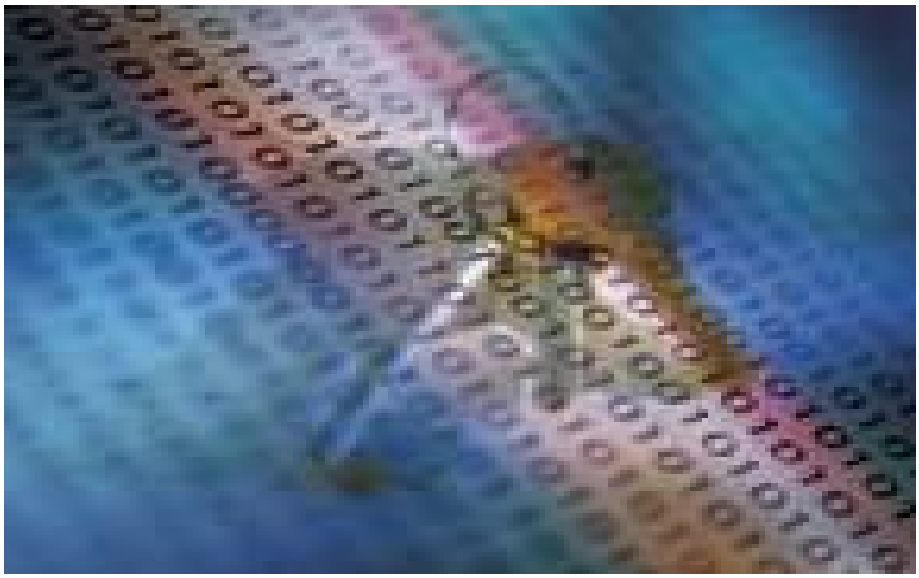
Τ.Ε.Ι. ΠΑΤΡΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ: ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ



ΚΑΘΗΓΗΤΗΣ:
Βλαχόπουλος Γεώργιος

ΣΠΟΥΔΑΣΤΡΙΑ:
Κουμουνδούρου 'Ολγα

ΠΑΤΡΑ 2008

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ: ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

1.ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1. 1 Αναφορά στις εμπορικές συναλλαγές μέσω internet

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μια συναλλαγή γίνεται όταν στέλνονται προσωπικές, ιδιωτικές ή οικονομικές πληροφορίες μέσω του Internet. Για παράδειγμα εισαγωγή των πληροφοριών της πιστωτικής μας κάρτας για να αγοράσουμε από ένα online κατάστημα. Επομένως, η ασφάλεια συναλλαγών στο Internet βρίσκει εφαρμογή σε υπηρεσίες που σχετίζονται με εμπορικές και επιχειρηματικές δραστηριότητες, όπως είναι το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές επιχειρήσεις. (εξετάζονται στο κεφάλαιο 5.4)

1.1.1 Εισαγωγή στο internet

1.1.1.1 Τι είναι το internet;

Το Internet είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές που εκτείνεται σχεδόν σε κάθε γωνιά του πλανήτη (πάνω από 150 χώρες) και παρέχει τις υπηρεσίες του σε εκατομμύρια χρήστες. Αποτελεί ένα "Παγκόσμιο Ηλεκτρονικό Χωριό", οι "κάτοικοι" του οποίου, ανεξάρτητα από υπηκοότητα, ηλικία, θρήσκευμα και χρώμα, μοιράζονται πληροφορίες και ανταλλάσσουν ελεύθερα απόψεις πέρα από γεωγραφικά και κοινωνικά σύνορα.

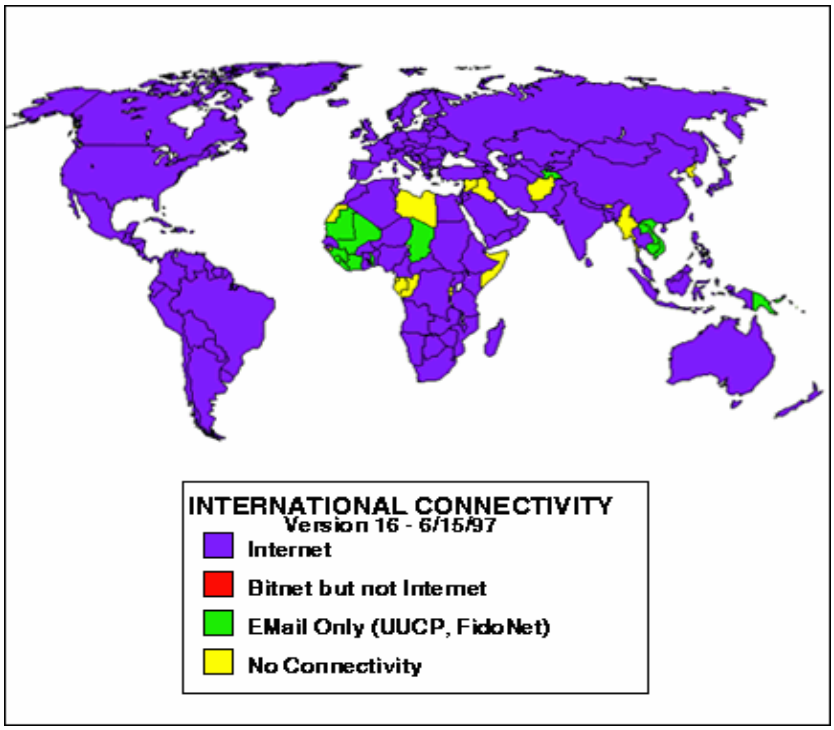
1.1.1.2 Η ιστορία του Internet

Το σημερινό Internet αποτελεί εξέλιξη του ARPANET, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του 60 στα πανεπιστήμια των ΗΠΑ. Το δίκτυο ARPANET γεννιέται το 1969 με πόρους του προγράμματος ARPA (Advanced Research Project Agency) του Υπουργείου Άμυνας, με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching). Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων.

Το 1973, με σκοπό τη διασύνδεση ανόμοιων δικτύων και την ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο ξεκινά ένα νέο πρόγραμμα που ονομάζεται Πρόγραμμα Διαδικτύωσης. Από την έρευνα γεννιέται το Internet Protocol (IP) (Πρωτόκολλο Διαδικτύωσης) με το οποίο διαφορετικά δίκτυα που το χρησιμοποιούν μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο στο οποίο όλοι οι υπολογιστές μπορούν να επικοινωνούν μεταξύ τους. Παράλληλα, σχεδιάζεται ένα νέο πρωτόκολλο για τον έλεγχο της μετάδοσης των δεδομένων, το Transmission Control Protocol (TCP) (Πρωτόκολλο Ελέγχου Μετάδοσης). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (E-mail). Σταδιακά συνδέονται με το ARPANET και ιδρύματα από άλλες χώρες.

Το 1983, το πρωτόκολλο TCP/IP (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983, χωρίζεται σε δύο τμήματα: στο MILNET και στο νέο ARPANET. Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το NSFNET χρησιμοποιώντας το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του ‘80, όλο και περισσότερες χώρες συνδέονται στο NSFNET. Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό σαν INTERNET. Το 1990, το ARPANET πλέον καταργείται.

Όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990. Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (WWW) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers -ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα.



Σχήμα: 1.4 Χώρες που έχουν συνδεθεί στο internet

1.1.2 Δομή του internet-πρωτόκολλα

Στην καθημερινή μας ζωή, πρωτόκολλο είναι ένα σύνολο από κανόνες που καθορίζουν το πώς πρέπει να πραγματοποιηθεί κάποια διαδικασία. Στον κόσμο των δικτύων,

πρωτόκολλο είναι ένα σύνολο από κανόνες που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών, κλπ. Το Internet δεν είναι ένα απλό δίκτυο, αλλά ένα διαδίκτυο. Χρειάζεται επομένως ένα σύνολο από κανόνες που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα.

1.1.2.1 Το πρωτόκολλο TCP/IP

Ακριβώς αυτό το σύνολο συμβάσεων προσφέρει το TCP/IP. Όλοι οι υπολογιστές που είναι συνδεδεμένοι στα χιλιάδες μικρότερα δίκτυα του Internet «τρέχουν» το πρωτόκολλο TCP/IP κι έτσι μιλούν μια κοινή γλώσσα που τους επιτρέπει να συνεννοούνται παρά τις διαφορές τους.

Έτσι λοιπόν ένα σύνολο κανόνων που καθορίζουν τη μορφή των μηνυμάτων και τις κατάλληλες ενέργειες που απαιτούνται για κάθε μήνυμα λέγεται πρωτόκολλο δικτύου (network protocol). Το λογισμικό που υλοποιεί αυτούς τους κανόνες λέγεται λογισμικό πρωτοκόλλων (protocol software).

Οι σχεδιαστές αντί να ορίσουν ένα μόνο γιγαντιαίο πρωτόκολλο που να καθορίζει όλες τις λεπτομέρειες, προτίμησαν να σχεδιάσουν από ένα ξεχωριστό πρωτόκολλο για κάθε πρόβλημα τις επικοινωνίας.

Η υποδιαίρεση σε ξεχωριστά πρωτόκολλα πρέπει να γίνει προσεκτικά, για να εξασφαλιστεί η αποδοτικότητα του συστήματος επικοινωνίας.

Πώς μπορεί να εξασφαλιστεί ότι τα πρωτόκολλα θα συνεργάζονται σωστά;

Η λύση είναι η εξής:

Αντί να αναπτύσσεται το κάθε πρωτόκολλο μεμονωμένα τα πρωτόκολλα σχεδιάζονται σε «οικογένειες». Κάθε πρωτόκολλο μιας οικογένειας επιλύει ένα μέρος του προβλήματος της επικοινωνίας και όλα μαζί επιλύουν ολόκληρο το πρόβλημα.

Ένα από τα βασικά εργαλεία για την σχεδίαση μιας οικογένειας πρωτοκόλλων είναι το μοντέλο διαστρωμάτωσης (layering model).

Στο παρακάτω σχήμα φαίνονται τα πέντε επίπεδα του μοντέλου διαστρωμάτωσης TCP/IP (TCP/IP Layering Model, ή αλλιώς μοντέλο διαστρωμάτωσης του Internet) καθώς και τα κυριότερα πρωτόκολλα και εφαρμογές.

ΕΦΑΡΜΟΓΗ (www. E-mail, ftp, http…)	← ΕΠΙΠΕΔΟ 5
ΜΕΤΑΦΟΡΑ (TCP, UDP)	← ΕΠΙΠΕΔΟ 4
ΔΙΑΔΙΚΤΥΟ (IP)	← ΕΠΙΠΕΔΟ 3
ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΟΥ	← ΕΠΙΠΕΔΟ 2
ΦΥΣΙΚΟ	← ΕΠΙΠΕΔΟ 1

Σχήμα:1.5 Τα 5 επίπεδα του μοντέλου διαστρωμάτωσης TCP/IP

ΕΠΙΠΕΔΟ 1: Φυσικό Επίπεδο. Αντιστοιχεί στο βασικό υλικό του δικτύου.

ΕΠΙΠΕΔΟ 2: Διασύνδεση δικτύου. Τα πρωτόκολλα του Επιπέδου 2 καθορίζουν το πώς οργανώνονται τα δεδομένα σε πακέτα και το πώς ένας υπολογιστής μεταδίδει τα πακέτα μέσω ενός δικτύου.

ΕΠΙΠΕΔΟ 3: Διαδίκτυο. Τα πρωτόκολλα του επιπέδου 3 καθορίζουν τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για να προωθούνται τα πακέτα από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσοτέρων δρομολογητών. (Δρομολογητής είναι ο εκείνος ο υπολογιστής, σε ένα δίκτυο από περισσότερους υπολογιστές, που ελέγχει την διακίνηση των δεδομένων.)

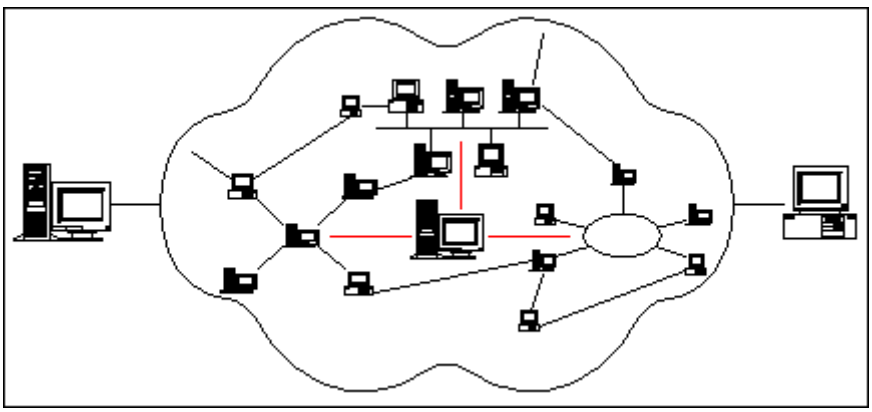
ΕΠΙΠΕΔΟ 4: Μεταφορά. Τα πρωτόκολλα του επιπέδου 4 καθορίζουν το πώς εξασφαλίζεται η αξιόπιστη μεταφορά

ΕΠΙΠΕΔΟ 5: Εφαρμογή. Κάθε πρωτόκολλο του επιπέδου 5 καθορίζει τον τρόπο με τον οποίο μια εφαρμογή χρησιμοποιεί ένα διαδίκτυο.[1]

1.1.2.2 Βασικές αρχές λειτουργίας του πρωτοκόλλου TCP/IP

Ας υποθέσουμε ότι θέλουμε να μεταφέρουμε δεδομένα από έναν υπολογιστή που είναι συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Αμερική, στο MIT, σε έναν άλλον που είναι επίσης συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Ελλάδα, στο Πανεπιστήμιο Πάτρας. Μεταξύ των δύο υπολογιστών παρεμβάλλεται το «σύννεφο» του Internet, δηλ. ένα πλέγμα από συνδέσεις και ενδιάμεσους υπολογιστές.

Το Internet χρησιμοποιεί την τεχνολογία μεταγωγής πακέτων για τη μεταφορά των δεδομένων: τα δεδομένα κόβονται σε κομμάτια που ονομάζονται πακέτα και σε κάθε πακέτο μπαίνει μια "επικεφαλίδα" με τις διευθύνσεις του υπολογιστή - αποστολέα και του υπολογιστή – παραλήπτη



Σχήμα 1.6: Οι δύο τελικοί υπολογιστές και το «σύννεφο» του Internet

.

Σημειώνουμε ότι σε κάθε υπολογιστή του Internet αντιστοιχεί μία διεύθυνση που ονομάζεται διεύθυνση IP. Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα του πακέτου από υπολογιστή σε υπολογιστή μέσα από το «σύννεφο» των συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ούτε ότι το πακέτο θα φτάσει στον προορισμό του ούτε ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη

σειρά με την οποία στάλθηκαν ούτε ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Το TCP προσφέρει ένα αξιόπιστο πρωτόκολλο πάνω από το IP. Εγγυάται ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα (δηλ. όπως στάλθηκαν).

Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής - παραλήπτης και ο υπολογιστής - αποστολέας, αλλά όχι οι ενδιάμεσοι υπολογιστές, παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, κλπ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του.

A. TCP PORTS

Κάθε υπολογιστής έχει μια μοναδική φυσική σύνδεση με το δίκτυο. Όλα τα δεδομένα που απευθύνονται στον υπολογιστή διακινούνται μέσω αυτής της σύνδεσης. Παρ’ όλα αυτά τα δεδομένα μπορεί να απευθύνονται σε διαφορετικές εφαρμογές που «τρέχουν» στον υπολογιστή. Με την χρήση των ports ο υπολογιστής γνωρίζει σε ποια εφαρμογή πρέπει να προωθήσει τα δεδομένα. Τα δεδομένα που διακινούνται στο διαδίκτυο συνοδεύονται από πληροφορία που καθορίζει τον υπολογιστή – προορισμό (IP διεύθυνση 32-bit) και το port (16 bit) που χρησιμοποιείται από το TCP και το UDP για την παράδοση των δεδομένων στη σωστή εφαρμογή. Επειδή θα μπορούσε ο καθένας να ορίσει δικές του διευθύνσεις TCP για τις υπηρεσίες, υπάρχει μια ενιαία αρίθμηση των διευθύνσεων TCP για τις γνωστές υπηρεσίες του Internet. Αυτές φαίνονται στο παρακάτω πίνακα:

TCP πόρτα	Υπηρεσία
21	FTP (File Tranfer protocol) – Μεταφορά αρχείων
23	Telnet – Απομακρυσμένη πρόσβαση
25	SMTP – Ηλεκτρονικό ταχυδρομείο
80	Web – Παγκόσμιος Ιστός
53	DNS – Υπηρεσία ονοματολογίας
143	IMAP – Απομακρυσμένη ανάγνωση ηλεκτρονικού ταχυδρομείου

Σχήμα 1.7 TCP ports γνωστών υπηρεσιών

Ο τρόπος λειτουργίας του TCP εξασφαλίζει αξιοπιστία και ταχύτητα διότι οι ενδιάμεσοι υπολογιστές δεν εκτελούν ελέγχους. Όπως θα δούμε παρακάτω, η διαδρομή που ακολουθεί ένα πακέτο μέσα από το «σύννεφο» των συνδέσεων δεν είναι προκαθορισμένη.

Β. Δρομολόγηση πακέτων

Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα ενός πακέτου δεδομένων από υπολογιστή σε υπολογιστή. Όλα τα δίκτυα που συνδέονται στο Internet «καταλαβαίνουν» τη γλώσσα IP κι έτσι μπορούν να συνεννοούνται και να ανταλλάσσουν δεδομένα με ομοιόμορφο τρόπο. Τα δίκτυα του Internet συνδέονται μεταξύ τους με ειδικούς υπολογιστές που ονομάζονται δρομολογητές (routers) ή πύλες (gateways). Ένας router είναι λοιπόν ένας υπολογιστής που συνδέει δύο ή περισσότερα δίκτυα (που μπορεί να είναι διαφορετικού τύπου) και έτσι ανήκει σε δύο ή περισσότερα δίκτυα ταυτόχρονα.

Ο ρόλος των routers είναι να δρομολογούν τα πακέτα των δεδομένων μέσα από τα διάφορα δίκτυα που αποτελούν το Internet μέχρις ότου τα επιδώσουν στον προορισμό τους.

Ας θεωρήσουμε πάλι ότι ένας υπολογιστής που βρίσκεται κάπου στο Internet θέλει να στείλει δεδομένα σε κάποιον άλλον υπολογιστή. Τα δεδομένα κόβονται σε πακέτα και το IP που εκτελείται στον υπολογιστή - αποστολέα ετοιμάζεται να στείλει το κάθε

πακέτο. Εισάγει λοιπόν στην επικεφαλίδα του πακέτου τις IP διευθύνσεις του αποστολέα και του παραλήπτη και κατόπιν, βάσει των διευθύνσεων αυτών, ελέγχει αν ο παραλήπτης βρίσκεται στο ίδιο δίκτυο με τον αποστολέα.

Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη χωρίς να χρειαστεί να διαβεί τα όρια του δικτύου. Εάν όχι, προωθείται στον router που είναι συνδεμένος με το δίκτυο. Ο router με τη σειρά του ελέγχει αν ο παραλήπτης βρίσκεται σε κάποιο από τα υπόλοιπα δίκτυα με τα οποία είναι συνδεδεμένος. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη στο δίκτυο αυτό. Εάν όχι, το πακέτο προωθείται στον επόμενο router, κ.ο.κ. μέχρις ότου το πακέτο προωθηθεί τελικά στον router που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη. Το πακέτο μπορεί έτσι να περάσει από πολλούς routers μέχρις ότου φτάσει στον προορισμό του.

Ένα μεγάλο πλεονέκτημα αυτής της μεθόδου είναι ότι η διαδρομή που ακολουθεί ένα πακέτο δεν είναι προκαθορισμένη, αλλά επιλέγεται δυναμικά. Έτσι, οι routers μπορούν να επιλέγουν εναλλακτικούς δρόμους για ένα πακέτο σε περίπτωση που μια συγκεκριμένη σύνδεση του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά σε αχρηστία.[2]

1.1.2.3 Το πρωτόκολλο UDP

Το UDP (USER DATAGRAM PROTOCOL) είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται σε πολλές περιπτώσεις αντί του TCP για τη μεταφορά δεδομένων .Ο σκοπός δημιουργίας του και ο βασικός τρόπος λειτουργίας του UDP είναι σχεδόν ο ίδιος με του αυτόν του TCP. Η βασική διαφορά του TCP με το UDP έγκειται στο ότι το UDP σε αντίθεση με το TCP δεν ασχολείται καθόλου με τα χαμένα πακέτα κατά τη μεταφορά αρχείων όπως επίσης δεν ασχολείται με την τοποθέτηση των πακέτων με την σωστή σειρά. Το UDP βρίσκει εφαρμογή σε αποστολή σύντομων μηνυμάτων, επίσης εάν δε λάβει μια απάντηση στέλνει πάλι το αίτημα του.

1.2. Διευθυνσιοδότηση στο Internet

1. 2.1 Διευθύνσεις IP

Το Internet όπως προείπαμε, αποτελείται από χιλιάδες δίκτυα στα οποία είναι συνδεδεμένοι εκατομμύρια υπολογιστές. Πώς λοιπόν μπορεί να προσδιοριστεί με ακρίβεια ο υπολογιστής για τον οποίον προορίζονται κάποια δεδομένα; Με άλλα λόγια, πώς ξεχωρίζει ένας υπολογιστής του Internet από έναν άλλον;

Σε κάθε υπολογιστή αντιστοιχίζεται μια μοναδική διεύθυνση, που ονομάζεται διεύθυνση IP (IP address) και η οποία αποτελεί την «ταυτότητα» του στο διαδίκτυο.

Μια διεύθυνση IP αποτελείται από 4 αριθμούς χωρισμένους με τελείες. Π.χ. ένας υπολογιστής που βρίσκεται στο Πανεπιστήμιο MIT έχει διεύθυνση 18.75.0.10, ένας άλλος που βρίσκεται στο ΕΜΠ 147.102.154.

Στην πραγματικότητα μία IP διεύθυνση είναι ένας δυαδικός αριθμός 32-bit που για να γίνει περισσότερο κατανοητός στους ανθρώπους, χωρίζεται σε 4 ομάδες των 8 bit και κατόπιν κάθε ομάδα μεταφράζεται στον αντίστοιχο δεκαδικό αριθμό.

Π.χ.: 00010010 01001011 00000000 00001010 (δυαδικός αριθμός 32-bit)

18. 75. 0. 10 (4 δεκαδικοί αριθμοί χωρισμένοι με τελείες)

Μια διεύθυνση IP περιέχει δύο κομμάτια πληροφορίας. Το πρώτο είναι ο αριθμός δικτύου (network id) στο οποίο ανήκει ο υπολογιστής. Κάθε δίκτυο χαρακτηρίζεται από έναν μοναδικό αριθμό που αποτελεί την «ταυτότητά» του στο Internet. Το δεύτερο είναι ένας τοπικός αριθμός υπολογιστή που προσδιορίζει τον υπολογιστή μέσα στο συγκεκριμένο δίκτυο (host id).

Οι διευθύνσεις στο Internet ανήκουν σε έναν από τους παρακάτω τέσσερις τύπους, ανάλογα με το πλήθος των συστημάτων που περιλαμβάνει το δίκτυο:

Κλάση Α- η μορφή των διευθύνσεων της κατηγορίας διαμορφώνεται από το πρώτο bit είναι το 0, στη συνέχεια τα επόμενα 7 bits αποτελούν το id του δικτύου και τα 24 υπόλοιπα αποτελούν το host id. Οι διευθύνσεις της μορφής είναι κατάλληλες για ένα τοπικό δίκτυο με πολλά συστήματα (hosts).

Κλάση B- όπου η μορφή των διευθύνσεων αρχίζει με τα bits 10και ακολουθούν τα 14 bits του network id και τα 16 bits του host id.

Κλάση C- με χαρακτηριστικά bits την ακολουθία 110, 21 bits τα οποία δηλώνουν το network id και τέλος, 8 bits για το host id, ενώ η κατηγορία αυτή είναι κατάλληλη για περιπτώσεις δικτύων με πολλά τοπικά δίκτυα και με λιγότερους hosts ανά υποδίκτυο σε σχέση με τα class A.

Κλάση D- με διευθύνσεις που σχηματίζονται από τα bits 1110 στην αρχή και ακολουθούν τα υπόλοιπα 28 bits, κατηγορία που απευθύνεται σε περιπτώσεις μετάδοσης multicast.

Κάθε οργανισμός που θέλει να συνδέσει στο Internet τους υπολογιστές του ζητά έναν αριθμό δικτύου από κάποιον επίσημο οργανισμό που ασχολείται με την κατανομή των διευθύνσεων στο Internet έτσι ώστε να εξασφαλίζεται η μοναδικότητα τους.[3]

1.2.2 Ποιος είναι υπεύθυνος για το internet;

Κανείς δεν είναι υπεύθυνος για το internet. Υπάρχουν μόνο κάποιες υπηρεσίες που ορίζουν την πολιτική που θα ακολουθείται στο internet.
Η ανάπτυξη του internet κατευθύνεται από τον Internet Society. [4] Ο οργανισμός αυτός περιγράφει τον εαυτό του σαν «…… μη κυβερνητικός, διεθνής οργανισμός για την καθολική συνεργασία και το συντονισμό του internet και των τεχνολογιών εφαρμογών του». Η κοινωνία του internet συνήθως υιοθετεί πολύ γρήγορα τις συστάσεις του Internet Society για νέες τυποποιήσεις.
Η καταγραφή των ονομάτων τομέα και η διαχείριση τους γίνεται από το Internet Corporation for Assigned Names and Numbers (ICANN) και του Network Solutions Incorporated.[5] Οι περισσότερες εταιρείες παροχής internet παρέχουν επίσης υπηρεσίες καταγραφής ονομάτων τομέων.

1.3. Οι υπηρεσίες και οι εφαρμογές του internet

1.3.1 Οι κυριότερες υπηρεσίες του Internet

1) E-mail (Ηλεκτρονικό Ταχυδρομείο)
Υποστηρίζει την ανταλλαγή μηνυμάτων μεταξύ χρηστών χάρη στην προσωπική ηλεκτρονική διεύθυνση του καθενός. Το περιεχόμενο του μηνύματος μπορεί να είναι κείμενο, ήχος, εικόνα, video ή δεδομένα.

2) Mailing lists (Λίστες E-mail)
Καθορισμένη ομάδα απομακρυσμένων μεταξύ τους χρηστών που ανταλλάσσουν μηνύματα σχετικά με κάποιο θέμα ορισμένο από κοινού, με κάποιον από αυτούς ως υπεύθυνο για την καλή λειτουργία της λίστας.

3) Remote Login (Απομακρυσμένη Σύνδεση)
Ένας χρήστης έχει δικαίωμα χρήσης σε έναν ή περισσότερους υπολογιστές του δικτύου. Αν αυτοί είναι απομακρυσμένοι μεταξύ τους τότε, εργαζόμενος σε έναν από αυτούς, μπορεί να συνδεθεί με οποιονδήποτε από τους υπόλοιπους και να (τηλε-) εργαστεί σαν να ήταν παρών, δηλαδή να χρησιμοποιήσει τις δυνατότητες του απομακρυσμένου υπολογιστή σαν να βρίσκονταν στον ίδιο φυσικό χώρο με αυτόν.

4) Finger Αναζήτηση της ύπαρξης ενός συγκεκριμένου χρήστη σε κάποιο σημείο του δικτύου.

5) FTP (File Transfer Protocol)
Μεταφορά αρχείων από απομακρυσμένο υπολογιστή σε τοπικό υπολογιστή και αντίστροφα.

6) Archie

Αναζήτηση υπολογιστών στο Internet που προσφέρουν την υπηρεσία FTP και περιέχουν πληροφορίες με περιεχόμενο οριζόμενο από το χρήστη.

7) Usenet

Ανταλλαγή μηνυμάτων οργανωμένη σε «οικογένειες ηλεκτρονικών συζητήσεων» με εξαιρετική ποικιλία θεμάτων προς συζήτηση και παγκόσμια συμμετοχή (πάνω από 10000 ηλεκτρονικές συζητήσεις).

8) Talk

Ανταλλαγή μηνυμάτων κειμένου σε πραγματικό χρόνο μεταξύ δύο χρηστών που βρίσκονται σε απομακρυσμένα σημεία του Internet.

9) IRC (Internet Relay Chat)

Παρόμοιο με το Talk αλλά υποστηρίζει μεγαλύτερο αριθμό χρηστών ταυτόχρονα και οργανώνει τις ομαδικές συνομιλίες ανάλογα με το θέμα τους.

10) Gopher

Αναζήτηση πληροφορίας μέσω επιλογών (menus) σε παγκόσμιο επίπεδο.

11) WAIS (Wide Area Information Service)

Έρευνα μέσα σε επιλεγμένες από το χρήστη βάσεις δεδομένων του Internet σχετικά με λέξεις - κλειδιά που ορίζει ο χρήστης.

12) WWW (World Wide Web)

Διαδικτυωμένες ηλεκτρονικές σελίδες με πληροφορίες σε γραφικό παραθυρικό περιβάλλον, οι οποίες αλληλοσυνδέονται μέσω λέξεων - κλειδιών. Αυτή η υπηρεσία ενοποιεί μέσα στο ίδιο λογισμικό τις FTP, Archie, Gopher, E-mail, Usenet, κλπ.

Εμείς θα εξετάσουμε πιο αναλυτικά την υπηρεσία του DNS και του WWW.

1.3.2 Εφαρμογή DNS.

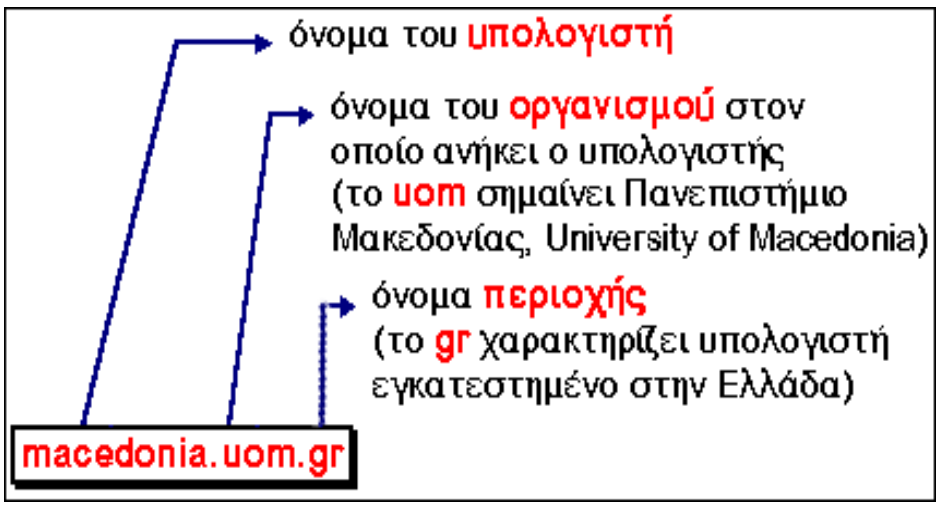
Όπως προείπαμε το πρόβλημα με τις IP διευθύνσεις είναι ότι δύσκολα μπορούμε να τις θυμόμαστε. Αν π.χ. θέλουμε ο υπολογιστής μας να επικοινωνήσει με τον υπολογιστή του MIT με IP διεύθυνση 18.75.0.10, θα πρέπει να θυμόμαστε τον συγκεκριμένο συνδυασμό των τεσσάρων αριθμών.

Ευτυχώς για μας, οι υπολογιστές του Internet μπορούν επίσης να προσδιοριστούν και με ονόματα.

Σε μια διεύθυνση IP αντιστοιχίζεται ένα όνομα που είναι μοναδικό, δηλ. ξεχωριστό για τον κάθε υπολογιστή. Η μέθοδος αυτή είναι γνωστή σαν DNS (Domain Name System).

Π.χ. ο υπολογιστής του MIT που μόλις αναφέραμε είναι γνωστός και σαν space.mit.edu ενώ οι υπολογιστές με IP διευθύνσεις 147.102.154.12 και 193.92.81.104 σαν transport.civil.ntua.gr και macedonia.uom.gr αντίστοιχα.

Ένα όνομα αποτελείται από λέξεις που χωρίζονται μεταξύ τους με τελείες. Ο αριθμός των λέξεων μπορεί να ποικίλει. Στην πράξη συναντάμε συνήθως ονόματα με 3 έως 5 λέξεις.



Σχήμα 1.7: Διαβάζοντας το όνομα ενός υπολογιστή

Το τελευταίο συνθετικό του ονόματος δηλώνει είτε το είδος του οργανισμού είτε τη γεωγραφική περιοχή όπου είναι εγκατεστημένος ο υπολογιστής.

Στις ΗΠΑ χρησιμοποιούνται συνήθως σαν τελευταία συνθετικά κωδικοί 3 γραμμάτων που δηλώνουν το είδος του οργανισμού, όπως φαίνεται παρακάτω:

Όνομα περιοχής 3 γραμμάτων - Είδος οργανισμού

Edu- εκπαιδευτικά ιδρύματα
Com- εμπορικές επιχειρήσεις
Gov- κρατικοί οργανισμοί
mil - στρατιωτικοί οργανισμοί
net - οργανισμοί διαχείρισης δικτύων
org - οργανισμοί που δεν εντάσσονται στις παραπάνω κατηγορίες

Στις υπόλοιπες χώρες, χρησιμοποιούνται ονόματα γεωγραφικών περιοχών που αποτελούνται από 2 γράμματα. Σε κάθε χώρα αντιστοιχεί ένα συγκεκριμένο όνομα 2 γραμμάτων (π.χ. gr για την Ελλάδα, uk για την Αγγλία, κ.λ.π.)

