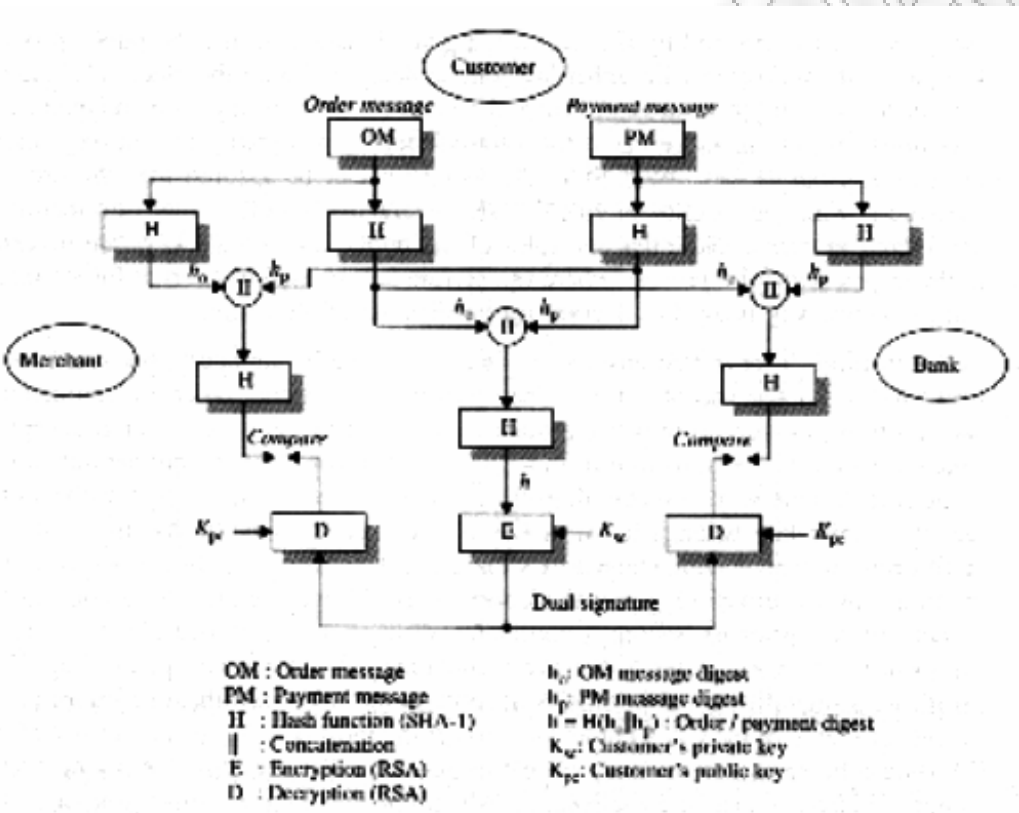
Στο ακόλουθο σχήμα (Σχήμα 14) φαίνεται ο μηχανισμός της διπλής υπογραφής και της ηλεκτρονικής συναλλαγής.

Συγκρτικά με το πρωτόκολλο SSL, το SET παρέχει μεγαλύτερη ασφάλεια και απαιτελι ψηφιακό πορτοφόλι εγκατεστημένο στον HY του πελάτη. Υστερεί όμως στο ότι είναι πολύπλοκο, δέχεται μυνήματα μόνο αν μπορούν να μετατραπούν σε πρωτόκολλο SET και έχει αργό ρυθμό απόκρισης.

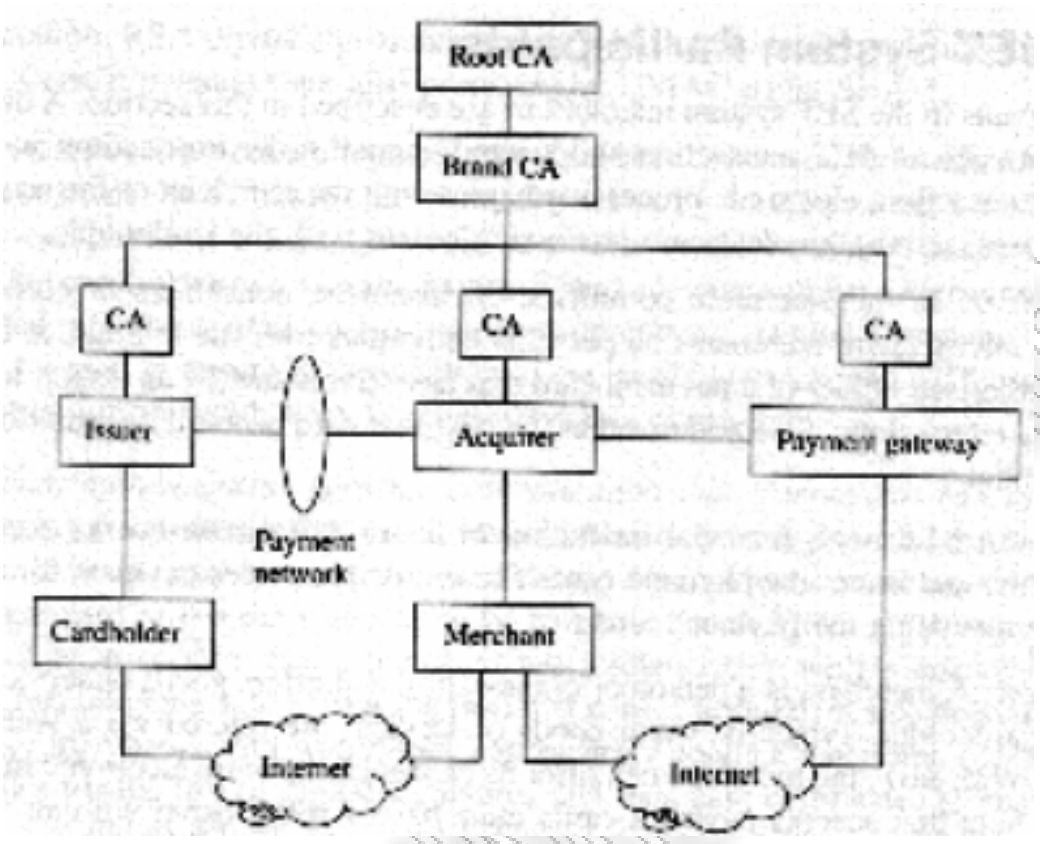
4.5.2 Τυπικά συστήματα πληρωμών στο ΗΕ

Πιστωτικές Κάρτες

Στη χρήση πιστωτικών καρτών κατά την εφαρμογή του SET υπάρχουν τέσσερις οντότητες (Σχήμα 15)



Σχήμα 14: Μηχανισμός της διπλής υπογραφής και της ηλεκτρονικής συναλλαγής



Σχήμα 15: Χρήση Πιστωτικής Κάρτας σύμφωνα με το πρωτόκολλο SET

1. Ο κάτοχος της κάρτας (cardholder)
2. Ο έμπορος (Merchant)
3. Ο εκδότης της κάρτας (Issuer)
4. Η Δίοδος πληρωμών (payment network ή payment gateway). Ο ρόλος του είναι να συνδέει το internet με τα ιδιόκτητα δίκτυα των τραπεζών. Επειδή σε αυτή τη διαδικασία κάθε οντότητα χρειάζεται ένα πιστοποιητικό (CA: Certification Authority) για τη διατήρηση του οποίου απαιτείται ειδικό λογισμικό (ψηφιακό πορτοφόλι) εγκατεστημένο στον HY του πελάτη ή σε μια κάρτα, θεωρείται πιο ασφαλής.

