ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ανάλυση των μεθόδων διασφάλισης των ηλεκτρονικών συναλλαγών

Πτυχιακή Εργασία *των*

Κουτρούλη Κ. Ευαγγελία

Παυλίδη Χ. Ιωάννα

Επιβλέπων Καθηγητής : **Παπαδόπουλος Δημήτρης**

Πάτρα, 30 Μαΐου 2012

Περίληψη

Σκοπός αυτής της εργασίας είναι να προσεγγίσουμε διεξοδικά την διασφάλιση των ηλεκτρονικών συναλλαγών, καθώς οι κίνδυνοι που ελλοχεύουν από τη ραγδαία εξέλιξη της τεχνολογίας και την ευρύτατη εξάπλωση του διαδικτύου στην εποχή μας είναι αρκετοί. Ξεκινώντας από το διαδίκτυο που πλέον χρησιμοποιείται ως θεμελιώδης βάση για την επικοινωνία και τις ηλεκτρονικές συναλλαγές που διεξάγονται συνεχίζουμε επισημαίνοντας πως η χρήση του για εμπορικούς σκοπούς δημιούργησε νέα δεδομένα στο χώρο των επιχειρήσεων. Οι επιχειρήσεις καλούνται να δημιουργήσουν τις υποδομές εκείνες που θα επιτρέψουν στους καταναλωτές την αγορά προϊόντων και υπηρεσιών στο διαδίκτυο. Μέσα σε ένα ψηφιακό περιβάλλον, όπως είναι το e-banking και το ηλεκτρονικό εμπόριο, το οποίο είναι ηλεκτρονικά διαχειρίσιμο, η χρηματική εκκαθάριση των διαδικτυακών συναλλαγών έπρεπε να συμβαδίζει με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές. Για το λόγο αυτό, μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκαν σταδιακά. Με την εξάπλωση όμως της τεχνολογίας και της χρήσης του διαδικτύου, αναπτύχθηκαν και κάποιες απειλές, καθιστώντας έτσι επιτακτική την ανάγκη για την ασφάλεια των προσωπικών δεδομένων τόσο στην επικοινωνία όσο και στις ηλεκτρονικές συναλλαγές. Η παρούσα πτυχιακή εργασία παρουσιάζει αναλυτικά τις απειλές που υπάρχουν και αναπτύσσει τις τεχνολογίες που χρησιμοποιούνται για την διασφάλιση των ηλεκτρονικών συναλλαγών. Πιο συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται λόγος για την διάδοση του διαδικτύου τα τελευταία χρόνια, τα πρωτόκολλα που χρησιμοποιεί, καθώς επίσης για τα δίκτυα υπολογιστών και το ηλεκτρονικό εμπόριο. Στο δεύτερο κεφάλαιο συνεχίζουμε με τα είδη των ηλεκτρονικών πληρωμών και στο τρίτο με τους κινδύνους που υπάρχουν. Στο τέταρτο κεφάλαιο γίνεται αναλυτική αναφορά των μεθόδων διασφάλισης. Η νομοθεσία για τη ρύθμιση των ηλεκτρονικών πληρωμών στην Ελλάδα και στην Ευρωπαϊκή Ένωση παρατίθεται στο πέμπτο κεφάλαιο. Τέλος, ακολουθεί το πρακτικό κομμάτι της εργασίας που αποτελείται από μια μελέτη περίπτωσης πέντε επιχειρήσεων σχετικά με τα πρωτόκολλα ασφαλείας που χρησιμοποιούν.

ABSTRACT

This thesis was drafted with the aim of approaching the security in electronic transactions because with the rapid development of technology and the wide spread of the Internet which characterizes our season, there are plenty of threats. Starting from the internet which nowadays is used as a fundamental database for communication and electronic transactions that are carried out we continue with pointing out that the use of the Internet has created new data in the field of enterprises for commercial aims. Enterprises are invited to create the infrastructure that will enable consumers to purchase products and services on the Internet. In a digital environment, such as e-commerce and e-banking, which are electronically administrable, the financial liquidation of online transactions should be going with the speed and reliability, which are required by the up- to-date Internet transactions. For this reason, a series of electronic payment systems have developed gradually. However, with the spread of technology and the use of the Internet, some threats have appeared making the security of personal data in both communication and electronic transactions urgently necessary. This thesis presents at great length the threats that exist with using the Internet and furthermore develop technologies that are used for the guarantee of electronic transactions. Specifically, the first chapter refers to the diffusion of the Internet in recent years, the protocols that are used by internet, as well as computer networks and electronic commerce. In the second chapter, we continue with the kinds of electronic payments and in the third we present the dangers that exist. The fourth chapter is a detailed statement of assurance methods. The legislation on the regulation of electronic payments in Greece and in the European Union are mentioned in the fifth chapter. Finally, the practical piece of work consisting of a case study of five enterprises and the assurance methods which are used in order to protect electronic transactions follows.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1^0: ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΚΕΦΑΛΑΙΟ 2^0 : ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

ΚΕΦΑΛΑΙΟ 3^0 : ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ-ΚΙΝΔΥΝΟΙ ΠΟΥ ΥΠΑΡΧΟΥΝ

ΚΕΦΑΛΑΙΟ 1^{Ο}

ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΓΕΝΙΚΑ

Από την ανακάλυψη της φωτιάς μέχρι το ταξίδι του ανθρώπου στο διάστημα, από τον τροχό μέχρι τα σύγχρονα ιπποδύναμα αυτοκίνητα, από την πυρίτιδα μέχρι την πυρηνική ενεργεία ο κοινός τόπος είναι ένας: ότι ο άνθρωπος αξιοποίησε δυο εργατικά χέρια , έναν πολυμήχανο νου και σε αγαστή συνεργασία με τον συνάνθρωπο κατάφερε να προάγει σε τελειότατα επίπεδα τον πολιτισμό. Στην ιστορία της ανθρωπότητας υπήρξαν εκπληκτικές εφευρέσεις, οι οποίες σημάδεψαν κάθε εποχή. Χωρίς να παραγνωρίζουμε ωστόσο την σημασία των επιτευγμάτων παρελθόντων χρόνων, θα υποστηρίζαμε με βεβαιότητα πως ο εικοστός αιώνας μπορεί να καυχιέται πως υπήρξε ο «ο χρυσός» αιώνας της τεχνολογίας. Υπήρξαν εφευρέσεις οι οποίες άλλαξαν την ροή και την πορεία της ανθρωπότητας. Μια τέτοια εφεύρεση υπήρξε το διαδίκτυο, αντίστοιχος αγγλικός όρος internet από την σύνθεση λέξεων internet-network.

1.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Η Ρωσία είχε ήδη στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1 κάνοντας τους Αμερικανούς να φοβούνται όλο και περισσότερο για την ασφάλεια της χώρας τους. Θέλοντας λοιπόν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Ρώσων δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ARPA (Advanced Research Project Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί

ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση. Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ. Λικλάιντερ (J.C.R. Licklider) που ανέφερε σε συγγράμματά του το "γαλαξιακό δίκτυο". Η θεωρία αυτή υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο έτσι ώστε ακόμα κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Τη λύση σε αυτό έδωσε ο Πόλ Μπάραν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλάινροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο. Στηριζόμενο λοιπόν σε αυτές τις τρεις θεωρίες δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 με 4 κόμβους μέσω των οποίων συνδέονται 4 μίνι υπολογιστές (mini computers 12k): του πανεπιστημίου της Καλιφόρνια στην Σάντα Μπάρμπαρα του πανεπιστημίου της Καλιφόρνια στο Λος Άντζελες, το SRI στο Στάνφορντ και το πανεπιστήμιο της Γιούτα. Η ταχύτητα του δικτύου έφθανε τα 50 kbps και έτσι επιτεύχθηκε η πρώτη dial up σύνδεση μέσω γραμμών τηλεφώνου. Μέχρι το 1972 οι συνδεδεμένοι στο ARPANET υπολογιστές έχουν φτάσει τους 23, οπότε και εφαρμόζεται για πρώτη φορά το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου(e-mail). Παράλληλα, δημιουργήθηκαν και άλλα δίκτυα, που χρησιμοποιούσαν διαφορετικές μεθόδους και τεχνικές (όπως το x.25 και το UUCP) τα οποία συνδέονταν με το ARPANET. Το πρωτόκολλο που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους υπολογιστών. Έτσι, δημιουργήθηκε η ανάγκη στις αρχές του 1970 για ένα πρωτόκολλο που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε. Το 1974 λοιπόν, δημοσιεύεται η μελέτη των Βίντ Σέρφ (Vint Cerf) και Μπόμπ Κάαν (Bob Kahn) από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol) που αργότερα το 1978 έγινε TCP/IP, προστέθηκε δηλαδή το Internet Protocol (IP) και τελικά το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET. Το 1984 υλοποιείται το

πρώτο DNS (Domain Name System) σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών. Ένα ακόμα σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο δημιούργησε την πρώτη διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet. Ο όρος Διαδίκτυο/Ιντερνετ ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το APRANET με το NSFNet και Ιντερνέτ σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε TCP/IP. Η μεγάλη άνθιση του Διαδικτύου όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Τιμ Μπέρνερς-Λι στο ερευνητικό ίδρυμα CERN το 1989, ο οποίος είναι, στην ουσία, η πλατφόρμα, η οποία κάνει εύκολη την πρόσβαση στο Ιντερνέτ, ακόμα και στη μορφή που είναι γνωστό σήμερα.[1]

1.2 ΟΡΙΣΜΟΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στην γενική του έννοια διαδίκτυο είναι ένα δίκτυο ηλεκτρονικών υπολογιστών που (δια)συνδέει άλλα δίκτυα. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιημένη του μορφή, με τον όρο διαδίκτυο περιγράφεται το παγκόσμιο πλέγμα διασυνδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρηστές. [2]

1.3 ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Τα δίκτυα υπολογιστών είναι ένα σύνολο από αυτονόμους ή μη αυτονόμους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι

[1] *http://el.wikipedia.org/wiki/Διαδίκτυο*
[2] *Αναγνώστου Παναγιώτης(2008):Εισαγωγή στα Διαδίκτυα Η/Υ και Internet (Εργαστηριακές σημειώσεις)*

δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (πχ εκκίνηση ή τερματισμού κάποιου άλλου).[3] Οι κυριότεροι λόγοι ύπαρξης ενός δικτύου είναι να μπορούν οι χρηστές των υπολογιστών να επικοινωνούν μεταξύ τους και να χρησιμοποιούν από απόσταση τις υπηρεσίες που προσφέρει κάποιος υπολογιστής του δικτύου. Οι υπολογιστές δικτύου χωρίζονται σε servers (διακομιστής) και σε clients (πελάτες). Διακομιστής είναι ο υπολογιστής ο όποιος εξυπηρετεί τους υπόλοιπους υπολογιστές του δικτύου (τους πελάτες), δίνοντας τους λογισμικό και στοιχειά (αρχεία κειμένου, ήχων εικόνων, κλπ) που είναι αποθηκευμένα στο σκληρό δίσκο. Για να παίζει κάποιος υπολογιστής τον ρολό του διακομιστή, πρέπει να είναι συνεχώς συνδεδεμένος με τους «πελάτες» του και να έχει και το απαραίτητο λογισμικό .

1.3.1 ΧΑΡΑΚΤΙΡΙΣΜΟΣ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Τα δίκτυα ηλεκτρονικών υπολογιστών φέρουν τους εξής χαρακτηρισμούς πού καθορίζουν την κατηγορία τους:

- Ανάλογα με το φυσικό μέσο διασύνδεσης τους χαρακτηρίζονται ως : **ενσύρματο** και **ασύρματο.**

1. Ένα *ενσύρματο* δίκτυο συνδέει δύο ή περισσότερους υπολογιστές μέσω καλωδίου. Το ενσύρματο δίκτυο είναι κατά κανόνα ένα Local Area Network (Τοπικό Δίκτυο, το οποίο θα το αναλύσουμε παρακάτω). Στο δίκτυο μπορούν να συνδεθούν και εκτυπωτές, καθώς και άλλες συσκευές. Για τη σύνδεση απαιτείται ένας μεταγωγέας (switch). Αυτός είναι συχνά ενσωματωμένος σε κάποιον δρομολογητή (router). Τα δεδομένα του δικτύου είναι διαθέσιμα μόνο σε εξουσιοδοτημένους χρήστες.[4]

2. Ως *ασύρματο* δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης

[3] Tanenbaum, Andrew S. 2000, *«Δίκτυα Υπολογιστών»*, Τρίτη Έκδοση, Πρώτη Ελληνική Έκδοση, Εκδόσεις Παπασωτηρίου, Αθήνα.
[4] http:/ /www.mediamarkt.gr

δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και, επομένως, κατά μία έννοια, είναι ουσιαστικώς δίκτυα υπολογιστών.[5]

Εικόνα 1.1: Ένας φορητός υπολογιστής ο οποίος επικοινωνεί ασύρματα μέσω ραδιοκυμάτων με ένα σημείο πρόσβασης το οποίο συνδέεται στο internet

- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως 1) **Ιδιωτικό** και 2) **Δημόσιο** Δίκτυο.

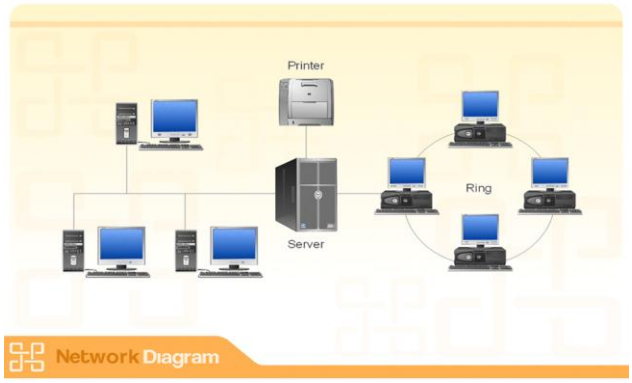
1) Τα *ιδιωτικά δίκτυα* (Private Networks) ανήκουν εξ ολοκλήρου σε ιδιωτικούς οργανισμούς και χρησιμοποιούν είτε αποκλειστικές γραμμές επικοινωνίας δημόσιων τηλεπικοινωνιακών φορέων (leased lines) χωρίς να τις μοιράζονται με άλλους χρήστες ή ιδιόκτητες γραμμές επικοινωνίας.