Όνομα περιοχής 2 γραμμάτων Χώρα
au Αυστραλία
ca Καναδάς
de Γερμανία
es Ισπανία
fr Γαλλία
gr Ελλάδα
jp Ιαπωνία
mx Μεξικό
ru Ρωσία
sd Σουδάν
uk Αγγλία

Όπως έχουμε πει, η δρομολόγηση των πακέτων γίνεται με βάση την διεύθυνση IP του παραλήπτη. Όταν λοιπόν ζητάμε να επικοινωνήσουμε με έναν απομακρυσμένο υπολογιστή δίνοντας το όνομά του, ο υπολογιστής μας πρέπει να μάθει την αντίστοιχη διεύθυνση IP. Αν π.χ. πληκτρολογήσουμε macedonia.uom.gr, το όνομα πρέπει να μεταφραστεί στην αντίστοιχη διεύθυνση IP (δηλ. 193.92.81.104).

Η μετάφραση αυτή, είναι δουλειά ενός υπολογιστή που ονομάζεται εξυπηρετητής DNS –Domain Name System (DNS server). Σε κάθε δίκτυο υπάρχει τουλάχιστον ένας υπολογιστής που παρέχει αυτή την υπηρεσία. Ανάλογα με τη θέση του υπολογιστή-παραλήπτη, η αίτηση για μετάφραση του ονόματός του μπορεί να περάσει από έναν ή περισσότερους DNS servers μέχρις ότου εντοπιστεί η αντίστοιχη διεύθυνση IP.[6]

Οι χρήστες Internet σε ολόκληρο τον κόσμο έχουν τη δυνατότητα να χρησιμοποιούν μια ποικιλία υπηρεσιών. Αυτό που είναι σημαντικό να κατανοήσουμε είναι ότι όλοι οι χρήστες, δεν έχουν πρόσβαση στις ίδιες υπηρεσίες.

Προκειμένου να χρησιμοποιήσουμε μια υπηρεσία του Internet θα πρέπει:

να έχουμε εγκατεστημένο στον υπολογιστή μας και να εκτελέσουμε το κατάλληλο πρόγραμμα γι αυτή την υπηρεσία. Το πρόγραμμα αυτό ονομάζεται πελάτης (client). Μέσω του πελάτη, ζητάμε την παροχή της συγκεκριμένης υπηρεσίας. να έχουμε πρόσβαση (μέσω Internet) σε μηχανή που υποστηρίζει την αιτούμενη υπηρεσία. Σε αυτή τη μηχανή πρέπει να εκτελείται ένα πρόγραμμα που παρέχει τη συγκεκριμένη υπηρεσία, ο εξυπηρετητής (server).

Η παροχή των περισσότερων υπηρεσιών στο Internet βασίζεται στο μοντέλο πελάτη-εξυπηρετητή (client-server) που λειτουργεί ως εξής:

Ο πελάτης ζητά από τον εξυπηρετητή πληροφορίες και ο τελευταίος εξυπηρετεί το αίτημα παρέχοντάς του τις πληροφορίες αυτές. Αφού τελειώσει η διαδικασία, ο εξυπηρετητής περιμένει έως ότου κάποιος πελάτης υποβάλλει πάλι κάποια αίτηση για εξυπηρέτηση.

Κάθε υπηρεσία στο Internet έχει το δικό της ξεχωριστό πρωτόκολλο, δηλαδή το δικό της σύνολο από κανόνες που καθορίζουν το πώς γίνεται η "συνομιλία" του αντίστοιχου ζεύγους πελάτη-εξυπηρετητή. Έτσι, άλλα πρωτόκολλο χρησιμοποιεί η υπηρεσία WWW, άλλα η υπηρεσία FTP, άλλα η υπηρεσία E-mail, κ.ο.κ.

Επίσης, σε έναν υπολογιστή μπορούν να εκτελούνται ταυτόχρονα εξυπηρετητές για περισσότερες από μία υπηρεσίες π.χ. ένας εξυπηρετητής για WWW, ένας εξυπηρετητής για FTP, κι ένας εξυπηρετητής για E-mail. Έτσι, ο ίδιος υπολογιστής μπορεί να παρέχει περισσότερες από μία υπηρεσίες.

Υπάρχουν διάφορα προγράμματα - πελάτες για καθεμία από τις υπηρεσίες του Internet για διάφορα λειτουργικά συστήματα. Πολλά από αυτά διατίθενται ελεύθερα μέσω του Internet και μπορούμε να τα μεταφέρουμε στον υπολογιστή μας.

1.3.3.1 Τα πρωτόκολλα POP3 και IMAP;

POP3 (Post Office Protocol)

Το POP3 (Post Office Protocol) είναι ένα πρωτόκολλο που χρησιμοποιείται για τη μεταφορά της εισερχόμενης αλληλογραφίας του χρήστη από το γραμματοκιβώτιο του mail server στον υπολογιστή του χρήστη. Η μεταφορά αυτή γίνεται από ένα άλλο πρόγραμμα που υποστηρίζει το πρωτόκολλο POP3 το οποίο ονομάζεται POP3 server. Πάλι ο χρήστης χρειάζεται έναν Mail client που να διαθέτει το πρωτόκολλο POP3 για να επικοινωνήσει με τον POP3 server που διαχειρίζεται την εισερχόμενη αλληλογραφία του.

Όταν συνδεθεί ο χρήστης και ζητήσει από τον POP3 client να μεταφέρει τα εισερχόμενα μηνύματά του ο client συνδέεται με τον POP3 server και μεταφέρει τα μηνύματα που υπάρχουν στο γραμματοκιβώτιό του, στο δίσκο του υπολογιστή του χρήστη. Οι POP3 clients μεταφέρουν όλα τα μηνύματα του χρήστη χωρίς να υπάρχει η δυνατότητα ανάγνωσης συγκεκριμένων μόνο μηνυμάτων. Μετά την ανάγνωση των μηνυμάτων αυτά διαγράφονται από το γραμματοκιβώτιο του Mail server.[8]

IMAP (Internet Message Access Protocol)

Ένα εναλλακτικό πρωτόκολλο είναι το πρωτόκολλο πρόσβασης μηνυμάτων Διαδικτύου (IMAP). Γενικά το πρωτόκολλο IMAP χρησιμοποιείται για την αποθήκευση (storing) και την ανάκτηση (retrieving) των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails).
Πιο αναλυτικά, το πρωτόκολλο IMAP (Internet Message Access Protocol) αφορά στην εισερχόμενη αλληλογραφία και χρησιμοποιείται μερικές φορές εναλλακτικά αντί του πρωτοκόλλου POP Αξίζει να αναφέρουμε ότι, όταν χρησιμοποιείτε το POP για την εισερχόμενη αλληλογραφία σας, όλα τα μηνύματα μεταφέρονται στον υπολογιστή σας και διαγράφονται από το διακομιστή. Αντίθετα, το IMAP μεταφέρει τα μηνύματα από

το διακομιστή στον υπολογιστή σας, χωρίς να τα διαγράφει. Η μεγάλη ευκολία του IMAP εμφανίζεται, όταν χρησιμοποιείτε διαφορετικούς υπολογιστές για το ηλεκτρονικό σας ταχυδρομείο. Με τον τρόπο αυτό, μπορείτε να διαχειρίζεστε τα μηνύματά σας από οποιονδήποτε υπολογιστή, χωρίς να καταλήγουν σε διαφορετικά μέρη. Το πρωτόκολλο που θα χρησιμοποιήσετε εξαρτάται από την εταιρεία που σας παρέχει το ηλεκτρονικό ταχυδρομείο, αν και στην πλειονότητά τους χρησιμοποιούν το POP. [9]

1.3.5 Η υπηρεσία WWW

Τα αρχικά WWW είναι συντομογραφία της γνωστότερης υπηρεσίας του Internet, του World Wide Web (Παγκόσμιος Ιστός) ή απλά Web. Τα συναντάμε συχνά σαν πρώτο συνθετικό διευθύνσεων, όπως π.χ. www.microsoft.com (η διεύθυνση της εταιρείας Microsoft) ή www.culture.gr (η διεύθυνση του Υπουργείου Πολιτισμού), καθώς κάθε πανεπιστήμιο, εταιρεία ή οργανισμός με παρουσία στο Internet προσφέρει συνήθως την υπηρεσία αυτή.
Το WWW γεννήθηκε στο εργαστήριο CERN της Ελβετίας το 1993 και αποτελεί ένα ισχυρό και εύχρηστο μέσο για την προσπέλαση, αναζήτηση και ανεύρεση πληροφοριών στο Internet. Σήμερα, λέγοντας Internet πολλοί εννοούν το WWW, μιας και το WWW είναι πλέον το επικρατέστερο μέσο για την πλοήγηση στον ωκεανό πληροφορίας του Internet. Το WWW διασύνδεει πληροφορίες που είναι αποθηκευμένες σε χιλιάδες υπολογιστές του Internet, διάσπαρτους σε ολόκληρο τον κόσμο. Οι χρήστες του Διαδικτύου μπορούν να προσπελαύνουν τις διαθέσιμες πληροφορίες χρησιμοποιώντας ένα πρόγραμμα που ονομάζεται browser (πρόγραμμα πλοήγησης).

Οι πληροφορίες είναι οργανωμένες σε ηλεκτρονικές σελίδες που ονομάζονται Web σελίδες (Ιστοσελίδες) και συνδέονται μεταξύ τους με συνδέσμους. Μια συλλογή Web σελίδων που βρίσκεται αποθηκευμένη σε ένα συγκεκριμένο σημείο του Internet και διατίθεται δημόσια ονομάζεται Web site. Η αρχική σελίδα ενός Web site είναι το σημείο εισόδου προς τις υπόλοιπες σελίδες της συλλογής και ονομάζεται home page.

Μπορούμε να φανταστούμε το WWW σαν μια τεράστια βιβλιοθήκη: τα Web sites - κομβικά σημεία του Web - μπορούν να παρομοιαστούν με βιβλία, καθένα από τα οποία αποτελείται από ένα σύνολο σελίδων. Η αρχική σελίδα του Web site μπορεί να παρομοιαστεί με το εξώφυλλο ή τον πίνακα περιεχομένων ενός βιβλίου. Οι σελίδες και οι σύνδεσμοι που τις συνδέουν σχηματίζουν έναν Ιστό (Web) πληροφοριών. Μέσω των συνδέσμων, ο χρήστης έχει τη δυνατότητα να μεταπηδά από μια σελίδα σε άλλες.

Βασικό χαρακτηριστικό του WWW είναι η παγκοσμιότητα του. Οι σελίδες που διασυνδέει μπορεί να βρίσκονται οπουδήποτε στον κόσμο. Σαν τελικοί χρήστες όμως, τις προσπελαύνουμε όλες με ομοιόμορφο τρόπο και έχουμε ίση πρόσβαση προς αυτές, χωρίς πρόσθετα έξοδα μεγάλων αποστάσεων ή περιορισμούς.

Το WWW βασίζεται στην ιδέα του υπερκειμένου (hypertext) ή για την ακρίβεια των υπερ-μέσων (hypermedia).Το υπερκείμενο είναι μια μορφή ηλεκτρονικού κειμένου, κάποια τμήματα (λέξεις ή φράσεις) του οποίου, που συνήθως εμφανίζονται υπογραμμισμένα, συνδέονται με άλλα κείμενα. Αν λοιπόν επιλέξουμε κάνοντας κλικ με το ποντίκι μας τα τμήματα αυτά, τα οποία ονομάζονται υπερσύνδεσμοι (hyperlinks) ή πιο απλά σύνδεσμοι (links), στην οθόνη μας εμφανίζεται το συνδεδεμένο κείμενο. Το κείμενο αυτό με τη σειρά του μπορεί να περιέχει άλλους συνδέσμους προς άλλα κείμενα, κ.ο.κ. Έτσι μπορούμε να ταξιδεύουμε από το ένα κείμενο στο άλλο ακολουθώντας τους συνδέσμους που μας ενδιαφέρουν, χωρίς να είμαστε υποχρεωμένοι να διαβάσουμε τα κείμενα με κάποια προδιαγεγραμμένη σειρά.

1.3.6 HTTP

Όταν ένα πρόγραμμα περιήγησης (web browser) αλληλεπιδρά με ένα διακομιστή του ιστού, τα δύο προγράμματα ακολουθούν το πρωτόκολλο HTTP (Hypertext Transfer Protocol-πρωτόκολλο μεταφοράς υπερκειμένου). Η βασική ιδέα του πρωτοκόλλου HTTP είναι απλή: επιτρέπει σε ένα πρόγραμμα περιήγησης να ζητά ένα συγκεκριμένο στοιχείο, το οποίο ο διακομιστής επιστρέφει. Στην πράξη, όμως το http είναι σύνθετο,

επειδή ένας διακομιστής στέλνει πρόσθετες πληροφορίες κατάστασης μαζί με κάθε απάντηση, και το πρωτόκολλο επιτρέπει σε ένα πρόγραμμα περιήγησης να στέλνει και να ζητά πληροφορίες..

Αρχικά, οι σελίδες του Web περιείχαν υπερκείμενο, δηλαδή κείμενο και συνδέσμους προς άλλες σελίδες που κι αυτές περιείχαν υπερκείμενο. Σιγά - σιγά το υπερκείμενο εμπλουτίστηκε με την ενσωμάτωση πολυμέσων (multimedia) απ' όπου προέκυψε ο συνδυασμός των δύο: τα υπερμέσα (hypermedia). Έτσι σήμερα, οι σελίδες του Web είναι πολύ ελκυστικότερες μιας και μπορεί να περιλαμβάνουν: γραφικά, εικόνες, κινηματογραφικές ταινίες, ήχους, τρισδιάστατους κόσμους και σχεδόν οποιαδήποτε άλλη μορφή ψηφιακής πληροφορίας μπορούμε να φανταστούμε [10].

2. ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

2.1 Το πρόβλημα της ασφάλειας

Το πρόβλημα της ασφάλειας των δεδομένων στο διαδίκτυο θα μπορούσε να περιγραφεί αρκετά καλά με τους παρακάτω όρους : εμπιστευτικότητα (Confidentiality) πιστοποίηση (Authentication) ακεραιότητα (Integrity) και μη άρνηση αποδοχής (Non-Repudiation).

Πιο συγκεκριμένα:

- Εμπιστευτικότητα είναι η διαβεβαίωση ότι μόνο ο επιλεγμένος λήπτης μπορεί να διαβάσει το μήνυμα. Έτσι οποιοσδήποτε τρίτος δεν έχει εξουσιοδότηση δεν μπορεί να έχει πρόσβαση στο περιεχόμενο του.

- Πιστοποίηση είναι η διαδικασία η οποία αποδεικνύει την ταυτότητα κάποιου (δηλαδή ότι αυτός που συνομιλούμε ή συναλλασσόμαστε είναι αυτός που ισχυρίζεται).

- Η ακεραιότητα διαβεβαιώνει τον λήπτη ενός μηνύματος ότι το μήνυμα δεν άλλαξε από κάποιον τρίτο μέχρι να το λάβει. Υπάρχουν μάλιστα «μηχανισμοί» σύμφωνα με τους οποίους ακόμα και μια μικρή επέμβαση στα περιεχόμενα ενός μηνύματος καθιστούν ολόκληρο τα περιεχόμενο του άχρηστο.

- Η μη άρνηση αποδοχής είναι ένας “μηχανισμός” ο οποίος διαβεβαιώνει ότι ο αποστολέας έστειλε το μήνυμα. Με αυτό τον τρόπο σε μία ηλεκτρονική συναλλαγή τα εμπλεκόμενα μέρη δεν έχουν νόμιμο δικαίωμα να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή.

2.1.1 Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ.

Cracking είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους. Η χωρίς δικαίωμα διείσδυση-πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το Άρθρο 370Γ Ποινικού κώδικα.

Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:

- Η Ανακοίνωση Επιτροπής COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων.
- Η Πρόταση Κανονισμού 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.
- Η Πρόταση Απόφασης Πλαισίου του Συμβουλίου COM/2002/0173 - CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεσης μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών.

2.2 Ιοί υπολογιστών

2.2.1 Τι είναι ένας Ιός υπολογιστή;

Ένας ιός (virus) είναι ένα πρόγραμμα που έχει σχεδιαστεί να μεταδίδεται μολύνοντας εκτελέσιμα αρχεία ή περιοχές του συστήματος σε σκληρούς δίσκους και δισκέτες και να κάνει αντίγραφα του εαυτού του. Οι ιοί συνήθως λειτουργούν χωρίς την γνώση ή την επιθυμία του χρήστη του υπολογιστή. Οι ιοί των υπολογιστών είναι οι πιο γνωστές και οι πιο επικίνδυνες απειλές για την ασφάλεια των υπολογιστών.
Όπως και ένας φυσικός ιός, ο ιός του υπολογιστή επιτίθεται στα υγιή προγράμματα και αρχεία του υπολογιστή για να προκαλέσει ζημιά. Υπάρχουν πάνω από 1000 διαφορετικοί τύποι ιών υπολογιστών ενώ η ζημιά που μπορούν να προκαλέσουν ποικίλλει ανάλογα με ποιο μέρος του Η/Υ επιτίθεται.

Τα πιο κοινά συμπτώματα που υποδηλώνουν επίθεση ιού στον υπολογιστή περιλαμβάνουν:

1. Διαγραφή αρχείων και δεδομένων.
2. Ο Η/Υ χρειάζεται περισσότερο χρόνο για να φορτώσει εφαρμογές/ προγράμματα.
3. Τα στοιχεία και οι εικόνες της οθόνης σας παραμορφώνονται και εμφανίζονται ξαφνικά εικονίδια και κείμενο.
4. Ο σκληρός δίσκος λειτουργεί όταν θα έπρεπε να είναι αδρανής.
5. Ο χώρος στον σκληρό δίσκο και τα ονόματα των αρχείων αλλάζουν χωρίς λόγο.
6. Τα εργαλεία συστήματος επιστρέφουν λάθος τιμές.

2.2.2 Τι είδους αρχεία μπορούν να διαδώσουν ιούς;

Οι ιοί έχουν τη δυνατότητα να μολύνουν οποιοδήποτε εκτελέσιμο κώδικα, όχι μόνον τα αρχεία που συνήθως ονομάζονται προγράμματα. Για παράδειγμα, μερικοί ιοί επηρεάζουν τον τομέα εκκίνησης των δισκετών ή των περιοχών του συστήματος. Ένας άλλος τύπος ιού, που είναι γνωστός σαν ιός μακροεντολών, μπορεί να επηρεάσει έγγραφα επεξεργασίας κειμένου και λογιστικά φύλλα που χρησιμοποιούν μακροεντολές. Και είναι δυνατόν HTML έγγραφα που περιέχουν κάποια είδη εκτελέσιμου κώδικα, να διαδώσουν ιούς ή μολυσμένο κώδικα.

Αφού ο κώδικας πρέπει να εκτελεστεί για να έχει κάποια επίδραση, τα αρχεία που χειρίζεται ο υπολογιστής σαν απλά δεδομένα είναι ασφαλή. Αυτό περιλαμβάνει γραφικά και αρχεία ήχου, όπως GIF, JPG, BMP, WAV όπως και απλά αρχεία κειμένου TXT. Για παράδειγμα, όταν απλά βλέπετε αρχεία εικόνων δεν μπορεί να μολυνθεί ο υπολογιστής σας με ένα ιό. Ο κώδικας του ιού πρέπει να είναι σε μια μορφή, όπως ένα .EXE πρόγραμμα ή ένα αρχείο .DOC του Word, που ο υπολογιστής μπορεί να τρέξει μέσω των μακροεντολών.

2.2.3 Πώς διαδίδεται ένας ιός;

Όταν εκτελούμε έναν κώδικα προγράμματος που είναι μολυσμένος από ιό, θα τρέξει επίσης και ο κώδικας του ιού και θα προσπαθήσει να μολύνει άλλα προγράμματα ή στον ίδιο υπολογιστή ή σε άλλους υπολογιστές συνδεδεμένους μαζί του μέσω δικτύου. Και τα νέα μολυσμένα προγράμματα θα προσπαθήσουν να επηρεάσουν ακόμα περισσότερα προγράμματα.
Όταν μοιράζεστε ένα αντίγραφο ενός μολυσμένου αρχείου με άλλους χρήστες, η εκτέλεση του αρχείου μπορεί να επηρεάσει τους υπολογιστές τους και τα αρχεία από αυτούς τους υπολογιστές μπορούν να μολύνουν ακόμα περισσότερους υπολογιστές. Αν ο υπολογιστής μολυνθεί με ένα ιό στον τομέα εκκίνησης, ο ιός θα προσπαθήσει να κάνει αντίγραφα του εαυτού του στις περιοχές του συστήματος των δισκετών και του

σκληρού δίσκου. Μετά, η μολυσμένη δισκέτα μπορεί να επηρεάσει άλλους υπολογιστές, οι οποίοι ξεκινούν από αυτήν και το αντίγραφο του ιού στο σκληρό δίσκο θα προσπαθήσει να μολύνει και άλλες δισκέτες.
Μερικοί ιοί, που είναι γνωστοί σαν multipartite ιοί, μπορούν να διαδοθούν μολύνοντας αρχεία και μολύνοντας τις περιοχές εκκίνησης των δισκετών.

2.2.4 Τύποι ιών υπολογιστών

Υπάρχουν διάφοροι τύποι ιών στους υπολογιστές, όπως:

1. Ιοί αρχείων: αυτοί οι ιοί είναι ουσιαστικά προγράμματα οι ίδιοι. Μολύνουν άλλα εκτελέσιμα αρχεία (συνήθως με επέκταση αρχείου .COM ή .EXE), και όταν εκτελείτε ένα από αυτά τα αρχεία, ενεργοποιείται ταυτόχρονα και ο ιός. Αυτοί οι ιοί διαδίδονται όταν μοιράζεστε τα μολυσμένα αρχεία προγράμματος, είτε μέσω δισκέτας είτε μέσω δικτύων.

2. Ιοί τομέα εκκίνησης (boot sector): Αυτοί οι ιοί είναι αρκετά κοινοί, αλλά μπορεί κάποιος να τους αποφύγει σχετικά εύκολα. Ένας ιός τομέα εκκίνησης μετακινείται σε ένα νέο τομέα όταν μια μολυσμένη δισκέτα, που αφήνεται τυχαία στον οδηγό δισκέτας και αλλάζει θέση όταν ανοιχτεί ο υπολογιστής. Ο υπολογιστής προσπαθεί να ξεκινήσει από τη δισκέτα, και ο ιός μετακινείται από τη δισκέτα στο σύστημα.

3. Πολυμερείς ιοί (multipartite): αυτός ο τύπος του ιού αποτελείται από έναν κακοήθη συνδυασμό και χαρακτηριστικών ιών τομέα εκκίνησης και ιών αρχείων.

4. Ιοί μακροεντολών: αυτοί είναι οι πιο κοινοί ιοί που χτυπούν τους υπολογιστές σήμερα. Ενώ μερικοί μπορούν να είναι καταστρεπτικοί, αφού αυτοί του τύπου οι ιοί κάνουν τα ενοχλητικά πράγματα, όπως η μετατροπή των εγγράφων επεξεργασίας κειμένου σας σε πρότυπα ή τυχαία αντικατάσταση μιας λέξης με μια άλλη άσχετη λέξη, όπως Wazoo, σε όλο το έγγραφο. Ενώ αυτές οι ενέργειες

μπορούν να μην βλάψουν μόνιμα τα στοιχεία, μπορούν να βλάψουν την παραγωγικότητα σας. Οι λόγοι της διάδοσης αυτών των ιών και οι λόγοι που είναι τόσο ενοχλητικοί, είναι διπλοί: είναι εύκολο να γραφθούν και υπάρχουν στα προγράμματα που δημιουργούνται για τη διανομή μέσω δικτύου ή διαδικτύου.

Οι παραδοσιακοί ιοί είναι σε θέση να πολλαπλασιάζουν τον εαυτό τους σε ένα σύστημα, ωστόσο χρειάζονται την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν.

Όμως, τα τελευταία χρόνια το νεότερο malware, Trojan Horses (Δούρειοι Ίπποι) και worms (σκουλήκια), είναι πιο πολυδιάστατο από τους προγόνους του και χαρακτηρίζεται κυρίως από τις δυνατότητές του για αυτόματη εξάπλωση (μέσω Internet, e-mail, IRC, NETBIOS κ.λπ.).

Τα Trojan Horses έχουν πάρει το όνομά τους από το Δούρειο Ίππο, κυρίως λόγω των ομοιοτήτων που παρουσιάζουν στον τρόπο λειτουργίας τους, αφού συνήθως μεταμφιέζονται σε κάτι χρήσιμο για το χρήστη και περιμένουν την κατάλληλη στιγμή για να ανοίξουν τις πύλες, που εν προκειμένω δεν είναι άλλες από τα ports του υπολογιστή.

Αξίζει να σημειωθεί ότι τα καθαρόαιμα προγράμματα Trojan (δηλαδή τα πρώτα Trojans που δεν ενσωματώνουν λειτουργίες ιού) δεν πολλαπλασιάζουν τον εαυτό τους στο μολυσμένο σύστημα.

Ειδικότερα, τα Trojan Horse καλείται το πρόγραμμα που, ενώ εμφανίζεται απόλυτα ακίνδυνο για το χρήστη, έχει έμμεσες ή άμεσες καταστρεπτικές συνέπειες για τον υπολογιστή, επιτρέποντας σε έναν ή περισσότερους crackers να έχουν πρόσβαση σε αυτόν.

Με το πρόσχημα των δωρεάν γραφικών, αστείων εικόνων, video κ.λπ., το Trojan Horse ξεγελά το χρήστη, ώστε να το τρέξει, και κατόπιν δημιουργεί ένα backdoor (σημείο πρόσβασης) με ανοιχτά δικαιώματα χρήσης.

Ένα τυπικό Trojan αποτελείται από δύο συστατικά μέρη-υποπρογράμματα: ένα client και ένα server. Αυτός που θέλει να αποκτήσει πρόσβαση σε κάποιον υπολογιστή εκτελεί το τμήμα client του Trojan και παράλληλα φροντίζει ώστε το τμήμα server να είναι εγκατεστημένο και ενεργό στο σύστημα.

Γνωστά προγράμματα Trojan είναι ο Sub7, το Netbus (με όλα τα παράγωγά του), ενώ το είδος, ο σκοπός χρήσης και η τεχνολογία αυτής της κατηγορία προγραμμάτων παρουσιάζει εντυπωσιακή ποικιλία [11].
Τα worms, από την άλλη πλευρά, πολλαπλασιάζονται - ωστόσο σε αντίθεση με τους παραδοσιακούς ιούς, δεν απαιτούν την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν από το ένα σύστημα στο άλλο. Η επικινδυνότητα των worms έγκειται στο ότι επιτρέπουν μια ποικιλία επιθέσεων μέσω του Internet.
Για παράδειγμα, ένα καλογραμμένο worm μπορεί να αναζητήσει μόνο του συστήματα που παρουσιάζουν μια συγκεκριμένη αδυναμία στην ασφάλειά τους, να τα μολύνει και να περιμένει την κατάλληλη στιγμή για να εκκινήσει μια συγχρονισμένη επίθεση DoS (Denial of Service) σε έναν καθορισμένο στόχο.

Στις μέρες μας -σε αντίθεση με το πρόσφατο παρελθόν- ο μέσος χρήστης είναι ενήμερος για τους κινδύνους που παρουσιάζουν τα συνημμένα αρχεία e-mail, ωστόσο η εξέλιξη στον χώρο των ιών είναι τέτοια που ακόμα και ένα κλικ σε ένα φαινομενικά αθώο link μιας ιστοσελίδας μέσα από τη χρήση ActiveX περιεχομένου μπορεί να επιτρέψει την εκτέλεση προγραμμάτων στον υπολογιστή.

2.3 Ηλεκτρονική κατασκοπεία

Μία άλλη απειλή για τους χρήστες υπολογιστών οι οποίοι χρησιμοποιούν το διαδίκτυο είναι τα λεγόμενα spywares. Τα προγράμματα spyware, όπως προδίδει και η ονομασία τους, έχουν ένα σκοπό την υποκλοπή πληροφοριών. Για παράδειγμα τα adware είναι ένας τύπος λογισμικού spyware τα οποία αποστέλλουν ανά τακτά χρονικά διαστήματα αναφορές σχετικές με τη δικτυακή δραστηριότητα του χρήστη σε διαφημιστικές εταιρείες. Δεν είναι όμως όλα τόσο ‘αθώα’ όπως παρουσιάστηκαν μέχρι τώρα, τα spywares μπορούν να αποβούν μοιραία όπως π.χ. στην περίπτωση των key loggers.Τα key loggers είναι προγράμματα τύπου spyware τα οποία καταγράφουν οτιδήποτε πληκτρολογείται από το χρήστη κάτι το οποίο είναι πολύ επικίνδυνο στην περίπτωση

που πληκτρολογούνται passwords ή αριθμοί πιστωτικών καρτών (Σημείωση: υπάρχουν και hardware key loggers τα οποία δρουν με τον ίδιο ακριβώς τρόπο). Πολλοί θεωρούν και τα Trojan horses που αναφέρθηκαν πιο πριν ως ένα είδος spyware αφού ανοίγουν διόδους ώστε να μπορεί ένας cracker να αποκτήσει πρόσβαση στα δεδομένα ενός υπολογιστή.

Ακόμα και τα πιο ακραία μέτρα ασφαλείας δεν μπορούν να εγγυηθούν την απόλυτη ασφάλεια. Μόνο η συνδυαστική χρήση μιας πληθώρας εργαλείων μπορεί να εξασφαλίσει την διατήρηση της ασφάλειας και της ανωνυμίας κατά τη διάρκεια της σύνδεσης στο Internet.

2.4 Phising

Το phishing είναι η αποστολή e-mail σε χρήστη, προσποιούμενο ότι προέρχεται από μία νόμιμη επιχείρηση, με σκοπό να εξαπατήσει τον χρήστη και να πάρει ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για την κλοπή της ταυτότητάς του. Το e-mail προτρέπει το χρήστη να επισκεφθεί ένα web-site, το οποίο είναι πλαστό και έχει δημιουργηθεί με μοναδικό σκοπό την υποκλοπή πληροφοριών, όπου του ζητείται να ενημερώσει τις προσωπικές του πληροφορίες όπως αριθμούς πιστωτικών καρτών, passwords κλπ, που υποτίθεται ότι η εταιρία έχει ήδη στην κατοχή της.

2.5 Pharming

Καθώς οι χρήστες γίνονται όλο και πιο προσεκτικοί οι επιτήδειοι προχώρησαν ένα βήμα παραπέρα. Η νέα τεχνική ονομάζεται pharming και βασίζεται σε δηλητηρίαση του DNS προκειμένου να ξεγελάσουν το χρήστη σχετικά με τα site το οποίο επισκέπτεται. Η pharming επίθεση γενικά προσπαθεί να πείσει τον χρήστη ότι βλέπει ένα πραγματικό site (π.χ. της Citibank), ενώ στην ουσία βλέπει ένα πλαστό, το οποίο έχει δημιουργηθεί με μοναδικό σκοπό την υποκλοπή προσωπικών δεδομένων, που εν συνεχεία θα χρησιμοποιηθούν για να προκαλέσουν ζημιά

3. ΚΡΥΠΤΟΓΡΑΦΙΑ

3.1 Ορισμοί

3.1.1 Κρυπτογράφηση

Η ανάγκη για ασφάλεια των πληροφοριών στις ηλεκτρονικές συναλλαγές ικανοποιείται με την *κρυπτογράφηση*. Κρυπτογράφηση ονομάζεται η επιστήμη η οποία ασχολείται με την μετατροπή ενός μηνύματος σε μη αναγνώσιμη μορφή για οποιοδήποτε τρίτο ο οποίος δεν πρέπει να έχει πρόσβαση στο περιεχόμενο του. Με την κρυπτογράφηση ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης, έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Έτσι το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί.

3.1.2 Plaintext – Chiphertext

Plaintext ονομάζεται το απλό κείμενο πριν την κρυπτογράφηση ενώ ciphertext ονομάζεται το κείμενο που προκύπτει μετά την κρυπτογράφηση του plaintext.

3.1.3 Κρυπτανάλυση

Παράλληλα με την κρυπτογραφία γεννήθηκε και μία άλλη επιστήμη η *κρυπτανάλυση*. Κρυπτανάλυση ονομάζεται η προσπάθεια για απόκτηση του περιεχομένου ενός κρυπτογραφημένου μνήματος χωρίς την γνώση του τρόπου κρυπτογράφησης του. Λόγω της κρυπτανάλυσης η κρυπτογραφία θα “μεταλλάσσεται” συνεχώς και θα επινοούνται όλο και πιο περίπλοκοι αλγόριθμοι – κλειδιά με σκοπό την ασφάλεια των

δεδομένων στο διαδύκτιο. Αρκεί μια σύντομη ιστορική αναδρομή για να γίνει το γεγονός αυτό κατανοητό.