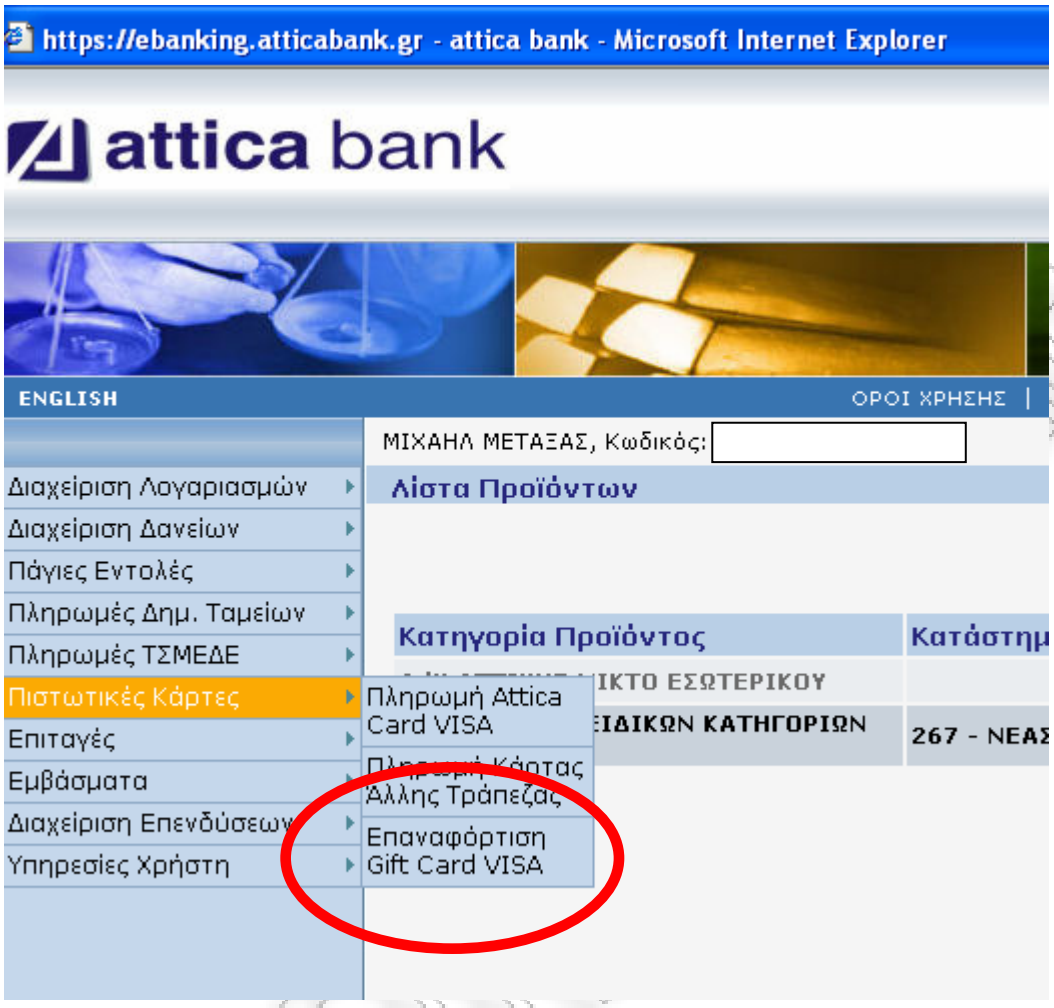
4.5.3 Μεταφορά Κεφαλαίων και Χρεωστικές Κάρτες

Ηλεκτρονική μεταφορά κεφαλαίων μπορεί να γίνει μεταξύ τραπεζικών λογαριασμών στην ίδια ή σε διαφορετικές τράπεζες. Η κρυπτογράφηση των μηνυμάτων είναι ιδιαίτερης σημασίας. Για την υιοθέτηση μιας ιδέας ενός πιστοποιητικού, απαιτείται η ανάπτυξη ενός πρωτοκόλλου τύπου SET ειδικά για τράπεζες που να συνδέονται με το internet μέσω διόδων πληρωμής.

Η χρεωστική κάρτα είναι μια κάρτα που εξουσιοδοτεί online την ηλκτρονική μεταφορά κεφαλαίων. Με τη χρήση της αφαιρείται αυτόματα το ποσό της συναλλαγής από τον τραπεζικό λογαριασμό και μπορεί κανείς να ξοδέψει μόνο όσα χρήματα βρίσκονται σε αυτόν. Μια χρεωστική κάρτα μπορεί να χρησιμοποιηθεί σε ένα ηλεκτρονικό κατάστημα όπως μια πιστωτική κάρτα και το πιστοποιητικό τους στο internet μπορεί να είναι κοινό.

4.5.4 Κάρτες Αποθηκευμένης Αξίας και Ψηφιακό Χρήμα

Η ιδέα του ηλεκτρονικού χρήματος επινοήθηκε τη δεκαετία του 1970 όταν δημιουργήθηκαν οι *έξυπνες* κάρτες. Πλαστικές κάρτες, μαγνητικές γραμμές έχουν χρησιμοποιηθεί για την αποθήκευση δεδομένων, ή μιας χρηματικής αξίας που συνεχώς μειώνεται με τη χρήση. Εφαρμόζονται π.χ. στις μεταφορές, στις τηλεφωνικές συνδιαλέξεις και στην ανατύπωση αντιγράφων στις βιβλιοθήκες. Η παρούσα γενιά των έξυπνων καρτών περιλαμβάνει μικροεπεξεργαστές με προγραμματιζόμενες λειτουργίες. Η κάρτα προπληρώνεται και έπειτα, η αξία των χρημάτων μπορεί να εξαντλτηθεί και στη συνέχεια να επαναπληρωθεί επώνυμα ή ανώνυμα.Σήμερα οι πελάτες πρέπει να διατηρούν ξεχωριστή κάρτα για κάθε εφαρμογή, οποίες πληρώνονται σε συγκεκριμένα σημεία. Ωστόσο, πιστεύεται ότι οι πληρώσεις θα γίνονται μέσω του Η/Υ είτε είναι συνδεδεμένο στο internet είτε στο δίκτυο μιας τράπεζας. Ήδη για παράδειγμα η πλήρωση της Visa Gift Card της Τράπεζας Αττικής μπορεί να γίνει ηλεκτρονικά μέσω του λογαριασμού του πελάτη στο ηλεκτρονικό κατάστημα (e-banking) της τράπεζας.



Εικόνα 13: Επαναφόρτιση προπληρωμένης κάρτας μέσω e-banking (www.atticabank.gr)

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλισης μικροποσών μέσω internet όπου το νόμισμα είναι απλά μια σειρά από ψηφία. Ο χρήστης κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό στον ΗΥ του. Φο ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύεται για λόγους ασφάλειας. Σε περίπτωση αγοράς προϊόντων ή υπηρεσιών από το internet, ο αγοραστής αποστέλλει το αντίτιμο σε ψηφιακό χρήμα στον προμηθευτή, ο οποίος με τη σειρά του το προθεί στην τράπεζα για να επιβεβαιώσει τη γνησιότητά του.

4.5.5 Ηλεκτρονικές Επιταγές

Ένα σύστημα πληρωμών για ηλεκτρονικές επιταγές (e-checks) περιλαμβάνει τα ακόλουθα μέρη:

Έναν πελάτη και την τράπεζα του.