2) Τα *δημόσια δίκτυα* (Public Networks) εξυπηρετούν τις διασυνδέσεις μεταξύ απομακρυσμένων σημείων. Χρησιμοποιούνται όταν η απόσταση είναι μεγάλη και καθίσταται απαγορευτική, λόγω κόστους, η χρήση αποκλειστικών γραμμών ή όταν ο φόρτος μεταξύ των σημείων δεν είναι μεγάλος και επιτυγχάνεται έτσι μεγάλη ταχύτητα μεταφοράς.[6]

- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως :

[5] Stallings William , 2007 *«Ασύρματες Επικοινωνίες και Δίκτυα»*, Εκδόσεις Τζιόλα, Θεσσαλονίκη.
[6] http://www.cnc.uom.gr/services/pdf/section1(2).pdf

1. ***Τοπικά δίκτυα ή και LAN(Local Area Networks):*** Ένα τοπικό δίκτυο LAN είναι ένα μικρό δίκτυο από υπολογιστές και εκτυπωτές που βρίσκεται σε ένα κτίριο ή πάτωμα. Ένα τοπικό δίκτυο χρησιμοποιείται για να συνδέει υπολογιστές και άλλες συσκευές δικτύου, έτσι ώστε οι συσκευές να μπορούν να επικοινωνούν μεταξύ τους και να μοιράζονται πόρους. Τα τοπικά δίκτυα LAN παίζουν σημαντικό ρόλο στην καθημερινή λειτουργία σχολείων, επιχειρήσεων και κυβερνήσεων. Τα δίκτυα αυτά εξοικονομούν χρόνο στους χρήστες, μειώνουν το κόστος του εξοπλισμού κάνοντας κοινόχρηστους τους εκτυπωτές και άλλους πόρους και επιτρέπουν να φυλάσσονται οι ευαίσθητες πληροφορίες σε ασφαλή θέση.[7] Τα δίκτυα LAN χαρακτηρίζονται από υψηλούς ρυθμούς μεταφοράς δεδομένων (10 έως 100Mbps) και μικρό αριθμό σφαλμάτων μετάδοσης. Τοπικά δίκτυα συναντάμε σε σχολεία, πανεπιστήμια, εταιρείες, οργανισμούς, ιδρύματα κ.α.[8]

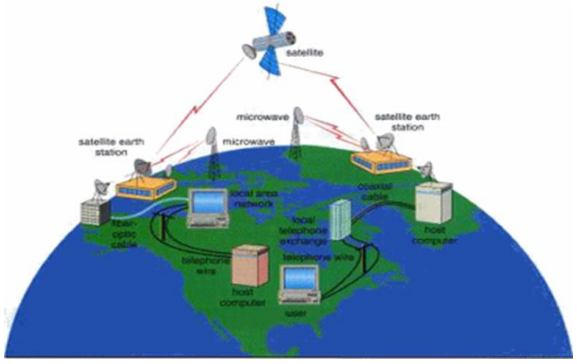


Εικόνα 1.2: Σχηματική αναπαράσταση ενός μικρού δικτύου LAN

2. ***Τα δίκτυα ευρείας περιοχής ή WAN (Wide Area Network):*** Τα δίκτυα αυτά παρέχουν δυνατότητες επικοινωνίας σε μεγάλες αποστάσεις. Οι περισσότερες τεχνολογίες WAN δεν έχουν περιορισμούς ως προς τις αποστάσεις που καλύπτουν. Για παράδειγμα, μια τεχνολογία WAN μπορεί να καλύψει μια ήπειρο ή να συνδέει υπολογιστές που βρίσκονται σε διαφορετικούς ηπείρους. Συνήθως, οι τεχνολογίες WAN λειτουργούν σε μικρότερες ταχύτητες από τις τεχνολογίες LAN και

[7] Patrick Ciccarelli, Christina Faulkner, *2005 «Δίκτυα υπολογιστών, Εισαγωγή στη Σύγχρονη Τεχνολογία»*, Εκδόσεις Μ. Γκιούρδας, Αθήνα.
[8] Παντελής Μπαλής, Βασίλης Φωτόπουλος, 2008*:Τεχνολογίες Πληροφορικής –Επικοινωνιών, Πληροφορική ΙΙ: Βασικές έννοιες Η/Υ στη σημερινή κοινωνία της πληροφορίας.* (Το παρόν εκπαιδευτικό υλικό παράχθηκε στο πλαίσιο του έργου «Κέντρα εκπαίδευσης ενηλίκων»).

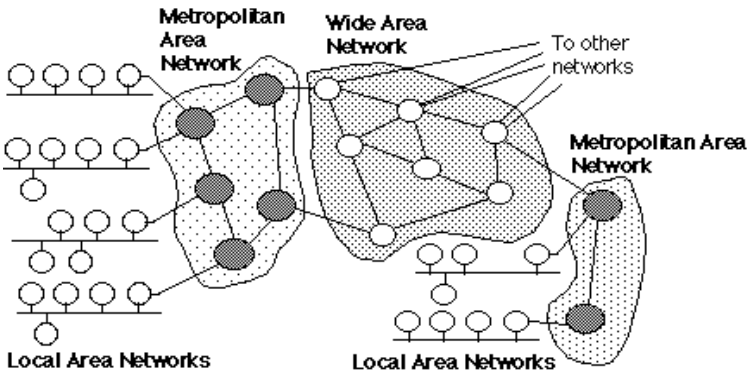
παρουσιάζουν πολύ μεγαλύτερη καθυστέρηση μεταξύ των συνδέσεων. Οι συνηθισμένες ταχύτητες για μια τεχνολογία WAN κυμαίνονται από 1.5 Mbps ως 155 Mbps (εκατομμύρια bit ανά δευτερόλεπτο). Οι καθυστερήσεις ποικίλλουν από λίγα χιλιοστά μέχρι αρκετά δέκατα του δευτερολέπτου.[9] Για την διασύνδεση αυτή χρησιμοποιούνται σχεδόν πάντα μισθωμένες δημόσιες τηλεπικοινωνιακές γραμμές ή μερικές φορές και δορυφορικές τηλεπικοινωνίες. Ένα τυπικό παράδειγμα WAN είναι τα δίκτυα Αυτόματων Ταμειολογιστικών Μηχανών (ATM) των τραπεζών, ενώ και το Internet εντάσσεται σε αυτή την κατηγορία.



Εικόνα 1.3: Τα δίκτυα ευρείας περιοχής ή WAN (Wide Area Network)

3. ***Ένα μητροπολιτικό δίκτυο ή και MAN(Metropolitan Area Network):*** είναι μια μεγαλύτερη εκδοχή ενός τοπικού δικτύου. Μπορεί να καλύπτει ομάδα γειτονικών γραφείων μιας επιχείρησης ή μια πόλη και μπορεί να είναι είτε ιδιωτικό είτε δημόσιο. Τα μητροπολιτικά δίκτυα είναι δημοφιλή γιατί παρέχουν ένα τρόπο να μοιράζονται διάφορες υπηρεσίες, ανεκτίμητους πόρους και να επικοινωνούν μεταξύ τους. Επίσης, ένα μητροπολιτικό δίκτυο μπορεί να υποστηρίζει δεδομένα και ίσως ακόμη να σχετίζεται με την καλωδιακή τηλεόραση. Το μητροπολιτικό δίκτυο χρησιμοποιεί ένα ή δύο καλώδια και δεν διαθέτει στοιχεία μεταγωγής που να διοδεύουν τα πακέτα προς τη μια από τις πολλές διαφορετικές γραμμές εξόδου. Η απουσία μεταγωγής απλοποιεί τη σχεδίαση.[10]

[9] Douglas E. Comer, 2010 *«ΔΙΑΔΙΚΤΥΑ με TCP/IP ΑΡΧΕΣ, ΠΡΩΤΟΚΟΛΛΑ, ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ»*, 4η Αμερικάνικη έκδοση, Εκδόσεις κλειδάριθμος, Αθήνα.
[10] Andrew S. Tanenbaum*, 2003 «Δίκτυα Υπολογιστών»,* Εκδόσεις Κλειδάριθμος, Αθήνα.



Εικόνα 1.4: Ένα μητροπολιτικό δίκτυο ή και MAN (Metropolitan Area Network)

4. Δίκτυα Προστιθέμενης Αξίας (Value Added Networks-VAN). Είναι δημόσια δίκτυα που "προσδίδουν αξία" μεταφέροντας δεδομένα και παρέχοντας πρόσβαση σε εμπορικές βάσεις δεδομένων και λογισμικό. Η χρήση των VAN γίνεται συνήθως με συνδρομή και οι χρήστες πληρώνουν ανάλογα με τον όγκο των δεδομένων που μεταφέρουν. Τα δίκτυα αυτά χρησιμοποιούνται για πολλούς λόγους. Μπορούν να θεωρηθούν ένας τρόπος μεταφοράς ηλεκτρονικών πληροφοριών, προσφέροντας μια υπηρεσία παρόμοια με αυτή των τηλεφωνικών δικτύων. Μέσω των δικτύων VAN είναι δυνατή η αποστολή δεδομένων μεταξύ υπολογιστών σε διαφορετικές πόλεις ή σε διαφορετικές χώρες. Ακόμη, χρησιμοποιούνται συχνά σε συστήματα Ηλεκτρονικής Ανταλλαγής Δεδομένων (EDI), καθώς διευκολύνουν τη σύνδεση με τα ποικίλα EDI που χρησιμοποιούν οι διάφοροι συνεργάτες. Τα VAN προσφέρονται για εύκολη επέκταση, γιατί είναι φτιαγμένα έτσι ώστε να χρησιμοποιούν αποτελεσματικά την χωρητικότητα τους και να την επεκτείνουν, εάν είναι απαραίτητο. Τέλος, τα δίκτυα VAN παρέχουν εύκολη πρόσβαση σε δεδομένα που διαφορετικά δεν θα ήταν διαθέσιμα.[11]

[11] http://www.ea.gr/ep/agroweb/htmls/lessons/commerce1gr/21d.htm

1.3.2 ΤΟΠΟΛΟΓΙΑ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Με τον ορό τοπολογία τοπικών δικτύων εννοούμε τον τρόπο με τον οποίο δυο ή περισσότεροι υπολογιστές επικοινωνούν μεταξύ τους. Οι πλέον διαδεδομένες τοπολογίες τοπικών δικτύων είναι τρεις: τοπολογία αστέρα, τοπολογία διαύλου και η τοπολογία δακτυλίου.

➢ Τοπολογία αστέρα**:** Μια φυσική τοπολογία αστέρα εγκαθίσταται στο σχήμα ενός αστεριού, όπως είναι οι ακτίνες ενός τροχού ποδηλάτου. Μια τοπολογία αστέρα αποτελείται από ένα κεντρικό σημείο σύνδεσης, τον συγκεντρωτή, όπου συναντώνται τα τμήματα των καλωδίων. Κάθε συσκευή σε ένα δίκτυο αστέρα συνδέεται στον κεντρικό συγκεντρωτή με το δικό της καλώδιο.

Πλεονεκτήματα τοπολογίας αστέρα:

- Αυξημένη αξιοπιστία.
- Σχετικά μικρό κόστος υλοποίησης.
- Αν χαλάσει ένα καλώδιο, δεν θα χαλάσει ολόκληρο το δίκτυο.
- Ο συγκεντρωτής παρέχει κεντρική διαχείριση.
- Μπορεί να αναβαθμιστεί σε πιο γρήγορες ταχύτητες μετάδοσης.

Μειονεκτήματα τοπολογίας αστέρα :

- Αν καταρρεύσει ο κεντρική μονάδα έχουμε πλήρη διακοπή της επικοινωνίας.
- Απαιτεί περισσότερο καλώδιο σε σχέση με τα άλλα δίκτυα,
- Το κόστος εγκατάστασης και εξοπλισμού είναι υψηλότερο.[12]

[12] Patrick Ciccarelli, Christina Faulkner, 2005 *«Δίκτυα υπολογιστών, Εισαγωγή στη Σύγχρονη Τεχνολογία»*, Εκδόσεις Μ. Γκιούρδας, Αθήνα.

Εικόνα 1.5: Τοπολογία Αστέρα

➢ Τοπολογία διαύλου: Στην τοπολογία διαύλου (bus topology), όλοι οι κόμβοι του δικτύου, συνδέονται άμεσα σε μια κοινή γραμμή επικοινωνίας που λέγεται δίαυλος (bus). Τα πακέτα δεδομένων μεταδίδονται σε όλο το μήκος του φυσικού μέσου, και μπορούν να παραληφθούν από όλους τους άλλους κόμβους. Κάθε κόμβος βλέπει το μήνυμα, ελέγχει τη διεύθυνση του παραλήπτη, και εάν τον αφορά, το αντιγράφει. Τα δίκτυα αυτού του τύπου αποτελούν καλή επιλογή όταν ο αριθμός των κόμβων που είναι συνδεδεμένοι στο δίκτυο είναι μικρός, ενώ το ίδιο συμβαίνει και με την κυκλοφορία του δικτύου.[13] Η τοπολογία αυτή χρησιμοποιείται συνήθως για μικρό αριθμό υπολογιστών και αφορά περιπτώσεις ηλεκτρονικού ταχυδρομείου ή αποθηκεύσεις δεδομένων σε διαφορετικούς υπολογιστές. Δεν είναι τόσο αποτελεσματική όσο η τοπολογία αστέρας για την διανομή πόρων του συστήματος αλλά είναι αρκετά φθηνότερη στην υλοποίηση της.

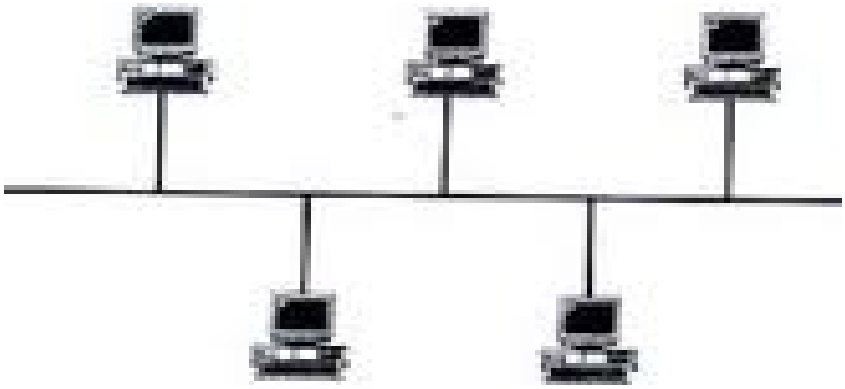
Πλεονεκτήματα τοπολογίας διαύλου:

- Ευκολία υλοποίησης
- Χαμηλό κόστος
- Οι προσθήκες και οι αλλαγές μπορούν να γίνουν εύκολα χωρίς να επηρεαστούν άλλοι σταθμοί εργασίας.

[13] http://users.sch.gr/mntoumos/erkef76.htm

Μειονεκτήματα τοπολογίας διαύλου:

- Η απόδοση εξαρτάται από την τεχνική πρόσβασης στο μέσο και το είδος των δεδομένων που μεταφέρονται.
- Μόνο μια συσκευή μπορεί να έχει πρόσβαση στο μέσον μετάδοσης κάθε φορά.