3.2 Η ιστορία της κρυπτογραφίας

Η λέξη κρυπτογραφία (cryptography) είναι σύνθετη. Το πρώτο συνθετικό της είναι το «κρυπτο» και στην αρχαία αλλά και σύγχρονη Ελληνική γλώσσα σημαίνει κρύβω. Το δεύτερο συνθετικό είναι το «γραφία» που βγαίνει από το γράφω. Άρα λοιπόν κρυπτογραφία σημαίνει κρύβω αυτά που γράφω. Η κρυπτογραφία λοιπόν είναι η επιστήμη ή τέχνη της απόκρυψης του γραπτού λόγου από ανεπιθύμητους αναγνώστες. Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα που ήταν από τους πρώτους που την χρησιμοποίησαν ευρύτατα για στρατιωτικούς σκοπούς. Έτσι όλα τα μηνύματα του Καίσαρα προς τους στρατηγούς των λεγεώνων του ήταν κρυπτογραφημένα ώστε ο εκάστοτε εχθρός να μην είναι σε θέση να γνωρίζει τα σχέδια του, ακόμη και αν ο αγγελιοφόρος έπεφτε στα χέρια του εχθρού. Ο τρόπος κρυπτογράφησης ήταν απλός. Αν ήθελε για παράδειγμα να μεταφέρει την εντολή ΕΠΙΘΕΣΗ έστελνε την λέξη ΗΣΛΚΗΥΙ πού προέκυπτε αν κάθε γράμμα της αρχικής λέξης το αντικαθιστούσε με το μεθεπόμενο γράμμα στο αλφάβητο. Ο παραλήπτης στρατηγός δεν είχε παρά να αντικαταστήσει κάθε γράμμα του μηνύματος με το προ-προηγούμενο γράμμα της αλφαβήτου. Οι εξόριστοι Ιουδαίοι γραφείς στη Βίβλο του Ιερεμία πολλές φορές έκρυβαν την λέξη ΒΒαβυλώνα σύμφωνα με τον κώδικα του Ατμπάς (αντικαθιστούσαν τα γράμματα του εβραϊκού αλφάβητου με τα αντίθετά τους στο δικό μας αλφάβητο θα το Α αντικαθίσταται με το Ω, το Β με το Ψ κ.ο.κ. Έτσι η λέξη ΒΑΒΥΛΩΝΑ γινόταν ΨΩΨΞΑΜΩ). Στην αρχαία Σπάρτη για την αποστολή απόρρητων στρατιωτικών μηνυμάτων, το μήνυμα γραφόταν σ' ένα κύλινδρο που γύρω του είχε τυλιχτεί μία στενή λωρίδα δέρματος σε διαδοχικές σειρές. Αυτή ήταν η περιβόητη σκυτάλη. Ο κύλινδρος αφαιρούνταν κι έμενε η λωρίδα που μπορούσε να ξαναδιαβαστεί μόνο αν τυλιγόταν με τον ίδιο τρόπο πάνω σε ολόιδιας διαμέτρου κύλινδρο. Κάθε άλλη διαφορετική διάμετρος κυλίνδρου έδινε ακατανόητα μηνύματα. Πολλές φορές γραφόταν σε συνδυασμό με καθρέπτη, ώστε να απαιτείται καθρέπτης και στην ανάγνωση. Άλλη

απλούστερη μέθοδος ήταν η αντιστροφή συλλαβών όπως "δημοκρατία" που θα φαινόταν σαν "ηδομαρκίτα". Στην αρχαία Κίνα το μήνυμα γραφόταν σε λεπτή μεταξωτή κορδέλα η οποία τυλιγόταν σαν μικρό μπαλάκι και καλυπτόταν με κερί. Το μικρό κέρινο μπαλάκι το κατάπινε ο αγγελιοφόρος και έτσι το μετέφερε με την μέγιστη δυνατή ασφάλεια. Το αόρατο μελάνι ήταν μία ακόμα μέθοδος που χρησιμοποιούταν αρκετά. Πάνω συνήθως από κάποιο άλλο κείμενο αδιάφορου περιεχομένου γραφόταν με χυμό λεμονιού αντί για μελάνι το κρυφό μήνυμα. Μετά μπορούσε να διαβαστεί στο φως κεριού μόνο από τον υποψιασμένο παραλήπτη.

Ακόμα και βρασμένα αυγά χρησιμοποιήθηκαν για την ασφαλή μεταφορά μηνυμάτων. Τον 16ο αιώνα στην Ιταλία ο Τζιοβάνι Πόρτα έγραφε με μελάνι φτιαγμένο από σκόρδο και ξύδι πάνω στο τσόφλι του αβγού. Το μελάνι απορροφούταν στο εσωτερικό και εξωτερικά δεν φαινόταν τίποτα. Το μήνυμα όμως παρέμενε αποτυπωμένο πάνω στο ασπράδι του βρασμένου αβγού.

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους. Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά. Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών.

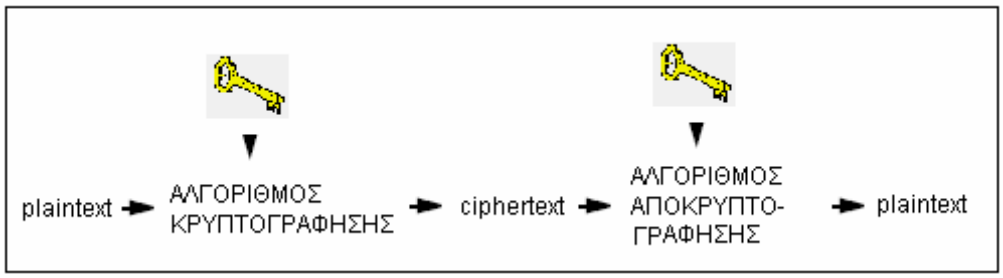
Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξ’ αιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Από την δεκαετία του 60 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω την ραγδαίας ανάπτυξης των υπολογιστών αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν υπήρξε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή, το DES, το πρότυπο κρυπτογράφησης στοιχείων, είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός της ιστορίας. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο. Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια τής κρυπτογραφίας δημοσίου κλειδιού και παρείχε επίσης μια νέα και έξυπνη μέθοδο για ανταλλαγή κλειδιού, η ασφάλεια του οποίου βασίζεται στην αμεταβλητότητα του προβλήματος διακριτού λογαρίθμου. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές. Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.

3.3 Πως λειτουργούν τα κρυπτογραφικά συστήματα

Η λειτουργία των κρυπτογραφικών συστημάτων έχει ως εξής : ο αποστολέας του μηνύματος χρησιμοποιώντας ένα κλειδί κρυπτογράφησης και με τη βοήθεια ενός αλγόριθμοy κρυπτογράφησης μετατρέπει το plaintext σε ciphertext.Στη συνέχεια ο παραλήπτης του ciphertext χρησιμοποιεί ένα αλγόριθμο και ένα κλειδί αντίστοιχα και αποκτά το plaintext. Η όλη διαδικασία περιγράφεται στο παρακάτω σχήμα



Σχήμα 3.1 Ο τρόπος λειτουργίας της κρυπτογραφίας

Στο σημείο αυτό πρέπει να σημειωθεί ότι όταν χρησιμοποιείται ο όρος ‘κλειδί’ στην ουσία εννοούμε μία ακολουθία αριθμών καθένας από τους οποίους παίρνει τιμές από 0 έως 255 (bytes). Επίσης το μήκος του κλειδιού εξαρτάται από τον αλγόριθμο που χρησιμοποιήθηκε για την παραγωγή του.

Υπάρχουν πολλοί τρόποι με τους οποίους μπορούν να κατηγοριοποιηθούν τα κρυπτογραφικά συστήματα, ο πιο σημαντικός όμως είναι ανάλογα με τον αριθμό των κλειδιών που χρησιμοποιούν.

3.3.1 Συμμετρική Κρυπτογραφία

Σύμφωνα με την συμμετρική κρυπτογραφία ο αποστολέας του μηνύματος χρησιμοποιεί ένα κλειδί, κρυπτογραφεί το μήνυμα και στη συνέχεια ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί και αποκρυπτογραφεί το μήνυμα. Δηλαδή χρησιμοποιείται το ίδιο κλειδί κατά την κρυπτογράφηση και κατά την αποκρυπτογράφηση του μηνύματος.

3.3.2 Ασύμμετρη Κρυπτογραφία

Αντίθετα η ασύμμετρη κρυπτογραφία χρησιμοποιεί ένα ζεύγος μαθηματικά συνδεδεμένων κλειδιών. Πιο συγκεκριμένα παράγονται δύο κλειδιά, το δημόσιο και το ιδιωτικό. Με αυτό τον τρόπο κάποιος γνωστοποιεί το δημόσιο κλειδί του ενώ παράλληλα κρατάει μυστικό το ιδιωτικό κλειδί του. Στη συνέχεια αν κάποιος θέλει να επικοινωνήσει μαζί του χρησιμοποιεί το δημόσιο κλειδί και κρυπτογραφεί τα δεδομένα, τα αποστέλλει και στη συνέχεια ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί και τα αποκρυπτογραφεί. Τα δεδομένα που κρυπτογραφούνται με το δημόσιο κλειδί αποκρυπτογραφούνται μόνο με το ιδιωτικό γι’ αυτό και η ευρεία γνωστοποίηση του δημοσίου κλειδιού δεν αποτελεί κίνδυνο για την ασφάλεια των δεδομένων.

3.3.3 Αλγόριθμοι κατακερματισμού

Τέλος υπάρχουν και οι αλγόριθμοι κατακερματισμού (hash functions). Σύμφωνα με αυτό τον τρόπο κρυπτογραφίας ο αλγόριθμος παίρνοντας σαν είσοδο το plaintext το μετατρέπει σε μία καθορισμένου μήκους τιμή κατακερματισμού (hash value), έτσι θα έλεγε κανείς ότι δεν χρησιμοποιείται καθόλου κλειδί. Με τη χρήση των αλγόριθμων κατακερματισμού το περιεχόμενο καθώς και το μέγεθος του plaintext είναι αδύνατο να ανακτηθούν από το chiphertext, επίσης είναι σχεδόν αδύνατο ότι δύο διαφορετικά plaintext θα έχουν την ίδια τιμή κατακερματισμού.

3.3.4 Η χρησιμότητα των τριών διαφορετικών τρόπων κρυπτογράφησης

Ο λόγος που χρησιμοποιούνται τρεις διαφορετικοί τρόποι κρυπτογράφησης είναι ότι ο καθένας είναι ιδανικός για διαφορετικές εφαρμογές. Για παράδειγμα οι αλγόριθμοι κατακερματισμού είναι ιδανικοί για ακεραιότητα δεδομένων, γιατί οποιαδήποτε αλλαγή γίνει στα περιεχόμενα του μηνύματος θα οδηγήσει στην αλλαγή ολόκληρου του μηνύματος. Η συμμετρική κρυπτογραφία βρίσκει εφαρμογή στην ανταλλαγή μηνυμάτων γιατί είναι πολύ πιο γρήγορη από την ασύμμετρη κρυπτογραφία ενώ η τελευταία έχει τη δυνατότητα να παρέχει μη άρνηση αποδοχής αφού αν ο παραλήπτης μπορεί να λάβει το δημόσιο κλειδί ,το οποίο παράγεται με τη χρήση του ιδιωτικού κλειδιού, τότε μόνο ο αποστολέας θα μπορούσε να είχε στείλει το μήνυμα.

3.4 Βασικές έννοιες της κρυπτογραφίας

Παρακάτω περιγράφονται ορισμένες βασικές έννοιες ώστε να γίνουν κατανοητές στη συνέχεια οι διάφορες τεχνικές κρυπτογράφησης

3.4.1 Message Authentication Code (MAC)

Το Μ.Α.C. είναι ένα μικρό κρυπτογραφημένο μήνυμα το οποίο εγγυάται για την ακεραιότητα ενός μηνύματος και πιστοποιεί την ταυτότητα του αποστολέα. Το Μ.Α.C. προκύπτει από το αρχικό μήνυμα σε συνδυασμό με ένα συμμετρικό κλειδί. Έτσι οποιαδήποτε αλλαγή στο μήνυμα θα πρέπει να παράγει διαφορετικό Μ.Α.C. και με αυτό τον τρόπο διασφαλίζεται η ακεραιότητα του περιεχομένου του μηνύματος Επίσης το γεγονός ότι μόνο κάποιος που γνωρίζει το συμμετρικό κλειδί μπορεί να παράγει ένα έγκυρο Μ.Α.C. πιστοποιεί την ταυτότητα του αποστολέα του μηνύματος.

3.4.2 Ψηφιακή Υπογραφή

Ως ψηφιακή υπογραφή, νοείται κάθε "κλειδωμένη" σύντμηση ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του. Έχει επιβεβαιωτική λειτουργία (ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις) και εμπιστευτική λειτουργία (μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα).

Η χρήση της ψηφιακή υπογραφή περιλαμβάνει δύο στάδια: τη δημιουργία /μετάδοση και την επαλήθευσή της. Παρακάτω περιγράφονται οι ενέργειες του αποστολέα και του παραλήπτη.

Ο αποστολέας

1. Δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού.
2. Με το ιδιωτικό του κλειδί κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδεται μέσω του διαδικτύου

Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη -με το ιδιωτικό κλειδί του αποστολέα- σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. Συγκρίνονται οι δύο συνόψεις και, αν βρεθούν ίδιες, το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

Σε αντιδιαστολή με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ψηφιακή υπογραφή διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα, αφού προκύπτει και βάσει αυτών.

3.4.3 Πιστοποίηση της ψηφιακής υπογραφής

Με τη λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης, όμως, πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος (ο κάτοχος δηλαδή του ιδιωτικού κλειδιού) είναι όντως αυτός που ισχυρίζεται ότι είναι. Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή, και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται, δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί.

Ο Παροχός Υπηρεσιών Πιστοποίησης, η αλλιώς αρχή πιστοποίησης (Certificate Authority), είναι ο "οργανισμός" που βεβαιώνει με ακρίβεια τη σχέση ενός φυσικού προσώπου με το δημόσιο κλειδί του, με την έκδοση ενός ηλεκτρονικού

πιστοποιητικού, στο οποίο ο Παροχός Υπηρεσιών Πιστοποίησης (ΠΥΠ) πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Κύριος τύπος ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificates). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Η συσχέτιση ενός δημόσιου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του ΠΥΠ, ο οποίος υπογράφει το πιστοποιητικό του δικαιούχου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο ΠΥΠ δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου.

Η ψηφιακή υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα, και αποτελεί την ψηφιακή τους «ετικέτα». Βασικοί στόχοι είναι:

1. Η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει (πιστοποίηση)
2. Η εγγύηση της γνησιότητας των ψηφιακών δεδομένων (ακεραιότητα) και
3. Η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, ότι δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί τη συμμετοχή του στην εν λόγω συναλλαγή (μη άρνηση αποδοχής) [12].

3.4.4 Τρόποι κρυπτογράφησης

Τα κρυπτογραφικά συστήματα (ciphers), σύμφωνα με τον τρόπο που κρυπτογραφούν, μπορούν να χωριστούν σε δύο κατηγορίες, τα stream και τα block ciphers. ***Τα block ciphers*** κρυπτογραφούν το plaintext ανά κομμάτια (blocks) συνήθως μεγέθους 64 και 128 bits.Αντίθετα τα ***stream ciphers*** κρυπτογραφούν το κάθε bit ή byte του plaintext χωριστά.

3.4.4.1 XOR

Η XOR μέθοδος είναι πιθανότατα ο πιο εύκολος τρόπος κρυπτογράφησης. Βασικά πρόκειται για ένα αλγόριθμο συμμετρικής κρυπτογράφησης ο οποίος όμως δεν παρέχει υψηλό επίπεδο ασφάλειας από μόνος του, ωστόσο η μέθοδος XOR ενσωματώνεται μέσα στη λειτουργία αλγόριθμων οι οποίοι παρέχουν υψηλά επίπεδα ασφάλειας. Για την πιο εύκολη κατανόηση του τρόπου που συνδυάζει τα δεδομένα η μέθοδος XOR δίνεται το παρακάτω παράδειγμα :

Έστω ότι έχουμε το παρακάτω plaintext : 70 65 81
αυτό μεταφράζεται σε δυαδική μορφή σε : 01110000 01100101 1000000

Έστω τώρα ότι έχουμε το παρακάτω κλειδί : 86
Το οποίο σε δυαδική μορφή είναι το : 10000110

Ο παρακάτω πίνακας δείχνει την κρυπτογράφηση του πρώτου byte από το plaintext :

plaintext	Κλειδί	chiphertext
0	1	1
1	0	1
1	0	1
1	0	1
0	0	0
0	1	1
0	1	0
0	0	0

Πίνακας 3.2: Κρυπτογράφηση του πρώτου byte

Με άλλα λόγια όταν τα αντίστοιχα bits έχουν την ίδια τιμή παίρνουμε σαν αποτέλεσμα την τιμή 0 ενώ αν έχουν διαφορετική τότε παίρνουμε σαν αποτέλεσμα την τιμή 1.

3.4.4.2 Η λειτουργία modulo

Η λειτουργία modulo είναι η εξής : έστω ότι θέλουμε να υπολογίσουμε y mod x (y modulo x) αφαιρούμε από τον y όλα τα πολλαπλάσια του x και κρατάμε το υπόλοιπο. Έτσι για παράδειγμα έχουμε :

15 mod 7 = 1
25 mod 5 = 0
33 mod 12 = 9
203 mod 256 = 203

3.4.4.3 Τρόποι λειτουργίας

Κατά τη διάρκεια της κρυπτογράφησης τα block ciphers χρησιμοποιούν διάφορες τεχνικές γνωστές ως τρόποι λειτουργίας. Προκειμένου να είναι χρήσιμο ένα mode πρέπει να είναι τουλάχιστον τόσο αποδοτικό και τόσο ασφαλές όσο το block cipher. Οι κυριότεροι τρόποι λειτουργίας οι οποίοι περιγράφονται παρακάτω είναι : ο Electronic

Code Book (ECB), ο Cipher Block Chaining (CBC), ο Cipher Feedback (CFB), και ο Output Feedback (OFB).

Electronic Code Book (ECB)

Όταν χρησιμοποιείται αυτός ο τρόπο λειτουργίας το κάθε block κρυπτογραφείται ξεχωριστά. Με τον τρόπο ECB δεν χρησιμοποιείται ανατροφοδότηση. Αυτό σημαίνει ότι δυο ίδια blocks είτε ανήκουν στο ίδιο plaintext είτε σε διαφορετικό, από τη στιγμή που θα κρυπτογραφηθούν με το ίδιο κλειδί θα δώσουν το ίδιο κομμάτι chiphertext (chiphertext block). Επίσης πρέπει να αναφερθεί ότι εάν ένα bit ενός chiphertext block αλλοιωθεί τότε όλο το περιεχόμενο του chiphertext block θα αλλοιωθεί. Με το ECB τρόπο λειτουργίας δίνεται η δυνατότητα σε κάποιον τρίτο που έχει την πρόθεση και την δυνατότητα να αλλάξει μέρος του περιεχομένου του chiphertext χωρίς να γίνει αντιληπτός. Αυτό μπορεί να το καταφέρει αλλάζοντας κομμάτια (blocks) του chiphertext.

Cipher Block Chaining Mode (CBC)

Αυτό το mode χρησιμοποιεί ανατροφοδότηση. Πιο συγκεκριμένα πριν κρυπτογραφηθεί το κάθε block συνδυάζεται με το chiphertext του προηγούμενου block με την μέθοδο XOR. Έτσι αυτό που επιτυγχάνεται είναι ότι ακόμα και αν υπάρχουν πολλά ίδια blocks στο plaintext μετά την κρυπτογράφηση τα αντίστοιχα chiphertext blocks θα διαφέρουν μεταξύ τους. Όπως και στον τρόπο ECB έτσι και στην περίπτωση του CBC εάν ένα bit ενός block αλλοιωθεί τότε αλλοιώνεται όλο το περιεχόμενο του block, μόνο που σε αυτή την περίπτωση θα αλλοιωθεί μαζί με αυτό το block και το περιεχόμενο των block που ακολουθούν. Τα λάθη κατά την μετάδοση των δεδομένων είναι αναπόφευκτα γι' αυτό και εάν λείπει έστω και ένα byte από το chiphertext το περιεχόμενο του plaintext δεν μπορεί να ανακτηθεί από εκείνο το σημείο και μετά.

Cipher Feedback mode (CFB)

Με τον τρόπο λειτουργίας CFB το προηγούμενο chiphertext block κρυπτογραφείται και το αποτέλεσμά του συνδυάζεται με το plaintext με τη μέθοδο XOR παράγοντας το παρόν ciphertext block. Είναι δυνατό να ρυθμιστεί ο CFB τρόπος λειτουργίας ώστε να χρησιμοποιεί ανατροφοδότηση η οποία να είναι μικρότερη του ενός block.

Output Feedback mode (OFB)

Ο τρόπος λειτουργίας OFB μοιάζει πολύ με το CFB με τη διαφορά ότι η ποσότητα που συνδυάζεται με τη μέθοδο XOR με κάθε plaintext block παράγεται ξεχωριστά από το plaintext και το chiphertext του προηγούμενου block. Το κυριότερο πλεονέκτημα του OFB έναντι του CFB είναι ότι τυχόν λάθη στα bit του chiphertext κατά τη μετάδοση δεν επηρεάζουν το περιεχόμενο των επόμενων blocks.

3.5 Αλγόριθμοι Κρυπτογράφησης

Παρακάτω περιγράφεται ένας αντιπροσωπευτικός αλγόριθμος από κάθε κατηγορία ώστε να γίνει κατανοητή η λειτουργία τους.

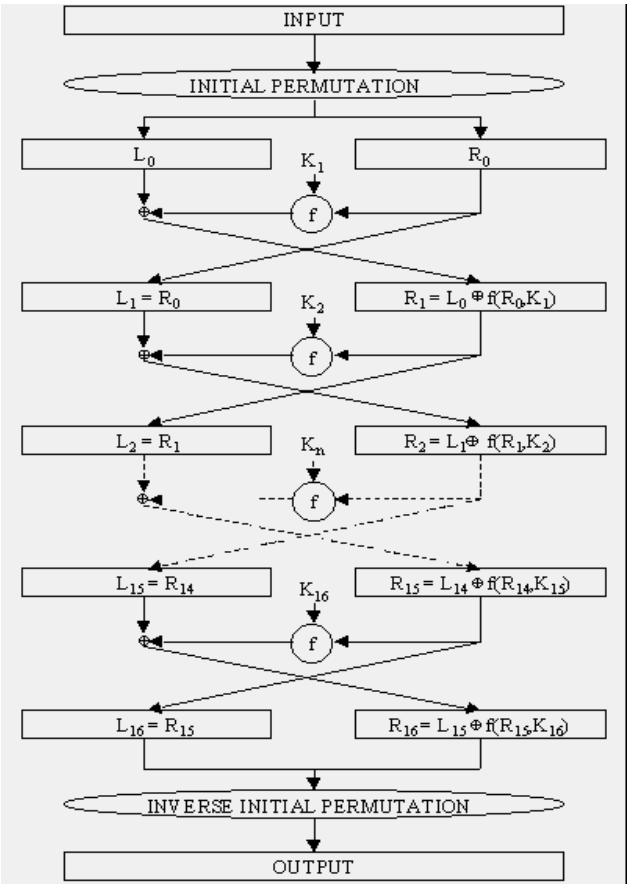
3.5.1 DES

Ο DES είναι ένας αλγόριθμος κρυπτογράφησης ο οποίος σχεδιάστηκε κατά τη δεκαετία του 1970 και χρησιμοποιείται μέχρι και τις μέρες μας. Ο DES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ο οποίος αρχικά σχεδιάστηκε να λειτουργεί με τη μορφή hardware από την N.S.A. Κάποια στιγμή η N.S.A. έδωσε πληροφορίες σχετικά με τον τρόπο που λειτουργεί ο DES και έτσι ο DES μπόρεσε και γράφτηκε σε μορφή λογισμικού. Πολλοί ισχυρίζονται ότι η γνωστοποίηση του τρόπου που λειτουργεί ο DES είναι ίσως το μεγαλύτερο λάθος της N.S.A.

Ο DES είναι ένα block cipher το οποίο κρυπτογραφεί το plaintext σε κομμάτια των 64 bits. Το κλειδί του DES έχει μήκος 56 bits αν και στις περισσότερες περιπτώσεις το

κλειδί μοιάζει να έχει μήκος 64 bits. Αυτό συμβαίνει γιατί κάθε όγδοο bit χρησιμοποιείται ώστε να γίνεται έλεγχος ισότητας οπότε και αγνοείται και μπορούμε να πούμε ότι το κλειδί έχει μήκος 56 bits.

Όπως αναφέρθηκε πιο πριν ο DES ανήκει στην κατηγορία των block ciphers και κρυπτογραφεί το plaintext σε κομμάτια (blocks) των 64 bits. Στην ουσία όμως ο DES μετά από μια αρχική μεταλλαγή χωρίζει το κάθε κομμάτι (block) σε άλλα δυο στο αριστερό και στο δεξί κομμάτι τα οποία έχουν μέγεθος 32 bit το καθένα. Στη συνέχεια ακολουθούν 16 κύκλοι κατά τους οποίους τα δεδομένα συνδυάζονται με το κλειδί. Μετά τον δέκατο έκτο κύκλο το αριστερό και το δεξί μισό του κομματιού (block) ενώνονται. Τέλος πρέπει να πούμε ότι ο DES έχει τους εξής τέσσερις τρόπους λειτουργίας : ECB CBC, OFB και CFB,



Σχήμα 3.3: Αλγόριθμος κρυπτογράφησης DES

Παρά την ηλικία του ο DES παραμένει αρκετά αξιόπιστος και χρησιμοποιείται μέχρι τις μέρες μας από πολλές εφαρμογές. Παρόλα αυτά δεν πρέπει να χρησιμοποιείται για

την κρυπτογράφηση δεδομένων υψίστης σημασίας αφού έχει καταφέρει να ‘σπαστεί’ σε διάστημα λιγότερο των τριών ημερών.

3.5.2 Diffie-Hellman

Το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman αναπτύχθηκε και δημοσιεύτηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Το πρωτόκολλο Diffie-Hellman επιτρέπει σε δυο άτομα να ανταλλάξουν πληροφορίες μέσω μιας ανασφαλούς μεθόδου μετάδοσης ώστε να καθορίσουν από κοινού ένα συμμετρικό κλειδί το οποίο θα χρησιμοποιήσουν στη συνέχεια για την επικοινωνία τους. Η χρησιμότητα του πρωτοκόλλου Diffie-Hellman έγκειται στο γεγονός ότι τα δύο άτομα καταφέρνουν να ορίσουν από κοινού ένα συμμετρικό κλειδί το οποίο μπορούν να ξέρουν μόνο αυτοί χωρίς να έχουν ανταλλάξει από πριν κάποιο μυστικό. Ακόμα και αν κάποιος υποκλέψει τις συνομιλίες και των δύο ατόμων δεν πρόκειται να αποκτήσει το συμμετρικό κλειδί.

Η λειτουργία του πρωτοκόλλου Diffie-Hellman έχει ως εξής : Το πρωτόκολλο έχει δυο παραμέτρους την p και την g. Το p είναι ένας πρώτος αριθμός και το g είναι ένας ακέραιος αριθμός μικρότερος του p με την παρακάτω ιδιότητα : για κάθε αριθμό n όπου 1<n<p-1 υπάρχει ένας αριθμός k έτσι ώστε να ισχύει : n = gk mod p.

Έστω ότι η Αλίκη και ο Βρασίδας θέλουν να ορίσουν από κοινού ένα συμμετρικό κλειδί. Η Αλίκη υπολογίζει μία αξία την a και ο Βρασίδας υπολογίζει μια αξία b. Η αξίες a και b κρατούνται μυστικές από την Αλίκη και τον Βρασίδα. Στη συνέχει η Αλίκη υπολογίζει και στέλνει στο Βρασίδας το αποτέλεσμα της πράξης ag mod p και ο Βρασίδας υπολογίζει και στέλνει στην Αλίκη το αποτέλεσμα της πράξης bg mod p. Τέλος η Αλίκη υπολογίζει το κλειδί k = $(gb)^a$ mod p, και ο Βρασίδας υπολογίζει το κλειδί k = $(ga)^b$ mod p, αφού $(gb)^a$ mod = $(ga)^b$ mod p.

Ο μεγαλύτερος κίνδυνος κατά την χρησιμοποίηση του πρωτοκόλλου Diffie-Hellman είναι κάποιος τρίτος να παρέμβει κατά την αναμετάδοση των δεδομένων και να τα τροποποιήσει. Στο προηγούμενο παράδειγμα πχ θα μπορούσε ο ένας τρίτος έστω ο ‘Χ’ να αναμεταδίδει δικές του πληροφορίες αντί για του Βρασίδα στην Αλίκη και το αντίστροφο. Με αυτό τον τρόπο θα είχε δύο συμμετρικά κλειδιά ένα για να επικοινωνεί

με την Αλίκη και ένα για να επικοινωνεί μα τον Βρασίδα οι οποίοι ενώ νομίζουν ότι μιλάνε απευθείας μεταξύ τους, να λαμβάνουν ουσιαστικά αναμεταδώσεις του 'Χ'. Με αυτό τον τρόπο ο 'Χ' θα μπορούσε να αποκρυπτογραφήσει όλα τα μηνύματα που ανταλλάσσουν ο Βρασίδας και η Αλίκη και αν ήθελε να αλλάξει το περιεχόμενό τους πριν την αναμετάδοση τους.

3.5.3 RSA

Ο αλγόριθμος RSA σχεδιάστηκε από τους **Ron Rivest**, **Adi Shamir** και **Len Adleman**, από όπου και πήρε το όνομά του ,το 1977. Πρόκειται για ένα αλγόριθμο ασύμμετρου κλειδιού, ο οποίος παρά την ηλικία του δεν έχει σπαστεί ακόμα και θεωρείται αρκετά ασφαλής, σε συνδυασμό βέβαια με το μήκος του κλειδιού που θα χρησιμοποιηθεί κάθε φορά. Γενικά ένα κλειδί μεγέθους 1024 bits θεωρείται ικανοποιητικά ασφαλές, παρόλα αυτά ορισμένοι υποστηρίζουν ότι στις μέρες μας το κλειδί πρέπει να έχει μήκος τουλάχιστον 2048 bits. Σε αυτό το σημείο πρέπει να σημειωθεί ότι όσο μεγαλύτερο είναι ένα κλειδί τόσο πιο αργά κρυπτογραφεί, οπότε μεγαλύτερο κλειδί από όσο χρειάζεται ισούται με χάσιμο χρόνου. Ο RSA όπως και όλοι οι αλγόριθμοι ασύμμετρου κλειδιού δεν βρίσκει εφαρμογή στην κρυπτογράφηση μεγάλων plaintext λόγω του γεγονότος ότι οι αλγόριθμοι συμμετρικού κλειδιού κρυπτογραφούν και αποκρυπτογραφούν πολύ πιο γρήγορα. Η ασφάλεια του RSA πηγάζει από τη δυσκολία της παραγοντοποίησης μεγάλων αριθμών, παρακάτω περιγράφεται ο τρόπος λειτουργίας του ώστε να γίνει κατανοητό αυτό.

3.5.3.1 Τρόπος λειτουργίας του RSA

Ο τρόπος λειτουργίας του RSA έχει ως εξής: αρχικά ορίζονται δύο μεγάλοι πρώτοι αριθμοί έστω ο p και ο q

Στη συνέχεια υπολογίζεται ο $n=pq$ και ο $\varphi(n)= (p-1)(q-1)$ και επιλέγεται ένας αριθμός ο e έτσι ώστε $1<e<\varphi(n)$ και ώστε ο e και ο $\varphi(n)$ να είναι σχετικοί πρώτοι αριθμοί.

Στη συνέχεια υπολογίζεται ο $d= e^{-1} \bmod ((p - 1)(q - 1))$.

Έτσι υπολογίσαμε το δημόσιο κλειδί το οποίο είναι οι αριθμοί n και e

και το ιδιωτικό που είναι ο αριθμός d.

Έστω ότι m είναι το μήνυμα πριν την κρυπτογράφηση c το ciphertext, τότε η κρυπτογράφηση έχει ως εξής:

$$c=m^e \bmod n$$

και η αποκρυπτογράφηση έχει ως εξής:

$$m = c^d \bmod n$$

3.5.3.2 MD5

Η συνάρτηση κατακερματισμού (hash function) MD5 σχεδιάστηκε από τον Ron Rivest το 1991 λόγω του γεγονότος οι «προγονοί», της δηλαδή οι συναρτήσεις κατακερματισμού MD2 MD4 θεωρούνταν ξεπερασμένες. Παρόλα αυτά ούτε η MD2 ούτε η MD4 έχουν σπαστεί, όμως έχουν δείξει εμφανή σημεία αδυναμίας.

Η MD5 είναι μια συνάρτηση κατακερματισμού που ανεξαρτήτως του μεγέθους του μηνύματος που δέχεται ως είσοδο, παράγει μια αξία κατακερματισμού μήκους 128 bit. Η αντοχή της συνάρτησης MD5 έγκειται στο γεγονός ότι για να δημιουργηθούν δύο αρχεία με την ίδια MD5 αξία κατακερματισμού πρέπει να γίνουν 2^{64} υπολογισμοί. Ενώ για να αντικατασταθεί ένα αρχείο με ένα άλλο που παράγει την ίδια αξία κατακερματισμού πρέπει να γίνουν 2^{128} η αλλιώς 340.282.366.920.938.463.463.374.607.431.768.211.456 υπολογισμοί! Πράγμα αδύνατο.