Έναν έμπορο και την τράπεζα του.

Μια τράπεζα διαμεσολάβησης και εγγύησης που θα υποβάλλει σε επεξεργασία τις επιταγές ανάμεσα στις διαφορετικές τράπεζες.

Από τεχνικής πλευράς οι ηλεκτρονικές επιταγές είναι απλές. Μία ηλεκτρονική επιταγή περιλαμβάνει ένα έγγραφο, το οποίο είναι υπογεγραμμένο ψηφιακά με το ιδιωτικό κλειδί του πελάτη. Ο παραλήπτης, δηλαδή ο έμπορος ή η τράπεζα του, χρησιμοποιεί το δημόσιο κλειδί του πελάτη για να επαληθεύσει την ψηφιακή υπογραφή του πελάτη. Αυτή η συναλλαγή περιλαμβάνει τρεις φάσεις:

Στην πρώτη φάση, ο πελάτης αγοράζει μερικά αγαθά ή υπηρεσίες και στέλνει μία αντίστοιχη επιταγή στον έμπορο. Ο έμπορος επικυρώνει την επιταγή μέσω της τράπεζας του για εξουσιοδότηση πληρωμής. Αν η επιταγή είναι έγκυρη, ο έμπορος αποδέχεται τη συναλλαγή και παραδίδει τα αγαθά ή τις υπηρεσίες στον πελάτη.

Στη δεύτερη φάση, ο έμπορος προωθεί την ηλεκτρονική επιταγή στην τράπεζα του για κατάθεση.

Στην τρίτη φάση, η τράπεζα του εμπόρου προωθεί την ηλεκτρονική επιταγή στην τράπεζα έκδοσης για να την εξαργυρώσει. Η τράπεζα εξαργύρωσης, με τη σειρά της, συνεργάζεται με την τράπεζα του πελάτη, πραγματοποιεί εκκαθάριση της επιταγής και μεταφέρει τα χρήματα στην τράπεζα του εμπόρου, η οποία με τη σειρά της ενημερώνει το λογαριασμό του εμπόρου. Η τράπεζα του πελάτη ενημερώνει επίσης τον πελάτη με την αντίστοιχη πληροφορία.

Συγκρινόμενες με τις συνήθεις επιταγές και τα άλλα συστήματα πληρωμών του πραγματικού κόσμου, οι ηλεκτρονικές επιταγές παρέχουν μερικά σημαντικά πλεονεκτήματα. Για παράδειγμα, οι ηλεκτρονικές επιταγές μπορούν να εκδοθούν χωρίς να χρειάζεται να συμπληρωθούν, να ταχυδρομηθούν, ή να παραδοθούν. Επίσης, εξοικονομείται χρόνος στην επεξεργασία των επιταγών. Με τις επιταγές σε χαρτί, ο έμπορος τυπικά συλλέγει τις επιταγές και τις καταθέτει όλες μαζί στην τράπεζα, ενώ με τις ηλεκτρονικές επιταγές ο έμπορος στιγμιαία μπορεί να προωθήσει τις επιταγές στην τράπεζα ή να τις λάβει πιστώνοντας τον τραπεζικό του λογαριασμό. Έτσι, οι ηλεκτρονικές επιταγές μπορούν να μειώσουν το χρόνο από τη στιγμή που ένας πελάτης συμπληρώσει μία επιταγή μέχρι τη στιγμή που θα πραγματοποιηθεί η κατάθεση στο λογαριασμό του εμπόρου. Επιπλέον, τα συστήματα ηλεκτρονικών

επιταγών μπορούν να σχεδιαστούν με τέτοιο τρόπο, ώστε ο έμπορος να λαμβάνει κατάλληλη εξουσιοδότηση από την τράπεζα του πελάτη πριν αποδεχτεί μία επιταγή. Ωστόσο, αφού ο χρόνος κυκλοφορίας των ηλεκτρονικών επιταγών είναι λίγα μόνο λεπτά, το σύστημα γίνεται πρακτικά ίδιο με εκείνο της Ηλεκτρονικής Μεταφοράς Κεφαλαίων. Το Financial Services Technology Consortium (FSTC) έχει διατυπώσει μια στρατηγική για τις τράπεζες που συμφωνούν με ηλεκτρονικές επιταγές και τον τρόπο που θα τις διαχειρίζονται, αλλά παράλληλα έχουν διατυπωθεί και εναλλακτικά συστήματα ηλεκτρονικών επιταγών για το internet. Τέτοια είναι το NetBill, NetCheque και το PayNow.

Κεφάλαιο 5

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ – ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Εισαγωγή

Στο κεφάλαιο αυτό αναφέρονται κάποιοι τρόποι αντιμετώπισης προβλημάτων που αναφέρθηκαν σε προηγούμενα κεφάλαια (π.χ. σε επιθέσεις DdoS και σε θέματα που αφορούν τους dialers), γίνεται αναφορά ορισμένων εργαλείων για αναζήτηση βοήθειας σχετικά με θέματα ασφάλειας στο διαδίκτυο (CASE) και κλείνοντας αναφέρονται μερικές πρακτικές συμβουλές στους χρήστες σχετικά με τη συμπεριφορά τους και τις δυνατότητες για προστασία από κακόβουλες επιθέσεις στο διαδίκτυο.

5.2 Παρεμβάσεις και Πρωτοβουλίες από Φορείς (ΕΕΤΤ και ENISA) Νομοθετικό Πλαίσιο

Σύμφωνα με το νέο νόμο περί ηλεκτρονικών επικοινωνιών (ν. 3431/2006), μεταξύ των γενικών αρχών που διέπουν το πλαίσιο ρύθμισης των ηλεκτρονικών επικοινωνιών είναι και η διασφάλιση της «διατήρησης της ακεραιότητας και της ασφάλειας των δημόσιων δικτύων επικοινωνιών» (άρθρο 3, παρ. τ').

Ο έλεγχος της τήρησης των αρχών αυτών είναι κατεξοχήν αρμοδιότητα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων **(ΕΕΤΤ)** (άρθρο 6, παρ.1 του ν. 3431/2006). Να επισημανθεί, βεβαίως, ότι στο άρθρο 4, παρ.2, του νόμου αυτού, προβλέπεται για πρώτη φορά ότι «ο Υπουργός Μεταφορών και Επικοινωνιών είναι αρμόδιος για τη χάραξη πολιτικής επί της ασφαλείας των δημόσιων δικτύων και υπηρεσιών ηλεκτρονικών επικιονωνιών από κοινού με τους κατά περίπτωση συναρμόδιους Υπουργούς». Η συγκεκριμένη αρμοδιότητα της ΕΕΤΤ υφίστατο και

υπό το κράτος ισχύος του προηγούμενου νόμου περί τηλεπικοινωνιών (ν. 2867/2000,) σύμφωνα με τον οποίο η ΕΕΤΤ ασκούσε έλεγχο ως προς την τήρηση από τους παρόχους τηλεπικοινωνιακών δικτύων των «ουσιωδών απαιτήσεων», μεταξύ των οποίων ρητά συγκαταλέγονταν α) η «ασφάλεια λειτουργίας δικτύου» και β) η «διατήρηση της ακεραιότητας του δικτύου» (άρθρο 2).