Εικόνα 1.6: Τοπολογία Διαύλου

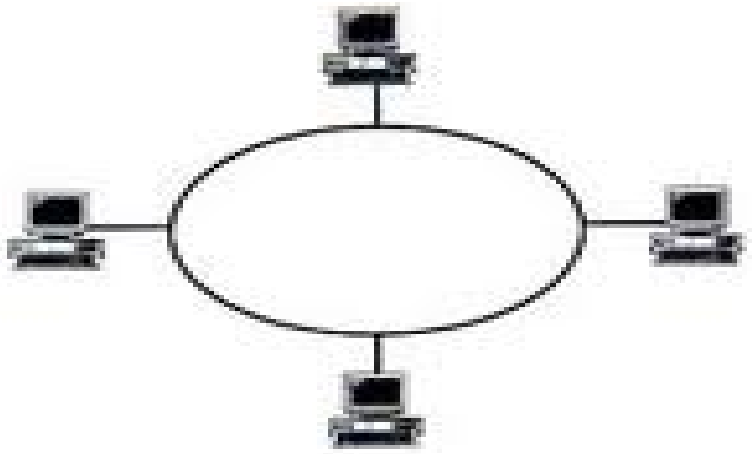
- Τοπολογία δακτυλίου : Η τοπολογία δακτυλίου (ring) είναι παρόμοια της τοπολογίας διαύλου με την μόνη διαφορά πως αντί για αντιστάσεις στα άκρα του διαύλου ενώνονται τα δύο ακριανά μέλη του δικτύου μεταξύ τους (το πρώτο και το τελευταίο δηλαδή), σχηματίζοντας έτσι σχήμα δακτύλιο. Οι πληροφορίες ή τα μηνύματα διατρέχουν τον δακτύλιο αυτό μέχρι ότου φτάσουν στον προορισμό τους. Η τοπολογία αυτή χρησιμοποιείται συνήθως για δικτύωση μεγάλων υπολογιστών που λειτουργούν κυρίως αυτόνομα, αλλά χρειάζεται κατά περιόδους να ανταλλάσουν δεδομένα ή προγράμματα.

Πλεονεκτήματα τοπολογίας δακτυλίου:

- Η κυκλοφορία ρέει μόνο προς μία κατεύθυνση με μεγάλη ταχύτητα.
- Πρόσθετα στοιχεία δεν επηρεάζουν την απόδοση του δικτύου.
- Κάθε υπολογιστής έχει ισότιμη πρόσβαση στους πόρους.

Μειονεκτήματα τοπολογίας δακτύλου:

- Ένας χαλασμένος δακτύλιος θα σταματήσει όλες τις μεταδόσεις.
- Μια συσκευή θα πρέπει να περιμένει ένα κενό διακριτικό για να μπορέσει να μεταδώσει δεδομένα.



Εικόνα 1.7: Τοπολογία Δακτυλίου

1.4 ΧΡΗΣΕΙΣ ΤΩΝ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

➢ ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΕΦΑΡΜΟΓΕΣ

Στα πλαίσια του συνεχώς αυξανόμενου ανταγωνισμού στον τομέα των επιχειρήσεων η χρήση των ηλεκτρονικών υπολογιστών έχει γίνει επιτακτική ανάγκη για την βιώσιμη ανάπτυξη και εξέλιξη τους. Πολλές επιχειρήσεις έχουν έναν σημαντικό αριθμό υπολογιστών. Για παράδειγμα, μια εταιρεία μπορεί να έχει ξεχωριστούς υπολογιστές για την παρακολούθηση της παραγωγής, της διαχείρισης των αποθηκών και την έκδοση της μισθοδοσίας. Αρχικά, καθένας από αυτούς τους υπολογιστές μπορεί να λειτουργούσε απομονωμένος από τους άλλους, αλλά σε κάποιο σημείο η διοίκηση μπορεί να αποφασίσει να τους συνδέσει μεταξύ τους, έτσι ώστε να είναι σε θέση να συλλέγει και να συσχετίζει πληροφορίες για ολόκληρη τη εταιρεία. Σε γενικούς όρους, το ζητούμενο σε αυτήν την περίπτωση είναι η κοινοχρησία πόρων ή μερισμός πόρων (resource sharing) και ο στόχος είναι όλα τα προγράμματα, ο εξοπλισμός και ιδιαίτερα τα δεδομένα να είναι διαθέσιμα σε

οποιονδήποτε στο δίκτυο, χωρίς να έχει σημασία η φυσική θέση του πόρου και του χρήση. Σε αυτό το σημείο πρέπει να τονίσουμε, ότι η κοινοχρησία πληροφοριών είναι πιθανότατα ακόμα πιο σημαντική από την κοινοχρησία φυσικών πόρων όπως οι εκτυπωτές, οι σαρωτές και οι μονάδες εγγραφής CD. Όλες οι επιχειρήσεις μεγάλου ή μεσαίου μεγέθους, καθώς και πολλές μικρές εταιρείες, είναι ζωτικά εξαρτημένες από πληροφορίες που είναι αποθηκευμένος σε υπολογιστές .Οι περισσότερες εταιρείες έχουν σε διαρκή σύνδεση επικοινωνίας (on-line) αρχεία πελατών, απογραφές αποθεμάτων, πληρωτέους λογαριασμούς, οικονομικές καταστάσεις, φορολογικά στοιχειά και πολλές άλλες πληροφορίες.[14]

➢ ΟΙΚΙΑΚΕΣ ΕΦΑΡΜΟΓΕΣ

Οι λόγοι για τους οποίους πλέον τα άτομα αγοράζουν υπολογιστές για οικιακή χρήση έχουν αλλάξει ριζικά σε σχέση με το παρελθόν. Σήμερα, είναι πιθανόν, ότι σημαντικότερος λόγος είναι η πρόσβαση στο internet. Μερικές από τις πιο δημοφιλείς χρήσεις του Internet για τους οικιακούς χρηστές είναι οι ακόλουθες:

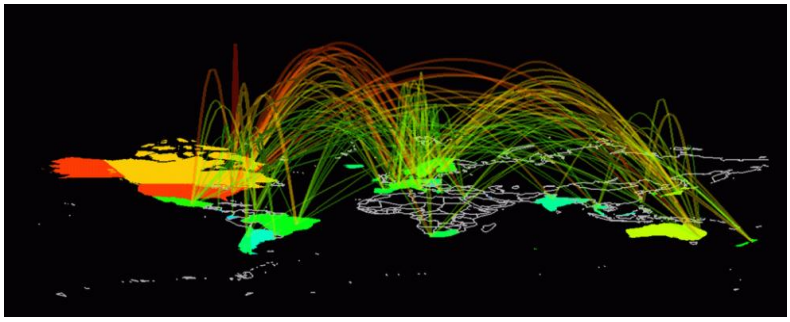
1. Πρόσβαση σε απομακρυσμένες πληροφορίες
2. Διαπροσωπική επικοινωνία
3. Αλληλεπιδραστική διασκέδαση
4. Ηλεκτρονικό εμπόριο

Ο χρήστης μέσω των μηχανών αναζήτησης (μια εφαρμογή που επιτρέπει την αναζήτηση κειμένων και αρχείων στο διαδίκτυο) έχει πρόσβαση σε απομακρυσμένες πληροφορίες. Οι διαθέσιμες πληροφορίες περιλαμβάνουν θέματα τεχνών, επιχειρήσεων, μαγειρικής, διοίκησης, υγείας, ιστορίας, σπορ, ταξιδιών, χόμπι, αναψυχής και πολλά άλλα. Η πρόσβαση στην ενημέρωση και την πληροφόρηση έχει γίνει πιο εύκολη από ποτέ μέσω του ηλεκτρονικού τύπου. Σχεδόν όλες εφημερίδες είναι σε άμεση σύνδεση (on-line) και μπορούν να εξατομικευτούν. Ο αναγνώστης έχει την δυνατότητα να εκφράσει την άποψη του άμεσα για κάποιο αναρτώμενο άρθρο ή για την εκάστοτε πολιτική κατάσταση της χώρας και γενικότερα για το

[14] Andrew S. Tanenbaum, *2003 «Δίκτυα Υπολογιστών»,* Εκδόσεις Κλειδάριθμος, Αθήνα.

κοινωνικό γίγνεσθαι. Το επόμενο βήμα πέρα από τις εφημερίδες (καθώς και τα περιοδικά και τις επιστημονικές εκδόσεις) είναι η άμεσα συνδεδεμένη ψηφιακή βιβλιοθήκη. Πολλοί επαγγελματικοί οργανισμοί, διαθέτουν ήδη σε άμεση σύνδεση πολλές επιστημονικές εκδόσεις και πρακτικά συνεδρίων. Όλες οι παραπάνω εφαρμογές περιλαμβάνουν αλληλεπίδραση ανάμεσα σε ένα άτομο και μια απομακρυσμένη βάση δεδομένων γεμάτη με πληροφορίες. Η δεύτερη κατηγορία χρήσης του δικτύου είναι η διαπροσωπική επικοινωνία (person-to-person). Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται ήδη σε καθημερινή βάση από εκατομμύρια ανθρώπους παγκοσμίως, καθώς επίσης συνηθίζεται να περιέχει ήχο και βίντεο, εκτός από κείμενο και εικόνες. Σχεδόν όλοι οι έφηβοι είναι εθισμένοι στα άμεσα μηνύματα (instant message). Αυτή η ευκολία επιτρέπει σε δυο άτομα να ανταλλάσουν μεταξύ τους μηνύματα σε πραγματικό χρόνο. Μια παραλλαγή αυτής της ιδέας με πολλούς συμμετέχοντες είναι το δωμάτιο συνομιλίας (chat room), όπου μια ομάδα ατόμων μπορεί να γράφει μηνύματα τα όποια είναι ορατά σε όλους. Οι παγκόσμιες ομάδες συζητήσεων (newsgroups) με συζητήσεις πάνω σε κάθε πιθανό θέμα, είναι ήδη γνωστές σε μια επιλεγμένη ομάδα ατόμων. Αυτές οι συζητήσεις, στις οποίες ένα άτομα δημοσιεύει ένα μήνυμα το όποιο οι άλλοι συνδρομητές της ομάδας μπορούν να διαβάσουν, καλύπτουν μια ευρεία γκάμα θεμάτων. Σε αντίθεση με τα δωμάτια συνομιλίας, οι ομάδες συζητήσεων δεν λειτουργούν σε πραγματικό χρόνο και τα μηνύματα αποθηκεύονται. Ένας άλλος τύπος διαπροσωπικής επικοινωνίας συχνά αναφέρεται με το όνομα ομότιμη επικοινωνία (peer-to-peer). Σε αυτή την μορφή επικοινωνίας, μεμονωμένα άτομα τα οποία σχηματίζουν μια ¨χαλαρή¨ ομάδα μπορούν να επικοινωνούν με άλλα άτομα της ομάδας. Κάθε άτομο μπορεί, θεωρητικά, να επικοινωνεί με ένα ή περισσότερα άλλα άτομα, δεν υπάρχει κάποια σταθερή διάκριση σε πελάτες και διακομιστές. Η τρίτη κατηγορία είναι η διασκέδαση, η οποία είναι μια τεράστια και συνεχώς αναπτυσσομένη βιομηχανία. Πρόκειται ίσως για την πιο ταχέως αναπτυσσόμενη βιομηχανία όπου δίνει στον χρήστη την δυνατότητα από την οθόνη του υπολογιστή του να επιλέγει την ταινία που επιθυμεί να δει, το τραγούδι που θέλει να ακούσει, το παιχνίδι που θέλει να παίξει και μέσα σε λίγα λεπτά να το έχει στον υπολογιστή του έναντι ενός ιδιαιτέρως χαμηλού ποσού. Στην περίπτωση δε που μιλάμε για ηλεκτρονικά παιχνίδια τότε η εγκατάσταση δικτύου υπολογιστών απογειώνει την ευχαρίστηση των φανατικών του

είδους. Στην τετάρτη κατηγορία ανήκει το ηλεκτρονικό εμπόριο, στο οποίο θα αναφερθούμε αναλυτικότερα παρακάτω. [15]



Εικόνα 1.8: Internet

1.5 ΠΡΩΤΟΚΟΛΛΑ

Στα δίκτυα υπολογιστών η αποστολή και η λήψη δεδομένων γίνεται σε βήματα, όπου διαδοχικά επίπεδα επεξεργασίας παρεμβάλλονται στα υπό εξέταση τηλεπικοινωνιακά δεδομένα και εκτελούν ανάλογες λειτουργίας. Το σύνολο κανόνων στο οποίο υπακούν αυτές οι λειτουργίες, καθώς και η προσωποποιημένη μορφή των δεδομένων που υφίστανται επεξεργασία σε κάθε επίπεδο, ονομάζεται πρωτόκολλο επικοινωνίας του αντίστοιχου επιπέδου. Τα πρωτόκολλα αυτά σχηματίζουν, όπως λέμε, μία "στοίβα" η οποία χαρακτηρίζει επακριβώς τον τύπο και τον τρόπο επικοινωνίας. Ακολουθεί η συνηθέστερη κατηγοριοποίηση επιπέδων από το χαμηλότερο προς το υψηλότερο της στοίβας:

- Φυσικό επίπεδο (physical layer)
- Επίπεδο ζεύξης δεδομένων (data link layer)
- Επίπεδο δικτύου (network layer)
- Επίπεδο μεταφοράς (transport layer)
- Επίπεδο εφαρμογών (application layer)

[15] Andrew S. Tanenbaum, *2003 «Δίκτυα Υπολογιστών»,* Εκδόσεις Κλειδάριθμος, Αθήνα.

1.5.1 ΠΡΩΤΟΚΟΛΛΑ IP ,TCP, TCP/IP

ΓΕΝΙΚΑ

Οι υπολογιστές που είναι συνδεδεμένοι σε ένα διαδίκτυο δεν έχουν όλοι το ίδιο λειτουργικό σύστημα. Επομένως, έπρεπε να βρεθεί ένας τρόπος έτσι ώστε να μπορούν να ανταλλάσουν μεταξύ τους πληροφορίες. Η μέθοδος που βρέθηκε είναι γνώστη ως πρωτόκολλο IP (internet protocol), το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το διαδίκτυο. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους. Η εξέλιξη, του πρωτόκολλου IP, είναι το TCP/IP (Πρωτόκολλο Ελέγχου Μετάδοση), παρακάτω θα γίνει εκτενέστερη ανάλυση των πρωτοκόλλων IP, TCP, TCP/IP

1.5.2 ΠΡΩΤΟΚΟΛΛΟ IP (Internet Protocol)

Το Πρωτόκολλο Διαδικτύου (IP) (Internet Protocol), αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση αυτοδύναμων πακέτων δηλαδή πακέτων δεδομένων, σε ένα διαδίκτυο.[16] 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.[17]

1.5.3 ΠΡΩΤΟΚΟΛΛΟ TCP (Transmission Control Protocol)

Το TCP *(*Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς), βρίσκεται πάνω από το IP protocol *(πρωτόκολλο IP)*. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι

[16] http://el.wikipedia.org/wiki/IP
[17] http://www2.uth.gr/main/help/help-desk/internet/internet4.html

περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP.[18]

1.5.4 ΠΡΩΤΟΚΟΛΛΟ TCP/IP (Transmission Control Protocol/Internet Protocol)

Τα αρχικά του TCP/IP (Transmission Control Protocol/Internet Protocol) δηλαδή, Πρωτόκολλο Ελέγχου Εκπομπής/Πρωτόκολλο του Internet . Το πρωτόκολλο TCP/IP (Transmission Control Protocol / Internet Protocol), είναι αυτό που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και διαμεταγωγής δεδομένων στο Internet. Βασίζεται στη λογική του «πακέτου» : στο κόμβο του αποστολέα το μήνυμα μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του όπως (π.χ. η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Στο κόμβο του παραλήπτη τα πακέτα συναρμολογούνται για να σχηματιστεί το αρχικό μήνυμα. Φυσικά, η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο διαδίκτυο έχει τη δική του διεύθυνση επικοινωνίας (IP address). [19]

1.6 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΓΕΝΙΚΑ

Όπως προαναφέραμε η ραγδαία ανάπτυξη του διαδικτύου έχει επιφέρει πρωτόγνωρες αλλαγές στον καθημερινό τρόπο ζωής μας, μέσα σε αυτό συμπεριλαμβάνονται και οι καθημερινές συναλλαγές μας. Σήμερα, οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα οι πωλήσεις των έμπορων δεν γίνονται με συμβατικά μέσα όπως γινόταν στο παρελθόν. Οι καταναλωτές προκειμένου να

[18] http://el.wikipedia.org/wiki/TCP

[19] Γ. Πάγκαλος, Ι. Μαυρίδης, 2003 «*Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*», Εκδόσεις ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη.