3.6 Πως μπορεί να ‘σπάσει’ η κρυπτογραφία

3.6.1 Επιθέσεις σε αλγόριθμους συμμετρικού κλειδιού

Υπάρχουν διάφοροι τρόποι με τους οποίους ένας αλγόριθμος συμμετρικού κλειδιού μπορεί να δεχθεί επίθεση. Ο πιο απλός είναι η δοκιμή όλων των δυνατών κλειδιών μέχρι να προκύψει κάποιο κείμενο που φαίνεται να έχει λογικό περιεχόμενο. Αυτό μπορεί να φαίνεται μια όχι και τόσο εύκολη δυνατότητα αλλά αν το μέγεθος του κλειδιού είναι σχετικά μικρό, τότε είναι εφικτό. Ωστόσο όταν χρησιμοποιούνται μεγάλα κλειδιά, για παράδειγμα με 128 bits, αυτή η μέθοδος γίνεται ανέφικτη.

Η ισχύς των υπολογιστών έχει αυξηθεί σημαντικά ώστε πλέον μπορούν να σπάσουν και κώδικες με μεγαλύτερα κλειδιά. Αυτό οδήγησε του ερευνητές που εργάζονται στον τομέα της κρυπτογραφίας να δημιουργήσουν τον όρο "κόστος δυνατότητας σπασίματος". Αυτό είναι ο αριθμός των bits που πρέπει να προστεθούν σε ένα κλειδί ενός κρυπτογραφικού αλγορίθμου ώστε να τον κρατήσουν ασφαλή σε σχέση με την τρέχουσα ποσότητα υπολογιστικής ισχύος.

Η πρώτη είναι μια μορφή επίθεσης γνωστή ως **επίθεση γνωστού κειμένου.**
Αυτή η τεχνική βασίζεται στο γεγονός ότι ο υποκλοπέας έχει ένα παράδειγμα απλού κειμένου μαζί με το αντίστοιχο του κωδικοποιημένο μήνυμα. Από αυτά ο υποκλοπέας μπορεί να υπολογίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση και στη συνέχεια μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει εύκολα και άλλα μηνύματα. Η απόκτηση ενός δείγματος κρυπτογραφημένου κειμένου και του αντίστοιχου αρχικού κειμένου είναι αρκετές φορές αρκετά εύκολο αφού αρκετές φορές μέρος των μηνυμάτων που ανταλλάσσονται είναι αρκετά απλό να βρεθεί, για παράδειγμα τα έχουν κάποια σταθερή μορφή επικεφαλίδας κ.λ.π.

Το δεύτερο είδος επίθεσης είναι η επίθεση επιλεγμένου κειμένου.
Σε αυτό το είδος επίθεσης ζητά από τον υπολογιστή που εκτελεί την αποκρυπτογράφηση να κωδικοποιήσει ένα ειδικό κομμάτι κειμένου, το οποίο έχει επιλεγεί ώστε η γνώση του αντίστοιχου κρυπτογραφημένου κειμένου να παρέχει αρκετά στοιχεία για το κλειδί.

Το τρίτο είδος επίθεσης είναι γνωστή ως διαφορική επίθεση κρυπτανάλυσης.
Εδώ ο υποκλοπέας δημιουργεί μια σειρά μηνυμάτων που διαφέρουν ελάχιστα μεταξύ τους και εξετάζει πάλι την αντίστοιχη κρυπτογραφημένη έκδοση τους. Με τον τρόπο αυτό ο υποκλοπέας μπορεί να αποκτήσει σημαντικές πληροφορίες για το κλειδί.

Η τελευταία μορφή επίθεσης είναι γνωστή ως διαφορική επίθεση λαθών. Αυτή είναι μια επίθεση με hardware όπου η συσκευή κωδικοποίησης δέχεται πίεση συγκεκριμένης μορφής ώστε να κάνει λάθη. Με προσεκτική εξέταση των λαθών αυτών μπορεί να ανιχνευθεί το κλειδί.

3.6.2 Επιθέσεις σε συστήματα δημόσιου κλειδιού.

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού. Η πρώτη είναι επίθεση με δεδομένα (factoring attack). Πρωτύτερα αναφέρθηκε ότι οι γνωστές μέθοδοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται στην τεράστια δυσκολία επίλυσης προβλημάτων. Όποιος μπορεί να αναλύσει μεγάλους αριθμούς μπορεί να σπάσει και ένα σύστημα δημοσίου κλειδιού βασιζόμενος σε ανάλυση.

Η επίθεση RSA-129
Η πιο διάσημη επίθεση ανάλυσης έγινε στον αριθμό RSA-129 (129 ψηφία). Αυτός ο μεγάλος αριθμός παρουσιάστηκε σε ένα τεύχος του περιοδικού Popular Science το 1977. Τελικά αναλύθηκε από μια ομάδα ερευνητών υπό τον Arjen Lenstra.

Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται. Για παράδειγμα, ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το knapsack. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.

4. ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ

4.1 Mime-S/Mime

Το email αρχικά ήταν σχεδιασμένο έτσι ώστε να στέλνονται με αυτό μόνο μηνύματα κειμένου. Με λίγα λόγια ήταν αδύνατη η μεταφορά ενός αρχείου π.χ σε δυαδική μορφή μέσω email. Αρχικά είχαν επινοηθεί διάφορες μέθοδοι ώστε να μπορούν να αποστέλλονται διάφορα είδη αρχείων. Οι μέθοδοι αυτοί κωδικοποιούσαν τα δεδομένα σε μορφή κειμένου και έτσι μπορούσαν να σταλούν μέσω του ηλεκτρονικού ταχυδρομείου. Το 1992 όμως η **Internet Engineering Task Force** (IETF) επινόησε το Multipurpose Internet Mailer Extensions (mime) το οποίο είχε σαν σκοπό την ενοποίηση και τον συντονισμό όλων των προηγούμενων μεθόδων. Το mime δεν υπαγορεύει ένα και μοναδικό πρότυπο για την κωδικοποίηση των δεδομένων αλλά επιτρέπει στους χρήστες του να χρησιμοποιήσουν την κωδικοποίηση που επιθυμούν αυτοί.

Το mime όμως δεν παρέχει κάποιο είδος ασφάλειας έτσι έχει επινοηθεί το s/mime (secure mime) το θα μπορούσαμε να πούμε ότι καλύπτει το κενό αυτό της ασφάλειας. Το s/mime χρησιμοποιεί ασύμμετρη κρυπτογραφία κατά την μεταφορά των αρχείων. Έτσι κάποιος που θέλει να στείλει ένα μήνυμα χρησιμοποιεί το δημόσιο κλειδί κρυπτογραφεί τα δεδομένα και τα αποστέλλει στον κατάλληλο εξυπηρετητή. Για να ανακτηθεί το plaintext τα δεδομένα αποκρυπτογραφούνται στον email server ή στον email client.

- Αποκρυπτογράφησή στον email client. Τη δεδομένη στιγμή δεν υπάρχουν πολλοί email clients που να υποστηρίζουν αποκρυπτογράφηση με το σύστημα s/mime, αλλά στην περίπτωση που αυτή είναι εφικτή μπορούν να προκύπτουν διάφορα προβλήματα. Για παράδειγμα μπορεί να χρειαστεί ένας email client να αλλάξει στο μέλλον το ζεύγος των κλειδιών του. Το πρόβλημα που προκύπτει σ' αυτή την περίπτωση είναι ότι από την στιγμή που τα μηνύματα

αποθηκεύονται στον email server τα μηνύματα που έχουν κρυπτογραφηθεί με το παλιό κλειδί δεν θα είναι πλέον διαθέσιμα.

- Αποκρυπτογράφησή στον email server.Τα δεδομένα σε αυτή την περίπτωση αποκρυπτογραφούνται στον email server, έτσι αυτός πρέπει να κατέχει όλα τα κλειδιά δημόσια και ιδιωτικά όλων των χρηστών και να αποκρυπτογραφεί όλα τα μηνύματά τους. Είναι ξεκάθαρο ότι το πρόβλημα που προκύπτει εδώ είναι το φόρτο εργασίας που αναλαμβάνει ο email server, όπως επίσης το γεγονός ότι αν κάποιος καταφέρει να αποκτήσει πρόσβαση σε αυτόν θα μπορεί να αποκτήσει το περιεχόμενο οποιουδήποτε email οπουδήποτε χρήστη.

4.2 P.G.P.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιείται για κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της. Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (**λογισμικό ανοιχτού/ ελεύθερου κώδικα και δωρεάν διανομής**), (όπως το gnupgp).

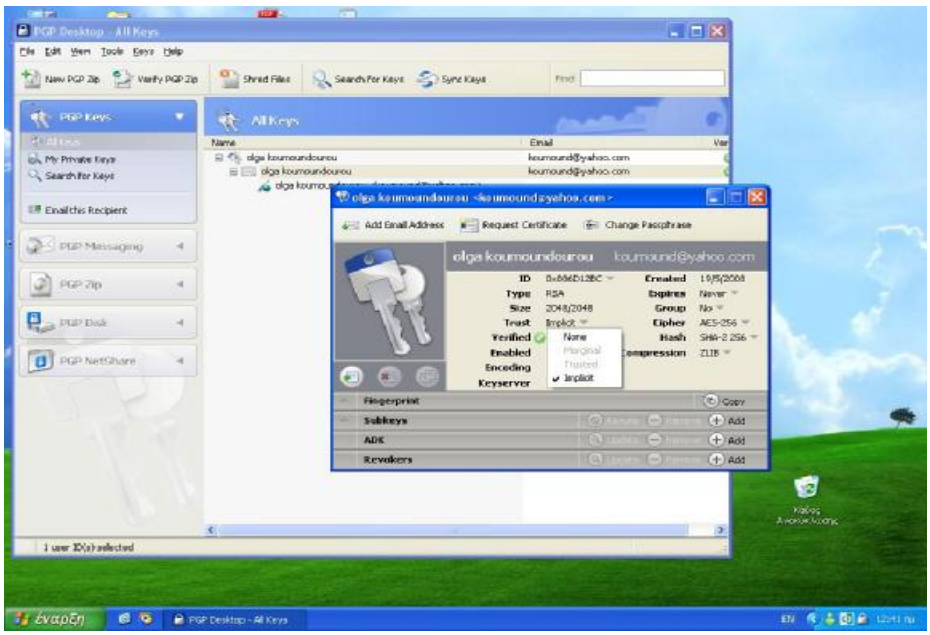
Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντας το στο Internet.Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη και ο δεύτερος το αποκρυπτογραφεί με το ιδιωτικό κλειδί του.

Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να

εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί. Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς:

- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)



Σχήμα 4.1: Το περιβάλλον κρυπτογράφησης του PGP.

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής πιστοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές **ηλεκτρονικού εμπορίου** και για όσες απαιτούν ισχυρή πιστοποίηση. Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό

βαθμού εμπιστοσύνης. Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή πιστοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών.[13]

4.3 S.S.L.

Το SSL (secure sockets layer-ασφαλές στρώμα υποδοχών) είναι ένα ευέλικτο γενικού σκοπού σύστημα κρυπτογράφησης το οποίο παρουσιάστηκε πρώτη φορά το 1994 μαζί με την πρώτη έκδοση του Netscape Navigator, αργότερα υποστηρίχτηκε και από άλλους φυλλομετρητές ιστού όπως ο Internet explorer για παράδειγμα. Σκοπός του SSL είναι να πιστοποιεί την ταυτότητα ενός εξυπηρετητή σε ένα φυλλομετρητή ιστού και να κρυπτογραφεί την επικοινωνία μεταξύ τους. Το SSL λειτουργεί στο επίπεδο συναλλαγής του TCP/IP κάτι που του δίνει την ανεξαρτησία και την ευελιξία πρωτοκόλλου. Ένα άλλο βασικό χαρακτηριστικό του SSL είναι η ευελιξία του όσον αφορά την επιλογή του συμμετρικού αλγόριθμου κρυπτογράφησης, της συνάρτησης σύνοψης μηνύματος και της μεθόδου πιστοποίησης. Για τη συμμετρική κρυπτογράφηση, το SSL μπορεί να χρησιμοποιήσει οποιοδήποτε DES τριπλό DES, RC2 ή RC4. Για σύνοψη μηνύματος το SSL έχει τη δυνατότητα να χρησιμοποιήσει τους αλγόριθμους κατακερματισμού MD5 ή SHA. Για πιστοποίηση το SSL μπορεί να χρησιμοποιήσει τα δημόσια κλειδιά RSA και πιστοποιεί ή λειτουργεί σε μία ανώνυμη κατάσταση λειτουργίας, στην οποία χρησιμοποιείται ο αλγόριθμος ανταλλαγής κλειδιού Diffie-Helman. Μια ποικιλία στο μέγεθος των κλειδιών είναι διαθέσιμη για τους αλγόριθμους κρυπτογράφησης, συμπεριλαμβανομένων και των περιορισμένων σε μήκος κλειδιών που χρησιμοποιούνται στις εξαγόμενες από τις Η.Π.Α. εκδόσεις του SSL λογισμικού. Ο συνδυασμός των συμμετρικών αλγόριθμων κρυπτογράφησης, των συναρτήσεων σύνοψης μηνύματος και της πιστοποίησης είναι γνωστός σαν «κρυπτογραφικό πακέτο». Όταν ένας πελάτης SSL έρχεται σε επαφή με ένα

εξυπηρετητή «διαπραγματεύονται» για ένα κοινό πακέτο, το οποίο είναι το πιο ασφαλές κοινό πακέτο το οποίο έχουν και οι δύο.

Όταν πραγματοποιείται μία SSL σύνδεση, όλες οι επικοινωνίες του φυλλομετρητή προς τον εξυπηρετητή και το αντίστροφο κρυπτογραφούνται συμπεριλαμβανομένων και

- Του URL του ζητούμενου εγγράφου
- Των περιεχομένων του ζητούμενου εγγράφου
- Των περιεχομένων από οποιεσδήποτε συμπληρωμένες φόρμες
- Των cookies που στάλθηκαν από το φυλλομετρητή στον εξυπηρετητή
- Των cookies που στάλθηκαν από τον εξυπηρετητή στο φυλλομετρητή
- Των περιεχομένων της http επικεφαλίδας

Τέλος πρέπει να σημειωθεί ότι το SSL παρέχει ενσωματωμένη συμπίεση των δεδομένων, κάτι πολύ σημαντικό αφού όταν ένα μήνυμα κρυπτογραφηθεί είναι αδύνατο πλέον να συμπιεστεί [14]

4.4 S.E.T.

Το S.E.T.(Secure Electronic Ttransactions-ασφαλείς ηλεκτρονικές συναλλαγές) είναι Netscape και Microsoft, και σκοπός του είναι να διαχειρίζεται συναλλαγές μέσω πιστωτικών καρτών στο διαδύκτιο. Σε αντίθεση με το SSL το οποίο είναι σύστημα κρυπτογραφίας γενικού σκοπού, το SET χρησιμοποιείται για τη διενέργεια μόνο χρεωστικών και πιστωτικών συναλλαγών καρτών μεταξύ πελατών και εμπόρων.
Το SET παρέχει :

• **Πιστοποίηση** και

• **Μη άρνηση αποδοχής** όλων των εμπλεκόμενων στην συναλλαγή με τη χρήση ψηφιακών υπογραφών. Αυτό περιλαμβάνει τον πελάτη, την τράπεζα που του έχει εκδώσει την πιστωτική κάρτα, τον έμπορο και την τράπεζα που χειρίζεται τον λογαριασμό του εμπόρου.

• **Εμπιστευτικότητα** μέσω της κρυπτογράφησης των συναλλαγών.

• **Ακεραιότητα** των δεδομένων μην επιτρέποντας σε κάποιο τρίτο να παραποιήσει κάποιο στοιχείο(π.χ τον αριθμό της πιστωτικής κάρτας, το ποσό της συναλλαγής κ.α.)

Το SET χρησιμοποιεί τον ασφαλή αλγόριθμο κατακερματισμού (SHA) ο οποίος παράγει ένα κατακερματισμό 160 δυαδικών ψηφίων, για το ζευγάρι δημόσιου – ιδιωτικού κλειδιού χρησιμοποιεί τον αλγόριθμο RSA μήκους 1024 δυαδικών ψηφίων. Για την συμμετρική κρυπτογράφηση το SET χρησιμοποιεί σαν προεπιλογή τον αλγόριθμο DES μήκους 56 δυαδικών ψηφίων, αλλά παρόλα αυτά μπορεί να χρησιμοποιήσει μια ποικιλία διαφορετικών αλγόριθμων συμμετρικού κλειδιού.

Το SET χρησιμοποιεί ζευγάρια ιδιωτικών – δημόσιων κλειδιών και ψηφιακά πιστοποιητικά για να πιστοποιήσουν την ταυτότητα του κάθε συμβαλλόμενου και να τους επιτρέψει την εμπιστευτική επικοινωνία μεταξύ τους. Το SET επίσης κρυπτογραφεί τις πληροφορίες που αφορούν την παραγγελία με τη χρήση ενός τυχαίου συμμετρικού κλειδιού συνόδου και τις ‘πακετάρει’ σε ένα ψηφιακό φάκελο χρησιμοποιώντας το δημόσιο κλειδί του εμπόρου. Οι πληροφορίες που αφορούν την πληρωμή της παραγγελίας (αριθμός πιστωτικής κάρτας του πελάτη και πληροφορίες της τράπεζας)κρυπτογραφούνται παρόμοια αλλά σε αυτή την περίπτωση με το δημόσιο κλειδί της τράπεζας του εμπόρου. Το λογισμικό στη συνέχεια υπολογίζει από κοινού κατακερματισμό της παραγγελίας και των πληροφοριών πληρωμής και τον υπογράφει με το ιδιωτικό κλειδί του πελάτη. Με αυτό τον τρόπο ο έμπορος και η τράπεζα του δεν μπορούν να έχουν πρόσβαση σε πληροφορίες που δεν πρέπει ενώ ταυτόχρονα επικυρώνεται η ακεραιότητα του μνήματος. Πρέπει να σημειωθεί ότι με τη χρήση του SET η τράπεζα που εξέδωσε πιστωτική κάρτα συν τοις άλλοις αποκρυπτογραφεί τις πληροφορίες πληρωμής του πελάτη τον πιστοποιεί και ελέγχει την εγκυρότητα του αριθμού της πιστωτικής κάρτας [15].

Ο λόγος που κάνει το SET καταλληλότερο από το SSL είναι ότι με το SET γίνεται έλεγχος της εγκυρότητας της πιστωτικής κάρτας και ότι ο έμπορος δεν έχει πρόσβαση στον αριθμός της ενώ ταυτόχρονα βεβαιώνεται για την εγκυρότητά της. Επίσης

υπάρχει και η νομοθεσία των Η.Π.Α. η οποία απαγορεύει την εξαγωγή οποιουδήποτε λογισμικού χρησιμοποιεί δυνατή κρυπτογραφία συμπεριλαμβανομένων και των λογισμικών που χρησιμοποιούν το SSL. Η συγκεκριμένη όμως νομοθεσία εξαιρεί τα συστήματα που μπορούν να χρησιμοποιηθούν μόνο για οικονομικές συναλλαγές όπως λ.γ. το SET.

4.5 P.C.T.

Το PCT (Private Communication Technology) αναπτύχθηκε το 1995 από τη Microsoft και είναι ένα πρωτόκολλο το οποίο υπόσχεται ασφάλεια στο διαδύκτιο. Το PCT είναι σχεδιασμένο να παρέχει σε εφαρμογές οι οποίες χρησιμοποιούν το μοντέλο πελάτη – εξυπηρετητή, εμπιστευτικότητα, ακεραιότητα και πιστοποίηση του εξυπηρετητή (και προαιρετικά του πελάτη αν ζητηθεί από τον εξυπηρετητή). Το πρωτόκολλο PCT ξεκινάει με μία «διαπραγμάτευση» μεταξύ του εξυπηρετητή και του πελάτη, ως προς τον αλγόριθμο κρυπτογράφησης, του (συμμετρικού) κλειδιού συνόδου και ταυτόχρονα πιστοποιείται η ταυτότητα του εξυπηρετητή (και του πελάτη σε περίπτωση που χρειαστεί) με τη χρήση πιστοποιημένων δημόσιων κλειδιών. Στη συνέχεια όλα τα δεδομένα που ανταλλάσσονται κρυπτογραφούνται με τη χρήση του κλειδιού συνόδου που αναφέρθηκε πιο πριν. Σε αυτό το σημείο πρέπει να τονιστεί ότι το πρωτόκολλο PCT δεν παρέχει πληροφορίες σχετικά με τα ψηφιακά πιστοποιητικά και τις αρχές πιστοποίησης. Αντί αυτού οι υλοποιήσεις του PCT έχουν πρόσβαση σε ένα «μαύρο κουτί» το οποίο δέχεται ρυθμίσεις σχετικά με το «κύρος» των λαμβανομένων πιστοποιητικών.

Όπως το SSL έτσι και το PCT χρησιμοποιεί ένα πλήθος κρυπτογραφικών αλγόριθμων συμμετρικού και ασύμμετρου κλειδιού, αλγόριθμους κατακερματισμού και ψηφιακά πιστοποιητικά για να πετύχει τους σκοπούς του. Γενικά θα έλεγε κανείς ότι το PCT δεν διαφέρει πολύ από το SSL. Παρόλα αυτά μπορούν να εντοπιστούν μερικές διαφορές μεταξύ τους κυρίως κατά τη φάση της χειραψίας (πριν αρχίσουν να ανταλλάσσονται τα δεδομένα).

Μερικές από τις βασικότερες διαφορές τους είναι:

- Η διαπραγμάτευση σχετικά με τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν κρατάει περισσότερο και καλύπτει περισσότερες περιπτώσεις.
- Για τη δημιουργία του MAC χρησιμοποιούνται διαφορετικά κλειδιά από αυτά που χρησιμοποιούνται για την κρυπτογράφηση. Έτσι τα κλειδιά που χρησιμοποιούνται για το MAC μπορεί να είναι μεγαλύτερα σε μέγεθος από τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση, έτσι στην περίπτωση που επιλέγονται μικρά κλειδιά με αποτέλεσμα αδύναμη κρυπτογράφηση, η πιστοποίηση του αποστολέα και ακεραιότητα μηνύματος δεν επηρεάζονται [16].

4.6 Cybercash

Το Cybercash είναι ένα προϊόν της cybercash corporation, παρόμοιο με το set. Σκοπός του cybercash είναι η πραγματοποίηση εμπορικών συναλλαγών με τη χρήση πιστωτικής κάρτας μέσω του διαδυκτίου. Για να μπορέσει ένας καταναλωτής να κάνει πληρωμές μέσω του cybercash πρέπει να κατεβάσει ένα δωρεάν λογισμικό από τη σελίδα της cybercash, το cybercash wallet. Ο έμπορος από την πλευρά του με το ανάλογο λογισμικό επικυρώνει και καταγράφει κάθε συναλλαγή συνδεόμενος με ένα εξυπηρετητή που συντηρείται από την cybercash. Για κάθε συναλλαγή που διενεργεί ο χρήστης διατηρείται μια εγγραφή επιτρέποντας με αυτό τον τρόπο στο χρήστη την γρήγορη αναθεώρηση των αγορών του και τον έλεγχο τους σε σχέση με τις δηλώσεις της πιστωτικής κάρτας. Όπως το set έτσι και το cybercash για να καταφέρει να παρέχει ασφαλείς συναλλαγές κάνει χρήση ισχυρής κρυπτογραφίας. Επίσης όπως και στο set έτσι και στο cybercash ο έμπορος δεν έχει πρόσβαση στις πληροφορίες της πιστωτικής κάρτας του πελάτη.

Κάθε συναλλαγή μέσω του cybercash επιβαρύνεται με ένα στάνταρ ποσό, έτσι η χρήση του cybercash δεν συνιστάται για μικρές αγορές. Παρόλα αυτά μια υπηρεσία της cybercash η cybercoin επιτρέπει στον πελάτη να πληρώσει εκ των προτέρων ένα ποσό στο σύστημα cybercash και να κάνει στη συνέχεια μικρές αγορές έναντι αυτού. Το λογισμικό του πελάτη και του εξυπηρετητή που χρησιμοποιείται για το cybercash και το cybercoin είναι το ίδιο αλλά η συμφωνία μεταξύ της τράπεζας του εμπόρου και του cybercash δεν είναι. Έτσι μερικές τράπεζες υποστηρίζουν το cybercash αλλά δεν

υποστηρίζουν το cybercoin. Τέλος πρέπει να αναφερθεί ότι πρόσφατα το cybercash μεταφέρθηκε στην κυριότητα της verisign, έναν από τους μεγαλύτερους οργανισμούς πιστοποίησης [17], [18].

4.7 Secure HTTP (HTTPS)

Όταν χρησιμοποιείται το πρωτόκολλο μεταφοράς υπερκειμένου (http) οι πληροφορίες που μεταφέρονται από και προς τον διακομιστή του ιστού μπορούν να υποκλαπούν ή να αλλοιωθούν από κάποιο τρίτο καθώς το http δεν χρησιμοποιεί κάποιο τρόπο ώστε να παρέχει ασφάλεια των δεδομένων που μεταφέρει και να πιστοποιεί τους χρήστες του. Για να αποφευχθούν τέτοιες περιπτώσεις σχεδιάστηκε το https (ορισμένοι το αναφέρουν και ως shttp). Το https υποστηρίζει τη χρήση της συμμετρικής και ασύμμετρης κρυπτογραφίας, ψηφιακών πιστοποιητικών, και αλγόριθμων κατακερματισμού με σκοπό να παρέχει πιστοποίηση μεταξύ φυλλομετρητή και διακομιστή του ιστού, ακεραιότητα των δεδομένων που ανταλλάσσουν, εμπιστευτικότητα και μη άρνηση αποδοχής. Συνεπώς το https έχει συμβάλλει σημαντικά στην ανάπτυξη του ηλεκτρονικού εμπορίου και στις ασφαλείς συναλλαγές μέσω του διαδικτύου. Όταν χρησιμοποιείται η URL διεύθυνση αρχίζει με το https.
Έτσι μία διεύθυνση https είναι της μορφής π.χ.
https://www.taxisnet.gr/web/default.html.

4.8 Kerberos

Ο Κέρβερος, πλην του μυθικού τέρατος με τα τρία κεφάλια που φύλαγε την είσοδο για τον Άδη, είναι και ένα πρωτόκολλο που αναπτύχθηκε από το M.I.T. στα μέσα της δεκαετίας του 80’ και έχει σκοπό την παροχή πιστοποίησης σε εφαρμογές που χρησιμοποιούν το μοντέλο πελάτη – εξυπηρετητή. Έκτοτε έχουν κυκλοφορήσει δυο εκδόσεις του Κέρβερος (v.4, v.5). Το Κέρβερος χρησιμοποιεί συμμετρική κρυπτογραφία και πιο συγκεκριμένα χρησιμοποιεί τον αλγόριθμο DES, επίσης

χρησιμοποιεί τους αλγόριθμους CRC-32, MD4, MD5, και DES για τη δημιουργία σύνοψης (βλέπε κεφάλαιο 3.4.2 ψηφιακή υπογραφή).

Σχήμα 4.2: Ο μυθικός Κέρβερος

4.8.1 Αρχιτεκτονική του Κέρβερος

Ο πυρήνας της αρχιτεκτονικής του Κέρβερος είναι ο εξυπηρετητής διανομής κλειδιών ή αλλιώς KDS (Key Distribution Server). Ο KDS αποθηκεύει πληροφορίες σχετικά με την πιστοποίηση και τις χρησιμοποιεί για να εξασφαλίσει ασφαλή πιστοποίηση στους χρήστες (εφαρμογές) του πρωτοκόλλου Κέρβερος. Ένας χρήστης ή μια εφαρμογή (στην ορολογία του Κέρβερος “principal”) για να χρησιμοποιήσει το Κέρβερος πρέπει να επικοινωνήσει με το KDC έτσι ώστε να του δοθεί εισιτήριο (ticket). Η χρησιμότητα των εισιτηρίων είναι η παροχή πιστοποίησης μεταξύ των principals. Όλα τα εισιτήρια ισχύουν για περιορισμένο χρονικό διάστημα και γι’ αυτό πρέπει να υπάρχει ένας ασφαλής τρόπος επικοινωνίας μεταξύ του KDC και των principals ώστε να ανανεώνονται. Η πρακτική πλευρά του Κέρβερος είναι η ενσωμάτωση του με διάφορες εφαρμογές. Εφαρμογές όπως το ftp το pop κ.α. έχουν ενσωματωθεί με το Κέρβερος.

4.8.2 Η αδυναμία του Κέρβερος

Το γεγονός ότι όλα τα κλειδιά που χρησιμοποιούνται από τους χρήστες του Κέρβερος αποθηκεύονται στον KDC, είναι ίσως η μόνη αδυναμία του πρωτοκόλλου. Αρκεί να σκεφτεί κανείς τις επιπτώσεις που θα υπήρχαν αν ένας cracker κατάφερνε να αποκτήσει πρόσβαση στον έλεγχο του KDC. [19]

4.9 DNSSEC (Domain Name System Security)

Το DNS αναπτύχθηκε πολύ πριν φανταστεί κανείς τα προβλήματα ασφάλειας του διαδικτύου που θα προέκυπταν. Λόγω του γεγονότος ότι το DNS είναι μια υπηρεσία η οποία βασίζεται στο πρωτόκολλο UDP προκύπτουν πολλά προβλήματα ασφαλείας. Σε αντίθεση με το TCP το UDP δεν διαθέτει κάποιο μηχανισμό ώστε να πιστοποιούνται οι αποστολείς των πακέτων που λαμβάνονται. Έτσι το UDP και κατά συνέπεια το DNS μπορεί να επιτρέψει την εξαπάτηση ως προς τον αποστολέα κάθε πακέτου κάτι που μπορεί να ξεκινήσει μια σειρά επιθέσεων ασφαλείας.

Σαν απάντηση στα παραπάνω προβλήματα του DNS αναπτύχθηκε ένα νέο ασφαλές πρωτόκολλο το DNSSEC. Το DNSSEC προσπαθεί με τη χρήση ενός διανομέα δημοσίων κλειδιών να αποτρέψει την εξαπάτηση ως προς τον αποστολέα των πακέτων (source-spoofing) και να εξασφαλίσει ακεραιότητα των δεδομένων. Παρόλα αυτά το DNSSEC θα μπορούσαμε να πούμε ότι δεν καλύπτει μερικά κενά ασφάλειας. Για παράδειγμα το DNSSEC δεν παρέχει καθόλου εμπιστευτικότητα αφού δεν κρυπτογραφεί τα δεδομένα που μεταφέρονται μέσω του διαδικτύου.

4.10 IPSec

Η υπάρχουσα έκδοση του IP πρωτοκόλλου που χρησιμοποιείται είναι η IPv4, αυτή σχεδιάστηκε στη δεκαετία του ’70. Έτσι παρά τη λειτουργικότητά του στις μέρες μας προκύπτει ένα πλήθος προβλημάτων από τη χρησιμοποίηση του.
Έτσι το Internet Engineering Task Force (IETF) ίδρυσε το **IP Security Protocol Working Group** το οποίο με τη σειρά του ανάπτυξε το IP SEC(IP security). Το IP sec δεν είναι από μόνο του ένα πρωτόκολλο αλλά ένα σύνολο πρωτοκόλλων με σκοπό την παροχή ασφάλειας κατά τη χρησιμοποίηση του πρωτοκόλλου IP. Αν και αρχικά το IPsec προοριζόταν για το IPV6 μπορεί να χρησιμοποιηθεί και πάνω στο πρωτόκολλο IP (v4).