Περαιτέρω, σύμφωνα με το Παράρτημα ΙΧ του νέου νόμου (3431/2006), η Γενική Αδεια παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών δύναται να συνοδεύεται μεταξύ άλλων από α) «όρους που εξασφαλίζουν τη διατήρηση της ακεραιότητας των δημόσιων δικτύων επικοινωνιών» (άρθρο 13 Παραρτήματος), β) κανόνες «ασφάλειας δημόσιων δικτύων ηλεκτρονικών επικοινωνιών από μή επιτρεπόμενη πρόσβαση» (άρθρο 14 Παραρτήματος) και γ) «προδιαγραφές χρήσης ώστε σε περίπτωση μείζονος καταστροφής να εξασφαλίζεται η επικοινωνία των υπηρεσιών έκτακτης ανάγκης με τις δημόσιες αρχές» (άρθρο 10 του Παραρτήματος). Τους όρους και κανόνες αυτούς, σύμφωνα με τον ίδιο νόμο (3431/2006), τους προσδιορίζει η ΕΕΤΤ κατά την έκδοση του Κανονισμού Γενικών Αδειών παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Η ασφάλεια των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, όπως αναφέρεται και στον Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (**European Network & Information Security Agency - ENISA),** αποτελεί αιτία ολοένα και μεγαλύτερης ανησυχίας στην κοινωνία, λόγω κυρίως της πιθανότητας να ανακύψουν προβλήματα σε βασικά συστήματα πληροφοριών, που να οφείλονται στην πολυπλοκότητα των συστημάτων, σε ατυχήματα, σφάλματα και επιθέσεις, και τα οποία μπορούν να έχουν συνέπειες για την υλική υποδομή παροχής υπηρεσιών ζωτικής σημασίας για την ευημερία των πολιτών.

Σύμφωνα με τον ανωτέρω Κανονισμό ο όρος **"ασφάλεια δικτύων και πληροφοριών"** ορίζεται ως εξής: η δυνατότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε συγκεκριμένο επίπεδο εμπιστοσύνης, σε ατυχήματα ή σε παράνομες ή κακόβουλες δράσεις, οι οποίες θέτουν σε κίνδυνο **τη διαθεσιμότητα**, **την αυθεντικότητα**, **την ακεραιότητα** και την **εμπιστευτικότητα όσον αφορά τα δεδομένα που έχουν αποθηκευθεί ή**

μεταδίδονται καθώς και οι σχετικές υπηρεσίες που προσφέρονται από τα εν λόγω δίκτυα ή συστήματα ή είναι προσβάσιμες μέσω αυτών.

Προκειμένου να εξασφαλισθεί η ακεραιότητα και διαθεσιμότητα των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, τόσο το Ευρωπαϊκό όσο και το εθνικό νομικό πλαίσιο, ορίζουν σαφώς τις δυνατότητες παρέμβασης της ΕΕΤΤ. Στα πλαίσια αυτά η ΕΕΤΤ μπορεί:

- Να ορίσει συγκεκριμένους δείκτες ποιότητας οι οποίοι θα πρέπει να μετριούνται και να δημοσιεύονται από τους παρόχους των δικτύων και υπηρεσιών
- Να ορίσει ελάχιστη ποιότητα Καθολικής Υπηρεσίας (υπηρεσίες σταθερής φωνητικής τηλεφωνίας) που θα πρέπει να παρέχεται στο σύνολο της χώρας από τον υπόχρεο πάροχο.
- Να καθορίσει ελάχιστη ποιότητα υπηρεσιών σε παρόχους στους οποίους χορηγούνται ειδικά δικαιώματα χρήσης ραδιοσυχνοτήτων κατόπιν διαγωνιστικών διαδικασιών

Τέλος ο Ν.3431/2006 προς υλοποίηση των ανωτέρω δίνει στην ΕΕΤΤ την δυνατότητα να ζητά από τις επιχειρήσεις την παροχή σχετικών πληροφοριών και δύναται κατόπιν δημόσιας διαβούλευσης με τους φορείς, να εισηγηθεί την υιοθέτηση κατάλληλων μέτρων τα οποία κρίνονται αναγκαία και τα οποία υιοθετούνται με κοινή απόφαση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης και Μεταφορών και Επικοινωνιών, κατόπιν εισήγησης της ΕΕΤΤ.

Μερικές από τις πρωτοβουλίες της Ευρωπαϊκής Ένωσης είναι:

SIS: Schengen Information Systems

EIS: Europol Information Systems

Eurodac: δακτυλικά αποτυπώματα στους παράνομους μετανάστες και όσους ζητούν άσυλο.

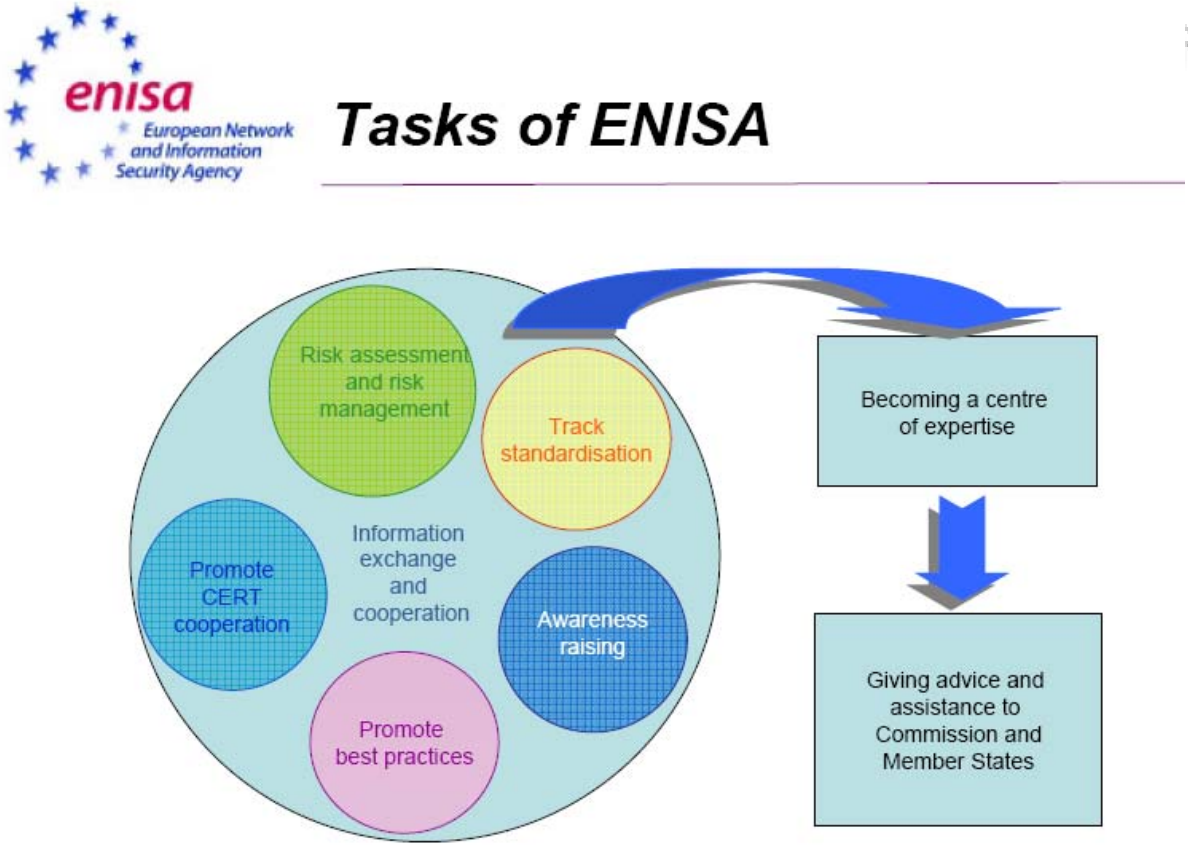
ICAO: Βιομετρικά διαβατήρια

Κατάσχεση των προϊόντων ηλεκτρονικού εγκλήματος

Τρομοκρατικού περιεχομένου επιθέσεις σε ηλεκτρονικούς υπολογιστές.