αγοράσουν αυτό που επιθυμούσαν ή να δεχτούν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά. Ένας από τους νέους και τάχιστους τρόπους εξυπηρέτησης των καταναλωτών είναι το Ηλεκτρονικό Εμπόριο το οποίο αναπτύσσεται ραγδαία τόσο στο εξωτερικό όσο και στην Ελλάδα.

1.6.1 ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. 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 ή πώληση αγαθών ή υπηρεσιών. Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και φαξ. [20]

1.6.2 ΔΙΑΚΡΙΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

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 και άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών.

[20] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., *Παπαζαφειροπούλου Ν.,*1998 *«Ηλεκτρονικό Εμπόριο»,* Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

1.6.3 ΕΙΔΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

➢ **B2B:** Πρόκειται για ευφυές αρκτικόλεξο του αγγλικού όρου «business to business» και αφορά ηλεκτρονικό εμπόριο που διενεργείται μεταξύ επιχειρήσεων.

➢ **B2C:** Πρόκειται ομοίως σε χρήση του αρκτικόλεξο του αγγλικού όρου «business to consumer» που αφορά ηλεκτρονικό εμπόριο που διενεργείται μεταξύ επιχειρήσεων και καταναλωτών αυτών.

➢ **Mobile E-commerce:** Αυτό αφορά το επιχειρούμενο ηλεκτρονικό τηλεφωνικό εμπόριο.[21]

1.6.4 ΟΦΕΛΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Για την επιχείρηση:

- Συνεχής προβολή της επιχείρησης και των προϊόντων της.
- Διεύρυνση του κύκλου εργασιών, μέσω της επέκτασης των γεωγραφικών ορίων των συναλλαγών της.
- Αναπροσαρμογή της πολιτικής της, μέσω της συλλογής στοιχείων από τις ηλεκτρονικές συναλλαγές της.
- Ενδυνάμωση της ανταγωνιστικής της θέσης μέσα στην αγορά.
- Εξατομίκευση των υπηρεσιών με βάση τις ιδιαίτερες ανάγκες του κάθε πελάτη.
- Συμπίεση του κόστους παραγωγής και διανομής προϊόντων.[22]

Για τον καταναλωτή:

- Μεγαλύτερη ποικιλία προϊόντων.
- Η συναλλαγή είναι γρήγορη και άμεση.

[21] http://el.wikipedia.org/wiki/Ηλεκτρονικό_εμπόριο

[22] Παπαδόπουλος Δ, εργαστηριακές σημειώσεις στο μάθημα Ηλεκτρονικό Εμπόριο, section 2-εισαγωγή στο ηλεκτρονικό εμπόριο.

- Ο καθένας βρίσκει αυτό που θέλει, όποτε το θέλει, χωρίς δηλαδή κόπο και χωρίς καμία σπατάλη χρόνου.
- Τα ηλεκτρονικά καταστήματα είναι ανοιχτά 24 ώρες το 24ωρο.
- Με τις ηλεκτρονικές αγορές εξοικονομούνται χρήματα.

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

2.1 Ηλεκτρονικές πληρωμές

Σε κάθε συναλλαγή το πιο σημαντικό σημείο είναι αυτό της πληρωμής. Το internet συνέβαλε στο να μην απαιτείται η προσωπική επαφή μεταξύ του εμπόρου και του πελάτη. Το σύγχρονο επιχειρηματικό περιβάλλον και ο διαρκώς αυξανόμενος όγκος συναλλαγών μέσω διαδικτύου την τελευταία δεκαετία έχει καταστήσει απαραίτητη την ανάπτυξη και διάδοση καινοτομικών συστημάτων ηλεκτρονικών πληρωμών. Τα συστήματα αυτά έχουν ως στόχο να υποστηρίξουν τα ιδιαίτερα χαρακτηριστικά των συναλλαγών στο διαδίκτυο όπως η ταχύτητα και η αμεσότητα χωρίς όμως να θυσιάζουν βασικά πλεονεκτήματα των παραδοσιακών μεθόδων πληρωμής όπως είναι η ασφάλεια και η ευκολία.

Ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με την μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας.[23]

2.2 Μέθοδοι ηλεκτρονικών πληρωμών

Για την εκπλήρωση της ανάγκης των ηλεκτρονικών συναλλαγών προτάθηκαν και εφαρμόστηκαν διάφοροι μέθοδοι ηλεκτρονικών πληρωμών και έτσι τώρα πια υπάρχει μια μεγάλη γκάμα μεθόδων πληρωμής που χρησιμοποιείται στο internet. Η πλέον διαδεδομένη είναι η χρήση της πιστωτικής κάρτας. Παράλληλα όμως χρησιμοποιούνται και άλλοι τρόποι πληρωμής τους οποίους αναλύουμε παρακάτω.

[23] http://www.ebusinessforum.gr, ομάδα Ε3: Ηλεκτρονικό Εμπόριο: Προβλήματα και Προοπτικές.

2.2.1 Πιστωτική κάρτα

Είναι η πιο διαδεδομένη μέθοδος πληρωμών στο Internet. Η χρήση τους στο διαδίκτυο δεν διαφέρει σημαντικά από τον τρόπο που χρησιμοποιούνταν μέχρι τώρα στις συναλλαγές στον φυσικό Κόσμο. Οι πιστωτικές κάρτες είναι η μορφή του λεγόμενου «πλαστικού χρήματος». Η έκδοση τους γίνεται από πιστωτικούς αποδεκτούς και αναγνωρισμένους οργανισμούς και δίνουν την δυνατότητα στους κατόχους τους, να μπορούν να αγοράζουν αγαθά ή να πληρώνουν υπηρεσίες μέσω αυτών χωρίς να απαιτείται άμεση καταβολή της αξίας τους.[24] Η πιστωτική κάρτα έχει τη μορφή μιας πλαστικής κάρτας η οποία φέρει στη μια πλευρά της με ανάγλυφα στοιχεία τον αριθμό μητρώου και το ονοματεπώνυμο του κατόχου της, τη λήξη ισχύος της, καθώς και το πιστωτικό κατάστημα το οποίο τη χορήγησε. Στην άλλη πλευρά συνήθως υπάρχει η μαγνητική ταινία, θέση για την υπογραφή του κατόχου της και το λογότυπο του πιστωτικού οργανισμού που την εξέδωσε. Για λόγους ασφάλειας δίνεται στον κάτοχο της και ένας μυστικός προσωπικός κωδικός (PIN), τον οποίο ο κάτοχος της είναι καλό να τον αποστηθίζει και να μην τον δίνει σε τρίτους.

Τα κύρια πλεονεκτήματα της πιστωτικής κάρτας είναι:

- Ευκολία στις συναλλαγές σε περιπτώσεις που ο κάτοχος δεν έχει μαζί του μετρητά ή δεν θέλει να έχει είτε επειδή φοβάται μήπως πέσει θύμα κλοπής, είτε επειδή υπάρχει πιθανότητα να τα χάσει.
- Όλο και περισσότερες εταιρίες στην Ελλάδα και στο Εξωτερικό παρέχουν την δυνατότητα αγοράς προϊόντων και υπηρεσιών μέσω του διαδικτύου ή τηλεφωνικά συνήθως σε τιμές αρκετά ευνοϊκότερες από τις τιμές της αγοράς. Ωστόσο, καλό είναι ο κάτοχος όταν πραγματοποιεί αγορές μέσω Internet/Τηλεφώνου να είναι ενήμερος για την αξιοπιστία της αντίστοιχης εταιρίας και να μην εκθέτει τα στοιχεία της πιστωτικής του κάρτας σε αγνώστου κύρους εταιρίες.
- Κάνοντας τις αγορές του μέσω πιστωτικής κάρτας, ο καταναλωτής ενημερώνεται στο τέλος του μήνα για όλες τις αγορές που πραγματοποίησε το προηγούμενο

[24] Πασχόπουλος Α, Σκαλτσάς Π.,2009 «*Ηλεκτρονικό Εμπόριο»*, 3η έκδοση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, Αθήνα.

διάστημα, καθώς όλες οι συναλλαγές του αναγράφονται αναλυτικά στο λογαριασμό που λαμβάνει από την τράπεζα. Με αυτόν τον τρόπο ο καταναλωτής έχει τη δυνατότητα να παρακολουθεί τα μηνιαία του έξοδα ευκολότερα από ότι στην περίπτωση που πλήρωνε με μετρητά.

- Πολλές επιχειρήσεις δίνουν στους πελάτες που πληρώνουν με πιστωτική κάρτα τη δυνατότητα αποπληρωμής σε μηνιαίες δόσεις. Οι δόσεις αυτές υπόκεινται σε χαμηλότερο επιτόκιο σε σύγκριση με το βασικό επιτόκιο των πιστωτικών καρτών.
- Παροχή της δυνατότητας στους κατόχους τους να διενεργούν τραπεζικές πράξεις μέσω των Αυτόματων Ταμειολογιστικών Μηχανών (ΑΤΜ), όπως αναλήψεις, καταθέσεις, μεταφορά ποσών από λογαριασμό σε λογαριασμό κ.ά.
- Υπάρχει ένα πιστωτικό όριο όπου βοηθά τον κάτοχο της να μην υπερβεί το ποσό το οποίο μπορεί να διαθέσει σύμφωνα με την οικονομική του κατάσταση, διότι μιλάμε για ένα άυλο χρήμα και υπάρχουν μεγάλες πιθανότητες κάποιος να μην έχει την αντίληψη για το τί ξοδεύει.
- Υπάρχει δυνατότητα ανάληψης μετρητών 24 ώρες το 24ωρο σε αντιστοιχία βέβαια με το πιστωτικό όριο του καθενός.
- Οι πιστωτικές κάρτες έχουν παγκόσμια ισχύ και αποτελούν ένα ασφαλές και βολικό μέσο για συναλλαγές στο εξωτερικό.

Λόγω της ευρείας διάδοσης των πιστωτικών καρτών και του ανταγωνισμού που υπάρχει ανάμεσα στις τράπεζες οι πιστωτικές κάρτες εμπλουτίστηκαν και με άλλες υπηρεσίες, όπως ταξιδιωτική ασφάλιση, ιατρική και νομική βοήθεια, καθώς επίσης καταρτίστηκαν και ειδικά προγράμματα συνεργασίας τραπεζών με επιχειρήσεις, ώστε να παρέχονται εκπτώσεις για την αγορά αγαθών ή υπηρεσιών, και τελευταία άρχισαν να εφαρμόζονται προγράμματα σύνδεσης πιστωτικών καρτών με οργανισμούς, σωματεία, λέσχες, φιλανθρωπικές ή οικολογικές οργανώσεις κ.ά. διευρύνοντας έτσι την κλασική λειτουργία της κάρτας ως μέσο πληρωμών.

Τα μειονεκτήματα που θα μπορούσε να έχει η πιστωτική κάρτα είναι :

- Μερικές φορές οι τόκοι που μπορεί να έχουν οι πιστωτικές κάρτες υπάρχει περίπτωση να μην συμφέρουν τον ενδιαφερόμενο και συνήθως αυτοί οι όροι είναι τα λεγόμενα «ψιλά γράμματα».

- Η κάρτα επειδή είναι ουσιαστικά μικρή σε μέγεθος, υπάρχει κίνδυνος απώλειας ή κλοπής. Γενικά είναι εύκολο να χαθεί.
- Αν ξεπεράσουν την ημερομηνία λήξης μιας αγοράς που είχαν κάνει για την εξόφληση της, οι τόκοι μπορεί να ανέβουν κατά πολύ.
- Ένα εύκολο PIN υπάρχει περίπτωση να ανακαλυφθεί και κυρίως από άτομα που γνωρίζουν τον κάτοχο της.

Υπάρχουν 3 κατηγορίες πιστωτικών:

- Οι πιστωτικές κάρτες που μπορούν να χρησιμοποιηθούν μόνο στο εσωτερικό της χώρας όπου έχουν δημιουργηθεί.
- Οι πιστωτικές κάρτες οι οποίες μπορούν να χρησιμοποιηθούν και στο εξωτερικό.
- Οι λεγόμενες Golden Cards ή Prestige Cards δηλαδή οι χρυσές κάρτες οι οποίες βέβαια διαθέτουν υψηλό πιστωτικό όριο σε σύγκριση με τις υπόλοιπες.

Εικόνα 2.1 Πιστωτική Κάρτα

Χρήση πιστωτικής κάρτας στο διαδίκτυο

Η χρήση της πιστωτικής κάρτας στο internet απαιτεί μεγαλύτερη προσοχή παρόλο που οι διαδικασίες που χρησιμοποιεί είναι περίπου οι ίδιες με την παραδοσιακή χρήση της. Για την ασφάλεια των ηλεκτρονικών συναλλαγών που γίνονται με την χρήση της πιστωτικής κάρτας έχουν ληφθεί κάποια επιπρόσθετα μέτρα προστασίας που σημαίνει περισσότερες πιστοποιήσεις τόσο για τον αγοραστή

όσο και για τον προμηθευτή. Το γεγονός αυτό οδήγησε στην δημιουργία μιας σειράς συστημάτων ηλεκτρονικών πληρωμών με πιστωτική κάρτα. Το επίπεδο ασφάλειας των συναλλαγών καθώς και το λογισμικό που χρησιμοποιούν τα εμπλεκόμενα μέρη είναι αυτά που διαφοροποιούν τα συστήματα. Όταν μια συναλλαγή γίνεται on-line ο χειρισμός πιστωτικών καρτών μπορεί να γίνει είτε με την αποστολή μη κρυπτογραφημένων στοιχείων από τον αγοραστή προς τον προμηθευτή όπου βέβαια ο κίνδυνος υποκλοπής στοιχείων από εισβολείς είναι μεγαλύτερη, είτε με την αποστολή κρυπτογραφημένων στοιχείων από τον αγοραστή προς τον προμηθευτή, φυσικά αυτός είναι και ο πιο ασφαλής τρόπος. Για την ασφάλεια αυτών των συναλλαγών έχουν δημιουργηθεί και τα αντίστοιχα πρωτόκολλα ασφαλείας στα οποία θα αναφερθούμε στις επόμενες ενότητες διεξοδικά.