4.11 IPV6

Σύμφωνα με υπολογισμούς το IPv4 σε μερικά χρόνια δεν θα μπορεί να καλύψει τον συνεχώς αυξανόμενο αριθμό των υπολογιστών που το χρησιμοποιούν, πρέπει οπότε να βρεθεί μια άλλη λύση η μάλλον να επινοηθεί ένα άλλο πρωτόκολλο για τη διευθυνσιοδότηση. Έτσι το Internet Engineering Task Force (IETF) ανάπτυξε το IPv6 το οποίο λύνει (μεταξύ των άλλων) αυτό το πρόβλημα αφού χρησιμοποιεί 128 bits για την διευθυνσιοδότηση. Για να γίνει πιο κατανοητό το παραπάνω πρέπει να επισημανθεί ότι ενώ το IPv4 αδυνατεί να δώσει σε κάθε άνθρωπο στον πλανήτη μια διεύθυνση IP το IPv6 επαρκεί για να δώσει περίπου 6.7×10^{17} IP διευθύνσεις ανά mm^2 της επιφάνειας της γης!(http://en.wikipedia.org/wiki/Pv6)

Ένα άλλο πολύ σημαντικό πρόβλημα που προσπαθεί να λύσει είναι αυτό της ασφάλειας το οποίο είναι και υπεύθυνο για την πληθώρα των πρωτοκόλλων κρυπτογράφησης που χρησιμοποιούνται. Το IPv6 διαθέτει προαιρετική κρυπτογραφία και έλεγχο ακεραιότητας των δεδομένων σε ένα βαθύ επίπεδο της διαδυκτιακής στοίβας, μια ευκολία γνωστή σαν IPsec (IP Security) (βλ. κεφ. 4.10 IP SEC). Οποιοιδήποτε υπολογιστές μπορούν να πιστοποιήσουν τον εαυτό τους και να κρυπτογραφήσουν τις επικοινωνίες τους. Το μοναδικό ίσως μειονέκτημα είναι ότι χρησιμοποιεί για κρυπτογράφηση ένα DES πλήθους 56 δυαδικών ψηφίων, κάτι που

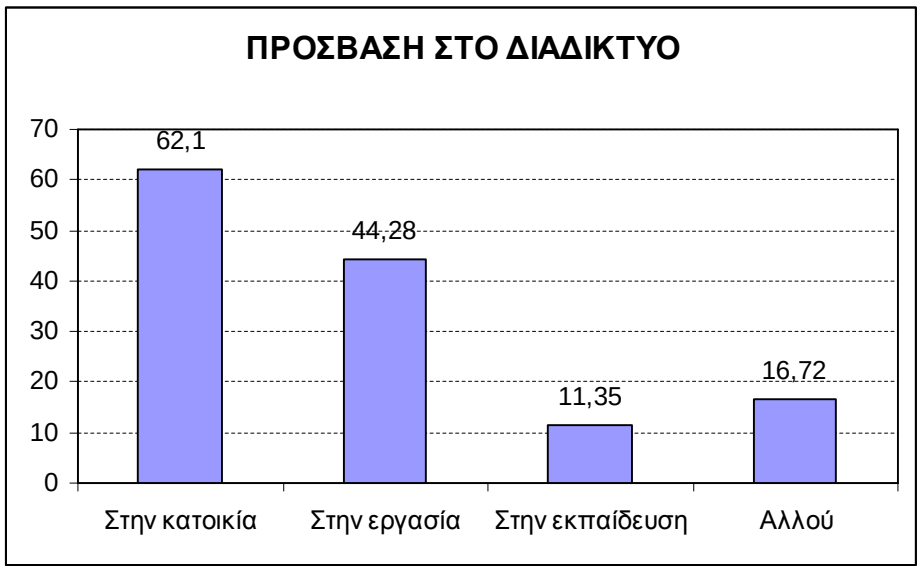
πολλοί θεωρούν ότι είναι ανεπαρκές για εφαρμογές υψηλής ασφάλειας. Υπολογίζεται ότι το IPv4 θα υποστηρίζεται τουλάχιστον ως το 2025 έτσι ώστε να δοθεί χρόνος για τη διόρθωση τυχόν προβλημάτων του IPv6 [20].

5. Η ΕΞΕΛΙΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ:ΠΡΟΒΛΗΜΑΤΑ ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ

5.1 Η εξέλιξη του internet στην Ελλάδα

Στην Ελλάδα η εμπορική προσφορά πρόσβασης στο Internet σε ιδιώτες ξεκίνησε τον Ιανουάριο του 1993 από τον Δημόκριτο. Μπορεί οι όροι της πρόσβασης για τους εξωπανεπιστημιακούς ενδιαφερόμενους να έμοιαζαν λίγο αυταρχικοί σε σχέση με τα προνόμια της πανεπιστημιακής κοινότητας, όμως το μεγάλο βήμα είχε γίνει και στη χώρα μας. Περίπου ένα χρόνο μετά άρχισε να προσφέρει ιντερνετική πρόσβαση και η Compulink, ενώ η νεαρότατη τότε Hellas On Line ακολούθησε σύντομα μετά. Παράλληλα το Forthnet, το δίκτυο του Πανεπιστημίου της Κρήτης, μετεξελίχτηκε σε ανώνυμη εταιρεία και άρχισε να δίνει πρόσβαση σε επιχειρήσεις αρχικά και καιρό αργότερα και σε ιδιώτες. Πολλοί άλλοι φορείς ιντερνετικής πρόσβασης εμφανίστηκαν τα χρόνια που μεσολάβησαν, με τελευταία και πιο ηχηρή άφιξη αυτή του ΟΤΕ, με τη θυγατρική του εταιρεία, OTEnet, στις αρχές του 1997.

Σύμφωνα με έρευνα της Εθνικής Στατιστικής Υπηρεσίας η πρόσβαση στο Internet κατά το πρώτο τρίμηνο του 2007 ανέρχεται στο 33,4%, παρουσιάζοντας μικρή αύξηση σε σχέση με το αντίστοιχο ποσοστό του 2006 (28,9%). Άνδρες είναι το 56,26% και γυναίκες το 43,74%. Κυριότερος χώρος πρόσβασης στο Internet κατά το πρώτο τρίμηνο του 2007 παραμένει η κατοικία (62,10%), ακολουθούν ο εργασιακός χώρος με 44,28% και οι χώροι εκπαίδευσης με 11,35%.



Σχήμα: 5.1 Στατιστικά πρόσβασης στο διαδίκτυο (πηγή: Εθνική Στατιστική Υπηρεσία)

Οι εργαζόμενοι αποτελούν την πλειονότητα των χρηστών του Διαδικτύου με 61,55% και ακολουθούν οι μαθητές/ φοιτητές με 54,30%. Σχετικά με το επίπεδο εκπαίδευσης, το υψηλότερο ποσοστό εμφανίζεται στους απόφοιτους Τριτοβάθμιας εκπαίδευσης (71,3%).

Οι κυριότεροι λόγοι χρήσης του Internet είναι η αποστολή/ λήψη ηλεκτρονικού ταχυδρομείου (63,9%), η αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες (95,9%), η ανάγνωση εφημερίδων και περιοδικών (54,72%), τα online παιχνίδια (26,2%) και το κατέβασμα μουσικής (50,5%) καθώς και η αναζήτηση πληροφοριών σχετικών με την εκπαίδευση (43%).

Επιπλέον, το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ) διεξάγει τρεις εθνικές έρευνες με θέμα τις νέες τεχνολογίες, οι οποίες χρηματοδοτούνται από το Επιχειρησιακό Πρόγραμμα "Κοινωνία της Πληροφορίας" του υπουργείου Οικονομίας και Οικονομικών:

- **Την Εθνική Έρευνα για τις Νέες Τεχνολογίες και την "Κοινωνία της Πληροφορίας",** η οποία πραγματοποιήθηκε για τρίτη συνεχή χρονιά κατά την περίοδο 24 Οκτωβρίου ως 24 Νοεμβρίου 2003 από την εταιρεία VPRC. Η

έρευνα πραγματοποιήθηκε με προσωπικές συνεντεύξεις σε δείγμα 2802 νοικοκυριών (περιλαμβάνονται και 153 μετανάστες).

- **Την έρευνα για τη χρήση Τεχνολογιών Πληροφορικής & Επικοινωνιών (ΤΠΕ)** από τις Μικρομεσαίες Επιχειρήσεις, η οποία ολοκληρώθηκε το Δεκέμβριο του 2003 από την εταιρία Centrum. Η έρευνα πραγματοποιήθηκε με προσωπικές συνεντεύξεις σε δείγμα 2026 ΜΜΕ.
- **Την έρευνα για τη χρήση ΤΠΕ από τις μεγαλύτερες επιχειρήσεις της χώρας**, η οποία ολοκληρώθηκε τον Οκτώβριο του 2003 από κοινοπραξία των ΟΠΑ/Hitech/Hellanet. Η έρευνα πραγματοποιήθηκε με προσωπικές συνεντεύξεις διευθυντικών στελεχών των τμημάτων πληροφορικής σε 500 από τις 1250 μεγαλύτερες επιχειρήσεις της χώρας, με βάση τον κύκλο εργασιών τους.

Ενδεικτικά αναφέρουμε τα συγκεντρωτικά αποτελέσματα σχετικά με τα βασικά μεγέθη χρήσης των ΤΠΕ στην Ελλάδα την τριετία 2004, 2005 και 2006 [21]:

	2004	2005	2006
Ποσοστό επιχειρήσεων που χρησιμοποιούν PC	42%	44%	45%
Ποσοστό επιχειρήσεων που χρησιμοποιούν internet	28,1%	31%	34%
Ποσοστό επιχειρήσεων που χρησιμοποιούν e-mail	25%	28%	31%
Ποσοστό πληθυσμού που χρησιμοποιεί PC	25,9%	27,3%	31%
Ποσοστό πληθυσμού που χρησιμοποιεί internet	19,7%	19,5%	24,6%
Ποσοστό πληθυσμού που έχει προσωπικό e-mail	12,5%	13,1%	16,4%

Σχήμα: 5.2: Έρευνα για τη χρήση ΤΠΕ στην Ελλάδα

5.2 Ηλεκτρονική διακυβέρνηση

Ηλεκτρονική διακυβέρνηση (E-government). Γενικός όρος που αναφέρεται σε οποιεσδήποτε κυβερνητικές λειτουργίες ή διαδικασίες πραγματοποιούνται σε

ηλεκτρονική μορφή μέσω του Διαδικτύου (συναλλαγές με τους πολίτες, δημόσιες υπηρεσίες που παρέχουν online εξυπηρέτηση ή πληροφόρηση κ.λ.π.).

5.2.1 Εισαγωγή

Τα πληροφοριακά συστήματα έχουν τη δυνατότητα να μεταμορφώνουν τη κρατική διοίκηση και τις υπηρεσίες που αυτή παρέχει στους πολίτες. Παρακάτω περιγράφουμε τα τεχνικά πρότυπα και τις πολιτικές που λειτουργούν σαν βάση στη στρατηγική του e-government. Τα εν λόγω πρότυπα θα επιτρέπουν την απρόσκοπτη ροή πληροφοριών στο Δημόσιο Τομέα και θα επιτρέπουν στον πολίτη και τον ιδιωτικό τομέα να έχουν καλύτερη πρόσβαση στις υπηρεσίες που παρέχει το κράτος. Η κύρια απαίτηση είναι η υιοθέτηση των προτύπων του Internet και του WWW για όλα τα κρατικά συστήματα. Η κυβέρνηση προώθησε τη πρωτοβουλία UK GovTalk. Η πρωτοβουλία αυτή είναι ένα κοινό forum κυβέρνησης και βιομηχανίας που καθοδηγείται από το Γραφείο του Πρωθυπουργού, για να συμφωνηθούν οι μορφές δεδομένων του τύπου XML (Extensible Markup Language) που θα χρησιμοποιηθούν σε όλο το δημόσιο τομέα.

Το e-gov περικλείει ενδοκρατικά πληροφοριακά συστήματα και συσχετίσεις μεταξύ των Υπουργείων, των Κρατικών Οργανισμών, του ευρύτερου δημόσιου τομέα, άλλες Κυβερνήσεις, καθώς και τον Ιδιωτικό τομέα.
Μέρος της στρατηγικής του e-gov είναι να αναπτυχθούν οι παρακάτω πρωτοβουλίες:

5.2.2 Ασφαλές Κυβερνητικό Δίκτυο

Πρόκειται για ένα ενοποιημένο δίκτυο φωνής και πληροφοριών μεταξύ των κυβερνητικών υπηρεσιών. Θα είναι βασισμένο σε ανοιχτές τεχνολογίες Intranet. Επιπλέον θα προσφέρει ασφάλεια στη μεταφορά βασισμένο σε κρυπτογραφία και θα προστατεύει τους χρήστες από εξωτερικές παρεμβάσεις. Για την ασφάλεια των τηλεπικοινωνιών πρέπει να χρησιμοποιείται το S/MIME, για την ασφάλεια των μηνυμάτων, όπου λόγοι ασφαλείας επιβάλλουν το απόρρητο του e-mail. Παράδειγμα όπου εμφανίζεται η εμπιστευτικότητα του e-mail είναι η αποστολή προσωπικών δεδομένων σε απροστάτευτα δίκτυα.

Επίσης τα κυβερνητικά πληροφοριακά συστήματα έχουν σχεδιαστεί έτσι ώστε να εξασφαλίζουν από κινδύνους ασφαλείας σύνδεσης στο διαδίκτυο συμπεριλαμβανομένης της ικανότητος να προστατεύουν από τον κίνδυνο της μη εξουσιοδοτημένης πρόσβασης.

Όπως είναι ήδη γνωστό, υπάρχει ένας αριθμός από σύγχρονες τάσεις στην ασφάλεια πληροφοριών:

1. Υιοθέτηση διεθνών βέλτιστων πρακτικών (best practices), που προκύπτουν από τη συνδυασμένη εμπειρία εταιρειών, που ήδη δραστηριοποιούνται στο χώρο της ασφάλειας πληροφοριών.

2. Πιστοποίηση μέτρων ασφάλειας πληροφοριών (certification of information security measures), που χρησιμοποιούνται ειδικά από δημόσιους φορείς.

3. Ενημέρωση των χρηστών (awareness of users).

4. Συνεχής παρακολούθηση και αξιολόγηση των στατιστικών μεγεθών που αφορούν στην ασφάλεια των πληροφοριών (continuous measurement of information security).

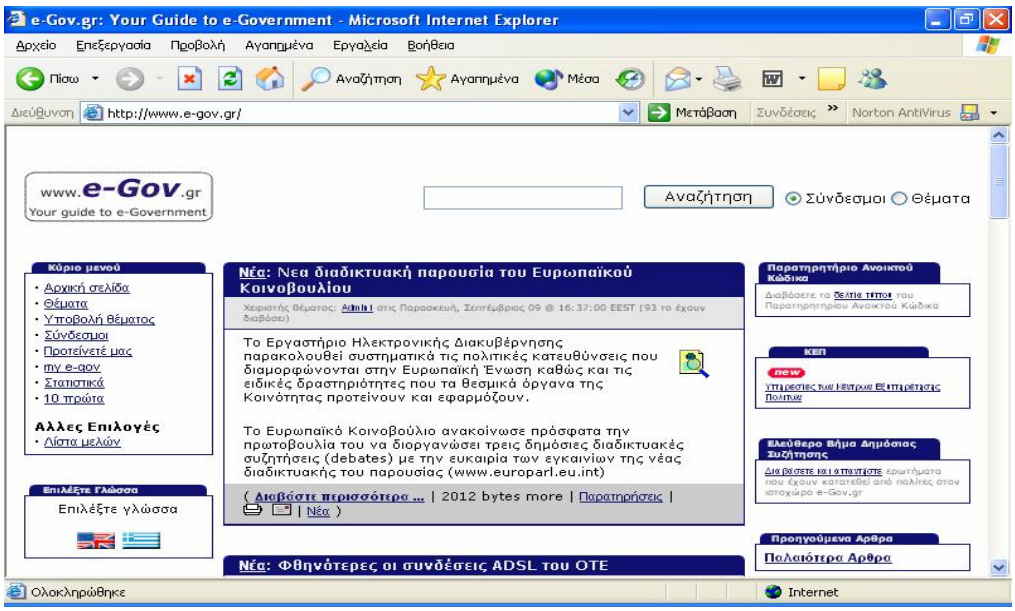
Οι ανωτέρω πρακτικές αποσκοπούν στη διασφάλιση της λειτουργίας των πληροφοριακών συστημάτων.

Παρακάτω θα αναλύσουμε μερικές από τις πιο βασικές εφαρμογές της ηλεκτρονικής διακυβέρνησης.

Ο οδηγός την ηλεκτρονικής πολιτείας (www.e-Gov.gr**)**

Το e-Gov είναι ένας κόμβος που έχει δημιουργηθεί από το Εργαστήριο Ηλεκτρονικής Διακυβέρνησης του Πανεπιστημίου Αθηνών και παρέχει πληροφορίες και πόρους σχετικά με την Ηλεκτρονική Πολιτεία. Σκοπός του e-Gov είναι να πληροφορεί τους

πολίτες και τις επιχειρήσεις στην Ελλάδα, τα στελέχη της διοίκησης και της τοπικής αυτοδιοίκησης, τους παροχής τεχνικών υπηρεσιών που επιθυμούν να είναι ενήμεροι για τα έργα και τα αποτελέσματα των ηλεκτρονικών κυβερνητικών υπηρεσιών, τους ερευνητές που ενδιαφέρονται για πρακτικά αποτελέσματα, ενώ περιλαμβάνει και δημοσιεύσεις και εκδηλώσεις σχετικά με την ηλεκτρονική διακυβέρνηση. Επίσης ο πολίτης μπορεί να υποβάλλει ερωτήσεις που αφορούν οικονομικές συναλλαγές και να πάρει άμεσα και έγκυρα απαντήσεις για όλα τα θέματα που τον απασχολούν. Στο e-Gov υπάρχουν και υποδείγματα αιτήσεων που μπορούν να χρησιμοποιηθούν στις συναλλαγές με το Δημόσιο (π.χ. έντυπο Υπεύθυνης Δήλωσης.)



Σχήμα 5.3: Ο δικτυακός τόπος www.e-Gov.gr

Οδηγός του πολίτη (www.polites.gr)

Ο κόμβος ανήκει στο Υπουργείο Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης και περιλαμβάνει μια πληθώρα υπηρεσιών που αφορούν τον πολίτη, τα δικαιώματα του, την καθημερινή ζωή, τη διαδικασία έκδοσης πιστοποιητικών και αδειών, την εργασία, την ασφάλιση και την ομογένεια. Ακόμα, ο πολίτης μπορεί να έχει την απαιτούμενη πληροφόρηση για τα δικαιώματα και τις υποχρεώσεις του απέναντι στις δημόσιες υπηρεσίες. ο δεύτερος πιο σημαντικός τομέας του κόμβου έχει να κάνει με την ενότητα ‘Καθημερινή Ζωή’, η οποία περιέχει πληροφορίες για τις δημόσιες επιχειρήσεις κοινής ωφελείας (ΟΤΕ, ΔΕΗ, ΔΕΥΑΠ, ΕΛΤΑ κ.τ.λ) και τους κανονισμούς που τις διέπουν.

Κέντρο Εξυπηρέτησης Πολιτών (www.1464.gr**)**

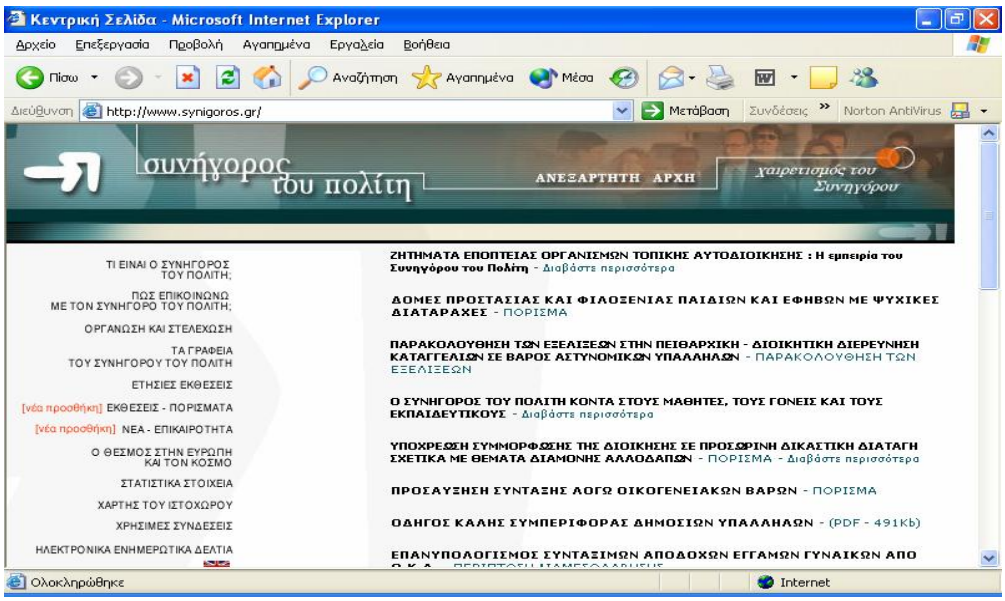
Στόχος του Κέντρου Εξυπηρέτησης Πολιτών είναι η ενημέρωση των πολιτών για τις διαδικασίες που ακολουθούνται στις δημόσιες υπηρεσίες και η διευκόλυνση στις συναλλαγές με το δημόσιο. Επίσης, μειώνει την χρονοβόρα γραφειοκρατική διαδικασία, ενώ υπάγεται στο υπό κατασκευή 'Δίκτυο Αριάδνη' που θα συμβάλει στην αποκέντρωση των κρατικών υπηρεσιών. Επιπλέον, μέσα στις σελίδες του **www.1464.gr** θα βρείτε το link προς τον κόμβο του Εθνικού Τυπογραφείου που παρέχει την δυνατότητα αναζήτησης των Φ.Ε.Κ, των Φύλλων της Εφημερίδας της Κυβερνήσεως, ενώ από την ίδια σελίδα μπορεί ο πολίτης να λάβει γνώση και του αναθεωρημένου Συντάγματος.

Σχήμα 5.4: Ο δικτυακός τόπος www.1464.gr

Συνήγορος του Πολίτη (www.synigoros.gr**)**

Πρόκειται για μια ανεξάρτητη αρχή, η οποία άρχισε να λειτουργεί πριν από τρία χρόνια και παρέχει δωρεάν τις υπηρεσίες της. Σκοπός της είναι να ερευνά ατομικές διοικητικές πράξεις, παραλείψεις των δημοσίων υπηρεσιών που παραβιάζουν τα νομικά δικαιώματα των πολιτών. Στον κόμβο του συνηγόρου (www.synigoros.gr) μπορεί ο

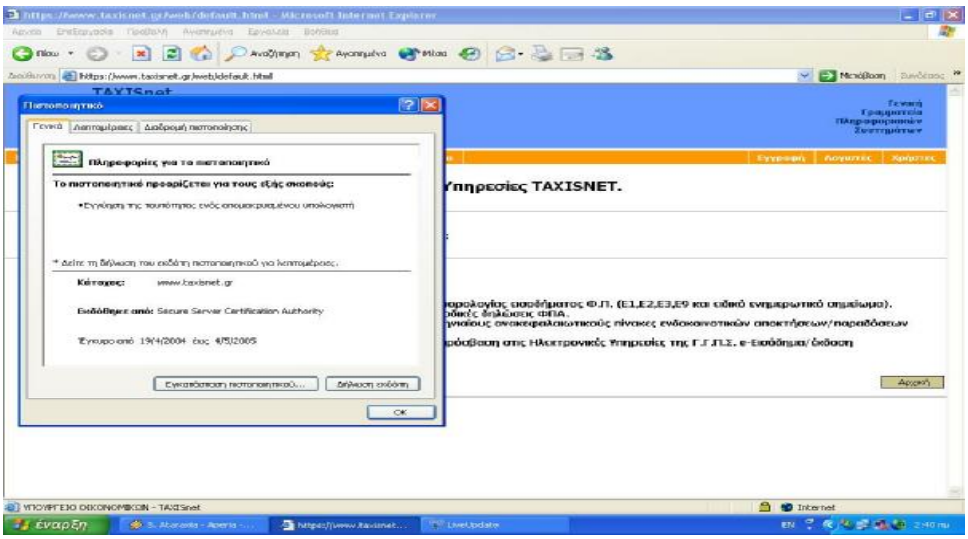
πολίτης να κάνει αίτηση στην οποία θα αναφέρονται τα στοιχεία του, για οποιοδήποτε πρόβλημα με δημόσια υπηρεσία.



Σχήμα 5.5: Ο δικτυακός τόπος www.synigoros.gr

Δήλωση εισοδήματος και Φ.Π.Α (www.taxisnet.gr)

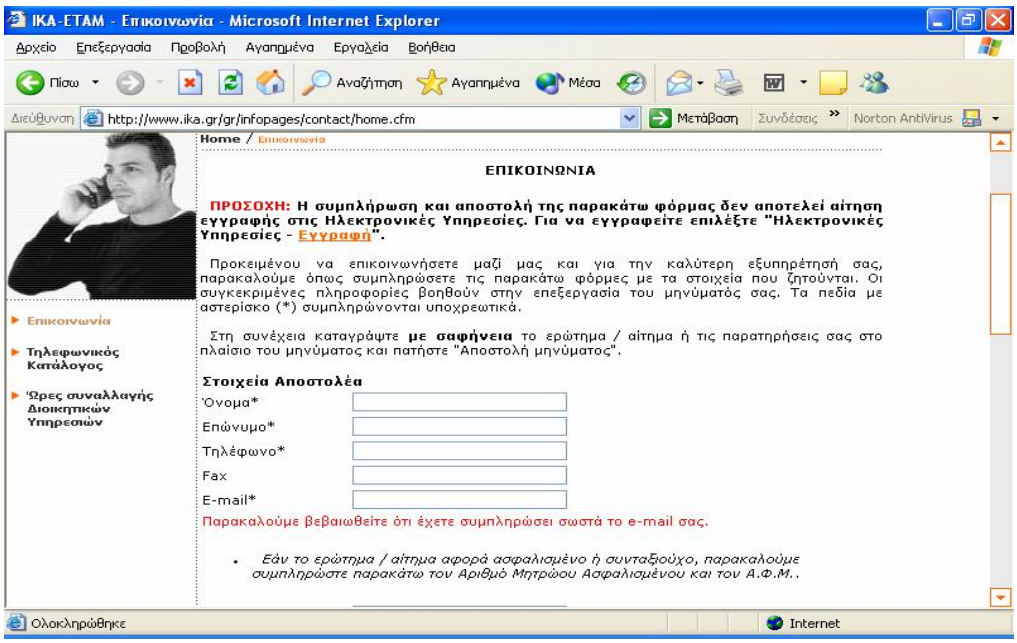
Ο ενδιαφερόμενος θα πρέπει να συμπληρώσει μια φόρμα εγγραφής στο σύστημα. Η φόρμα απαιτεί ορισμένες βασικές πληροφορίες καθώς και την ηλεκτρονική διεύθυνση του ενδιαφερόμενου. Μετά την εγγραφή και την πιστοποίηση του ενδιαφερόμενου αποστέλλεται απαντητικό e-mail με τον κωδικό χρήστη και το συνθηματικό του για πρόσβαση στην ηλεκτρονική υπηρεσία. Τα στοιχεία που έχουν υποβληθεί ελέγχονται και, εφ' όσον πιστοποιηθεί η ορθότητα τους, εκδίδεται ένας κωδικός χρήστη (username) και μια συνθηματική λέξη (password) τα οποία και αποστέλλονται στο νέο χρήστη μέσω e-mail. Οι κωδικοί ονόματος και τα συνθηματικά που εκδίδονται από το Υπουργείο Οικονομικών για κάθε χρήστη είναι μοναδικά και προσωπικά.



Σχήμα 5.6: Ο δικτυακός τόπος www.taxisnet.gr

Ηλεκτρονικές υπηρεσίες για ασφαλιστικά θέματα (www.ika.gr**)**

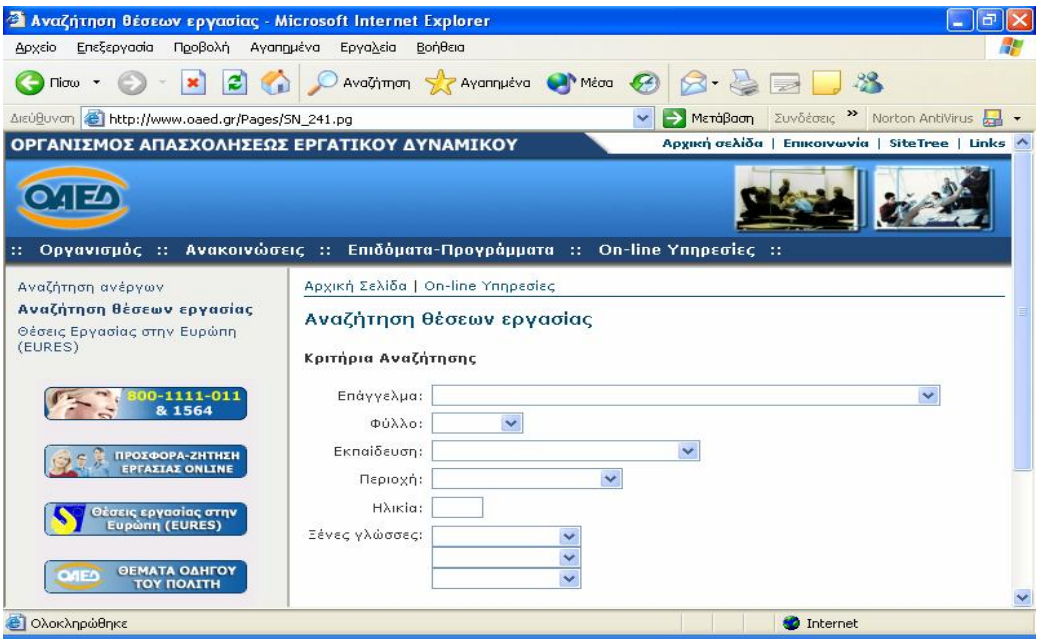
στο πλαίσιο του e-government, μια από τις υπηρεσίες που εκσυγχρονίζονται είναι και η αποστολή της Αναλυτικής Περιοδικής Δήλωσης (ΑΠΔ) του ΙΚΑ. για να έχετε πρόσβαση στην online υπηρεσία θα πρέπει να γίνει η εγγραφή πρώτα, δίνοντας την διεύθυνση e-mail θα αποσταλεί από το ΙΚΑ ένας προσωρινός κωδικός πρόσβασης και το link για να συνεχιστεί η διαδικασία εγγραφής. Εκεί θα πρέπει να συμπληρωθούν τα πλήρη στοιχεία εν συνεχεία το ΙΚΑ αποστέλλει ταχυδρομικά (με courier) τον κωδικό πρόσβασης (PIN) και τον κωδικό μεταβολής στοιχείων και επικοινωνίας (PUK), ενώ ταυτόχρονα μέσω E-mail αποστέλλεται και το user name. Μόλις ληφθεί το PIN και το PUK, συνίσταται η αλλαγή τους για λόγους ασφάλειας.



Σχήμα 5.7: Ο δικτυακός τόπος www.ika.gr

Αναζήτηση εργασίας μέσω του δικτύου (www.oaed.gr/on-line.htm)

Το site του ΟΑΕΔ παρέχει μια ουσιαστικά υπηρεσία στους άνεργους που είναι εγγεγραμμένοι στον οργανισμό όσο και στους ελεύθερους επαγγελματίες που χρειάζονται προσωπικό. Η υπηρεσία δεν απαιτεί κανένα είδους εγγραφή και είναι προσβάσιμη από όλους, ενώ προσφέρει μόνο ενημερωτικό υλικό. Για τις περαιτέρω διαδικασίες θα πρέπει να απευθυνθεί κάποιος στα γραφεία του ΟΑΕΔ.



Σχήμα 5.8: Ο δικτυακός τόπος www.oaed.gr

5.3 E-Banking

5.3.1 Εισαγωγή

Με τον όρο e-banking εννοούμε κάθε τραπεζική συναλλαγή που γίνεται μέσω του Διαδικτύου.

Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο. Υπάρχουν εκτιμήσεις ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών. Ενδεικτικά, στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7%.

Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω Διαδικτύου. Τα αποτελέσματα της Εθνικής Έρευνας για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας δείχνουν ότι το 2001 περίπου 150.000 πελάτες (1%-1,5% του πληθυσμού) πραγματοποίησαν τραπεζικές συναλλαγές ηλεκτρονικά. Το 2002 ο αριθμός αυτός ξεπέρασε τους 250.000 (2,5% του συνολικού πληθυσμού). Σύμφωνα με εκτιμήσεις τραπεζών, το 2001 ο τζίρος από online τραπεζικές συναλλαγές έφθασε τα 2 δισ. ευρώ. Το 2002 το ποσό αυτό εκτιμάται ότι αυξήθηκε σε 10 δισ. ευρώ.

Σύμφωνα με στοιχεία της Τράπεζας Πειραιώς, οι συναλλαγές μέσω Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξάνονται με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης, το 50% όλων των πληρωμών ΙΚΑ πραγματοποιείται online, ενώ οι ηλεκτρονικές χρηματιστηριακές συναλλαγές υπερβαίνουν το 15% επί του συνόλου.

5.3.2 Η σημερινή κατάσταση

Μέχρι σήμερα μπορούμε να πούμε ότι οι συναλλαγές μέσω Internet στον χώρο του συνόλου των χρηματοοικονομικών υπηρεσιών αφορούν κατά κύριο λόγο στις χρηματιστηριακές συναλλαγές. Από τα μέχρι σήμερα δεδομένα τα συμπεράσματα για την πορεία του online banking δεν είναι ενθουσιώδη αλλά ούτε και αποκαρδιωτικά.

Ένα σημαντικό στοιχείο που παίζει μεγάλο ρόλο είναι το ζήτημα της ασφάλειας. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό αφού ακριβώς εδώ θα βασίζονται οι τράπεζες για να αναπτύξουν τα ηλεκτρονικά συστήματα συναλλαγών μέσω Internet. Επιπλέον, το μεγαλύτερο πλεονέκτημα των ηλεκτρονικών τραπεζικών συναλλαγών σίγουρα το χαμηλό λειτουργικό κόστος τους. Σε γενικές γραμμές, τα λειτουργικά έξοδα μιας ηλεκτρονικής τράπεζας υπολογίζονται περίπου στο μισό αυτών μιας συμβατικής τράπεζας, ενώ μια τραπεζική συναλλαγή κοστίζει περίπου πέντε φορές φθηνότερα όταν πραγματοποιείται μέσω Internet από ό,τι μέσω του παραδοσιακού τρόπου. Το σημαντικό αυτό γεγονός αυτό δίνει στις τράπεζες το περιθώριο να παρέχουν υψηλότερο τόκο στις καταθέσεις και να χορηγούν δάνεια με χαμηλότερο επιτόκιο μέσω Internet.