Στο site του ENISA (www.enisa.eu.int) μπορεί κανείς να ενημερωθεί για τις δραστηριότητες , για τις εξελίξεις σε θέματα ασφάλειας δικτύων και πληροφοριών σε ευρωπαϊκό επίπεδο και να λαμβάνει δωρεάν το ενημερωτικό υλικό κάθε τρίμηνο. Ο

ENISA είναι συμβουλευτικός ως προς την ευρωπαϊκή επιτροπή και τα κράτη μέλη όπως φαίνεται και στο παρακάτω Σχήμα 16.



Σχήμα 16: Αρμοδιότητες ENISA.

5.3 Αντιμετώπιση Προβλημάτων

5.3.1 DDoS Attacks

Για την αντιμετώπιση των επιθέσεων DDoS που αναφέρθηκαν στο Κεφ. 2, κατ'αρχήν θα πρέπει μέσω συστημάτων ανίχνευσης να επισημαίνονται οι ύποπτες δραστηριότητες και οι επικίνδυνες ροές στο δίκτυο. Συνίσταται η χρήση Host and Network based IDS (Intrusion Detection Systems), τα οποία είναι αρκετά

αποτελεσματικά καθώς και η διερεύνηση κάθε είδους ύποπτης δραστηριότητας. Σε επίπεδο δικτύου, πρέπει να αναγνωρίζονται το συντομότερο δυνατό οι δικτυακές ροές επίθεσης και αυτό μπορεί να γίνεται με φίλτρα που επιτρέπουν τη διέλευση κίνησης στους δρομολογητές συνόρου (border routers), ώστε να μπορεί κάποιος να δει τι μπορεί να ανιχνεύσει (π.χ. μεγάλος αριθμός συγκεκριμένου είδους κίνησης μπορεί να σημαίνει επίθεση). Αυτό γίνεται με χρήση εργαλείων παρακολούθησης της κίνησης, π.χ. Netflow. Επίσης πρέπει να γίνεται παρακολούθηση των ενδείξεων στους δρομολογητές για ασυνίθηστες κινήσεις. Προληπτικά, καλό είναι να γίνονται συχνά security audits για κρυμμένο κακόβουλο κώδικα (zombies) ή rootkits. Επίσης συνίσταται η χρήση πακέτου antivirus για προστασία από επιθέσεις ιών.

Όταν επισημαίνονται κακόβουλες ροές, η αντίδραση πρέπει να είναι έγκαιρη. Τα χαρακτηριστικά της επίθεσης πρέπει να μεταδοθούν σε δίκτυα στα προηγούμενα βήματά της (upstream). Κάτι τέτοιο είναι όμως συνήθως χρονοβόρο. Πρέπει να χρησιμοποιηθούν φίλτρα για να μπλοκάρουν την κακόβουλη κίνηση. Τα φίλτρα αυτά πρέπει να διατηρούνται ενεργοποιημένα για όσο διάστημα διαρκεί η επίθεση και να επιβεβαιώνεται η αποτελεσματικότητά τους. Άλλη λύση είναι το σταμάτημα της κίνησης προς τον στόχο και η δρομολόγηση στο null (blackhole routing). Αν υπάρχουν οι πραγματικές πηγές της δρομολόγησης και δεν έχουν παραποιηθεί μπορεί να γίνει trace back της διαδρομής της επίθεσης. Αυτό γίνεται βήμα βήμα με τη βοήθεια του ISP. Το κύριο συμπέρασμα όμως είναι ότι η αντιμετώπιση δεν είναι υπόθεση ενός μόνο δικτύου.

Αναγκαίες ενέργειες που πρέπει να γίνονται είναι η τακτική αναβάθμιση των συστημάτων (patches), η ύπαρξη σχεδίου αντιμετώπισης και επαναφοράς καθώς και η ύπαρξη εφεδρικού δικτύου, να γίνονται τακτικά backup στα αρχεία και να υπάρχει στοιχειώδης εκπαίδευση των χρηστών σε θέματα ασφαλείας. Επίσης καλό είναι να είναι ξεκάθαρες οι υποχρεώσεις του ISP, να είναι γνωστά τα άτομα που θα πρέπει να επικοινωνήσουν σε περίπτωση έκτακτης ανάγκης και να υπάρχουν και ομάδες CERT (Computer Emergency Response Teams).

5.3.2 Dialers

Σχετικά με το πρόβλημα των dialers η ΕΕΤΤ έχει εκδόσει σχετική οδηγία και προτείνει τις παρακάτω συμβουλές:

Να κλείνετε τον Η/Υ σας όταν δεν τον χρησιμοποιείτε

Ποτέ μην ανοίγετε attachments ηλεκτρονικών μηνυμάτων αν δεν γνωρίζετε τι είναι, διότι θα μπορούσε να είναι ένας κακόβουλος dialer.

Μπορείτε να απευθυνθείτε στον ISP σας ο οποίος θα σας συμβουλεύσει όσον αφορά τη χρήση συγκεκριμένων προγραμμάτων για την προστασία σας.

Εξετάζετε συχνά τις παραμέτρους σύνδεσης του Η/Υ σας με το διαδίκτυο για να βεβαιώνεστε ότι ο αριθμός που καλεί το modem σας για να συνδεθεί είναι ο σωστός.

Να είστε επιφυλακτικοί όταν επιλέγετε με το ποντίκι σας (click) σε αναδυόμενα παράθυρα (pop-up windows) που εμφανίζονται ξαφνικά στην οθόνη σας. Αν έχετε αμφιβολία για το αν επιθυμείτε να δείτε το συγκεκριμένο περιεχόμενο, πάντα να επιλέγετε με το ποντίκι σας την απάντηση «no» ή να κλείνετε το παράθυρο.

Να είστε ιδιαίτερα επιφυλακτικοί αν κατά την περιήγησή σας στο διαδίκτυο μεταφερθείτε σε κάποια ιστοσελίδα την οποία δεν περιμένατε

Να έχετε δυνατά την ένταση του modem σας έτσι ώστε να ακούσετε τους ήχους στην περίπτωση που το modem σας αποσυνδεθεί και επιχειρεί να πραγματοποιήσει άλλη σύνδεση.

Αν προσέξετε κάποιο εικονίδιο (icon) στην επιφάνεια εργασίας σας (desktop) που σας φαίνεται άγνωστο, εξετάστε το και σβήστε ο,τιδήποτε δεν αντιστοιχεί σε έγκυρες εφαρμογές. Σε αυτήν την περίπτωση δεν θα σβήσετε μόνο τα εικονίδια αλλά θα απεγκαταστήσετε (uninstall) και τις σχετικές εφαρμογές.

Ενημερώστε την οικογένειά σας για την απειλή των κακόβουλων dialers και ελέγξτε τη χρήση του διαδικτύου από τα παιδιά σας.