2.2.2 Χρεωστικές Τραπεζικές Κάρτες

Είναι μια ευρέως γνωστή μέθοδος ηλεκτρονικής πληρωμής. Οι κάρτες αυτές είναι ένας άμεσος τρόπος πληρωμής. Οι χρεωστικές τραπεζικές κάρτες είναι στην ουσία μία προπληρωμένη κάρτα όπου δεν υπάρχει έκδοση χρημάτων απλά είναι ένας δίαυλος παράδοσης χρηματικού ποσού σε ηλεκτρονική μορφή. Στην κάρτα αυτή έχει την δυνατότητα ο χρήστης της να είναι ανώνυμος ή επώνυμος. Ακόμα, όταν ο κάτοχος της επιθυμεί να είναι ανώνυμος μπορεί να την μεταβιβάσει από αυτόν σε ένα άλλο άτομο ενώ η επώνυμη δεν παρέχει αυτή την κίνηση. Η χρεωστική κάρτα μπορεί να εφαρμοστεί και στο διαδίκτυο. Για την πραγματοποίηση συναλλαγών απαιτείται η ύπαρξη ειδικού τερματικού το οποίο θα επαληθεύει την εγκυρότητα των πληροφοριών που είναι αποθηκευμένες στην κάρτα και θα ελέγχει αν αυτή βρίσκεται σε ισχύ.

Το βασικό μειονέκτημα των χρεωστικών καρτών είναι ότι από την σκοπιά του πελάτη δεν είναι σαφή τα πλεονεκτήματα τους έναντι των πιστωτικών καρτών. Ειδικά στις συναλλαγές στο διαδίκτυο, οι χρεωστικές προσφέρουν μικρότερη προστασία έναντι των πιστωτικών σε περιπτώσεις που τα αντικείμενα που αγοράστηκαν δεν παραδίδονται ή είναι ελαττωματικά. Από την πλευρά των εμπόρων πάντως οι χρεωστικές κάρτες είναι προτιμότερες καθώς δεν επιβαρύνουν με προμήθεια των έμπορων. Επιπλέον, στην επιχειρηματικές συναλλαγές μέσω διαδικτύου οι

χρεωστικές κάρτες μπορεί να αποδειχθούν φθηνότερη λύση ακριβώς για τον ίδιο λόγο.[25]

Δυνατότητες που έχει η χρεωστική τραπεζική κάρτα:

- Πληρωμές λογαριασμών και συνδρομών (π.χ. ΔΕΗ, ΟΤΕ, ΙΚΑ, ΦΠΑ, εταιρείες κινητής τηλεφωνίας, συνδρομητική τηλεόραση).
- Απευθείας σύνδεση με τον Τρεχούμενο ή Λογαριασμό Ταμιευτηρίου.
- Ενημέρωση για τις κινήσεις των εξόδων που γίνονται.
- Ο τρόπος πληρωμής είναι αρκετά εύκολος και πρακτικός (απλή εντολή, πάγια εντολή, μεταχρονολογημένη εντολή) ·
- Δεν υπάρχει πληρωμή τόκων ή χρεώσεων.
- Οι συναλλαγές γίνονται χωρίς μετρητά και επιταγές.
- Διακίνηση χρημάτων από την χώρα του κατόχου σε οποιαδήποτε άλλη χώρα.
- Μπορούν να γίνουν αγορές και αναλήψεις μετρητών από ATMs και ταμεία τραπεζών.
- Ασφάλεια Αγορών στην χώρα του κατόχου αλλά και στο εξωτερικό, από κλοπή, απώλεια και τυχαία ζημιά.

Για να είναι εφικτή η συναλλαγή με χρεωστική κάρτα ο χρήστης δεν πρέπει να υπερβεί στις αγορές του, το διαθέσιμο κεφάλαιο του λογαριασμού του, καθώς επίσης ο έμπορος πρέπει να είναι συμβεβλημένος με τον φορέα έκδοσης της χρεωστικής κάρτας.

[25] Turban, E. Lee, J. King, D.& Chung, H. M., 2003 *«Electronic commerce: A managerial perspective»* international edition, Upper Saddle River: Prentice Hall.

2.2.3 Προπληρωμένες κάρτες

Η ονομαστική αξία των προπληρωμένων καρτών ισούται με το ποσό που δαπανά ο χρήστης για να την αγοράσει. Χρησιμοποιούνται κυρίως για την διεκπεραίωση συναλλαγών μικρής αξίας στο διαδίκτυο (και όχι μόνο). Οι λογαριασμοί με τα προπληρωμένα ποσά είναι αποθηκευμένοι σε ένα ειδικό διακομιστή.[26] Τα δύο βασικά χαρακτηριστικά που διαφοροποιούν τις προπληρωμένες κάρτες, είναι ότι δεν διαθέτουν την δυνατότητα πίστωσης (όπως οι πιστωτικές) καθώς επίσης και ότι δεν χρειάζεται να συνδεθούν με κάποιον καταθετικό λογαριασμό (όπως οι χρεωστικές), απλά ο χρήστης μπορεί να τοποθετήσει στην κάρτα το ποσό που επιθυμεί κάθε φορά να χρησιμοποιήσει και μετά από κάθε χρήση της, η κάρτα μπορεί να διατηρείται με μηδενικό ή μικρό ποσό.

Οι προπληρωμένες κάρτες χρησιμοποιούνται κυρίως για αγορές, διαδικτυακές ή και με φυσική παρουσία ή για ανάληψη μετρητών μέσω ATM. Τα χρήματα με τα οποία την έχει φορτίσει ο χρήστης, καθορίζουν και το ύψος των συναλλαγών που μπορεί να κάνει. Επίσης, παρόλο που στα καταστήματα δεν έχει την αποδοχή που έχει μια κλασική πιστωτική (visa ή mastercard) το ποσοστό των καταστημάτων στα οποία γίνονται δεκτές συνεχώς αυξάνεται.

Εικόνα 2.2 Prepaid card Atebank

Πλεονέκτημα προπληρωμένων καρτών

Ένα από τα βασικότερα πλεονεκτήματα που παρέχουν οι προπληρωμένες κάρτες (και στο οποίο οφείλουν το γεγονός ότι είναι δημοφιλής) είναι η αίσθηση ασφάλειας που προσφέρουν. Χωρίς επιπλέον διαθέσιμη πίστωση ή σύνδεση της με καταθετικό λογαριασμό, η προπληρωμένη κάρτα μπορεί να χρησιμοποιηθεί ακόμα

[26] Παπαδόπουλος Δ, εργαστηριακές σημειώσεις στο μάθημα Ηλεκτρονικό Εμπόριο, section 3-ηλεκτρονικές πληρωμές.

και σε αμφιλεγόμενες συναλλαγές αφού το ενδεχόμενο ρίσκο αφορά μόνο το ποσό με το οποίο την έχει φορτίσει ο καταναλωτής. Ακόμα και αν κλαπούν τα στοιχεία της κάρτας, δεν μπορεί να χρησιμοποιηθεί εφόσον δεν υπάρχει διαθέσιμο υπόλοιπο. Παράλληλα, η παροχή υποστήριξης από μεγάλες εταιρίες καρτών, όπως η visa, καθώς και η δυνατότητα για άμεση ακύρωση της κάρτας σε περίπτωση κλοπής, την καθιστούν ασφαλέστερη επιλογή από ένα πορτοφόλι με μετρητά. Ακόμη, φορτίζονται εύκολα, καθώς εκτός από την κλασική επιλογή του γκισέ προσφέρεται η δυνατότητα για φόρτιση της μέσω ΑΤΜ, μέσω τηλεφώνου (phone banking), ακόμα και διαδικτυακά (e-banking). Επιπλέον, η απόκτηση της είναι μια αρκετά εύκολη διαδικασία μιας και τα δικαιολογητικά που απαιτούνται είναι ελάχιστα (σε κάποιες περιπτώσεις αρκεί μόνο η ταυτότητα και το ΑΦΜ), ενώ η διαδικασία έκδοσης της συνήθως δεν διαρκεί περισσότερο από λίγα λεπτά. Ο τρόπος λειτουργίας των προπληρωμένων καρτών μοιάζει ως ένα βαθμό στον τρόπο λειτουργίας των καρτοκινητών. Από τον παραπάνω παραλληλισμό προκύπτει και το πρώτο σημαντικό μειονέκτημα, να μην έχει δηλαδή ο χρήστης διαθέσιμο υπόλοιπο όταν πραγματικά το χρειαστεί. Ένα ακόμα μειονέκτημα είναι ότι η διείσδυση των προπληρωμένων καρτών στις επιχειρήσεις δεν είναι τόσο διαδεδομένη όσο αυτή των πιστωτικών. Έτσι, ενδέχεται οι συναλλαγές να μην γίνουν δεκτές από το σύστημα αποδοχής πληρωμών κάποιων καταστημάτων. Τέλος, οι κάρτες αυτές δεν εξασφαλίζουν την συμμετοχή σε προγράμματα bonus, επιστροφής μετρητών ή άλλων αντίστοιχων παροχών όπως συμβαίνει με τις περισσότερες πιστωτικές κάρτες της αγοράς.

2.2.4 Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι ένα σύστημα ηλεκτρονικών πληρωμών το οποίο χρησιμοποιείται σε χώρες με παράδοση χρήσης επιταγών. Μια επιταγή έχει μία σειρά από νούμερα (αριθμό λογαριασμού κλπ) που καθιστούν την επιταγή μοναδική. Ο αγοραστής εισάγει αυτά τα νούμερα, η τράπεζα ειδοποιείται και ακυρώνει τη συγκεκριμένη επιταγή, αν το επιτρέπει το υπόλοιπο του λογαριασμού του.[27] Ένα βασικό προτέρημα των ηλεκτρονικών επιταγών είναι ότι μπορούν να μεταφέρουν

[27] Πασχόπουλος Α, Σκαλτσάς Π.,2009 «*Ηλεκτρονικό Εμπόριο*», 3η έκδοση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, Αθήνα.

περισσότερα δεδομένα όπως είναι οι συμπληρωματικές οδηγίες πληρωμής, ημερομηνίες επιβεβαίωσης της παραγγελίας και άλλα[28]. Όσον αφορά την ασφάλεια η ηλεκτρονική επιταγή θεωρείται πιο έμπιστη σε σχέση με την παραδοσιακή, διότι ο αποστολέας έχει την δυνατότητα να κωδικοποιήσει τον αριθμό του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, και έτσι δεν αποκαλύπτεται ο αριθμός του λογαριασμού του. Οι ηλεκτρονικές επιταγές χρησιμοποιούν μηχανισμού ασφαλείας, τις οποίες θα αναλύσουμε εκτενέστερα σε επόμενο κεφάλαιο, όπως :

- **Κρυπτογράφηση (Encryption)**
- **Ψηφιακή Υπογραφή (Digital Signature)**
- **Πιστοποιητικά (Certificates)**

2.2.5 Ψηφιακό πορτοφόλι (Digital wallet)

Ένα ψηφιακό πορτοφόλι (επίσης γνωστό ως ηλεκτρονικό πορτοφόλι) επιτρέπει στον χρήστη να κάνει τις συναλλαγές ηλεκτρονικού εμπορίου γρήγορα και με ασφάλεια. Ένα ψηφιακό πορτοφόλι λειτουργεί σαν ένα φυσικό πορτοφόλι. Το ψηφιακό πορτοφόλι χρησιμοποιήθηκε αρχικά ως μια μέθοδος για την αποθήκευση διάφορων μορφών ηλεκτρονικών χρημάτων (e-cash), αλλά με λίγη δημοτικότητα έχει εξελιχθεί σε μια υπηρεσία που παρέχει στους χρήστες του Internet έναν κατάλληλο τρόπο να αποθηκεύουν και να χρησιμοποιούν πληροφορίες σε online αγορές. Οι καταναλωτές δεν χρειάζεται να συμπληρώσουν τα έντυπα διάταξης σε κάθε περιοχή όταν αγοράζουν ένα στοιχείο επειδή οι του πληροφορίες έχουν αποθηκευτεί ήδη και ενημερώνονται αυτόματα και εισάγονται στους τομείς διαταγής στις εμπορικές περιοχές κατά την χρησιμοποίηση ενός ψηφιακού πορτοφολιού. Οι καταναλωτές ωφελούνται επίσης κατά τη χρησιμοποίηση των ψηφιακών πορτοφολιών επειδή οι πληροφορίες τους κρυπτογραφούνται - ή προστατεύονται από τον ιδιωτικό κώδικα λογισμικού. Δηλαδή, με λίγα λόγια είναι ένας τρόπος χρήσης της πιστωτικής κάρτας όπου ο κάτοχος δίνει τον αριθμό της κάρτας του, όπου είναι κρυπτογραφημένος στην εταιρεία που διαθέτει το ψηφιακό πορτοφόλι και έτσι αυτή η μέθοδος δίνει μία

[28] Πομπόρτσης Ανδρέας Σ., Τσουλφάς, Ανέστης Γ., 2002« *Εισαγωγή στο ηλεκτρονικό εμπόριο*» Εκδόσεις ΤΖΙΟΛΑ, Θεσσαλονίκη.

ασφαλή και γρήγορη λύση. Τέλος, με το ψηφιακό πορτοφόλι ο χρήστης μπορεί να ενημερωθεί για προσφορές που τον ενδιαφέρουν όπως και να αποθηκεύσει τις προτιμήσεις του σε κάποια προϊόντα που τον απασχολούν. [29]

2.2.6 Έξυπνες κάρτες (Smart Cards)

Γενικά

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 έχουν την δυνατότητα να αποθηκεύουν μεγάλη ποσότητα δεδομένων, καθώς επίσης παρέχουν και 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 αξιολόγηση τους εκδόθηκαν νέες ολοκληρωμένες προδιαγραφές. Η τεχνολογία των έξυπνων καρτών προσφέρει απεριόριστες δυνατότητες χρήσης στο εμπόριο, την βιομηχανία και στην δημόσια διοίκηση. Οι έξυπνες κάρτες αποθήκευσης δεδομένων ήταν η αφορμή για την δημιουργία του ηλεκτρονικού χρήματος. Πλέον, η νέα γενιά έξυπνων καρτών διαθέτει προγραμματισμένες λειτουργίες με μικροτσίπ προσωπικής ταυτότητας.