5.3.3 Ηλεκτρονική Πληρωμή

Για την αναβάθμιση του τρόπου εκκαθάρισης των τραπεζικών συναλλαγών προτάθηκαν και εφαρμόστηκαν τρεις κυρίως λύσεις που συνοψίζονται στον όρο ηλεκτρονική πληρωμή. Πρώτος είναι η ηλεκτρονική καταβολή μέσω ηλεκτρονικής μεταφοράς κεφαλαίων (EFT), δεύτερος η χρήση πιστωτικών καρτών για συναλλαγές που γίνονται στο διαδίκτυο και τρίτος το ηλεκτρονικό χρήμα.

Ηλεκτρονική μεταφορά κεφαλαίων

Η ηλεκτρονική μεταφορά πίστωσης είναι πράξη πραγματοποιούμενη με πρωτοβουλία του εντολέως μέσω ιδρύματος ή υποκαταστήματος ιδρύματος, με σκοπό να τεθεί στη

διάθεση του δικαιούχου χρηματικό ποσό σε ένα ίδρυμα ή υποκατάστημα ιδρύματος. Ο εντολέας και ο δικαιούχος είναι δυνατόν να είναι ένα και το αυτό πρόσωπο. Η ηλεκτρονική μεταφορά κεφαλαίων είναι δυνατόν να είναι και διασυνοριακή, δηλαδή η μεταφορά να γίνεται όχι μόνο μέσα στο ίδιο κράτος αλλά και μεταξύ κρατών. Στην Ελλάδα τα θέματα των διασυνοριακών μεταφορών πιστώσεων ρυθμίζει το Π.Δ. 33/2000, το οποίο εναρμονίζει την ελληνική νομοθεσία με την Οδηγία 1997/5. Στην Ευρώπη ισχύει ακόμη και ο Κανονισμός 2560/2001.

Πιστωτικές κάρτες

Κατά την πληρωμή μέσω πιστωτικών καρτών στο διαδίκτυο ο αγοραστής κοινοποιεί στον πωλητή τον αριθμό της πιστωτικής του κάρτας, την οποία ο τελευταίος χρεώνει με το συμφωνηθέν τίμημα. Αυτός ο τρόπος πληρωμής πρόκειται για ένα σύστημα ταυτόχρονης πληρωμής, που παρέχει άμεση πρόσβαση στους τραπεζικούς λογαριασμούς του αγοραστή και του πωλητή και καταγράφει άμεσες μεταβολές στους λογαριασμούς τους. Στην Ελλάδα τα θέματα των συναλλαγών που γίνονται με πιστωτική κάρτα ρυθμίζει η Υπουργική απόφαση Ζ1-178/2001 που εναρμόνισε τις διατάξεις της Σύστασης 97/489 στην ελληνική νομοθεσία. Στην Ευρώπη ισχύουν επίσης η Οδηγία 1997/7/ΕΚ και οι Οδηγίες 1987/102 και 1990/88 που ρυθμίζουν θέματα σχετικά με την καταναλωτική πίστη. Ενδεικτικά αναφέρονται και δύο αποφάσεις ελληνικής νομολογίας που σχετίζονται με θέματα πληρωμής μέσω πιστωτικών καρτών, η απόφαση του Εφετείου Αθήνας 2319/1999 και η απόφαση του Αρείου Πάγου 589. 2001.

Ηλεκτρονικό Χρήμα

Ηλεκτρονικό χρήμα ένα σύγχρονό μέσο πληρωμής στο διαδίκτυο. Βασίζεται στην ανταλλαγή πραγματικού χρήματος σε μια τράπεζα με ηλεκτρονικό τρόπο. Ένα συγκεκριμένο, δηλαδή, ποσό αληθινών χρημάτων ανταλλάσσεται με «κυβερνονομίσματα». Για την ύπαρξη δηλαδή ηλεκτρονικού χρήματος είναι απαραίτητα τρία στοιχεία α) η νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη να είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα, 2) να έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού τουλάχιστον ίσου με την εκδοθείσα

νομισματική αξία, και 3) γίνεται δεκτή ως μέσο πληρωμής από άλλες επιχειρήσεις πέραν της εκδότριας. Στην Ελλάδα θέματα σχετικά με το ηλεκτρονικό χρήμα ρυθμίζουν η Απόφαση του Συμβουλίου Νομισματικής Πολιτικής 50/2002, ο Νόμος 3148/2003 και η ΠΔΤΕ 2501/2002. Στην Ευρώπη ισχύουν η Οδηγία 2000/12 που ρυθμίζει όλα τα σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων, με τις τροποποιήσεις της Οδηγίας 2000/28. Επίσης η Οδηγία 2000/46 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, η Σύσταση 87/598 για τον ευρωπαϊκό κώδικα δεοντολογίας σε θέματα ηλεκτρονικών πληρωμών και η Σύσταση 88/590.

5.3.4 Τι μπορώ να κάνω ONLINE;

Παρακάτω θα δούμε συνοπτικά ποιες τραπεζικές συναλλαγές μπορούν να πραγματοποιηθούν μέσω Internet, έχοντας φυσικά ως προϋπόθεση ότι έχει ανοιχτεί λογαριασμός σε κάποια από τις τράπεζες που έχουν αναπτύξει το online banking.
Οι πελάτες μιας ηλεκτρονικής τράπεζας μπορούν να διενεργούν μεταφορές χρημάτων, να στέλνουν χρήματα σε οποιοδήποτε σημείο του κόσμου, να βλέπουν ανά πάσα στιγμή τις κινήσεις των λογαριασμών τους, τα υπόλοιπά τους και να κάνουν αιτήσεις για προϊόντα που παρέχονται από την Τράπεζα, 24 ώρες το 24ωρο, χωρίς να επηρεάζονται από εξωτερικούς παράγοντες και με μέγιστη ασφάλεια.

Αν έχετε ήδη λογαριασμό σε μία από τις τράπεζες που έχουν αναπτύξει ηλεκτρονικό σύστημα συναλλαγών μπαίνετε στο site τους και συμπληρώνετε τη σχετική αίτηση. Λίγες ημέρες αργότερα λαμβάνετε με ταχυδρομείο ή παραλαμβάνετε προσωπικά από ένα υποκατάστημα τους κωδικούς σας και κατόπιν μπορείτε μέσω Internet να πραγματοποιείτε εύκολα και γρήγορα τις συναλλαγές σας:

- Διαχείριση λογαριασμών (Υπόλοιπο-Τόκοι)
- Έλεγχος τελευταίων κινήσεων λογαριασμών
- Αναλυτικές Κινήσεις λογαριασμών

- Μεταφορά κεφαλαίων μεταξύ λογαριασμών όψεως ή ταμιευτηρίου
- Εντολές πληρωμής υπολοίπου πιστωτικών καρτών, δόσεων δανείου, εμβασμάτων ή επιταγών
- Διαχείριση των παραμέτρων ασφαλείας (Αλλαγή PIN κ.λπ.)
- Αιτήσεις για διάφορα τραπεζικά προϊόντα

5.3.5 Πόσο ασφαλές είναι το e-banking;

Υπάρχουν πολλά συστήματα που χρησιμοποιούνται στο Internet για τη διασφάλιση των μεταδιδόμενων πληροφοριών κατά την διεξαγωγή ηλεκτρονικών συναλλαγών. Τα κυριότερα πρωτόκολλα που χρησιμοποιούνται για την ασφαλή μεταβίβαση πληροφοριών είναι τα ακόλουθα: Cybercash, SET (ηλεκτρονικές πληρωμές), SSL, PCT, TLS (κρυπτογράφηση σε επίπεδο TCP/IP), PGP, S/MIME (e-mail), S-HTTP (Web browsing). Στο Web το SSL είναι το κυρίαρχο και χρησιμοποιείται για τη δημιουργία ενός κρυπτογραφημένου καναλιού μέσα από το οποίο μεταφέρονται κρυπτογραφημένες κάθε είδους πληροφορίες, ενώ το SET αποτελεί ένα σχετικά νεότερο πρωτόκολλο.

5.3.5.1 SSL

Το SSL (Secure Sockets Layer) εξασφαλίζει τη δημιουργία ενός ασφαλούς διαύλου επικοινωνίας. Μέσα από το κανάλι αυτό μπορεί να μεταδίδεται πληροφορία από τους Web servers και clients (HTTP) αλλά και κάθε άλλης μορφής (π.χ. e-mail, news). Το κανάλι εγγυάται ότι τα δεδομένα θα μεταφερθούν ακέραια και ότι το περιεχόμενό τους δεν πρόκειται να αλλάξει κατά τη διάρκεια της μεταφοράς, ενώ πιστοποιεί τον Web server, δηλαδή ο Web browser επιβεβαιώνει ότι ο server είναι αυτός που δηλώνει ότι είναι. Η πληροφορία πρώτα κρυπτογραφείται και έπειτα μεταδίδεται (ταυτόχρονα συμπιέζεται) για να αποκρυπτογραφηθεί από τον Web browser. Αποτελεί αδιαφανή για το χρήστη διαδικασία, ο οποίος δεν αντιλαμβάνεται τίποτα από όλα αυτά παρά μόνο τα σημάδια στον browser του: Το "http" έχει μετατραπεί σε "https://" και υπάρχει ένα

σύμβολο κλειστής κλειδαριάς (λουκέτου) στο κάτω μέρος της οθόνης. Όταν σε μια σύνδεση χρησιμοποιείται το SSL, οτιδήποτε μεταφέρεται ανάμεσα στο χρήστη και τον Web server είναι κρυπτογραφημένο, όπως το URL του κειμένου, τα περιεχόμενα του κειμένου που μεταδίδεται, τα περιεχόμενα που αποστέλλονται από το χρήστη μέσω φορμών (άρα και τα στοιχεία του πελάτη και ο αριθμός της πιστωτικής κάρτας του). Το SSL εγγυάται ότι οι πληροφορίες που εισαγάγουμε σε μια φόρμα θα φτάσουν στον προορισμό τους αναλλοίωτες. Για να το πετύχει αυτό χρησιμοποιεί συμμετρική κρυπτογράφηση. Οι πληροφορίες που μεταδίδονται κρυπτογραφούνται με βάση ένα μυστικό κλειδί που έχει δημιουργηθεί για την περίσταση, το οποίο γνωρίζουν ο browser του χρήστη και ο server. Επίσης, εγγυάται ότι οι πληροφορίες στέλνονται στο σωστό άνθρωπο και όχι σε τρίτους.(βλέπε κεφ. 4.3)

5.3.5.2 SET

Σε αντίθεση με το SSL, το SET (Secure Electronic Transactions) αποτελεί εξειδικευμένο πρωτόκολλο για τη διασφάλιση των ηλεκτρονικών συναλλαγών μέσω πιστωτικών καρτών, ενώ πρόσφατα αρχίζει να χρησιμοποιείται και στις ηλεκτρονικές τραπεζικές συναλλαγές. Κατασκευάζεται από τις Visa, MasterCard, IBM, Netscape, Microsoft, GTE, Verisign. Στο SET αυτοί που συμμετέχουν σε μια συναλλαγή είναι ο πελάτης, ο έμπορος, η τράπεζα του πελάτη και η τράπεζα του εμπόρου, καθένας από τους οποίους πρέπει να έχει ψηφιακά πιστοποιητικά (digital certificates). Με τη χρήση των ψηφιακών αυτών πιστοποιητικών επιβεβαιώνεται από τα συναλλασσόμενα μέρη (πωλητής και έμπορος) η ταυτότητά τους. Αυτό αποτελεί την πρώτη φάση της συναλλαγής (αυθεντικοποίηση των δύο μερών). Οι πελάτες επιβεβαιώνουν ότι οι έμποροι από τους οποίους επιθυμούν να αγοράσουν είναι νόμιμοι μέσα από την ψηφιακή ταυτότητά τους, όπως και οι έμποροι για τους πελάτες. Η εμπιστοσύνη αυτή εδραιώνεται μέσω των πιστοποιητικών που έχουν εκδοθεί από τρίτες αρχές (π.χ. τράπεζες). Ένα πιστοποιητικό περιέχει το όνομα του προσώπου για το οποίο εκδίδεται (έμπορος ή πελάτης), την ψηφιακή υπογραφή του, το δημόσιο (και το αντίστοιχο ιδιωτικό κλειδί του) και την υπογραφή της αρχής που εξέδωσε το πιστοποιητικό. Όταν ο πελάτης δώσει μια παραγγελία, ο browser του λαμβάνει το πιστοποιητικό του εμπόρου, προκειμένου να ελεγχθεί αν είναι όντως νόμιμος - αν σχετίζεται με κάποιον

χρηματοπιστωτικό οργανισμό. Στη συνέχεια στέλνεται στον έμπορο η παραγγελία κρυπτογραφημένη με το δημόσιο κλειδί του εμπόρου. Στην τράπεζα στέλνεται πληροφορία σχετικά με την πληρωμή, κρυπτογραφημένη με το δημόσιο κλειδί της τράπεζας. Το μεγάλο πλεονέκτημα του SET είναι ότι με αυτό τον τρόπο δε στέλνεται πληροφορία με τον αριθμό της πιστωτικής κάρτας στον έμπορο. Το SET δεν έχει ακόμα χρησιμοποιηθεί ευρέως, σε αντίθεση με το SSL, το οποίο διατηρεί το μεγαλύτερο μερίδιο στις ασφαλείς ηλεκτρονικές συναλλαγές. Σιγά σιγά εμφανίζονται προϊόντα από μεγάλες εταιρείες του χώρου που χρησιμοποιούν το πρωτόκολλο.(βλέπε κεφ. 4.4)

5.3.5.3 Ψηφιακά Πιστοποιητικά

Είναι γεγονός αναμφισβήτητο ότι η απόκτηση εμπιστοσύνης που επιτυγχάνεται κατά τις συμβατικές συναλλαγές μέσω της οπτικής επαφής των δύο συναλλασσομένων μερών δεν είναι δυνατή όταν πρόκειται για συναλλαγές μέσω Web. Έτσι, είναι αναγκαία η ύπαρξη ενιαίας υποδομής, η οποία θα προστατεύει τις ιδιωτικές πληροφορίες από τρίτους (Privacy). Η πληροφορία που ανταλλάσσεται ανάμεσα στα δύο μέρη (αποστολέας και παραλήπτης, πελάτης και έμπορος) δεν πρέπει να καταλήγει σε τρίτους. Εξίσου σημαντικό στοιχείο είναι η επικύρωση της ταυτότητας (authentication) των επικοινωνούντων μερών. Η πιστοποίηση της ταυτότητας του χρήστη και κάθε συναλλαγή του εξασφαλίζονται με τη βοήθεια ενός μοναδικού ψηφιακού πιστοποιητικού (digital certificate). Αυτό το πιστοποιητικό αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές και τις μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο υπολογιστή. Τα πιστοποιητικά αυτά εξασφαλίζονται εγκαθιστώντας ένα πρόγραμμα από την αντίστοιχη εταιρία πιστοποίησης.

Ο αποστολέας πρέπει να γνωρίζει ότι οι πληροφορίες που στέλνει έχουν ως παραλήπτη το συγκεκριμένο πρόσωπο. Ο Α πρέπει να είναι σίγουρος ότι ο Β, με τον οποίο επικοινωνεί, είναι όντως αυτός που ισχυρίζεται ότι είναι. Άλλο σημαντικό θέμα είναι η διασφάλιση της ακεραιότητας των δεδομένων που αποστέλλονται. Τα στοιχεία μιας συναλλαγής πρέπει να φτάσουν στον προορισμό τους αυτούσια. Ακόμα κι αν πέσουν σε χέρια τρίτων, να είναι έτσι κρυπτογραφημένα ώστε να τους είναι άχρηστα - να μην

μπορούν να τα εκμεταλλευτούν. Τα συναλλασσόμενα μέρη πρέπει να μην έχουν τη δυνατότητα άρνησης της συμμετοχής τους σε μια συναλλαγή.

Το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές τραπεζικές συναλλαγές πρέπει να αναγνωρίζονται από το νομικό καθεστώς της χώρας στην οποία πραγματοποιείται. Μια ψηφιακή υπογραφή σε ένα κείμενο πρέπει να έχει την ίδια βαρύτητα με τη φυσική υπογραφή σε μια νομική αρχή, σε ένα δικαστήριο. Η ασφάλεια των αριθμών των πιστωτικών καρτών είναι βασική προϋπόθεση για την ευρεία διάδοση του ηλεκτρονικού εμπορίου. Οι πελάτες θέλουν να είναι σίγουροι ότι οι πληροφορίες των πιστωτικών καρτών τους είναι ασφαλείς καθώς μεταβιβάζονται μέσω Internet και ότι έχουν ως αποδέκτη έναν νόμιμο πωλητή ή αρχή. Αντίστοιχα, οι έμποροι πρέπει να γνωρίζουν ότι οι πληροφορίες που λαμβάνουν αντιστοιχούν σε νόμιμους κατόχους πιστωτικών καρτών. Η υποδομή αυτή στηρίζεται στην κρυπτογράφηση. Με τη συμμετρική κρυπτογράφηση επιτυγχάνεται η διασφάλιση του απορρήτου και της ακεραιότητας των πληροφοριών που στέλνονται μεταξύ των συναλλασσόμενων μερών. Έτσι, αν βρεθούν στα χέρια τρίτων, θα τους είναι άχρηστες, αφού οι τελευταίοι δε θα μπορούν να αντιληφθούν το περιεχόμενό τους.

Για την επίτευξη της ταυτοποίησης χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού. Με αυτό τον τρόπο κάθε συναλλασσόμενο μέρος αναγνωρίζεται ως τέτοιο με βάση το ψηφιακό πιστοποιητικό (Digital ID) που έχει αποκτήσει. Το ψηφιακό πιστοποιητικό είναι αντίστοιχο με την ταυτότητα, το δίπλωμα οδήγησης, το διαβατήριο και την πιστωτική κάρτα και εκδίδεται από αρχές πιστοποίησης (Certification Authorities, CA). Η ακεραιότητα διασφαλίζεται και με τη χρήση των ψηφιακών υπογραφών. Ο αποστολέας υπογράφει ψηφιακά την πληροφορία με το ιδιωτικό κλειδί του και την αποστέλλει. Όταν ο παραλήπτης λάβει το μήνυμα, ελέγχει την ψηφιακή υπογραφή του αποστολέα. Αν όντως υπάρχει, το μήνυμα έχει φτάσει ακέραιο, διαφορετικά έχει αλλάξει κατά τη μεταφορά του.

Οι browsers χρησιμοποιούν το πιστοποιητικό για να αποκρυπτογραφήσουν πληροφορία που στέλνεται προς εμάς. Με τη δημιουργία του πιστοποιητικού δημιουργούμε ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό). Όποιος θέλει να μας στείλει εμπιστευτικές πληροφορίες τις κρυπτογραφεί με το δημόσιο κλειδί μας, οπότε μόνο εμείς με το ιδιωτικό κλειδί μας μπορούμε να τις αποκρυπτογραφήσουμε. Η συνεχής

εξέλιξη των πρωτοκόλλων ασφαλείας στο Internet αποτελεί την καλύτερη εγγύηση αλλά και την πιο ικανοποιητική απάντηση στο ερώτημα αν οι πραγματοποίηση τραπεζικών συναλλαγών μέσω του Διαδικτύου είναι σίγουρη και ασφαλής[22][23].

5.3.6 Υπηρεσίες e-banking

Στην Ελλάδα, υπηρεσίες e-banking προσφέρουν οι εξής τράπεζες:

- Εθνική Τράπεζα
- Marfin Egnatia Bank
- Winbank, Τράπεζα Πειραιώς
- Citibank Online
- Alpha Web Banking
- Eurobank
- NovaWeb της NovaBank
- Τράπεζα Κύπρου
- Emporiki e.Banking

Παρακάτω θα αναφερθούμε σε κάποιες από αυτές.

5.3.6.1 ALPHA ΤΡΑΠΕΖΑ ΠΙΣΤΕΩΣ (www.alpha.gr)

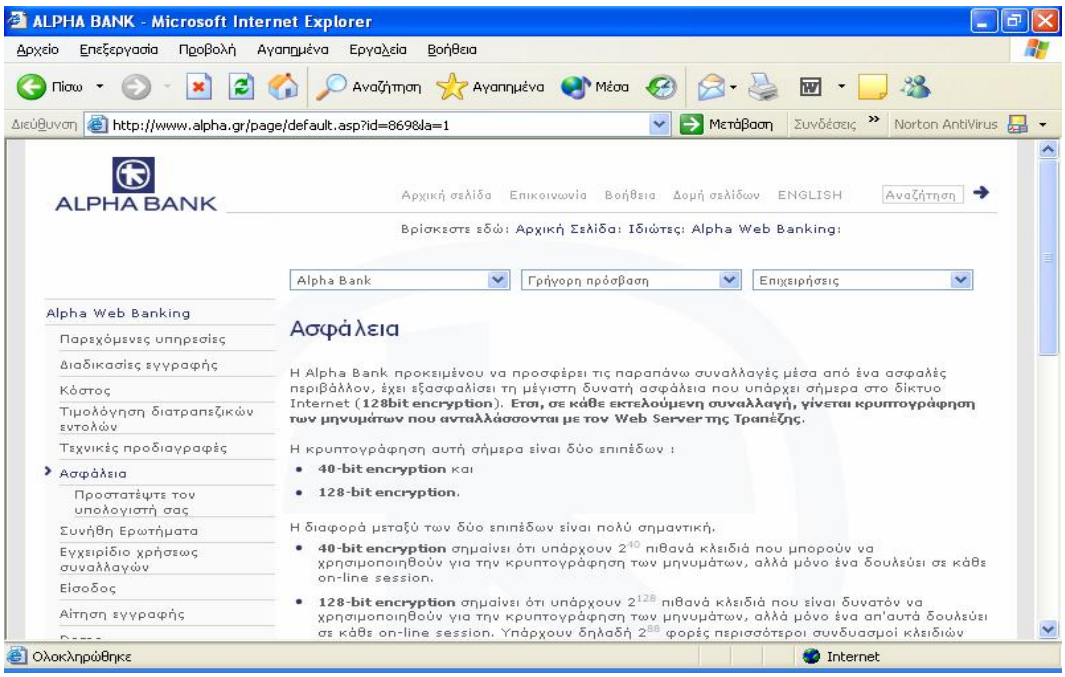
Η Alpha Τράπεζα Πίστεως (η πρώτη ελληνική τράπεζα που ανέπτυξε σύστημα ATM) προσφέρει από το Νοέμβριο του 1998 στους Πελάτες της τη δυνατότητα εκτελέσεως τραπεζικών συναλλαγών μέσω του Internet με το σύστημα Alpha Web Banking. Η

τεχνολογική υποδομή αναπτύχθηκε σε συνεργασία με την Unisystems και με βάση το πακέτο FBA – Netbanker.

Οι δυνατότητες εκτελέσεως τραπεζικών συναλλαγών μέσω του Alpha Web Banking, που εκτελούνται μέσα από ένα πλήρως ασφαλές περιβάλλον, είναι οι εξής:

- Μεταφορές χρημάτων μεταξύ τραπεζικών λογαριασμών
- Πληρωμή λογαριασμών κοινής ωφελείας (ΔΕΗ, ΟΤΕ κλπ) και Καρτών
- Ενημέρωση για τις κινήσεις, το υπόλοιπο και τους τόκους των λογαριασμών
- Ενημέρωση για τις τιμές ξένων χαρτονομισμάτων και συναλλάγματος
- Ενημέρωση για τις τιμές μετοχών επιλεγμένων εταιριών
- Ενημέρωση για τις επιταγές
- Ενημέρωση για το λογαριασμό των καρτών

Οι υπηρεσίες του Alpha Web Banking προσφέρονται δωρεάν στους συνδρομητές του. Με το Alpha Web Banking όλες οι συναλλαγές είναι ασφαλείς, αφού η Alpha Τράπεζα Πίστεως έχει πιστοποιηθεί από την, ειδική για θέματα ασφαλείας, διεθνή αμερικανική εταιρία Verisign Inc. για την ασφάλεια των συναλλαγών. Έτσι η Τράπεζα εξασφαλίζει τη μέγιστη δυνατή ασφάλεια που υπάρχει σήμερα στο δίκτυο Internet (128 bit encryption). Σε κάθε εκτελούμενη συναλλαγή, γίνεται κρυπτογράφηση των μηνυμάτων που ανταλλάσσει ο πελάτης με τον Web Server της Τραπέζης. 128 bit encryption σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που είναι πιθανόν να χρησιμοποιηθούν για την κρυπτογράφηση των μηνυμάτων αλλά μόνο ένα από αυτά δουλεύει σε κάθε on-line session. Εκτός της κρυπτογραφήσεως, ο συνδρομητής χρησιμοποιεί προσωπικούς κωδικούς (Κωδικός Συνδρομητή, Μυστικούς Κωδικούς Προσβάσεως) για να συνδεθεί στο σύστημα, ενώ η Τράπεζα χρησιμοποιεί επιπρόσθετα συστήματα ασφαλείας (Firewall), τα οποία ελέγχουν και καταγράφουν την πρόσβαση κάθε συνδρομητή στα συστήματα της.



Σχήμα 5.9: Ο δικτυακός τόπος **www.alpha.gr**

5.3.6.2 MARFIN EGNATIA BANK (www.marfinegnatia.gr)

Μέσω της υπηρεσίας eBanking της MARFIN EGNATIA BANK μπορείτε να επισκεφθείτε την τράπεζά σας οποιαδήποτε ώρα της μέρας και να πραγματοποιήσετε ένα ευρύ φάσμα τραπεζικών συναλλαγών. Πιο συγκεκριμένα σας δίνεται η δυνατότητα για:

- Αυτόματη μεταφορά χρηματικών ποσών εντός MARFIN EGNATIA BANK αλλά και σε λογαριασμούς τρίτων στην Ελλάδα και στο εξωτερικό
- Πληρωμές Δημοσίου, ΦΠΑ, ΙΚΑ, ΤΕΒΕ, Φόρου Εισοδήματος και Τελών Κυκλοφορίας
- Πληρωμές λογαριασμών ΔΕΚΟ, ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ και άλλων οργανισμών
- Πληρωμές λογαριασμών κινητής και σταθερής τηλεφωνίας
- Πληρωμές πιστωτικών καρτών έκδοσης MARFIN EGNATIA BANK και άλλων τραπεζών
- Αίτηση για ανάκληση επιταγής

- Αίτηση παραγγελίας συναλλάγματος
- Δυνατότητα μεμονωμένων συναλλαγών (που αφορούν συγκεκριμένη πληρωμή) ή επαναλαμβανόμενων συναλλαγών (πάγιες / περιοδικές πληρωμές)
- Δυνατότητα ειδοποιήσεων (Alerts) στο κινητό τηλέφωνο μέσω SMS ή στον υπολογιστή μέσω e-mail κάθε φορά που οι συναλλαγές πραγματοποιούνται με επιτυχία ή δεν εκτελούνται από την Τράπεζα για οποιονδήποτε λόγο

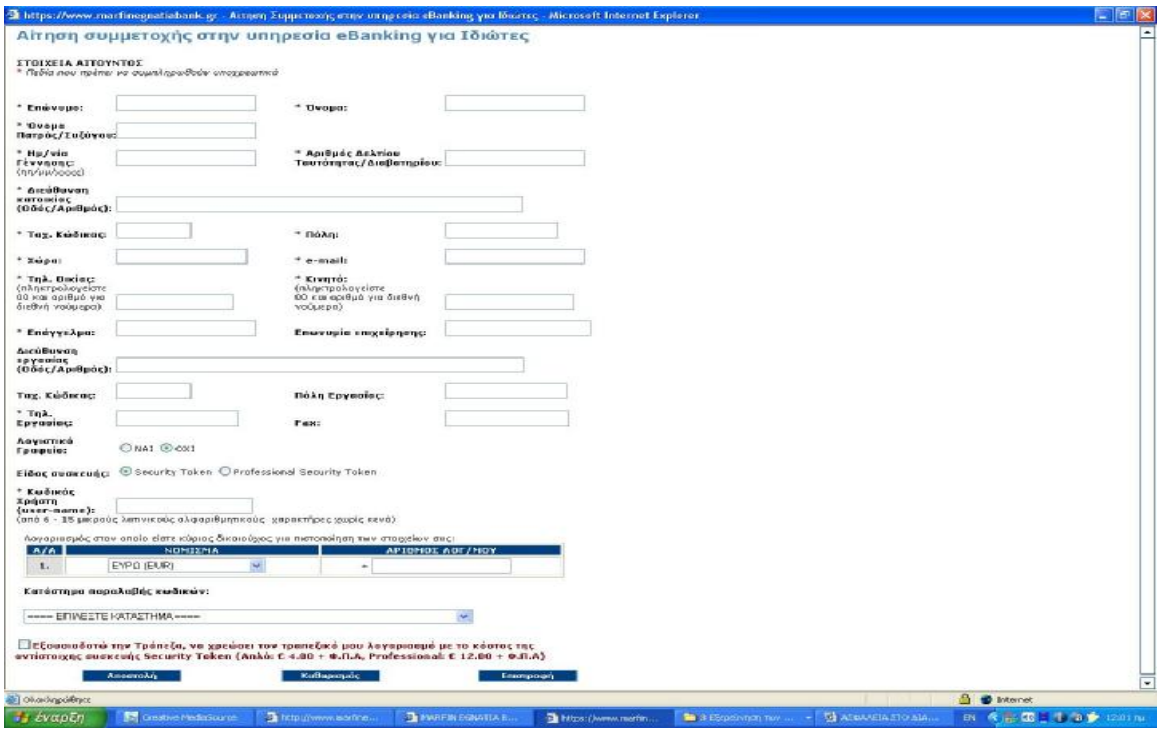
Ειδικά για τις εταιρίες

- Αποστολή αρχείου μέσω διαδικτύου για μαζικές πληρωμές προς τρίτους ή μισθοδοσίας
- Δυνατότητα διαχείρισης του επιπέδου πρόσβασης των χρηστών της εταιρίας σε λογαριασμούς και συναλλαγές
- Πραγματοποίηση συναλλαγών με έγκριση δεύτερου χρήστη της εταιρίας

Για την πρόσβαση στο egnatiaTeller το μόνο που χρειάζεται είναι να συμπληρώσει ο πελάτης τη σχετική Αίτηση που θα βρει και στο site. Να σημειώσουμε εδώ ότι δεν χρειάζεται να είναι ήδη πελάτης της τράπεζας (να έχει δηλαδή τραπεζικό λογαριασμό) αφού και το άνοιγμα λογαριασμού μπορεί να γίνει μέσα από το ίδιο site.
Όσον αφορά στο θέμα της ασφάλειας, για την είσοδο στο απαιτείται η χρήση κωδικών ασφαλείας (κωδικό όνομα χρήστη και κωδικός αριθμός χρήστη). Το κωδικό όνομα χρήστη (user-id) επιλέγεται από τον ίδιο τον πελάτη στην Αίτησή Εγγραφής του ενώ ο κωδικός ασφαλείας (PIN) δημιουργείται αυτόματα από το σύστημα και μπορεί να αλλαχθεί από τον πελάτη όποτε το θελήσει. Οι κωδικοί αυτοί ενεργοποιούνται μόνο όταν ειδοποιήσει ο πελάτης ότι τους παρέλαβε και "κλειδώνονται" εάν γίνουν 3 συνεχόμενες αποτυχημένες προσπάθειες εισόδου. Εκτός από τους κωδικούς αυτούς, για να εκτελεστεί οποιαδήποτε τραπεζική συναλλαγή στο egnatiaTeller (π.χ. μεταφορά χρημάτων μεταξύ λογαριασμών) απαιτείται η χρήση ενός από τους αριθμούς επικύρωσης συναλλαγής (TAN) που δίνεται στον πελάτη με τη μορφή λίστας. Χωρίς

τον αριθμό αυτό ο πελάτης μπορεί μόνο να βλέπει πληροφορίες για το λογαριασμό του (υπόλοιπα, κινήσεις κλπ.) αλλά όχι να διενεργεί συναλλαγές.