Μπορείτε να ζητήσετε από τον ΟΤΕ να σας ενεργοποιήσει την υπηρεσία της φραγής για εξερχόμενες κλήσεις προς αριθμούς αυξημένης χρέωσης και αριθμούς εξωτερικού. Στην περίπτωση που έχετε προεπιλογή φορέα μπορείτε εναλλακτικά να ζητήσετε από τον προεπιλεγμένο σας πάροχο να σας ενεργοποιήσει την υπηρεσία της φραγής για εξερχόμενες διεθνείς κλήσεις.

Οι περισσότεροι dialers ανιχνεύονται από τα πρόσφατα αντιικά προγράμματα. Βεβαιωθείτε ότι το αντιικό σας πρόγραμμα παρέχει αυτή τη δυντότητα και φροντίστε να το ενημερώνετε συστηματικά.

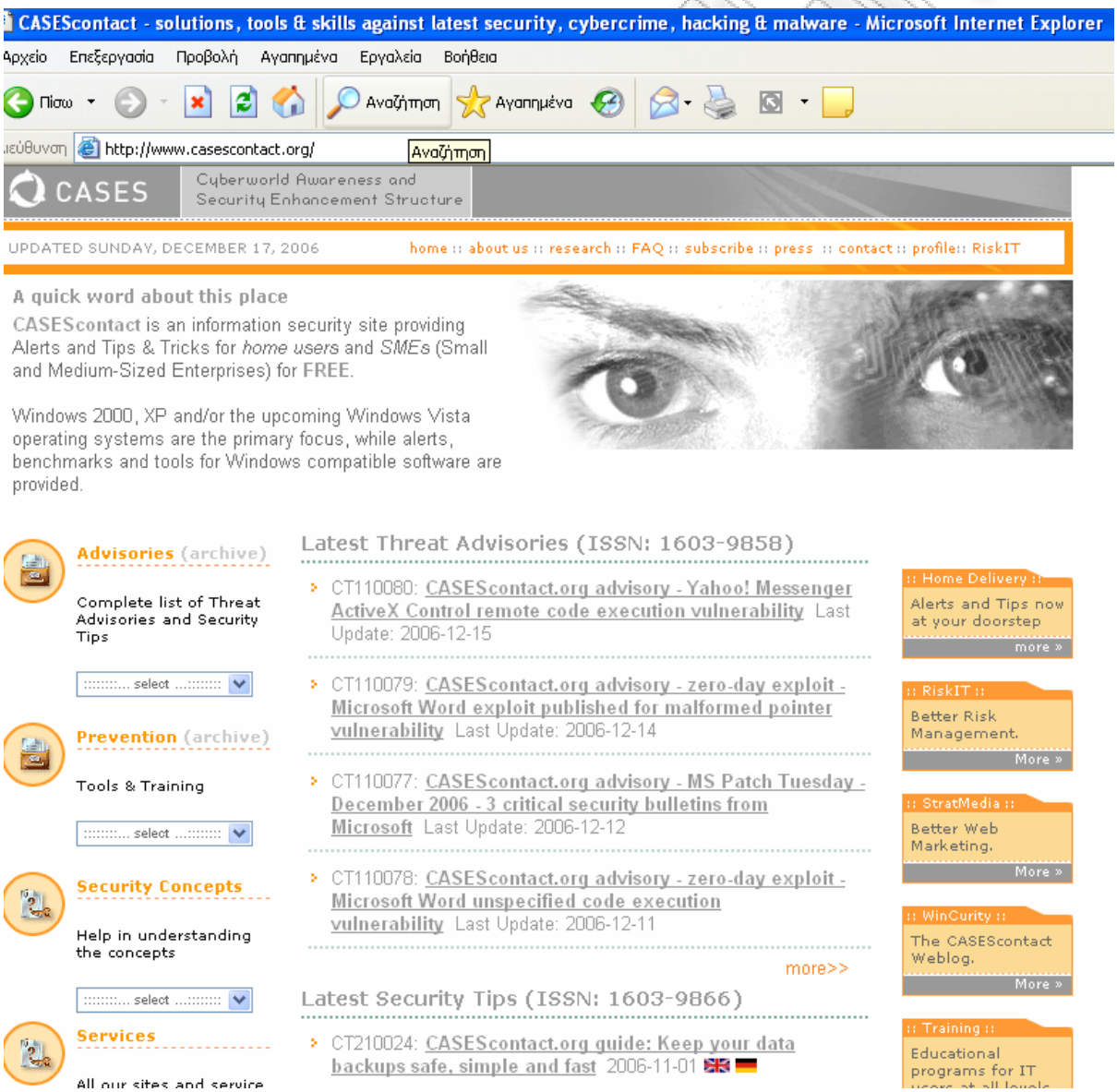
Μπορείτε να εντοπίσετε την ύπαρξη ήδη εγκατεστημένων ή προς εγκατάσταση dialers στον Η/Υ σας με λογισμικό το οποίο θα εντοπίσει τα ύποπτα προγράμματα, θα σας περιγράψει τι κάνουν και στη συνέχεια θα σας βοηθήσει να τα απεγκαταστήσετε. Τέτοιο λογισμικό (είτε ελεύθερο, είτε με πληρωμή) μπορείτε να βρείτε στο διαδίκτυο. (Ενδεικτικά, τέτοιο λογισμικό μπορείτε να βρείτε στους ακόλουθους διαδικτυακούς τόπους: www.tucows.com, www.freedownloads.com)

Τέλος, συνίσταται η μετατροπή της σύνδεσης σε ADSL προκειμένου να αποφευχθεί ο κίνδυνος των dialers, ειδικά τώρα που είναι πιο προσιτές.

5.3.3 Βοήθεια και ενημέρωση για θέματα Ασφάλειας (CASEScontact.org)

Η υπηρεσία CASEScontact.org (www.casescontact.org) αφορά κυρίως ΜΜΕ (Μικρές και Μεσαίου Μεγέθους Επιχειρήσεις) και ιδιώτες και σκοπός της είναι η εκπαίδευση σε θέματα ασφάλειας ηλεκτρονικών υπολογιστών και δικτύων, η ενημέρωση για νέα ζητήματα ασφάλειας και η παροχή συμβουλών αντιμετώπισης και πρόληψης. Η ανάγκη για μια τέτοια υπηρεσία είναι προφανής, καθώς το θέμα της ασφάλειας των συναλλαγών και του ηλεκτρονικού εγκλήματος είναι σε διαρκή εξέλιξη (24 ώρες την ημέρα και 7 ημέρες την εβδομάδα και γίνεται πιο επικίνδυνο σε περιόδους αργιών και εορτών όπου οι επιτιθέμενοι εκμεταλλεύονται το γεγονός αυτό). Ο κάθε ιδιώτης πρέπει να γνωρίζει ορισμένα πράγματα για την ασφάλεια του δικτύου (όπως π.χ. πλένουμε τακτικά τα χέρια μας, αντίστοιχα πρέπει να γίνεται τακτικά scan για πιθανούς ιούς, ή όπως σε κάποιο μπαρ δεν πρέπει να δεχόμαστε ποτά με την υποψία ναρκωτικών, αντίστοιχα δεν πρέπει να ανοίγουμε άγνωστα attachments από άγνωστους αποστολείς). Επειδή οι ιοί εξαπλώνονται με πολύ μεγάλη ταχύτητα, όπως π.χ. ο ιός Nyxem τον περασμένο Ιανουάριο, και επειδή οι χρήστες πρέπει να περάσουν από διάφορα στάδια για να περιοριστεί το φαινόμενο (Awareness , Prevention, Opposition), αλλά και επειδή μεταξύ των κρατών-μελών της ΕΕ πρέπει να αναπτυχθούν συνέργειες για την πρόληψη του φαινομένου επιθέσεων σε συστήματα ασφάλειας των ΗΥ, δημιουργήθηκε αυτή η υπηρεσία. Το CASEScontact