Διαφορά μεταξύ έξυπνης κάρτας και πιστωτικής κάρτας:

Η έξυπνη κάρτα μοιάζει εξωτερικά με την πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό,

[29] http://en.wikipedia.org/wiki/Digital_wallet

προσαρμοσμένο στη μια πλευρά της. Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια. Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας, στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα.[30]

Είδη έξυπνων καρτών

Στις μέρες μας οι έξυπνες κάρτες μπορούν να κατηγοριοποιηθούν με δύο βασικά κριτήρια:

α) επεξεργαστική ικανότητα και

β) δυνατότητες εισόδου-εξόδου

Με βάση το <u>πρώτο κριτήριο</u> διακρίνουμε 3 κατηγορίες έξυπνων καρτών:

❖ <u>Κάρτες μνήμης – Κάρτες αποθήκευσης πληροφοριών (memory cards).</u> Οι κάρτες αυτές περιέχουν κάποια μνήμη και λογική σε υλικό (hardware logic), η οποία μπορεί να θέσει ή να διαγράψει τιμές στην μνήμη. Οι κάρτες μνήμης αναφέρονται καταχρηστικά ως έξυπνες κάρτες, καθώς δεν έχουν την δυνατότητα επεξεργασία των δεδομένων.

[30] http://el.wikipedia.org

❖ Έξυπνες κάρτες (smart cards. IC cards, microprocessor cards). Είναι οι "κλασσικές" έξυπνες κάρτες ή κάρτες με μικροεπεξεργαστή. Ο επεξεργαστής τους πέρα από την αποθήκευση και ασφάλιση πληροφοριών, μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν.

❖ Έξυπνες κάρτες πολλαπλών εφαρμογών (multi application smart cards). Οι έξυπνες κάρτες τελευταίας γενιάς έρχονται με ανοικτά λειτουργικά συστήματα (java, MULTOS) και μπορούν να εκτελούν περισσότερες από μία εφαρμογές. Παρέχεται επίσης η δυνατότητα στο χρήστη να "φορτώνει" νέες εφαρμογές, ή να διαγράφει άλλες ανάλογα με τις ανάγκες του.

Μια δεύτερη κατηγοριοποίηση αφορά τον τρόπο επικοινωνίας των έξυπνων καρτών με το εξωτερικό περιβάλλον. Με βάση αυτό το κριτήριο, διακρίνουμε τις εξής κατηγορίες:

❖ Έξυπνες κάρτες με επαφές (Contact Cards). Οι κάρτες αυτές επικοινωνούν με ηλεκτρονικές επαφές και πρέπει να εισαχθούν σε μία συσκευή ανάγνωσης προκειμένου να διαβαστούν ή να εισαχθούν πληροφορίες, ως παράδειγμα μπορούμε να αναφέρουμε την χρήση του σε ειδικές τερματικές διατάξεις για την εξόφληση των τηλεφωνικών λογαριασμών.

❖ Ασύρματες έξυπνες κάρτες (Contactless Cards). Οι κάρτες αυτές έχουν ενσωματωμένη εσωτερικά μία μικροσκοπική κεραία και μπορούν να επικοινωνούν με μία κεραία λήψης χωρίς τη φυσική τους επαφή με κάποια συσκευή ανάγνωσης προκειμένου οι πληροφορίες να ανανεωθούν, να αλλάξουν ή να υποβληθούν σε επεξεργασία, ως παράδειγμα αναφέρουμε ότι μπορεί να χρησιμοποιηθεί όταν ένας οδηγός διέρχεται τα διόδια, με αυτόν τον τρόπο θα

μπορεί να αποφευχθεί η στάση και η τυχόν καθυστέρηση του οδηγού εκεί, διότι η χρέωση γίνεται αυτόματα.

- Υβριδικές κάρτες ή συνδυασμένες κάρτες (Hybrid or Combination cards). Οι κάρτες αυτές ενσωματώνουν και τους δυο τρόπους μετάδοσης και συνεπώς μπορούν να επικοινωνήσουν κατά περίπτωση είτε με ενσύρματο τρόπο είτε με ασύρματο τρόπο.[31]

Οι έξυπνες κάρτες διαθέτουν δύο τύπους συστήματος ηλεκτρονικών πληρωμών:

- Τα *ανοικτά συστήματα* όπου η άμεση μεταφορά χρηματικού ποσού μεταξύ καρτών είναι εφικτή.
- Τα *κλειστά συστήματα* όπου το ποσό της κάρτας μπορεί να αυξηθεί από ένα τραπεζικό λογαριασμό ο οποίος θα είναι μοναδικός και το χρήμα που έχει κινηθεί θα μεταφερθεί στον τραπεζικό λογαριασμό του αποδέκτη.

Γενικά οι έξυπνες κάρτες είναι χρήσιμες γιατί :

- Τα δεδομένα τα οποία διαθέτει είναι κρυπτογραφημένα έτσι ώστε, να μην κινδυνεύει από υποκλοπές και τροποποιήσεις. Επίσης, η δυνατότητα παραγωγής ψηφιακών πιστοποιητικών καθιστά η κάθε κάρτα να είναι μοναδική. Έτσι αν υπάρχει παραποίηση, ανιχνεύεται αυτόματα όπως επίσης και η μη εξουσιοδοτημένη χρήση είναι αδύνατον να πραγματοποιηθεί, γιατί η χρήση των έξυπνων καρτών είναι αυστηρά προσωπική και για να γίνει χρέωση ενός ποσού στην κάρτα, είναι προσβάσιμη μόνο στον νόμιμο κάτοχο της.
- Το λογισμικό τους διαθέτει πολύ ασφαλή και αξιόπιστα μέτρα προστασίας και αυτό συμβαίνει για την αποτροπή εξωτερικών εισβολών.

- Έχουν πολύ μικρό κόστος κατασκευής διότι το υλικό που είναι φτιαγμένα, είναι πραγματικά πολύ φθηνό σε αντίθεση με την μεγάλη ανάπτυξη που γνωρίζει η βιομηχανία τεχνολογικών προϊόντων.

[31] http://www.ebusinessforum.gr Ομάδα εργασίας Γ3: Έξυπνες Κάρτες

Τα μειονεκτήματα που θα μπορούσαν να έχουν οι έξυπνες κάρτες είναι :

- Η πιθανότητα να κλαπούν ή να χαθούν.
- Να καταρριφθεί η ασφάλεια της από την εξέλιξη και της αρνητικής τεχνολογίας, ώστε να είναι μετά θέμα χρόνου να μπορέσουν να «σπάσουν» τους κωδικούς της.
- Λόγω των νέων συνθηκών ζωής που όλα πλέον έχουν ηλεκτρονική μορφή ένα πρόβλημα να υπάρξει σε αυτόν τον μηχανισμό μπορεί να αποφέρει την κατάρρευση όλου του συστήματος
- Την ανεξέλεγκτη χρήση του χρήματος από τον άνθρωπο όπου επειδή έχει χάσει την επαφή του με το πραγματικό χρήμα δεν αντιλαμβάνεται πόσα λεφτά ξοδεύει.[32]

2.2.7 ΨΗΦΙΑΚΟ ΧΡΗΜΑ

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλησης μικροποσών μέσω του Διαδικτύου. Ένας τέτοιος μηχανισμός μπορεί να αποτελέσει το επόμενο βήμα στις εφαρμογές ηλεκτρονικών πληρωμών. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία. Ένας χρήστης μπορεί να κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό αυτό στον ηλεκτρονικό υπολογιστή του. Το ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύεται για λόγους ασφαλείας και εγκυρότητας. Σε περίπτωση αγοράς από το internet ο αγοραστής αποστέλλει στον προμηθευτή το αντίτιμο σε ψηφιακό χρήμα. Ο τελευταίος με τη σειρά του, προωθεί στη τράπεζα την ψηφιακή ροή που έλαβε προκειμένου να διερευνηθεί κατά πόσο η ροή αποτελεί έγκυρη χρηματοροή ή όχι. Για να διασφαλίσει ότι η κάθε χρηματοροή (token) χρησιμοποιείται μόνο μια φορά, η τράπεζα καταγράφει τον σειριακό αριθμό κάθε που ξοδεύεται. Μια εναλλακτική λύση που αναπτύχθηκε επιτρέπει στον χρήστη να κρατήσει την ανωνυμία του. Ο εν λόγω μηχανισμός ονομάζεται τυφλή υπογραφή (blind signature). Η τυφλή υπογραφή επιτρέπει στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τις χρηματοροές που του διανέμονται. Η τράπεζα πρέπει να εκτιμήσει το token που λαμβάνει από έναν έμπορο, μέσω της ψηφιακής στάμπας που έχει αρχικά

[32] Κομνηνός θ. - Σπυράκης Π., 2002 «*Ασφάλεια δικτύων υπολογιστικών συστημάτων, αναχαιτίστε τους εισβολείς*», Εκδόσεις Ελληνικά Γράμματα, Αθήνα.

τοποθετήσει στα token του χρήστη αλλά τέλος η τράπεζα δεν μπορεί να καταλάβει ποιος έκανε την πληρωμή.[33]

2.3 E-BANKING

Το e-banking (ή internet banking) είναι το ηλεκτρονικό κατάστημα της Τράπεζας. Το e-banking παρέχει στους πελάτες τη δυνατότητα να πραγματοποιούν μέσω του Διαδικτύου, με χρήση υπολογιστή και από τον χώρο στον οποίο δραστηριοποιούνται, μια σειρά από τραπεζικές/χρηματιστηριακές συναλλαγές όλες τις ημέρες του έτους και χωρίς να περιορίζονται από το ωράριο λειτουργίας των Τραπεζών. Το e-banking διευρύνει τα δίκτυα διανομής προϊόντων και υπηρεσιών που παρέχει η Τράπεζα καθώς επίσης παρέχει μια πιο ποιοτικά αναβαθμισμένη εξυπηρέτηση.[34] Για τις εταιρείες, το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

Η επιβεβαίωση της ταυτότητας του αποπληρώνοντας αγοραστή γίνεται με την χρήση κωδικών μίας χρήσης τα οποία παράγονται από ένα μικρό, σαν μπρελόκ μηχάνημα. Σε κάποιο στάδιο της συναλλαγής η Τράπεζα ζητά τον κωδικό που παράγει εκείνη την στιγμή το μηχάνημα. Αν είναι ορθός θεωρείται έγκυρη και ολοκληρώνεται η συναλλαγή[35]. Σε ήδη διαμορφωμένες τεχνολογικά αγορές η ανάπτυξη διαδικασιών μέσω του internet έχει ρόλο προοδευτικής και όχι ριζοσπαστικής καινοτομίας. Η ταχύτητα που αναπτύσσεται ένα νέο σύστημα όπως αυτό εξαρτάται από την διάθεση των πελατών και τη δυσκολία στην διεκπεραίωση τραπεζικών συναλλαγών μέσω των άλλων δικτύων διανομής χρηματοοικονομικών

[33] Γ. Πολλάλης - Δ. Γιαννακόπουλος,2007 «*Ηλεκτρονικό επιχειρείν*», Εκδόσεις Σταμούλη, Αθήνα.
[34] http://www.nbg.gr/
[35] Πασχόπουλος Α, Σκαλτσάς Π., 2009 «*Ηλεκτρονικό Εμπόριο*», 3η έκδοση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, Αθήνα.

υπηρεσιών. Συνεπώς, όπως συμβαίνει με την εφαρμογή κάθε νέου συστήματος, μόνο οι τολμηροί το χρησιμοποιούν στην αρχή.

2.3.1 Δυνατότητες του e-banking

- Ενημέρωση του πελάτη για το υπόλοιπο των λογαριασμών του
- Ενημέρωση του πελάτη σχετικά με την κίνηση (ημερήσια/μηνιαίας) ανάλυση των λογαριασμών που έχει συνδέσει με το σύστημα
- Μεταφορά ποσών μεταξύ λογαριασμών του πελάτη
- Έμβασμα σε λογαριασμούς τρίτων
- Ενημέρωση του πελάτη σχετικά με το χαρτοφυλάκιο των μετοχών του (όπως κωδικός μετοχής- περιγραφή, διαθέσιμα τεμάχια, τιμή κλεισίματος προηγούμενης ημέρας, αποτίμηση με τιμή προηγούμενης μέρας, συνολική αποτίμηση χ/κίου)
- Ενημέρωση του πελάτη σχετικά με το χαρτοφυλάκιο του Αμοιβαίων Κεφαλιών
- Παραγγελία μπλοκ επιταγών.
- Παρακολούθηση επιταγών.
- Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών.
- Εντολές αγοραπωλησίας μετοχών.
- Πληρωμή μισθοδοσίας.
- Πληρωμή εταιρικών πιστωτικών καρτών.
- Επιλογές ασφαλιστικών πακέτων.
- Λοιπά πληροφοριακά στοιχεία.[36]

Μορφές e-Banking

- Mobile-banking
- TV-banking
- Online-banking
- Home-banking

[36] http://www.nbg.gr/
http://www.atebank.gr

2.3.2 Η Διάδοση του E-Banking στην Ελλάδα

Στις τραπεζικές συναλλαγές μέσω Internet στρέφονται πλέον ολοένα και περισσότεροι Έλληνες, σε σχέση όμως με τις υπόλοιπες Ευρωπαϊκές χώρες το επίπεδο διείσδυσης στο e-banking παραμένει πιο χαμηλό. Το γεγονός αυτό οφείλεται στην δυσπιστία του Ελληνικού λαού ως προς τις ηλεκτρονικές συναλλαγές, αφού ακόμη και σήμερα δεν έχουν εξοικειωθεί πλήρως με τις νέες τεχνολογίες. Πλέον στην Ελλάδα οι περισσότερες Τράπεζες δραστηριοποιούνται ενεργά στο χώρο της ηλεκτρονικής τραπεζικής. Το e-banking στη Ελλάδα αναπτύχθηκε αργά αλλά σταθερά καθώς τα στελέχη της πληροφορικής κλήθηκαν να εκπονήσουν νέα προγράμματα για το σύστημα, χωρίς να διαθέτουν καμία εμπειρία. Μεγάλο ρόλο στην εναρμόνιση της λειτουργίας των Ελληνικών τραπεζών με τα Ευρωπαϊκά πρότυπα διαδραμάτισε η ένταξη της στην Οικονομική και Νομισματική Ένωση. Ένας ακόμη ανασταλτικός παράγοντας στη διάδοση του e-banking στην Ελλάδα είναι το θέμα της ασφάλειας, διότι τα πιστωτικά ιδρύματα έχουν μεταβιβάσει στον χρήστη την ευθύνη αναγνώρισης του αυθεντικού web site τους. Παρότι αυτά φροντίζουν να δίνουν λεπτομερή στοιχεία για τη διευκόλυνση του έλεγχου από πελάτες, εν τούτοις αυτό δεν αποκλείει ένα web site ψεύτικης διεύθυνσης υποτιθέμενης τράπεζας να τα αντιγράψει ή να δημιουργήσει κάποιες δικές της αντίστοιχες ενδείξεις και να παραπλανήσει του χρήστες. Οι χρηματοοικονομικοί οργανισμοί διαβεβαιώνουν ότι εφαρμόζουν απαραβίαστα τεχνολογικά συστήματα. Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SSL(secure socketLayer) καθώς επίσης και το SET (Secure Electronic Transaction).