Η MARFIN EGNATIA BANK αναγνωρίζοντας την πρωταρχική σημασία της ασφάλειας στην διενέργεια των συναλλαγών, παρέχει τις πιο προηγμένες και πρωτοποριακές μεθόδους διασφάλισης όλων των ηλεκτρονικών συναλλαγών που πραγματοποιούνται μέσω Internet. Η υπηρεσία ebanking υποστηρίζεται από το πρωτόκολλο επικοινωνίας SSL με κρυπτογράφηση 128bit. Η κρυπτογράφηση στα 128 bit θεωρείται πρακτικά αδύνατο να παραβιαστεί, δεδομένου ότι ένα σύγχρονο υπολογιστικό σύστημα θα χρειαζόταν αρκετά δισεκατομμύρια έτη για να διαβάσει τέτοια κρυπτογραφημένα δεδομένα. Μπορείτε να επιβεβαιώνετε ότι βρίσκεστε σε σελίδα με ενεργοποιημένη κρυπτογράφηση, εφόσον στην ηλεκτρονική διεύθυνση της σελίδας το «http» έχει μετατραπεί σε «https» (όπου s σημαίνει secure) και ταυτόχρονα υπάρχει το εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας αυτής.Ακόμα στην υπηρεσία ebanking έχει εγκατασταθεί το Πιστοποιητικό Αυθεντικότητας της ADACOM. Η εμφάνιση του εικονιδίου με το λουκέτο στο κάτω δεξιά μέρος της οθόνης σας υποδηλώνει ότι είστε στην σωστή σελίδα. Προκειμένου να επιβεβαιώσετε την αυθεντικότητα της σελίδας του egnatiaTeller, μπορείτε να κάνετε κλικ στο σήμα της ADACOM που υπάρχει στην οθόνη login της υπηρεσίας. Η υπηρεσία ebanking προστατεύεται επίσης από Firewalls τελευταίας τεχνολογίας, που αποτελούν σήμερα τα καλύτερα φίλτρα ελέγχου πρόσβασης στο σύστημα της Τράπεζας.Με αυτό το φιλτράρισμα προστατεύονται όλα τα σημεία του δικτύου της Τράπεζας στα οποία ο εξωτερικός και εσωτερικός μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση. Το εικονικό πληκτρολόγιο παρέχει μια ακόμα δικλείδα ασφάλειας αφού με τον τρόπο αυτό αποτρέπεται κάθε δυνατότητα υποκλοπής των κωδικών σας, μέσω ιών που μπορούν να καταγράψουν τις πληκτρολογήσεις από το πραγματικό πληκτρολόγιο. Τέλος η επικοινωνία με την υπηρεσία ebanking τερματίζεται αυτόματα εφόσον δεν πραγματοποιηθεί κάποια ενέργεια μέσω αυτής για διάστημα μεγαλύτερο των 5 λεπτών



Σχήμα 5.10: Ο δικτυακός τόπος www.marfinegnatia.gr

5.3.6.3 EFG EUROBANK (www.eurobank.gr)

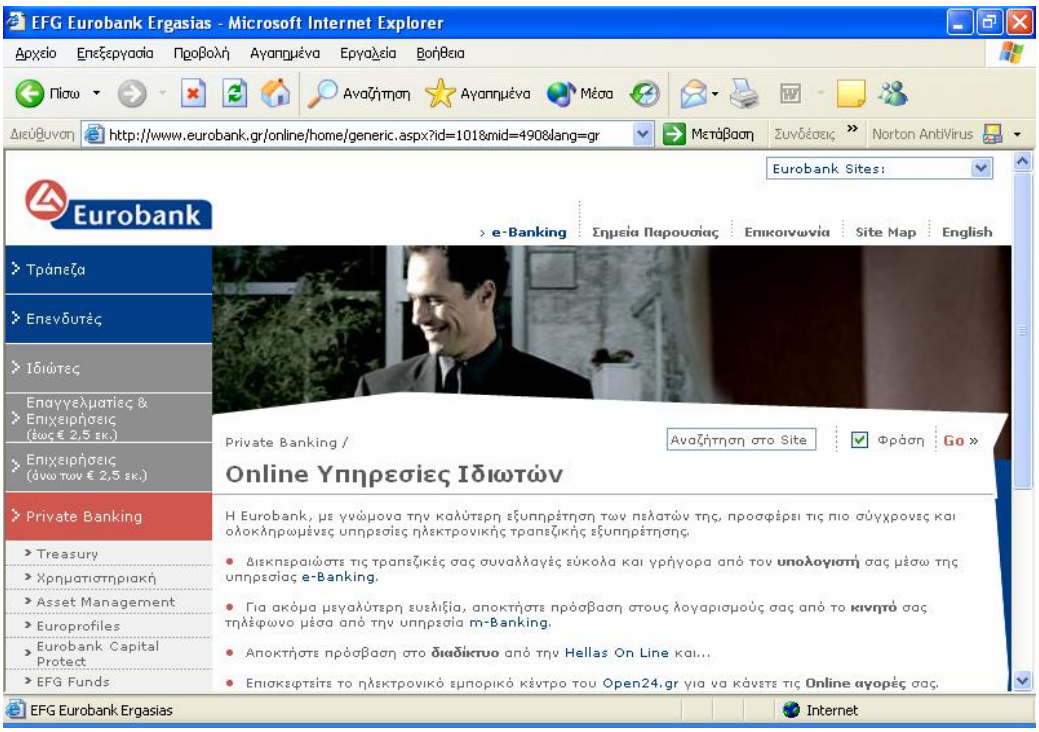
Το e-Banking της Eurobank τέθηκε σε λειτουργία στις 7 Φεβρουαρίου 2000 ενώ λειτουργεί σε πιλοτική μορφή από τις αρχές Νοεμβρίου.

Οι πελάτες μπορούν να:

- Βλέπουν το υπόλοιπο και την ανάλυση των λογαριασμών τους
- Μεταφέρουν χρήματα μεταξύ προσωπικών λογαριασμών
- Μεταφέρουν χρήματα σε λογαριασμούς τρίτων
- Πληρώνουν τις πιστωτικές κάρτες Eurobank MasterCard & Eurobank VISA
- Ενημερώνονται για τις ισοτιμίες ξένων χαρτονομισμάτων
- Στο "χαρτοφυλάκιο μου" οι πελάτες μπορούν να
- Αγοράζουν και να πουλάνε μετοχές on-line
- Πληροφορούνται για τη θέση του χαρτοφυλακίου του
- Ενημερώνονται για τη αποτίμηση των μετοχών και του χαρτοφυλακίου ζωντανά

- Βλέπουν την εξέλιξη των εντολών αγοράς πώλησης.
- Τέλος μόλις μια πώληση πραγματοποιηθεί ο πελάτης μπορεί αμέσως να επενδύσει σε νέες μετοχές (intra-day trading)
- Τέλος στο οι πελάτες μπορούν να
- Δημιουργούν εικονικό χαρτοφυλάκιο όπου μπορούν να δοκιμάζουν εναλλακτικά σενάρια
- Παρακολουθούν τις τιμές των μετοχών του ΧΑΑ ανά κλάδο

Όλες οι συναλλαγές είναι εγγυημένες από την Eurobank. Οι σελίδες που αφορούν το e-Banking βρίσκονται σε ασφαλές server. Η Eurobank είναι η μοναδική τράπεζα στην Ελλάδα που προσφέρει τρία επίπεδα ασφαλείας. Σε επίπεδο δικτύου, έχει υιοθετήσει το πρωτόκολλο SSL 128bit που αποτελεί και την πιο εξελιγμένη μορφή ασφαλείας και τρία επίπεδα firewall. Το πρωτόκολλο αυτό αναλαμβάνει την κρυπτογράφηση των στοιχείων. Για τον χρήστη αυτό σημαίνει ότι οι πιθανοί συνδυασμοί είναι τόσοι πολλοί που υπολογίζεται ότι ο μέσος χρόνος που χρειάζεται για να 'σπάσει' ο κωδικός αυτός είναι περισσότερος από το χρόνο που θα κάνει ο ήλιος του ηλιακού μας συστήματος να μετατραπεί σε κόκκινο γίγαντα καταστρέφοντας τη γη. Η πιστοποίηση της ταυτότητας του server γίνεται από την διεθνώς αναγνωρισμένη στα συστήματα ασφαλείας VeriSignTM. Πρέπει να τονιστεί πως η EFG Eurobank είναι η μοναδική τράπεζα στην Ελλάδα και από τις λίγες ανά τον κόσμο που εκδίδει ένα ψηφιακό πιστοποιητικό (digital certificate) μοναδικό για κάθε χρήστη. Με αυτό το πιστοποιητικό αναγνωρίζεται ο υπολογιστής του κάθε χρήστη και επιτρέπονται οι συναλλαγές και μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από τον συγκεκριμένο υπολογιστή. Τέλος, η τράπεζα εκδίδει προσωπικούς κωδικούς πρόσβασης για τον κάθε χρήστη οι οποίοι, σε συνδυασμό με τον αριθμό της κάρτας που χρησιμοποιείται για τις τραπεζικές συναλλαγές, επιτρέπουν την είσοδο στο σύστημα.



Σχήμα 5.11: Ο δικτυακός τόπος **www.eurobank.gr**

5.3.6.4 WINBANK (www.winbank.gr)

Η νέα ηλεκτρονική τράπεζα(WinBank) θα παρέχει τη δυνατότητα εκτέλεσης με ασφάλεια κάθε μορφής τραπεζικών συναλλαγών μέσω Internet αλλά και μέσω σταθερού ή κινητού τηλεφώνου. Πιο συγκεκριμένα, η υπηρεσία WinBank συνίσταται σε 4 δράσεις:

- WinInternet (@): αξιοποιώντας την ευκολία του Διαδικτύου παρέχεται η δυνατότητα πραγματοποίησης τραπεζικών και χρηματιστηριακών συναλλαγών χωρίς επιπλέον χρέωση και με πλήρη ασφάλεια (VeriSign SSL 128 bit encryption - firewall)
- WinMobile (m): οι διάφορες τραπεζικές συναλλαγές πραγματοποιούνται με η βοήθεια των γνωστών σύντομων μηνυμάτων (SMS) εύκολα και γρήγορα

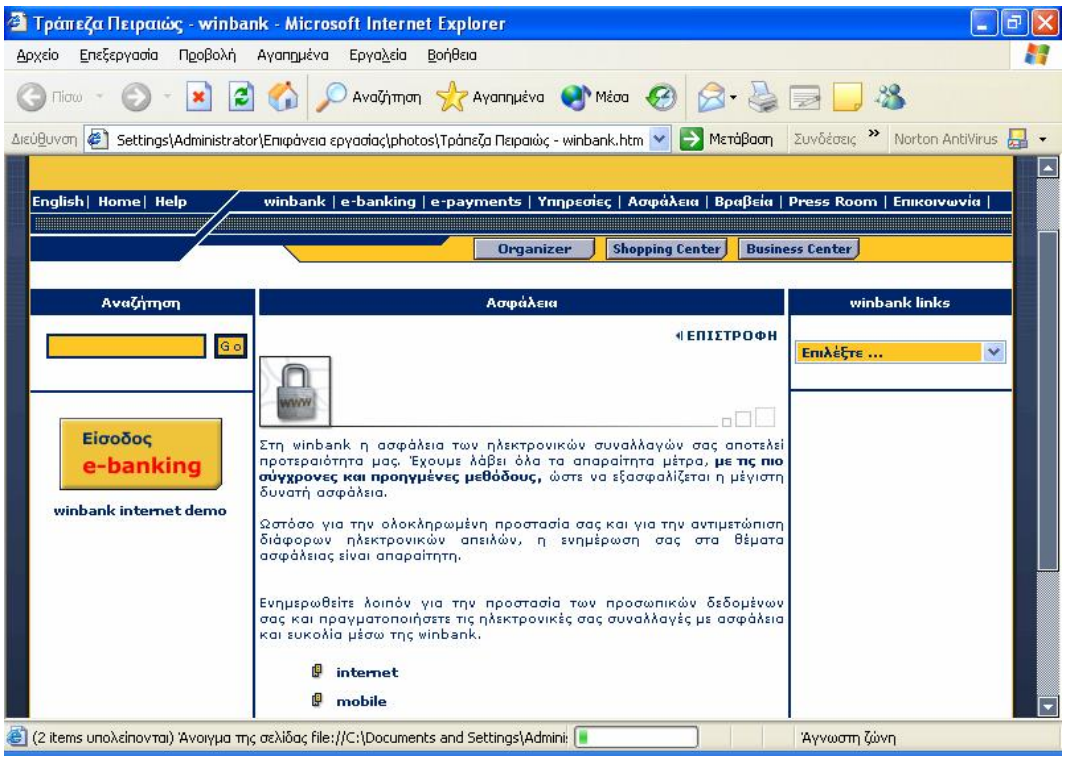
- WinPhone (τ): εύκολη πρόσβαση σε όλες τις υπηρεσίες με τη χρήση σταθερού τηλεφώνου (μέσω αυτόματου συστήματος φωνής ή με τη βοήθεια του εξειδικευμένου προσωπικού της Τράπεζας)
- WinATM (atm): ένα ολοκληρωμένο δίκτυο 210 Μηχανών Αυτόματης Τραπεζικής Εξυπηρέτησης (ATMs) για 24ωρη εξυπηρέτηση, όλες τις ημέρες του χρόνου, χρησιμοποιώντας τις κάρτες του Ομίλου: Multicash (Τράπεζα Πειραιώς), Cashcard (Τράπεζα Μακεδονίας-Θράκης), Xioscash (Τράπεζα Χίου).

Οι συναλλαγές που θα μπορούν να πραγματοποιηθούν μέσω Internet ή τηλεφώνου είναι:

Πληροφορίες Λογαριασμού, Περίληψη Λογαριασμών, Ανάλυση Υπολοίπου, Εμφάνιση Κινήσεων, Αποστολή Κινήσεων, Κινήσεις σε Αρχείο, Αίτηση Επιταγών, Ανάκληση Επιταγών, Αναλυτικά στοιχεία λογαριασμού, Μεταφορές ποσών μεταξύ λογαριασμών σας και επιπλέον διάφορες Χρηματιστηριακές συναλλαγές όπως Ενημέρωση χαρτοφυλακίου πελάτη, Αγορά μετοχών, Πώληση μετοχών, Λίστα εντολών του πελάτη, Πινακίδια.

Στον τομέα της ασφάλειας η Winbank προσφέρει:

- Αναγνώριση πελάτη με τη χρήση του κωδικού πελάτη (user id) και του προσωπικού του κωδικού (PIN).
- Εξασφάλιση απορρήτου μεταφοράς δεδομένων με κρυπτογράφηση SSL-128bit των δεδομένων. Το όλο σύστημα υλοποιήθηκε με τη συνεργασία της Verisign - ειδικής σε θέματα ασφαλείας των συναλλαγών.
- Ελεγχόμενη πρόσβαση από firewall, το οποίο επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών από τους πελάτες-επισκέπτες και απαγορεύει πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της τράπεζας.
- Προστασία από hacking: Ο Όμιλος έχει υπογράψει ειδική συμφωνία με την IBM Γερμανίας για την επιτήρηση της ασφάλειας του συστήματος και τη διασφάλισή του από ανεπιθύμητους επισκέπτες (hackers).



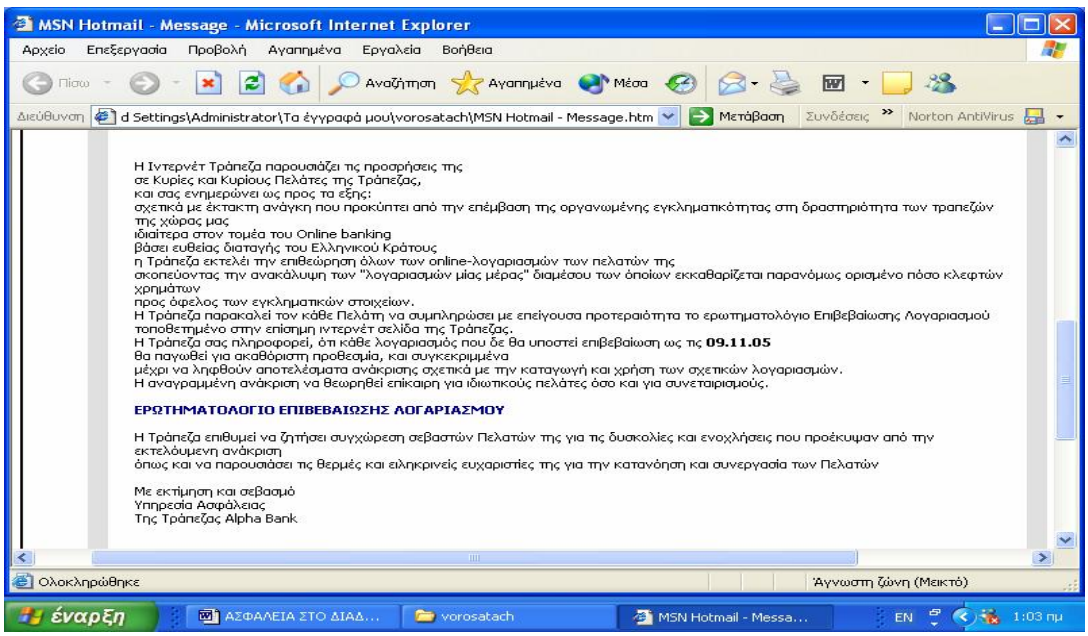
Σχήμα 5.12: Ο δικτυακός τόπος **www.winbank.gr**

5.3.7 e-banking και διαδικτυακό έγκλημα

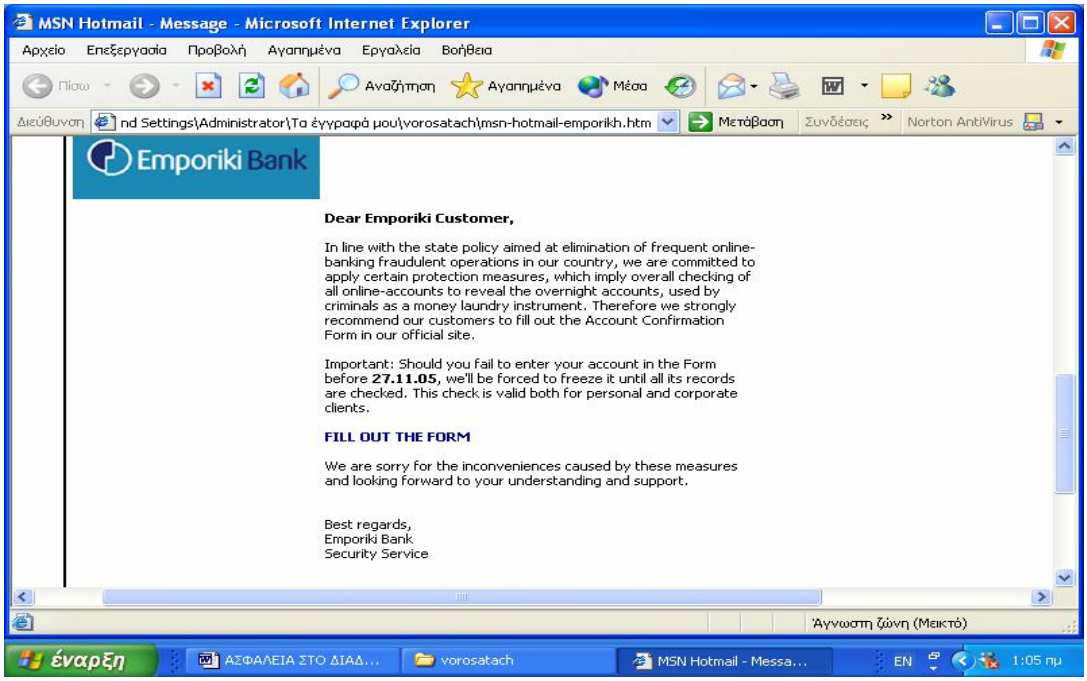
Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται επιχειρήσεις. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια -συνήθως- βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών. Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν

χρησιμοποιούν λογισμικό για ασφάλεια. Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα επιτρέποντας σε επιτήδειους να έχουν πρόσβαση σε αυτό. Ωστόσο και οι επιχειρήσεις δεν είναι πάντοτε ασφαλείς. Σε ορισμένες περιπτώσεις, εταιρίες συνεργάζονται με τράπεζες προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με εταιρικούς πελάτες. Οι τράπεζες ενίοτε επιτρέπουν στις εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, οι επιτήδειοι μελετούν τον τρόπο με τον οποίο οι επιχειρήσεις επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία, μεταφέρουν με λίγες απλές κινήσεις ολόκληρους εταιρικούς λογαριασμούς στις προσωπικές τους θυρίδες.

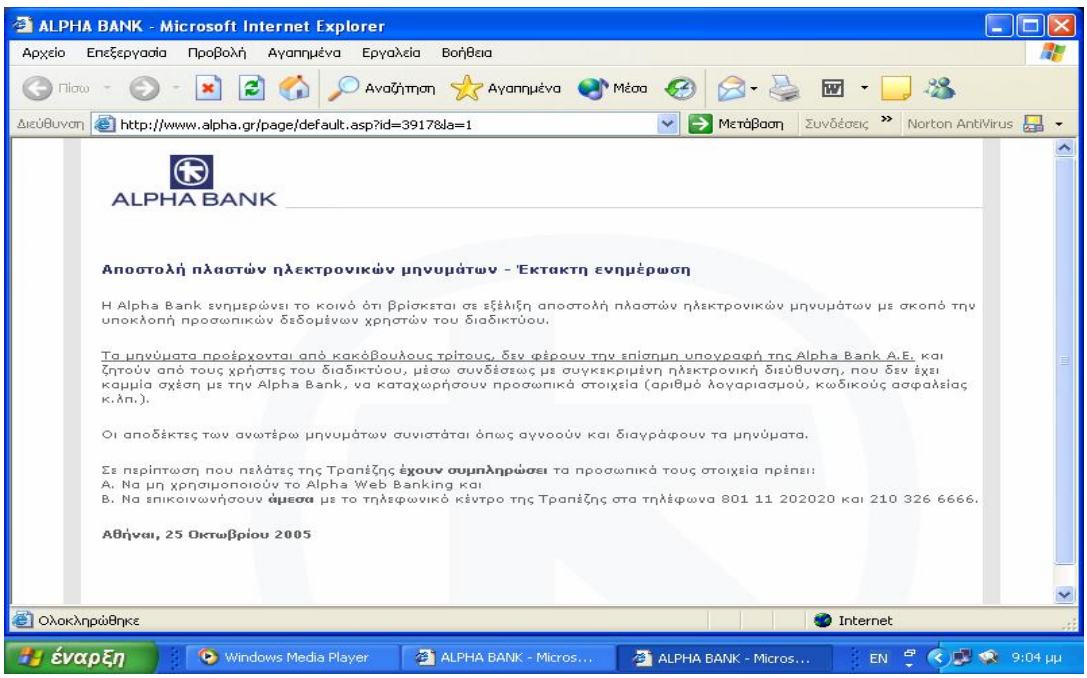
Να σημειωθεί, πάντως, πως τον Νοέμβριο του 2005 εμφανίστηκε η εξής απάτη που αφορούσε τις τράπεζες Alpha Bank και Emporiki Bank. Πρόκειται για αποστολή πλαστών ηλεκτρονικών μηνυμάτων που καλούσαν τους πελάτες του e-banking των άνω τραπεζών να μεταβούν σε μια σύνδεση της ηλεκτρονικής σελίδας και να καταχωρήσουν προσωπικά στοιχεία (αριθμό λογαριασμού, κωδικούς ασφαλείας κ.τ.λ.). Τα παρακάτω σχήματα δείχνουν τα e-mail που έλαβαν οι πελάτες καθώς και την απάντηση της Alpha Bank σχετικά με την απάτη. Ακόμα δεν έχει γνωστοποιηθεί πόσοι έπεσαν θύματα της συγκεκριμένης απάτης.



Σχήμα 5.13: Παράδειγμα πλαστού ηλεκτρονικού μηνύματος



Σχήμα 5.14: Παράδειγμα πλαστού ηλεκτρονικού μηνύματος



Σχήμα 5.15:Έκτακτη ενημέρωση της Alpha Bank για τα πλαστά μηνύματα.

5.3.8 Προς το μέλλον

Αυτή τη στιγμή δεν μπορεί να θεωρηθεί ότι οι ηλεκτρονικές χρηματοοικονομικές συναλλαγές στην Ελλάδα βρίσκονται σε ικανοποιητικό στάδιο. Αρκετές τράπεζες προσφέρουν τη δυνατότητα βασικών τραπεζικών εργασιών και υπηρεσιών μέσω του Internet, όπως παρακολούθηση της κίνησης του λογαριασμού, κατάθεση αίτησης για πιστωτική κάρτα ή δάνειο, αναλυτική ενημέρωση για προϊόντα και υπηρεσίες που προσφέρουν κ.ά. αλλά απέχουμε πολύ ακόμη από την πλήρη μεταφορά του συνόλου των τραπεζικών συναλλαγών σε ηλεκτρονικό επίπεδο.
Πάντως, και παρά τα θετικά βήματα, γεγονός είναι πως η λειτουργία ηλεκτρονικών τραπεζών στη χώρα μας καθυστερεί σημαντικά και εξαιτίας της έλλειψης ενός μοντέρνου και κατάλληλου νομοθετικού πλαισίου, το οποίο είναι απαραίτητο για τη σωστή ανάπτυξη και λειτουργία του online banking.

5.4. Ηλεκτρονικο Εμποριο

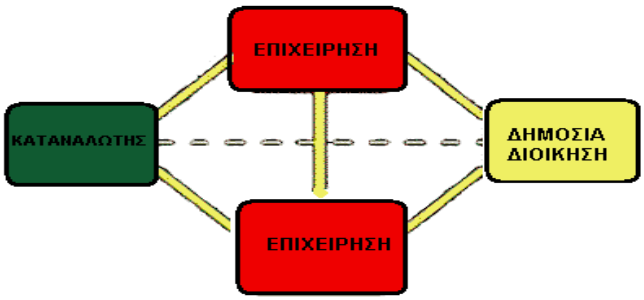
5.4.1 Ορισμός

Ως Ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. Το ηλεκτρονικό εμπόριο αποτελεί μορφή των λεγόμενων υπηρεσιών εξ αποστάσεως (Προεδρικό Διάταγμα 39.2001). Ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών. Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και Φαξ. Το ηλεκτρονικό εμπόριο διακρίνεται σε έμμεσο και άμεσο. Ο πρώτος όρος χρησιμοποιείται όταν πρόκειται για την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο. Άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άϋλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα.

5.4.2 Κατηγορίες Ηλεκτρονικού Εμπορίου

Όπως φαίνεται στο σχήμα 23.1 το Ηλεκτρονικό Εμπόριο μπορεί να υποδιαιρεθεί σε 4 κατηγορίες :

- επιχείρηση - επιχείρηση
- επιχείρηση - καταναλωτής
- επιχείρηση - δημόσια διοίκηση
- καταναλωτής - δημόσια διοίκηση



Σχήμα 5.15: Κατηγορίες ηλεκτρονικού εμπορίου

Επιχείρηση - Επιχείρηση

Συναλλαγές μεταξύ επιχειρήσεων (Business-to-Business - B2B): Το ηλεκτρονικό εμπόριο επιτρέπει σε επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες και το κόστος των προμηθειών, την ταχύτερη αποστολή των προμηθειών και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επιπλέον καθιστά ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και ποιοτικότερη την εξυπηρέτηση πελατών. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς καθώς και η πραγματοποίηση ηλεκτρονικών πληρωμών βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές

περιορίζουν το ανθρώπινο σφάλμα, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών. Το ηλεκτρονικό εμπόριο προσφέρει τη δυνατότητα αυξημένης πληροφόρησης σχετικά με τα προσφερόμενα προϊόντα - είτε από τους προμηθευτές είτε από ενδιάμεσους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου.(Χονδρικό εμπόριο)

Επιχείρηση - Καταναλωτής

Ηλεκτρονικό εμπόριο μεταξύ επιχείρησης και καταναλωτών (Business-to-Consumer - B2C): Πρόκειται για την πιο διαδεδομένη μορφή ηλεκτρονικού εμπορίου. Ο καταναλωτής έχει πρόσβαση σε μια τεράστια ποικιλία προϊόντων σε δικτυακούς κόμβους-καταστήματα, βλέπει, επιλέγει, αν επιθυμεί να αγοράσει είδη ένδυσης μπορεί ενίοτε και να τα δοκιμάζει (μέσω ειδικών προγραμμάτων), ανακαλύπτει προϊόντα τα οποία δεν θα μπορούσε να βρει εύκολα στη χώρα του, συγκρίνει τιμές και τέλος αγοράζει. Κι όλα αυτά χωρίς να βγει από το σπίτι του, κερδίζοντας πολύτιμο χρόνο και κόπο. (Λιανικές πωλήσεις)

Επιχείρηση - Δημόσια Διοίκηση

Καλύπτει όλες τις συναλλαγές μεταξύ επιχειρήσεων και δημόσιων οργανισμών. Προς το παρόν, αυτή η κατηγορία είναι σε νηπιακό στάδιο, αλλά μπορεί να αναπτυχθεί ραγδαία όσο οι κυβερνήσεις χρησιμοποιούν τις δικές τους λειτουργίες για να προωθήσουν την αντίληψη τους για το Ηλεκτρονικό Εμπόριο.

Καταναλωτής - Δημόσια Διοίκηση

Δεν έχει αναπτυχθεί ακόμα. Αφορά τις ηλεκτρονικές συναλλαγές σε τομείς όπως πληρωμές κοινωνικής πρόνοιας και ιδιωτικών φόρων.

5.4.3 Τι ισχύει στην Ελλάδα

Η εξάπλωση του διαδικτύου αποτελεί τον θεμέλιο λίθο του ηλεκτρονικού εμπορίου μέσω του οποίου ικανοποιούνται οι απαιτήσεις της σύγχρονης εμπορικής δραστηριότητας και φυσικά των σύγχρονων καταναλωτών.

Πρόσωπα μεταξύ των οποίων διενεργείται το ηλεκτρονικό εμπόριο
Καταναλωτής (αγοραστής) – Προμηθευτής (πωλητής)

Σύμφωνα με την Οδηγία 97/7 καταναλωτής είναι κάθε φυσικό πρόσωπο το οποίο, ενεργεί για λόγους οι οποίοι δεν εμπίπτουν στα πλαίσια της επαγγελματικής δραστηριότητας και Προμηθευτής κάθε φυσικό ή νομικό πρόσωπο το οποίο, ενεργεί στα πλαίσια της επαγγελματικής του δραστηριότητας. [24]

5.4.3.1 Σύμβαση μεταξύ καταναλωτή και προμηθευτή

Για να συμφωνηθεί μεταξύ του καταναλωτή (αγοραστή) και του προμηθευτή (πωλητή) η πώληση των αγαθών ή των υπηρεσιών στο ηλεκτρονικό εμπόριο απαιτείται η ύπαρξη σύμβασης, η λεγόμενη εξ αποστάσεως σύμβαση. Σύμβαση εξ αποστάσεως είναι κάθε σύμβαση μεταξύ ενός προμηθευτή και ενός καταναλωτή που αφορά αγαθά ή υπηρεσίες, και η οποία συνάπτεται στα πλαίσια ενός συστήματος πωλήσεων ή παροχής υπηρεσιών εξ αποστάσεως, που οργανώνεται από τον προμηθευτή. Ο προμηθευτής χρησιμοποιεί αποκλειστικά ένα ή περισσότερα μέσα επικοινωνίας εξ αποστάσεως έως τη σύναψη της συμβάσεως, συμπεριλαμβανομένης και αυτής καθεαυτής της σύναψης της συμβάσεως.(Οδηγία 97/7). Για να καταρτιστεί μια τέτοια σύμβαση πρέπει να υπάρχει ηλεκτρονική δήλωση βούλησης, που περιέχει πρόταση σύναψης σύμβασης και ηλεκτρονική αποδοχή αυτής.

Η δέσμευση μεταξύ των μερών γίνεται και μέσω ηλεκτρονικής υπογραφής με τους όρους που αναφέρονται στο Π.Δ. 150.2001. Ρυθμίσεις για την ηλεκτρονική υπογραφή διαθέτει και το Π.Δ. 342.2002.Οι συμβάσεις μεταξύ του προμηθευτή και του καταναλωτή περιέχουν γενικούς όρους συναλλαγών που ορισμένες φορές είναι καταχρηστικοί με αποτέλεσμα να μη δεσμεύουν τον καταναλωτή (οδηγία 93/13).Ο καταναλωτής πριν προβεί στην σύναψη της σύμβασης πρέπει να έχει στη διάθεσή του

κάποιες πληροφορίες όπως η ταυτότητα του προμηθευτή, η περιγραφή του προϊόντος κ.α. είτε η σύμβαση καταρτίζεται εκτός εμπορικού καταστήματος (Νόμος 2251.1994) είτε από απόσταση (Οδηγία 97/7).[23]

5.4.3.2 Δικαιώματα και προστασία του καταναλωτή

Η προστασία του καταναλωτή και η προάσπιση των δικαιωμάτων του είναι απαραίτητη προϋπόθεση για την ομαλή διεξαγωγή των συναλλαγών. Στην Ευρωπαϊκή ένωση ισχύουν νομοθετήματα που αναφέρονται σε όλο το εύρος της εμπορικής συναλλαγής και προστατεύουν τον καταναλωτή σε κάθε πτυχή αυτής. Αυτά είναι:

1. η Οδηγία 93/13 σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές όπου ρυθμίζεται ο τρόπος προστασίας των καταναλωτών από τις καταχρηστικές ρήτρες και πώς ένας καταναλωτής μπορεί να καταλάβει πότε μια ρήτρα είναι καταχρηστική ,

2. η Οδηγία 87/102 όπως τροποποιήθηκε από την οδηγία 90/88 για την καταναλωτική πίστη όπου ορίζεται ο τρόπος κατάρτισης των συμβάσεων πίστωσης και τι πρέπει να αναφέρεται απαραίτητα μέσα σε αυτές

3. η Οδηγία 97/7 για τη σύναψη συμβάσεων από απόσταση όπου ο καταναλωτής μπορεί να ενημερωθεί για τις απαραίτητες πληροφορίες που πρέπει να έχει στην διάθεσή του εγγράφως κατά την εκτέλεση μιας εξ αποστάσεως σύμβασης, για τις προθεσμίες που διαθέτει ώστε να υπαναχωρήσει αλλά και την προστασία που του παρέχεται όταν έχει πληρώσει με πιστωτική κάρτα.