σκοπό έχει να αναπτύξει την επαγρύπνιση των χρηστών ώστε να γίνεατι πιο αποτελεσματική πρόληψη. Είναι προσβάσιμο σε όλους και οι υπηρεσίες διατίθενατι δωρεάν. Απευθύνεται σε ιδιώτες χρήστες, ελεύθερους επαγγελματίες, αλλά και μικρές επιχειρήσεις που δεν μπορούν να απασχολούν εξειδικευμένο προσωπικό για θέματα ασφάλειας των ηλεκτρονικών δικτύων. Η φιλοσοφία είναι ότι η πρόληψη είναι το κλειδί για ένα ασφαλέστερο Internet (Prvention is the key on the road to a safer Internet). Στην επόμενη εικόνα φαίνονται οι επιλογές που έχει ο επισκέπτης της CASEScontact.org



Εικόνα 14: www.casescontact.org

5.4 Πρακτικές Συμβουλές Ασφάλειας

Παρατίθενται μερικές πρακτικές αλλά χρήσιμες συμβουλές για την ασφάλεια στο internet:

Η χρήση ενός λογισμικού πακέτου για την προστασία του ΗΥ το οποίο να αναβαθμίζεται σε τακτά διαστήματα. Πρέπει να περιλαμβάνει antivirus προστασία, antispyware, anti-spam καθώς και για όλες τις μορφές κακόβουλων αρχείων (worms, trojan, etc).

Να πραγματοποιούνται ηλεκτρονικές συναλλαγές σε αξιόπιστα sites που να ακολουθούν αξιόπιστα πρωτόκολλα ασφαλείας (πχ SSL-128bit encrytion) και να ακολουθούνται οι συμβουλές ασφαλείας που δημοσιεύονται στις ιστοσελίδες τους.

Να μη χρησιμοποιούν κωδικούς που είναι εύκολα προβλέψιμοι (π.χ. ημερομηνίες ή αριθμοσειρές όπως 1234…), Εξάλλου πολλά sites έχουν συγκεκριμένη πολιτική για τους κωδικούς ώστε να είναι πιο δύσκολο να προβλεφθούν (πρέπει γι απαράδειγμα το password να περιέχει και αριθμούς και γράμματα, να μην επαναλαμβάνονται κάποια ψηφία κλπ).

Να μη χρησιμοποιείται το ίδιο password για περισσότερα sites καθώς αν διαρεύσει αυξάνεται ο κίνδυνος για παραβίαση περισσότερων συναλλαγών.

Να μην κοινοποιείται σε κανένα το password. Στις πολιτικές ασφάλειας τονίζεται ότι κανένας υπάλληλος του οργανισμού δε θα ζητήσει το password και αν κάτι τέτοιο γίνει πρόκειται για προσπάθεια εξαπάτησης και πρέπει να καταγγελθεί.

Σε περίπτωση αγοράς υπηρεσιών ή προϊόντων, καλό είναι να χρησιμοποιείται η ίδια πιστωτική κάρτα, η οποία να προορίζεται για ηλεκτρονικές αγορές. Μια τέτοια κάρτα συνίσταται να έχει χαμηλό πιστωτικό όριο (συνήθως όσο χρειάζεται για τις αγορές του χρήστη), ώστε ακόμα και αν υποκλαπούν τα στοιχεία της, να μην μπορεί να χρεωθεί.

Η χρήση προπληρωμένων καρτών με επίσης χαμηλό ποσό είναι περισσότερο ασφαλής γιατί υπάρχει καλύτερος έλεγχος από την πλευρά του χρήστη.

Υπάρχουν τράπεζες που ενημερώνουν τον πελάτη μετά από ηλεκτρονικές συναλλαγές για επιβεβαίωση της αυθεντικότητας της συναλλαγής.

Ο ΗΥ όταν δε χρησιμοποιείται πρέπει να είναι κλειστός, ώστε να μειώνεται ο κίνδυνος για κακόβουλη επίθεση. Δεν πρέπει να ξεχνάμε το γεγονός ότι αν κάποιος αποκτήσει

πρόσβαση στους κωδικούς μας, μπορεί να μας εμπλέξει σε παράνομες πράξεις και να χρησιμοποιήσει τα δικά μας στοιχεία για να βλάψει άλλους.

Πρέπει ακόμα να ελέγχεται η αυθεντικότητα της ιστοσελίδας (δηλαδή η ηλεκτρονική διεύθυνση και να μην εφησυχάζουμε στο λογότυπο και το περιεχόμενο της σελίδας καθώς μπορεί να έχουν αντιγραφεί).

Σε περίπτωση ασφαλών συναλλαγών (https) να ελέγχεται ο κάτοχος της σελίδα και το πιστοποιητικό ασφαλείας), όπως φαίνεται στην ακόλουθη εικόνα 15 από το e-banking της Εθνικής Τράπεζας Ελλάδας.

Σε καμμία περίπτωση να μην δίνονται προσωπικά στοιχεία σε email τα οποία είναι παραπλανητικά ή διαφημιστικού περιεχομένου και προέρχονται από άγνωστους αποστολείς.

Επίσης να μην ανοίγονται άγνωστα συνημμένα αρχεία σε παράξενα email ανγωστης προέλευσης

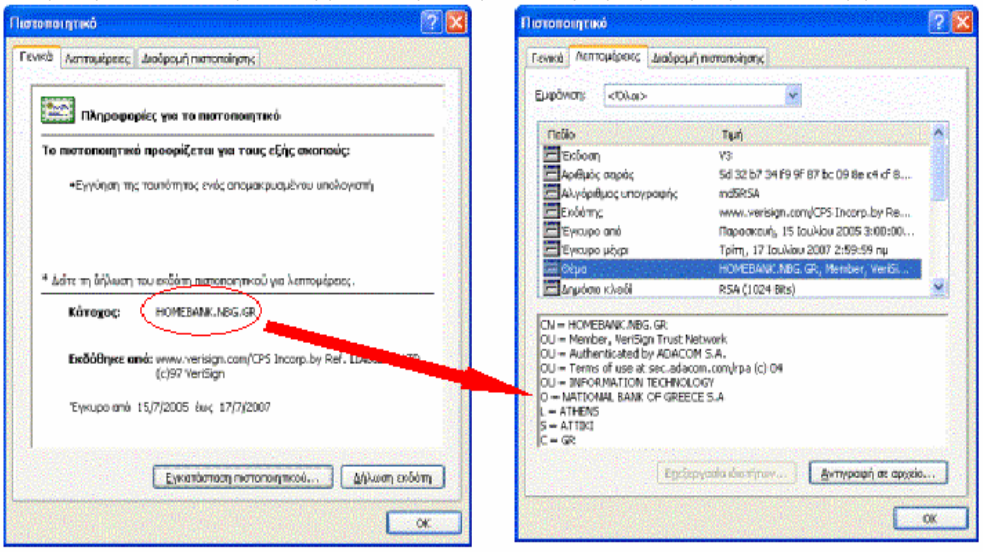
Να μην υπάρχει εμπιστοσύνη στις πληροφορίες και υποσχέσεις παράξενων και αμφίβολων ιστοσελίδων.