ΚΕΦΑΛΑΙΟ 3^0

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ-ΚΙΝΔΥΝΟΙ ΠΟΥ ΥΠΑΡΧΟΥΝ

3.1 ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Μια κύρια αδυναμία σε πολλά προγράμματα ασφαλείας είναι η αποτυχία του υπεύθυνου πληροφορικής να συνδυάσει τις τρέχουσες με τις προσβαλλόμενες ανάγκες. Για τον λόγο αυτό οι όποιες ενέργειες σε θέματα ασφαλείας πρέπει να είναι τεκμηριωμένες και άριστα υλοποιημένες τεχνικά. Η ασφάλεια συνδέεται έμμεσα με την αξιοπιστία του πληροφοριακού συστήματος και έχει δυο βασικούς στόχους:

- Μυστικότητα: περιλαμβάνει την διατήρηση της εμπιστευτικότητας της πληροφορίας με την προστασία της από την ακούσια ή μη εξουσιοδοτημένη αποκάλυψη, όπως και από επιθέσεις ατόμων με κίνητρα που κυμαίνονται από μια απλή επιθυμία απόκτησης πρόσβασης έως την ανορθόδοξη επίτευξη πολιτικών και οικονομικών στόχων.

- Ακρίβεια: περιλαμβάνει τη διατήρηση της ακεραιότητας της πληροφορίας, δηλαδή τη βεβαιότητα ότι είναι ολοκληρωμένη και αλάνθαστη, καθώς και την κατοχύρωση της αυθεντικότητας των τελικών χρηστών.

Απαιτήσεις ασφάλειας για το ηλεκτρονικό χρήμα:

- Ακεραιότητα (Integrity). Είναι η διαδικασία εκείνη που εξασφαλίζει ότι τα δεδομένα που έχουν σταλεί από τον τελικό χρήστη θα φτάσουν στον παραλήπτη ατροποποίητα.

- Αυθεντικότητα (Authentication). Ονομάζεται η διαδικασία εκείνη κατά την οποία πιστοποιείται ότι οι χρήστες που επικοινωνούν είναι όντως αυτοί που ισχυρίζονται ότι είναι, επαληθεύει δηλαδή τις ταυτότητες τους και, εν συνεχεία, τη μοναδικότητα τους στον κυβερνοχώρο.

- Εξουσιοδότηση (Authorization). Θεωρείται η διαδικασία επικύρωσης ή άρνησης μιας εντολής που σχετίζεται με την δημιουργία, προσπέλαση, ενημέρωση ή διαγραφή πληροφοριών.

- Μη απαρνησιμότητα (Non-repudiation). Είναι η διαδικασία εκείνη που απαγορεύει σε ένα οποιαδήποτε άτομο να απαρνηθεί τη συμμετοχή του στη δοσμένη συναλλαγή. [37]

3.1.1 ΛΟΓΟΙ ΑΝΑΣΦΑΛΕΙΑΣ

Το Διαδίκτυο όπως έχουμε αναφέρει αποτελεί το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων, που αλληλεπιδρούν μεταξύ τους και χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε όλη την Γη. Είναι λοιπόν αντιληπτό ότι είναι πολύ δύσκολο να αντιμετωπιστεί ολικά από άποψη ασφάλειας, εξαιτίας της ετερογένειας που το χαρακτηρίζει. Η ασφάλεια επιτυγχάνεται ως πρόσθετο χαρακτηριστικό του δικτυακού σχεδίου και όχι ως κομμάτι του, επειδή οι μηχανισμοί που στηρίζουν την λειτουργικότητα του σχεδιάστηκαν έχοντας ως στόχο την βελτίωση των διάφορων δυνατοτήτων και όχι για να παρέχουν ασφάλεια.

Οι λόγοι που κάνουν το Διαδίκτυο ανασφαλές είναι:

- Τα στάνταρ που χρησιμοποιούνται για τα βασικά πρωτόκολλά του διαδικτύου είναι δημόσια. Αυτό σημαίνει ότι κακόβουλοι χρήστες έχουν πολλές πληροφορίες για τον τρόπο λειτουργίας του διαδικτύου. Επίσης, η ανοιχτή φύση του διαδικτύου υπονομεύει την ασφάλεια, αφού όλες οι επιθέσεις και οι αδυναμίες γίνονται αμέσως γνωστές και τα προγράμματα που τα αντιμετωπίζουν εκδίδονται αμέσως.
- Το διαδίκτυο είναι διαδεδομένο. Βρίσκεται σε σπίτια, σε καφετέριες, σε βιβλιοθήκες και σε γραφεία. Δεν απαιτείται πολύπλοκο υλικό για κάποια μη

[37] Παυλίδης Γ, 2003 «*Ολοκληρωμένη Τεχνολογία Πληροφορικής*», εκδόσεις Gutenberg, Αθήνα.

εξουσιοδοτημένη πρόσβαση: ένας προσωπικός υπολογιστής και ένας φυλλομετρητής διαδικτύου θα σας επιτρέψουν την γρήγορη πρόσβαση στην ιστοσελίδα ενός οικονομικού οργανισμού.

- Οι διακομιστές διαδικτύου είναι επεκτάσιμοι: μπορούν να συνδεθούν σε πολλές τεχνολογίες, για παράδειγμα συστήματα διαχείρισης δεδομένων. Το λογισμικό που διαχειρίζεται αυτές τις επεκτάσεις είναι αρκετά πολύπλοκο και μπορεί να μετατρέψει ένα διακομιστή διαδικτύου σε κάτι που δεν είχε σκοπό να γίνει. Ένα τέτοιο λογισμικό είναι ευπαθές σε επιθέσεις.
- Το διαδίκτυο περιέχει πολλά αλληλοσυνδεδεμένα στοιχεία που απαιτούν το ένα το άλλο για να εκτελέσουν βασικές λειτουργίες.
- Η ταχύτητα ανάπτυξης του διαδικτύου απαιτούσε και τη συνεχή βελτίωση, ώστε να ανταποκριθούν στις αυξανόμενες απαιτήσεις λειτουργικότητας. Αυτό γινόταν δυνατόν μέσω ανασφαλών προσθετικών προγραμμάτων (**plug-ins)**, που είχαν σοβαρά προβλήματα ασφαλείας.[38]

3.2 Κίνδυνοι διαδικτυακής δραστηριότητας

Προκειμένου να εστιάσουμε στους κινδύνους που απειλούν την διαδικτυακή δραστηριότητα, καλό είναι να ορίσουμε τι είναι κίνδυνος. Κίνδυνος λοιπόν είναι κάθε απειλή που σκοπό έχει να βλάψει την ακεραιότητα των ηλεκτρονικών συναλλαγών και να εκμεταλλευτεί οποιαδήποτε πληροφορία που μπορεί να αποκομίσει παραβιάζοντας την ιδιωτικότητά τους. [39]

3.2.1 MALWARE

Ο όρος προέρχεται από τον συνδυασμό των συνθετικών των λέξεων MALicious (βλαβερό) και softWARE (λογισμικό). Πρόκειται δηλ, για λογισμικό που μπορεί να απειλήσει την ασφάλεια του χρήστη και του ηλεκτρονικού υπολογιστή.

[38] http://users.uom.gr/~kaklaman/book/Chapters/C11/

[39] *Κάτσικας Σ., Γκριτζάλης Δ., Γκριτζάλης Σ.,2004 <<Ασφάλεια πληροφοριακών συστημάτων>>, εκδόσεις Νέων Τεχνολογιών, Αθήνα.*

Malware χαρακτηρίζονται μεταξύ των άλλων και τα παρακάτω αυτόνομα κακόβουλα προγράμματα όπως οι ιοί (virus), trojan horses (δούρειοι ίπποι) και τα σκουλήκια (worms).

3.2.1.1 Virus (ιός)

Ο ιός είναι ένα είδος κακόβουλα γραμμένου κώδικα που θέτει σε κίνδυνο την ασφαλή λειτουργία του συστήματος και μπορούν να χρησιμοποιηθούν για μια ποικιλία διαφορετικών επιθέσεων. Περιγράφονται ξεχωριστά εδώ καθώς απαιτούν αρκετά υψηλό επίπεδο τεχνικών γνώσεων. Οι συνηθισμένες επιθέσεις άρνησης υπηρεσιών είναι απλές και όχι ιδιαίτερα εξεζητημένες ενώ η επίθεση με ιό απαιτεί μεγαλύτερο βαθμό τεχνικών γνώσεων.

Ένας **ιός** είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή - μια διαδικασία που είναι γνωστή ως **μόλυνση .** Αφού ένας ιός εγκατασταθεί σε έναν υπολογιστή, μπορεί να αντιγράψει τον εαυτό του και σε άλλα αρχεία στον υπολογιστή.[40]

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

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

[40] http://users.uom.gr/~kaklaman/book/Chapters/C11/

Εικόνα 3.1

Είδη ιών:

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:

- Τομείς σκληρού δίσκου συστήματος (system sectors)
- Αρχεία
- Ιοί μακροεντολών (Macros)
- Ιοί πηγαίου κώδικα (Source Code Viruses)
- Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters

Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:

- Πολυμορφικοί ιοί
- Αόρατοι ιοί (Stealth Viruses)
- Θωρακισμένοι ιοί (Armored Viruses)
- Πολυτμηματικοί ιοί (Multipartite Viruses)
- Ιοί πλήρωσης κενών (Space filler Viruses)
- Ιοί παραλλαγής (Camouflage Viruses) [41]

Τρόποι μετάδοσης ιών:

- Εκκίνηση του Η/Υ από μολυσμένη δισκέτα ή μολυσμένο
- Από άνοιγμα/ ανάγνωση μολυσμένου φορητού αποθηκευτικού χώρου

[41] http://el.wikipedia.org/wiki/

- Άνοιγμα/εκτέλεση μολυσμένου φακέλου και ή αρχείου
- Άνοιγμα/ανάγνωση μολυσμένου e-mail
- Κατέβασμα και εγκατάσταση αμφίβολου προελεύσεως προγραμμάτων
- Περιήγηση στο internet
- Από κακόβουλη επίθεση στον υπολογιστή

Οι ιοί στην πρωταρχική τους μορφή μεταδίδονταν μόνο μέσω δισκετών, έτσι η εξάπλωση γίνονταν με αργούς ρυθμούς και οι ιοί που κυκλοφορούσαν μόλυναν κυρίως δισκέτες. Με την εξάπλωση του internet όμως οι ιοί ήταν πιο εύκολο να μεταφερθούν καθώς προσαρμόστηκε η δομή τους και τα λειτουργικά συστήματα και κυρίως τα windows έχουν "τρύπες" ασφαλείας τις οποίες εκμεταλλεύονται οι ιοί για να μολύνουν τον υπολογιστή.

3.2.1.2 TROJAN HORSES (ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ)

Ένας δούρειος ίππος είναι ένα κακόβουλο κομμάτι κώδικα το οποίο υπάρχει μέσα σε ένα κατά τα άλλα αθώο πρόγραμμα και το οποίο επιχειρεί να κάνει κάτι το οποίο ο χρήστης δεν περιμένει να κάνει. Για παράδειγμα, ένα ελεύθερης πρόσβασης πρόγραμμα το οποίο παρέχει σε ένα διαχειριστή συστημάτων πληροφορίες σχετικά με τη χρήση των αρχείων σε ένα δικτυακό σύστημα, αλλά το οποίο μετά από κάποια στιγμή υποκλέπτει πληροφορίες ή αλλάζει αρχεία είναι ένας δούρειος ίππος. Οι δούρειοι ίπποι μπορούν να χρησιμοποιηθούν για διάφορους λόγους όπως την υποκλοπή passwords και άλλων πληροφοριών ή για να καταστρέψουν πόρους (π.χ. αρχεία) και να προκαλέσουν κατάρρευση ενός συστήματος. Το κύριο πρόβλημα με τους δούρειους ίππους είναι ότι είναι πολύ δύσκολο να εντοπιστούν. Οι λόγοι είναι δυο: ο πρώτος είναι ότι συχνά παίρνουν τη μορφή ιδιαίτερα συνηθισμένων εργαλείων ή εργαλείων που απαιτούν την χειροκίνητη εγκατάσταση τους από το χρήστη. Για παράδειγμα, το 1997 ένας δούρειος ίππος κυκλοφόρησε με τη μορφή του δημοφιλούς προγράμματος συμπίεσης αρχείων *Stuffit* που χρησιμοποιείται στους υπολογιστές Macintosh. Αυτός ο συγκεκριμένος δούρειος ίππος έσβηνε σημαντικά αρχεία μετά την εγκατάσταση του

σε έναν υπολογιστή. Ο δεύτερος λόγος για τον οποίο είναι δύσκολο να εντοπιστούν είναι ότι υπάρχουν σε κάποιο υπολογιστή με τη μορφή ενός μεταφρασμένου προγράμματος το οποίο είναι δύσκολο να ελεγχθεί τι ακριβώς κάνει.[42]

3.2.1.3 WORMS (ΣΚΟΥΛΗΚΙΑ)

Είναι λογισμικό το οποίο αναπαράγεται μόνο του μολύνοντας τους ηλεκτρονικούς υπολογιστές σε ένα τοπικό δίκτυο ή στο διαδίκτυο. Το επιτυγχάνει αυτό βασιζόμενο σε κάποιο κενό ασφάλειας και στέλνοντας αντίγραφα του εαυτού του σε άλλους υπολογιστές χωρίς να αποκτήσει την αναγκαία εξουσιοδότηση από τον χρήστη. Πέραν της αναπαραγωγικής του ιδιότητας μερικές φορές οι κακόβουλοι προγραμματιστές τους που τα σχεδιάζουν τους προσθέτουν και καταστροφικές λειτουργικές όπως είναι η καταστροφή αρχείων, η υποκλοπή κ.τ.λ.

3.2.2 SPAM

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιο μας χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως **απρόκλητη** ή **ανεπιθύμητη αλληλογραφία,** δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

Τα κυριότερα χαρακτηριστικά του Spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

[42] http://users.uom.gr/~kaklaman/book/Chapters/C11/

- **Απρόκλητο:** Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.
- **Εμπορικό :** Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.
- **Μαζικό:** Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών.[43]

3.2.3 PHISHING

Μια επίθεση ηλεκτρονικού "ψαρέματος" (phishing) πραγματοποιείται όταν κάποιος υποδύεται κάποιον άλλο ώστε να ξεγελάσει τον χρήστη και να τον κάνει να μοιραστεί μαζί του προσωπικές ή άλλες ευαίσθητες πληροφορίες, συνήθως μέσω ενός πλαστού ιστότοπου. Το κακόβουλο πρόγραμμα είναι ένα λογισμικό που εγκαθίστανται στον υπολογιστή, εν αγνοία του χρήστη, και είναι σχεδιασμένο να βλάψει τον υπολογιστή ή να κλέψει πληροφορίες από τον υπολογιστή.[44] Αυτή η μέθοδος εφαρμόζεται αρκετά τα τελευταία χρόνια με τη χρήση συνδυασμού spam mail και «πλαστών» ιστοσελίδων, που μιμούνται όσο πειστικότερα μπορούν, τα αντίστοιχα των νόμιμων επιχειρήσεων/χρηματοπιστωτικών οργανισμών. Συνήθως ο επίδοξος εισβολέας στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου όπου εμφανίζεται ως κάποια νόμιμη εταιρεία (τράπεζα, μεταφορική κλπ) και ζητάει από το υποψήφιο θύμα να στείλει προσωπικά ή άλλα στοιχεία (όπως αριθμό πιστωτικής κάρτας).