4. η Οδηγία 2002/65 που ρυθμίζει την διαδικασία υπαναχώρησης του καταναλωτή από μία σύμβαση, την προστασία του από spam (άχρηστη) διαφήμιση, αλλά και την προστασία του από υπηρεσίες που δεν ζήτησε.
   Εξίσου σημαντικό είναι το Προεδρικό διάταγμα 131.2003 που εναρμονίζει στο ελληνικό δίκαιο την Οδηγία 2000/31/ΕΚ της Ευρωπαϊκής Ένωσης για το ηλεκτρονικό εμπόριο.[25]

Στην Ελλάδα ισχύει ο νόμος 2251/1994 για την προστασία του καταναλωτή, ο οποίος παρέχει επαρκή προστασία και αναφέρεται

1. στους γενικού και καταχρηστικούς όρους συναλλαγών
2. στις συμβάσεις εκτός εμπορικού καταστήματος,
3. στις συμβάσεις από απόσταση
4. στην ευθύνη των παραγωγών για τα ελαττωματικά προϊόντα
5. στην διαφήμιση,
6. στις ενώσεις των καταναλωτών που έχουν σαν αποκλειστικό σκοπό την προστασία των συμφερόντων του καταναλωτικού κοινού
7. στα συλλογικά μέσα προστασίας των καταναλωτών.

5.4.3.3 Φορολογία και ηλεκτρονικό εμπόριο

Εκτός από τις ρυθμίσεις για την υποβολή δηλώσεων ΦΠΑ με ηλεκτρονικά μέσα και την είσπραξή του (Υ.Α.1023404/1363/0016 του 2001) και τη χορήγηση αριθμών ΦΠΑ σε υποκείμενους σε φόρο που είναι εγκατεστημένοι εκτός της κοινότητας υπάρχουν ρυθμίσεις και για την φορολόγηση του ηλεκτρονικού εμπορίου. Οι οδηγίες 2002/38/ΕΚ και 77/388 θέτουν τις προϋποθέσεις, υπό τις οποίες κάποιος υποκείμενος στο φόρο δεν είναι υπόχρεος για το ΦΠΑ κατά την παροχή υπηρεσιών με ηλεκτρονικά μέσα και ο Κανονισμός 792/2002 αναφέρει τις νέες ρυθμίσεις για την επιβολή εμμέσων φόρων στον ηλεκτρονικό εμπόριο στις ενδοκοινοτικές συναλλαγές.

5.4.3.4 Οι τεχνολογίες του ηλεκτρονικού εμπορίου

Οι τεχνολογίες του ηλεκτρονικού εμπορίου δεν είναι όλες νέες. Οι περισσότερες από αυτές χρησιμοποιούνται εδώ και αρκετά χρόνια από συγκεκριμένες επιχειρήσεις ή κλάδους. Ηλεκτρονική

Ανταλλαγή Δεδομένων (EDI - Electronic Data Interchange)

Δημιουργήθηκε στις αρχές της δεκαετίας του '70. Η EDI είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέψει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα. Πρόκειται για την ηλεκτρονική ανταλλαγή εμπορικών και διοικητικών δεδομένων από υπολογιστή σε υπολογιστή, με την ελάχιστη παρέμβαση χειρόγραφων διαδικασιών. Τα δεδομένα αυτά είναι οργανωμένα σε αυτοτελή μηνύματα (τιμολόγια, παραγγελίες, τιμοκατάλογοι, φορτωτικές κλπ.), το περιεχόμενο και η δομή των οποίων καθορίζονται από κάποιο κοινώς αποδεκτό πρότυπο. Τα πρότυπα που χρησιμοποιούνται σε παγκόσμιο επίπεδο προέρχονται από τον Οργανισμό Ηνωμένων Εθνών και καλύπτουν ένα ευρύ φάσμα επικοινωνιακών αναγκών των εμπορικών εταιριών. Το πρότυπο αυτό είναι το EDIFACT (EDI For Administration, Commerce and Transportation).

Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)

Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Το SSL χρησιμοποιεί "κλειδί" δημόσιας κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα καθώς διακινούνται μέσα στο Internet.

Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)

Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, απολαμβάνει μεγάλης αποδοχής από την τραπεζική κοινότητα.

Γραμμωτός κώδικας (Barcode)

Η τεχνολογία του γραμμωτού κώδικα αποτελεί τμήμα του γενικότερου τομέα των τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Είναι ένα σύγχρονο εργαλείο, το οποίο βοηθά καταλυτικά στην ομαλή διακίνηση και διαχείριση (logistics) προϊόντων και υπηρεσιών.

Η ανάπτυξη της τεχνολογίας του γραμμωτού κώδικα ξεκίνησε στις αρχές της δεκαετίας του 1960, με σκοπό να εξυπηρετήσει την πληρωμή προϊόντων στα καταστήματα τροφίμων. Οι πρώτες εφαρμογές σε βιομηχανικό περιβάλλον εμφανίστηκαν στα τέλη της ίδιας δεκαετίας σε μεγάλες αυτοκινητοβιομηχανίες, για τον περιορισμό του κόστους εργασίας που σχετιζόταν με την παραγωγή. Εκτεταμένη χρήση παρουσιάστηκε μετά την ανάπτυξη των πρώτων προτύπων (λόγω των πιέσεων των αρκετών πλέον χρηστών – προμηθευτών των μεγάλων βιομηχανιών) στα τέλη της δεκαετίας του 1970. Κατά τη δεκαετία του 1980 υπήρξε αλματώδης ανάπτυξη του εξοπλισμού, κατ' επέκταση και των τρόπων χρήσης της τεχνολογίας γραμμωτού κώδικα.

Έξυπνες κάρτες (Smart Cards)

Οι "έξυπνες κάρτες" αποτελούν εξέλιξη των καρτών μαγνητικής λωρίδας (παθητικό μέσο αποθήκευσης, τα περιεχόμενα του οποίου μπορούν να διαβαστούν και να αλλαχθούν). Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν μεγάλη ποσότητα δεδομένων και παρέχουν δυνατότητες κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους. Η ιδέα της έξυπνης κάρτας ξεκίνησε στη Γαλλία το 1974. Το 1975 τα δικαιώματα ανάπτυξης πέρασαν σε μεγάλες εταιρίες ηλεκτρονικού εξοπλισμού. Η νέα αυτή τεχνολογία παρουσιάστηκε στο κοινό το 1981. Μια σειρά από πιλοτικά σχέδια ξεκίνησε αμέσως, και το 1984 με μια συλλογική αξιολόγησή τους εκδόθηκαν νέες ολοκληρωμένες προδιαγραφές. Η τεχνολογία των έξυπνων καρτών προσφέρει απεριόριστες δυνατότητες χρήσης στη βιομηχανία, το εμπόριο και τη δημόσια διοίκηση.

5.4.4 Τεχνικές προστασίας για τις ηλεκτρονικές συναλλαγές με τράπεζες

Για την ασφάλεια των ηλεκτρονικών συναλλαγών χρησιμοποιούνται επίσης οι τρεις παρακάτω τεχνικές:

FIREWALL

Ο όρος firewall χρησιμοποιείται για να περιγράψει κάθε συσκευή ή πρόγραμμα που τοποθετείται μεταξύ δύο διαφορετικών δικτύων προκειμένου να ελέγχει τη ροή των δεδομένων από το ένα δίκτυο στο άλλο. Το firewall ελέγχει όλη την κίνηση που εκτελείται στο δίκτυο και αν κάτι δεν είναι εγκεκριμένο ή μπορεί να προκαλέσει ζημιά, όπως π.χ. ένας ιός, δεν επιτρέπει την είσοδό του στα συστήματα. Γι' αυτό κρίνεται αναγκαίο να διεξάγονται συχνοί έλεγχοι από τις τράπεζες ως προ τη σωστή λειτουργία τους, αφού μόνο έτσι μπορούν να αποτραπούν επιθέσεις στα συστήματα λόγω κάποιας αδυναμίας που έχει προκύψει.

Οι λειτουργίες που εκτελεί ένα firewall είναι: απομόνωση δικτύου (όπου χρησιμοποιείται ένας domain server που μετατρέπει τις γνωστές δημόσιες διευθύνσεις σε απόρρητες εσωτερικές προκειμένου να αποτραπεί η πρόσβαση των εισβολέων), προστασία διευθύνσεων (όπου τα μηνύματα που δεν έχουν εσωτερική διευθυνσιοδότηση και θεωρούνται ύποπτα ενώ όσα έχουν προέλευση εσωτερικών διευθύνσεων προστατεύονται), προστασία εφαρμογής (προκειμένου να μην επιτρέπεται μη εξουσιοδοτημένη πρόσβαση σε επίπεδο διαχειριστή του server ή να αποτραπεί η εισαγωγή ακατάλληλων εντολών στ σύστημα της τράπεζας) και τέλος επιθεώρηση ροής μηνυμάτων ή συνολικής κατάστασης(στη λειτουργία αυτή ανιχνεύονται μη κατάλληλες αποκρίσεις του συστήματος, ενώ αυτό δημιουργεί μία βάση δεδομένων και εξετάζει για μη κατάλληλες αποκρίσεις του server σε μηνύματα ή ερωτήσεις)

PKI

Η PKI (Public Key Infrastructure) είναι μια τεχνολογία που χρησιμοποιείται για να αναγνωρίζει και να διαχειρίζεται σχέσεις μεταξύ των μελών μιας ανταλλαγής δεδομένων, ενώ εξυπηρετεί ένα μεγάλο εύρος αναγκών ασφαλείας όπως, έλεγχο πρόσβασης, εμπιστευτικότητα, ακεραιότητα και μη αποποίηση ευθύνης. Η PKI χρησιμοποιεί επίσης μοναδικά Ψηφιακά Πιστοποιητικά για να διασφαλίζει το e-banking, το e-commerce κλπ. Χρησιμοποιείται ακόμα για να πιστοποιήσει την ταυτότητα και τα δικαιώματα του χρήστη. Επιπρόσθετα η Αρχή Πιστοποίησης (Certificate Authority), που είναι αυτή που εγγυάται την PKI τεχνολογία, παρέχει ένα ολοκληρωμένο πακέτο διαχείρισης των δημόσιων κλειδιών και πιστοποιητικών, που περιλαμβάνει την έκδοση, την πιστοποίηση, την αποθήκευση, την πρόσβαση, το back-

up, την ανάνηψη, την ενημέρωση και την ανανέωση. Όλοι οι χρήστες PKI πρέπει να έχουν μια εγκεκριμένη ταυτότητα η οποία είναι αποθηκευμένη σ' ένα πιστοποιητικό που εκδίδει η Αρχή Πιστοποίησης. Αυτό λειτουργεί ως ο σύνδεσμος εμπιστοσύνης στην PKI.

Η PKI χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά τα οποία είναι μοναδικά για κάθε χρήστη σ' ένα σύστημα. Τα ιδιωτικά κλειδιά, για να προστατεύονται από υποκλοπές αποθηκεύονται σε φυσικές συσκευές ενώ τα δημόσια είναι διαθέσιμα σε όλους. Προκειμένου να διασφαλίσει ότι τα εμπλεκόμενα μέρη είναι όντως αυτά που ισχυρίζονται η PKI χρησιμοποιεί τις ψηφιακές υπογραφές, ενώ το επόμενο στάδιο στη διασφάλιση του μηνύματος περιλαμβάνει την κρυπτογράφηση την κρυπτογράφησή του αλλά και της ψηφιακής υπογραφής. Τέλος όλοι οι χρήστες PKI χρησιμοποιούν ψηφιακά πιστοποιητικά (τα οποία περιέχουν τα στοιχεία του χρήστη αλλά και του ίδιου του πιστοποιητικού) προκειμένου να επαληθεύσουν την ταυτότητά τους.

ΠΙΣΤΟΠΟΙΗΣΗ

Η πιστοποίηση είναι μια διαδικασία η οποία παρέχει ένα επιπλέον επίπεδο εμπιστοσύνης στις συναλλαγές που βασίζονται στην PKI τεχνολογία. Υπάρχουν τρία «είδη» πιστοποίησης: Challenge Response, Event-Synchronous και Time-Synchronous. Από τις παραπάνω μεθόδους η time-synchronous θεωρείται πιο αποτελεσματική για αρκετούς λόγους όπως: ενισχυμένη ασφάλεια, αφού βασίζεται στο μυστικό seed(=τυχαίος αριθμός) του token το οποίο δεν μπορεί να σπάσει. Ευκολία χρήσης, γιατί είναι διαδικασία δύο βημάτων σε αντίθεση με τις άλλες δύο (τριών κα πέντε βημάτων αντίστοιχα), άρα και πιο ευάλωτη σε λάθη χρηστών. Μικρότερο διαχειριστικό κόστος, γιατί επειδή είναι λιγότερα τα απαιτούμενα πατήματα πλήκτρων, υπάρχει μικρότερη πιθανότητα να κλειδωθεί ο χρήστης κα να πρέπει να τον ξεκλειδώσει ο διαχειριστής του συστήματος. Τέλος προσφέρει φορητότητα καθώς τα time-synchronous tokens είναι εντελώς φορητά.[26]

Η εμπιστευτική πληροφορία που διακινείται στο δίκτυο μπορεί να προστατευθεί με κρυπτογράφηση και χρήση μυστικών κωδικών. Η ασφάλεια του ηλεκτρονικού εμπορίου βασίζεται κατεξοχήν στην κρυπτογράφηση, δηλαδή στην κωδικοποίηση του μεταδιδόμενου κειμένου κατά τέτοιο τρόπο ώστε να μπορεί να αποκρυπτογραφηθεί μόνο με τη χρήση του ειδικού κλειδιού αποκρυπτογράφησης. Η κρυπτογράφηση συνοδεύεται πολλές φορές και από την ψηφιακή υπογραφή του αποστολέα, έτσι ώστε ο παραλήπτης να μπορεί να βεβαιωθεί για την ταυτότητα του πρώτου.

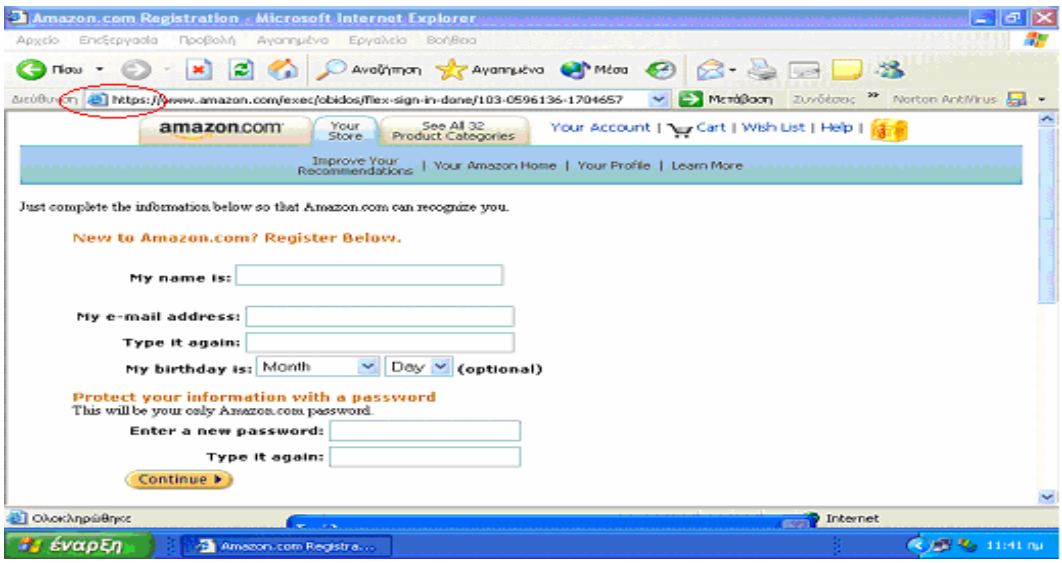
Σε μια ηλεκτρονική επικοινωνία, η εμπιστοσύνη μεταξύ των συναλλασσομένων μερών είναι πολύ σημαντική, γι' αυτό και θα πρέπει να δοθεί ιδιαίτερη έμφαση στο θέμα της ασφάλειας των συναλλαγών. Σήμερα, η τεχνολογία παρέχει προηγμένες λύσεις στο θέμα αυτό. Ένα ηλεκτρονικό κατάστημα που μεριμνά για την ασφάλεια των πελατών του οφείλει να χρησιμοποιεί και να αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφαλείας καθώς και να παρέχει τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του.

5.4.4.1 Πληροφορίες ηλεκτρονικών καταστημάτων

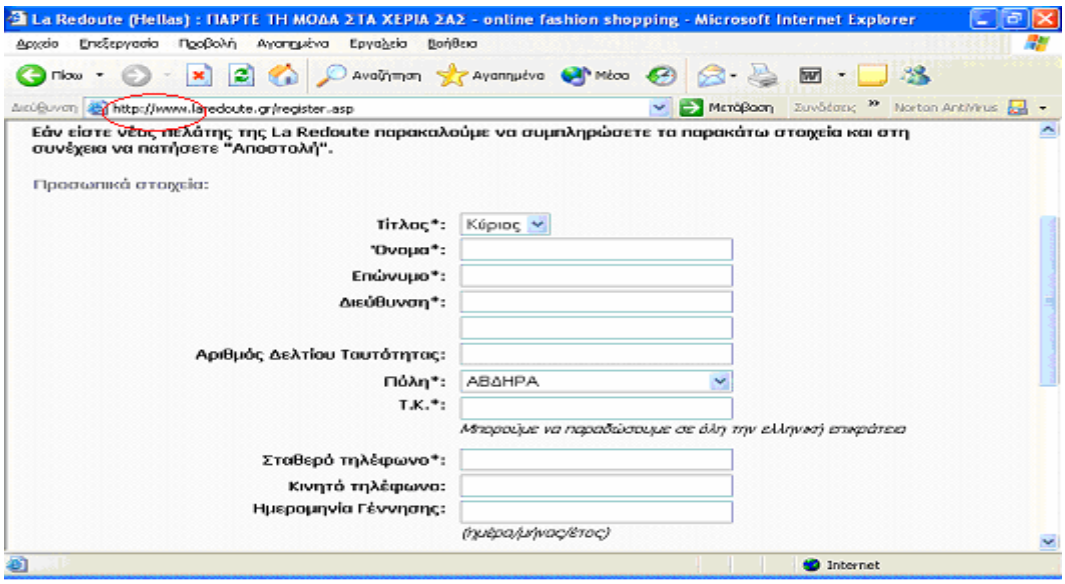
Συνοπτικά, αναφέρουμε τις εξής:

- Πραγματική ταυτότητα του εμπόρου (όνομα, γεωγραφική διεύθυνση, τηλέφωνο κλπ.)
- Τρόποι επικοινωνίας τόσο με ηλεκτρονικό όσο και με συμβατικό τρόπο (ηλεκτρονικό ταχυδρομείο [email], fax, τηλέφωνο, κλπ.)
- Τελική τιμή του προϊόντος ή της υπηρεσίας συμπεριλαμβανομένων των φόρων, εξόδων αποστολής, κλπ.)
- Εγγύηση του προϊόντος.
- Μέθοδος αποστολής και χρόνος παράδοσης, δυνατότητα υπαναχώρησης, τρόπος πληρωμής και παράδοσης, κλπ.
- Τρόπος ακύρωσης της παραγγελίας σε περίπτωση λάθους ή αλλαγής γνώμης.
- Επιβεβαίωση της παραλαβής της παραγγελίας.

- Πληροφορίες για την προστασία των προσωπικών δεδομένων (Privacy Statement)
- Πού μπορεί να απευθυνθεί ο καταναλωτής για τα παράπονά του εάν κάτι δεν πάει καλά (π.χ. αργοπορημένη παράδοση ή μη παράδοση).
- Πώς θα επιστραφεί το προϊόν, τι πρόσθετες επιβαρύνσεις υπάρχουν για την επιστροφή, κλπ.
- Ποιό δικαστήριο είναι αρμόδιο και ποιό Δίκαιο θα εφαρμοσθεί σε περίπτωση διαφοράς.[27]

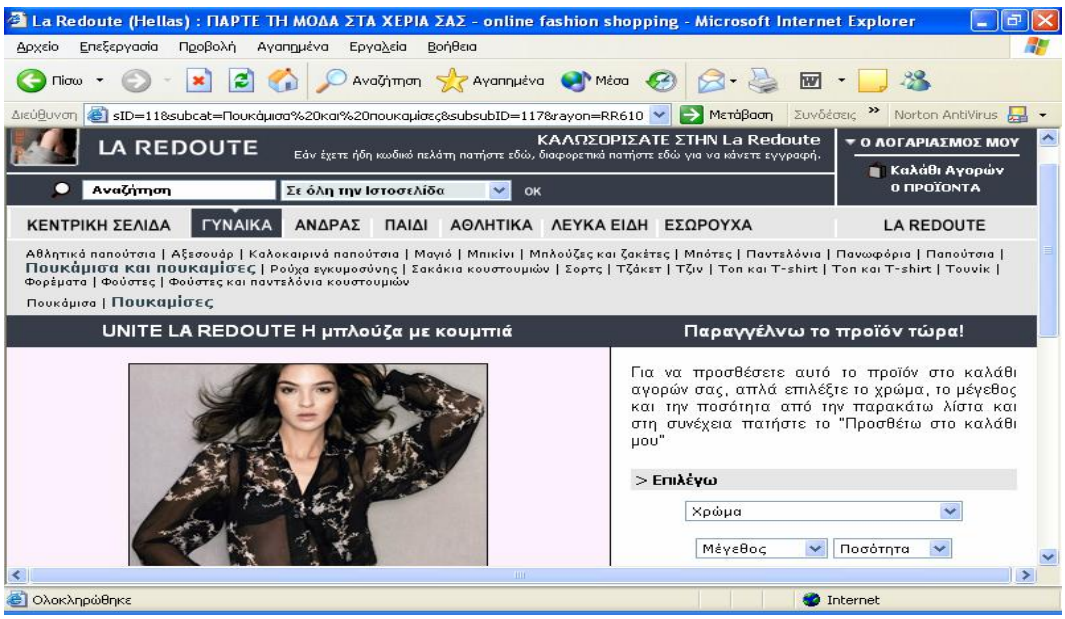


Σχήμα 5.16: Ασφαλής τοποθεσία.



Σχήμα 5.17: Μη ασφαλής τοποθεσία.

Όπως παρατηρούμε στις παραπάνω εικόνες οι ασφαλείς τοποθεσίες του Web αρχίζουν με https ενώ όταν δεν είναι ασφαλείς αρχίζουν με http.(βλέπε κεφ.4.7)



Σχήμα 5.18: Παράδειγμα ηλεκτρονικού καταστήματος.

5.4.5 Κίνδυνοι από απάτες με πιστωτικές κάρτες

Αρκετός λόγος έχει γίνει κατά καιρούς για τους κινδύνους που συνεπάγεται η χρήση πιστωτικών καρτών στις online συναλλαγές. Συνήθως δίνεται έμφαση σε κινδύνους

που αντιμετωπίζει το καταναλωτικό κοινό, χωρίς να λαμβάνονται υπόψη οι κίνδυνοι που αντιμετωπίζει ο ίδιος ο επιχειρηματίας. Τα φαινόμενα απάτης μέσω online χρήσης πιστωτικών καρτών δεν είναι ιδιαίτερα συχνά, ωστόσο υπάρχουν. Η διαδικασία επαλήθευσης των στοιχείων μιας πιστωτικής κάρτας αρχίζει με την είσοδο της κάρτας στο τερματικό ή με την πληκτρολόγηση του κωδικού της αριθμού. Η διαδικασία αυτή ουσιαστικά ελέγχει το αν η κάρτα έχει αναφερθεί ως κλεμμένη και αν η παρεχόμενη πίστωση επιτρέπει τη συγκεκριμένη συναλλαγή.

Είναι γεγονός ότι το Διαδίκτυο καθιστά τις απάτες που σχετίζονται με τη χρήση πιστωτικών καρτών ευκολότερες. Στο Internet κυκλοφορούν λίστες κλεμμένων αριθμών ή και προγραμμάτων που παράγουν νέους κωδικούς αριθμούς πιστωτικών καρτών. Επιπλέον, η έλλειψη επαφής πρόσωπο με πρόσωπο στο Διαδίκτυο τείνει να κάνει τους απατεώνες τολμηρότερους.

Οι τρέχουσες τεχνικές για την πρόληψη της απάτης μέσω πιστωτικών καρτών, που επικεντρώνονται στον έλεγχο των υπογραφών στο πίσω μέρος της κάρτας, των ολογραμμάτων ή και την τυπωμένη εικόνα του κατόχου της, δεν μπορούν να λειτουργήσουν στις online συναλλαγές, όπου ο κάτοχος δεν είναι παρών (συναλλαγή τύπου CNP, cardholder not present), δεδομένου ότι ο έμπορος δεν μπορεί να δει την πιστωτική κάρτα και να ελέγξει την υπογραφή.

Οι online συναλλαγές μέσω πιστωτικών καρτών εμπίπτουν στην κατηγορία MOTO (Mail Order/Telephone Order, παραγγελία ταχυδρομείου/ τηλεφωνική παραγγελία), ή αλλιώς CNP. Οι περισσότερες εμπορικές συναλλαγές μέσω πιστωτικών καρτών καθιστούν τον έμπορο 100% υπεύθυνο για απάτες που πραγματοποιούνται μέσω αυτού του τύπου συναλλαγής. Σε περιπτώσεις online απάτης μέσω κλεμμένων καρτών που έχουν διεξαχθεί στο εξωτερικό, οι επιχειρηματίες δεν βρίσκουν την αναμενόμενη αρωγή των αστυνομικών αρχών. Αυτό οφείλεται στο γεγονός πως οι Αρχές θεωρούν πολύ μικρά τα ποσά που διακυβεύονται (κυρίως όταν πρόκειται για λίγες δεκάδες ευρώ). Επίσης, σε περιπτώσεις διεθνών συναλλαγών, υπάρχουν εμπόδια που σχετίζονται με την αρμοδιότητα των εκάστοτε εθνικών αστυνομικών αρχών.

Υπάρχουν αρκετές δικλείδες ασφαλείας και μέθοδοι που διασφαλίζουν την καλή πίστη των συναλλαγών μέσω καρτών, ορισμένες από τις οποίες παραθέτουμε:

1. Πρέπει να υπάρχει ταύτιση της διεύθυνσης που δηλώνει ο πελάτης με τη διεύθυνση αποστολής του προϊόντος. Όσο υπερβολικό κι αν ακούγεται, πολλές επιχειρήσεις του εξωτερικού δεν δέχονται να αποστείλουν προϊόντα σε διεύθυνση διαφορετική από αυτήν που έχει δηλωθεί στην πιστωτική κάρτα του καταναλωτή. Σε περίπτωση που ο πελάτης επιθυμεί η παράδοση να γίνει σε διεύθυνση διαφορετική από τη δική του, θα πρέπει να γίνεται κατόπιν ειδικής συνεννόησης.

2. Να είστε προσεκτικοί σε παραγγελίες πελατών οι οποίοι παρέχουν διεύθυνση ηλεκτρονικού ταχυδρομείου δωρεάν υπηρεσίας. Πολλές online επιχειρήσεις του εξωτερικού δεν δέχονται παραγγελίες από πελάτες με email του τύπου username @yahoo.com, username @hotmail.com κ.λπ. Αυτό γίνεται διότι ο ιδιοκτήτης ενός ελεύθερου λογαριασμού email παραμένει ανώνυμος. Εάν ένας απατεώνας διαθέτει κλεμμένο κωδικό πιστωτικής κάρτας και κλεμμένη διεύθυνση κατοικίας, θα χρειαστεί και μια ηλεκτρονική διεύθυνση η οποία δεν μπορεί να ανιχνευθεί.

3. Ελέγξτε το δικτυακό τόπο του πελάτη, εάν υπάρχει και εάν είναι εφικτό. Είναι πιθανό να βρείτε το URL του πελάτη απλά πληκτρολογώντας www. μπροστά από το δεύτερο μέρος της διεύθυνσης ηλεκτρονικού ταχυδρομείου του. Για παράδειγμα, εάν ένας πελάτης παρέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείου username @domain.com, πληκτρολογήστε www. domain.com. Είναι αρκετά πιθανό να εντοπίσετε με αυτό τον τρόπο το site του. Εκεί θα πρέπει να ελέγξετε αν πρόκειται για δικτυακό τόπο υπό κατασκευή ή για site το οποίο παρέχει στοιχεία επικοινωνίας διαφορετικά από αυτά της κατατεθείσας παραγγελίας.

4. Προσέξτε τις ασυνήθιστες παραγγελίες. Οι επιτήδειοι συνηθίζουν να κάνουν παραγγελίες που διαφέρουν σημαντικά από αυτές ενός απλού (και νόμιμου) πελάτη, όπως για παράδειγμα ακριβά προϊόντα ή πολύ μεγάλες ποσότητες, και συχνά εμφανίζονται διατεθειμένοι να πληρώσουν πολύ περισσότερα χρήματα ώστε να λάβουν το εμπόρευμα ταχύτερα.

5. Τηλεφωνήστε στον πελάτη εάν έχετε αμφιβολίες. Ένα σύντομο τηλεφώνημα μπορεί να είναι αρκετό ώστε να εξασφαλίσει το έγκυρο της συναλλαγής.

6. Συλλέξτε όσο το δυνατόν περισσότερα στοιχεία για την παραγγελία: τη διεύθυνση του πελάτη και τον αριθμό τηλεφώνου, την τράπεζα που εξέδωσε την πιστωτική κάρτα και τη διεύθυνση IP του υπολογιστή από τον οποίο έγινε η παραγγελία. Βέβαια αυτό έρχεται σε αντίθεση με την πολιτική του να μη ζητάμε περισσότερα από τα απαραίτητα στοιχεία για τον πελάτη, ωστόσο οφείλετε να διασφαλίσετε τη νομιμότητα της συναλλαγής.

7. Προειδοποιήστε τους επισκέπτες του ηλεκτρονικού σας καταστήματος για τις μεθόδους που χρησιμοποιείτε κατά της απάτης, καθώς και τις συνέπειές της. Δείξτε ότι έχετε τον τρόπο να εντοπίσετε τους επιτήδειους και πως είστε διατεθειμένοι να τους "κυνηγήσετε".

8. Εάν χρησιμοποιείτε κάποια υπηρεσία λήψης και εκτέλεσης παραγγελιών σε πραγματικό χρόνο (real time service), βεβαιωθείτε ότι είναι αξιόπιστη.

9. Χρησιμοποιήστε κάποια προηγμένη υπηρεσία η οποία θα μπορέσει να σας βοηθήσει στον εντοπισμό των επίδοξων απατεώνων και στην αποτροπή τους. Υπηρεσίες όπως η CyberSource αυτοματοποιούν όλους τους ελέγχους που καλείστε να διεξάγετε προκειμένου να εξασφαλίσετε τη νομιμότητα και την αξιοπιστία των συναλλαγών σας. Εάν βρίσκεστε σε επαγρύπνηση και δεν αφήνετε τις online παραγγελίες που λαμβάνετε στην… τύχη τους, τότε η επιχείρησή σας δεν πρόκειται να αντιμετωπίσει σοβαρό πρόβλημα με τη χρήση πιστωτικών καρτών.

Οι οικονομικές συναλλαγές μέσω Διαδικτύου, και δη με τη χρήση πιστωτικής κάρτας, έχουν ακόμη μεγάλο περιθώριο διάδοσης στο μέλλον, καθώς η έλλειψη "εμπιστοσύνης" στα ηλεκτρονικά μέσα αποτρέπει σήμερα μεγάλο μέρος των χρηστών από το να πραγματοποιούν τις αγορές τους online.[28]

ΑΝΑΦΟΡΕΣ-ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Douglas E. Comer, Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο internet, (Εκδόσεις: κλειδάριθμος)

[2] Lincoln D. Stein, Ασφάλεια δικτύων web, (Εκδόσεις: 'ΙΩΝ', 1998)

[3] Θόδωρος Κομνηνός – Παύλος Σπυράκης, Ασφάλεια δικτύων υπολογιστικών συστημάτων, αναχαιτίστε τους εισβολείς, (εκδόσεις: Ελληνικά γράμματα , 2002)

[4] http://www.isoc.org

[5] http://www.netsol.com

[6] http://www.cnc.uom.gr/activities/servers.htm

[7] http://noc.uom.gr

[8] http://webopedia.com/TERM/I/IMAP. htm

[9]http://imap.org

[10] http://www.go-online.gr/ebusiness/specials/article.html?article_id=5668.

[11] http://www.sys-security.com/html/papers/trojan_list.html

[12] Lincoln D. Stein, Ασφάλεια δικτύων web, (Εκδόσεις : 'ΙΩΝ', 1998)

[13] Garfinkel Simson, Pretty Good Privacy, (εκδόσεις: O'Reilly & Associates, 1997)

[14] http://www.graphcomp.com/info/specs/ms/pct.htm

[15] Rfcs του Internet Engineering Task Force (http://www.ietf.org/rfc.html) και γενικά το World Wide Web.

[16] http:// www.graphcomp.com/info/specs/ms/pct.htm

[17] http://www.cybercash.com

[18] http://www.vivtek.com/cybercash.html

[19] Smith Richard E., Internet Cryptography, (εκδόσεις:Addison Wesley Longman, 1997)

[20] http://en.wikipedia.org/wiki/IPv6

[21]http://www.ebusinessforum.gr/information/statistics/tpe_greece/index.php?language=el

[22] http://www.setco.org

[23] http://www.lawnet.gr/case.stydy.asp?PageLabel=3&MeletID=98

[24] http://www.esee.gr/page.asp?id=565

[25] http://www.cosmo-one.gr/nl_archive/2008/january_eb.htm

[26] Βασίλης Γ. Αγγελής, Η βίβλος του e-banking (Εκδόσεις Νέων Τεχνολογιών)

[27] http://www.kepka.org/indexphp?option=com_content&task=view+id=288&itemid=50

[28] http:// www.oecd.org/subject/e.commerce