Εκπαίδευση και ενημέρωση για τις απειλές και safety tips (π.χ. casescontact.org)

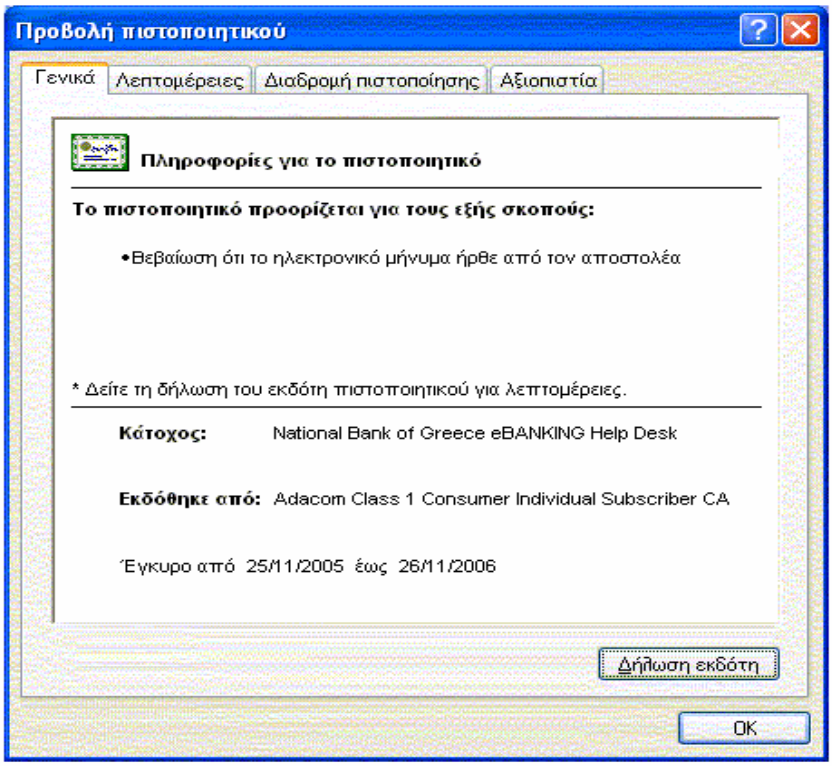
- Πληκτρολογήστε την διεύθυνση της ιστοσελίδας μόνοι σας (homebank.nbg.gr) και όχι μέσω σύνδεσης (link) που πιθανόν σας σταλεί μέσω e-mail

- Βεβαιωθείτε ότι η διεύθυνση είναι **homebank.nbg.gr**
- Ελέγξτε το εικονίδιο το οποίο εμφανίζεται στις ασφαλείς ιστοσελίδες της Τράπεζας.

Επιλέγοντας το εικονίδιο θα πρέπει να εμφανιστεί στην οθόνη του υπολογιστή σας το παράθυρο το οποίο επιβεβαιώνει ότι κάτοχος της σελίδας είναι η Εθν



Εικόνα 15: Οδηγίες Ασφάλειας στο e-banking της ΕΤΕ



Εικόνα 16: Οδηγίες Ασφάλειας στο e-banking της ΕΤΕ (Έλεγχος Πιστοποιητικού)

5.5 Συμπεράσματα

Συμπερασματικά μπορούμε να πούμε ότι το θέμα της ασφάλειας του internet , των δικτύων υπολογιστών και των συναλλαγών στα πλαίσια του ΗΕ, είναι ένα θέμα «ζωντανό» που εξελίσσεται κάθε μέρα. Υπάρχει μια διαρκής αμφίδρομη σχέση ανάμεσα στους κακόβουλους χρήστες από τη μια πλευρά (από απλούς hackers που παρεμβαίνουν για "hobby" μέχρι οργανωμένα μέλη ηλεκτρονικού εγκλήματος) και τους αναλυτές συστημάτων, προγραμματιστές από την άλλη να προσπαθούν να αντιμετωπίσουν τις επιθέσεις και τις ενέργειες των πρώτων. Η συνεχής αυτή πάλη είναι ανάλογη με το πρόβλημα της χρήσης απαγορευμένων ουσιών στον αθλητισμό. Μόλις βρίσκεται ο τρόπος να ανιχνευθεί μια ουσία, αρχίζει να εμφανίζεται η χρήση κάποιας άλλης μη ανιχνεύσιμης. Έτσι και στις ηλεκτρονικές συναλλαγές μόλις αντιμετωπισθεί ένας ιός, εμφανίζεται κάποιος νεώτερος και όταν εμφανλιζεται ένα νέο σύστημα είναι μια πρόκληση το πώς θα παραβιαστεί.

Η απάντηση στο εάν κάποτε θα μπορούμε να είμαστε εντελώς ασφαλείς στο διαδίκτυο σχετικά με τα δεδομένα που ανταλλάσσονται δε νομίζω πως μπορεί να είναι ποτέ θετική. Όμως προς την κατεύθυνση αυτή πρέπει να κινούνται παράλληλα όλοι οι εμπλεκόμενοι (χρήστες, IPS, φορείς ελέγχου, δημόσιες υπηρεσίες) ώστε να βελτιώνονται οι υποδομές, να γίνεται έρευνα προς τη σωστή κατεύθυνση, να θωρακίζεται η κοινωνία από ουσιαστικές νομοθετικές ρυθμίσεις και πρωτοβουλίες, οι έμποροι/εταιρίες να εφαρμόζουν τις κατάλληλες πολιτικές ασφαλείας και οι χρήστες να είναι ενήμεροι (awareness) για τους κινδύνους που υπάρχουν και να συμπεριφέρονται ανάλογα (prevention). Όπως αναφέρθηκε και παραπάνω η προστασία είναι το κλειδί για ένα ασφαλέστερο διαδίκτυο. (Prevention is the key on the road to a safer Internet).

Βιβλιογραφία

1. Χονδροκούκης Γρηγόρης (Πανεπηστήμιο Πειραιώς), Εισαγωγή στο Ηλεκτρονικό Εμπόριο e-Επιχειρείν, 2003
2. Γκρίτζαλης Στέφ. – Κάτσικας Ιωάν. – Γκρίτζαλης Δημ. (Πανεπιστήμιο Αιγαίου – Οικονομικό Πανεπιστήμιο Αθηνών), Ασφάλεια Δικτύων Υπολογιστών, 2003
3. Rhee Man Young, (Wiley) Internet Security: Cryptographic Principles, Algorithms and Protocols, 2003
4. Κατραμάδος Ιωάννης, Πανεπιστήμιο Πειραιά, ΔΜΠ-Logistics, Διπλωματική Εργασία, Ηλεκτρονικές Βάσεις Δεδομένων: Απειλές και Μέθοδοι Προστασίας, 2003

Διαδικτυογραφία

5. Δικηγορικός Σύλλογος Αθηνών και Τεχνικό Επιμελητήριο Ελλάδας: Ημερίδα για την Ασφάλεια των Ηλεκτρονικών Επικοινωνιών, Αθήνα 01-06-2006 http://www.ictsecurity2006.gr/
6. ITU (International Telecomunications Union), Internet Report 2006, www.itu.int
7. http://www.nytimes.com/2006/12/06/technology/06spam.html
8. http://ta-nea.dolnet.gr/data/D2006/D1214/1el13a.jpg
9. http://www.time.com/time/covers/0,16641,20061225,00.html
10. https://homebank.nbg.gr/nbgib/helpFiles/el_GR/info/security_info.jsp
11. http://money.cnn.com