[43] http://www.sch.gr/sch-portlets/static/manual/aboutSpam/
[44] http://support.google.com/chrome/

3.2.4 DIALERS

Είναι ένα πρόγραμμα το οποίο χωρίς να το γνωρίζει ο χρήστης, χρησιμοποιεί την τηλεφωνική του γραμμή κυρίως για αριθμούς αυξημένου κόστους Αυτό συμβαίνει συνήθως, όταν ο χρήστης επισκεφθεί μια ιστοσελίδα με ύποπτο ή πορνογραφικό περιεχόμενο, ή αναξιόπιστες ιστοσελίδες. Οι dialers μπορούν να δράσουν μόνο στις συνδέσεις μέσω modem. Ένας dialer, μπορεί επίσης να εισέλθει στον υπολογιστή μέσω spam.

3.2.5 SPYWARE (ΛΟΓΙΣΜΙΚΑ ΚΑΤΑΣΚΟΠΕΙΑΣ)

Όπως δηλώνει και η ονομασία τους, τα λογισμικά κατασκοπείας κατασκοπεύουν το μολυσμένο υπολογιστή. Το πρόγραμμα καταγράφει στοιχεία σχετικά με το χρήστη (ιστοσελίδες που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πρόσβασης πιστωτικών καρτών) και στέλνει τις πληροφορίες που συγκεντρώνει στον κατασκευαστή του λογισμικού κατασκοπείας ή σε τρίτα πρόσωπα εν αγνοία του χρήστη. Τα λογισμικά κατασκοπείας απαιτούν μεγάλη υπολογιστική ισχύ. Οι χρήστες μπορούν να υποψιαστούν την παρουσία τους λόγω της μείωσης στην ταχύτητα του υπολογιστή. Εκτός αυτού, τα λογισμικά κατασκοπείας μπορούν να προκαλέσουν πρόσθετα κενά ασφαλείας, εμποδίζοντας τις ενημερώσεις λογισμικού[45]. Ακόμη, τα λογισμικά κατασκοπείας αλλάζουν την αρχική σελίδα του browser, τροποποιούν την λίστα με τα αγαπημένα (σελιδοδείκτες) του browser και εμφανίζουν και νέες γραμμές εργαλείων στο browser, οι επιθέσεις αυτές είναι γνωστές ως πειρατεία φυλλομετρητή (browser hijacking).

3.2.6 KEY LOGGER

Το key logger είναι πρόγραμμα τύπου spyware. Είναι ο πιο συχνός τρόπος υποκλοπής προσωπικών στοιχείων κατά την περιήγηση μας στο Διαδίκτυο. Ο επιτιθέμενος εγκαθιστά στο σύστημα ένα εργαλείο το οποίο έχει την δυνατότητα να καταγράφει σε ένα αρχείο οτιδήποτε ο χρήστης πληκτρολογεί, τα εργαλεία αυτά ονομάζονται keylogger**.** Μέσω ενός keylogger ο επιτιθέμενος μπορεί να υποκλέψει διάφορες πληροφορίες που πληκτρολογεί ο χρήστης, όπως διάφορα passwords που

[45] http://www.mediamarkt.gr

έχει για διαφορετικές εφαρμογές ή και αριθμούς πιστωτικών καρτών όταν ο χρήστης κάνει συναλλαγές μέσω του Internet. Συνήθως ενσωματώνονται σε trojan ή υπάρχουν σε ιστοσελίδες σε μορφή javascript. Το keylogger, είναι εξαιρετικά επικίνδυνο, διότι μπορεί να οδηγήσει στην κλοπή ταυτότητας ή την κλοπή γενικά. Το keylogger, είναι ιδιαίτερα επικίνδυνο σε καθέναν που χρησιμοποιεί το διαδίκτυο για τραπεζικές και άλλες οικονομικές συναλλαγές .

3.2.7 ADWARE (ΛΟΓΙΣΜΙΚΟ ΥΠΟΚΛΟΠΗΣ)

Είναι μια μορφή spyware που συλλέγει προσωπικά δεδομένα ή πραγματοποιεί αλλαγές στο σύστημα χωρίς στην συγκατάθεση του χρήστη. Το adware συλλέγει πληροφορίες για το προφίλ του χρήστη και με βάση αυτές τις πληροφορίες σχετικά με τις συνήθειες του στο σερφάρισμα προβάλλει αργότερα διαφημίσεις στο φυλλομετρητή του (web browser). Η εγκατάσταση στον υπολογιστή γίνεται χωρίς να γίνει αντιληπτή από τον χρήστη και ο εντοπισμός τους να είναι αρκετά δύσκολος.

3.2.8 SPOOFING

Αυτός είναι ένας όρος ο οποίος χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία ένας εισβολέας χρησιμοποιεί κάποιο υπολογιστή προσποιούμενος στο σύστημα στο οποίο επιτίθεται ότι ο υπολογιστής που χρησιμοποιεί είναι κάποιος άλλος, τον οποίο το σύστημα εμπιστεύεται και συνεπώς μπορεί να εκτελέσει λειτουργίες που κανονικά δεν θα επιτρεπόταν. Το spoofing δεν απαιτεί πολλές γνώσεις σχετικά με passwords και μεθόδους πιστοποίησης χρηστών όπως οι προηγούμενες μέθοδοι. Έχει σχέση μόνο με το να νομίζει το δίκτυο ότι ο υπολογιστής που χρησιμοποιεί ο εισβολέας είναι κάποιος άλλος υπολογιστής που το δίκτυο εμπιστεύεται. Για να καταλάβουμε πως λειτουργεί το spoofing μπορούμε να δούμε μια συγκεκριμένη μορφή της τεχνικής αυτής που λέγεται **IP spoofing.** Αυτή η επίθεση χρησιμοποιεί το πρωτόκολλο TCP-IP για να παρακάμψει τις κανονικές λειτουργίες πιστοποίησης σε ένα σύστημα και γίνεται χρησιμοποιώντας έναν υπολογιστή που ισχυρίζεται πως έχει μια έμπιστη IP διεύθυνση.

Για παράδειγμα, σε πολλά εταιρικά δίκτυα είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των IP διευθύνσεών τους. Συγκεκριμένα, ενδέχεται ένας υπολογιστής να είναι ρυθμισμένος ούτως ώστε να επιτρέπει την πρόσβαση χωρίς username και password όταν διαπιστώσει ότι η σύνδεση προέρχεται από κάποια συγκεκριμένη IP (πχ. την IP του υπολογιστή που χρησιμοποιεί ο διευθυντής). Αυτό όμως συνιστά τρύπα ασφαλείας, αφού οποιοσδήποτε εργαζόμενος μπορεί να χρησιμοποιήσει την τεχνική IP spoofing για να κατασκευάσει πακέτα IP με ψεύτικη διεύθυνση προέλευσης και έτσι να αποκτήσει πρόσβαση στον εν λόγω υπολογιστή. Ο όρος spoofing χρησιμοποιείται γενικά για να περιγράψει κάθε μορφής αλλοίωση στην κεφαλίδα ενός πακέτου, η οποία έχει ως στόχο να παραπλανήσει τον παραλήπτη του πακέτου. Η τεχνική αυτή χρησιμοποιείται και από spammers για την αλλοίωση των κεφαλίδων των email, ούτως ώστε ο παραλήπτης να μην μπορεί να τους εντοπίσει.[46]

3.2.9 SCUMWARE

Το scumware, αλλάζει τον τρόπο με τον οποίο βλέπει ο χρήστης τους ιστοχώρους που επισκέπτεται. Στην ουσία , αντικαθιστά το πραγματικό τους περιεχόμενο με διαφημίσεις, από τους διαφημιστές scumware και παράγει κίνηση για αυτούς.

3.2.10 ROOTKIT

Τα rootkit βοηθούν στο καμουφλάρισμα άλλων κακόβουλων λογισμικών, αποκρύπτοντας κακόβουλα προγράμματα από τα λογισμικά ασφαλείας. Ελέγχουν, δηλαδή, το λειτουργικό σύστημα δυσκολεύοντας την αναζήτηση του κακόβουλου λογισμικού. Τα λογισμικά αυτού του είδους προστατεύουν και τους χάκερ, καθώς οι πληροφορίες του εισβολέα διαγράφονται ή κωδικοποιούνται.

Για παράδειγμα αν ένα rootkit ενσωματωθεί στο πρόγραμμα του λειτουργικού συστήματος το οποίο ελέγχει την ορθότητα του συνθηματικού για να επιτρέψει σε κάποιον χρήστη να συνδεθεί με τον υπολογιστή, τότε, κάθε φορά που

[46] http://el.wikipedia.org/wiki/IP_spoofing

κάποιος δίνει τον κωδικό του για να συνδεθεί με τον υπολογιστή ενεργοποιεί αυτό το πρόγραμμα το οποίο μπορεί πλέον να αποκτήσει τον έλεγχο του υπολογιστή ή απλά να αντικαθιστά οποιοδήποτε άλλο πρόγραμμα (π.χ. το αντιϊκό που χρησιμοποιεί) το οποίο με τη σειρά του να περιέχει ενσωματωμένο άλλο, κακόβουλο, λογισμικό.[47]

3.2.11 COMPUTER CRIME (ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ)

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison (1994) προσδιόρισε το ηλεκτρονικό έγκλημα ως *«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της»*. Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια τριπλή προσέγγιση (Αγγέλης, 2000) που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών.
- μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές.
- μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει με οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.[48]

3.2.11.1 Κατηγορίες "εγκληματιών του Κυβερνοχώρου" ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα:

I. HACKERS

Με τον όρο **hacker** χαρακτηρίζεται το άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές αλλά και προχωρημένες γνώσεις προγραμματισμού, μπορεί να εντοπίσει αδυναμίες σε συστήματα υπολογιστών, να λύνει τεχνικά προβλήματα, να

[47] http://el.wikipedia.org/wiki/Rootkit
[48] http://www.e-crime.gr/crime.htm

βελτιώνει εφαρμογές αλλά και που συνεργάζεται μ' άλλους ομοίους για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά. Όλα αυτά γίνονται χωρίς να παραβιάζεται η κείμενη νομοθεσία και πάντα με την προϋπόθεση ότι αφού λύσει ο όποιος hacker κάποιο πρόβλημα θα πρέπει να γνωστοποιήσει τη λύση αυτή και στους υπόλοιπους. Η κοινοποίηση της λύσης ενός προβλήματος αποσκοπεί στο ότι όλοι όσοι ασχολούνται με το ίδιο πρόβλημα θα μπορούν να αφιερώσουν τον χρόνο τους σε κάτι άλλο χρήσιμο ή ακόμα μπορεί να αποσκοπεί σε οικονομικά οφέλη. Ο hacker αφού καταφέρει να εισέλθει σ' ένα δίκτυο υπολογιστών και εντοπίσει τις αδυναμίες του, θα ειδοποιήσει τους υπευθύνους του συστήματος για να διορθώσουν τα όποια προβλήματα, σώζοντας έτσι τη θέση τους, τους πελάτες τους και τα μυστικά της εταιρείας. Οι ίδιοι ισχυρίζονται ότι προσφέρουν κοινωνικό έργο και ότι μοναδικό τους κίνητρο είναι η αγάπη τους για τη γνώση. Όλα τα παραπάνω καθώς και η σωστή συμπεριφορά είναι απαραίτητα ώστε να μπορεί να θεωρηθεί κάποιος μέλος της κοινότητας των hackers. Είναι γεγονός ότι πολλοί, αν όχι οι περισσότεροι, δημιουργοί και διαχειριστές των δικτυακών τόπων (Web sites) δεν φροντίζουν όσο θα έπρεπε την ασφάλειά τους και έτσι είναι σαν να χτίζουν ένα οικοδόμημα χωρίς την κατάλληλη αντισεισμική προστασία. Ένας κακόβουλος hacker μπορεί συνεπώς να κάνει ζημιά στην ιστοσελίδα τους και να τους εκθέσει.[49]

Κατηγορίες των Hackers

Η κοινότητα των hackers χωρίζεται σε αρκετές ξεχωριστές ομάδες, όπου η καθεμία έχει τα δικά της χαρακτηριστικά. Μια κατηγορία είναι αυτοί που αντιμετωπίζουν την πειρατεία ως έναν τρόπο σκέψης και όχι απλά ως μια παράνομη είσοδο σ' έναν υπολογιστή. Μια άλλη θεωρία αντιμετωπίζει το hacking ως την απασχόληση επί ώρες ολόκληρες για να μπορέσει κάποιος να δημιουργήσει ένα πρόγραμμα που θα κάνει κάποια λειτουργία, χρήσιμη ή όχι.

Στην κατηγορία των ***ηθικών hackers (ethical hackers)*** ανήκουν όσοι ανακαλύπτουν μεν ορισμένα σημαντικά τρωτά σημεία (αδυναμίες) κάποιων συστημάτων υπολογιστών και ενημερώνουν σχετικά τον διαχειριστή του εν λόγω

[49] http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html

συστήματος, χωρίς όμως να υπάρχει εκ μέρους τους κάποια πρόθεση εκμετάλλευσης αυτής της αδυναμίας. Είναι οι Ρομπέν των Δασών στους υπολογιστές. Πολλοί απ' αυτούς που ανήκουν στην κατηγορία των ηθικών hackers δημιούργησαν δικές τους εταιρείες συμβούλων ασφαλείας για να προσφέρουν τις γνώσεις, τις εμπειρίες και τις υπηρεσίες τους σε κάθε ενδιαφερόμενο.

Υπάρχουν και οι hackers που δρουν με κοινωνικά κριτήρια και θέλουν να αλλάξουν τον κόσμο προς το καλύτερο, παρεμβαίνοντας με τις πράξεις τους συμβολικά ή και ουσιαστικά. Υπάρχουν και οι hackers που θέλουν να αποδείξουν τις τεχνικές δυνατότητες που διαθέτουν και να βελτιώσουν τα συστήματα ασφαλείας, αποδεικνύοντας πόσο ευαίσθητα είναι.

Μια άλλη κατηγορία hackers είναι οι ***hacktivists,*** οι οποίοι έχουν ως στόχο να βοηθήσουν μια πολιτική άποψη ή ένα πολιτικό κόμμα ή και να εργαστούν με τον τρόπο τους εναντίον ενός πολιτικού συστήματος. Συνήθως αντιπροσωπεύουν κάποια κοινωνική ή πολιτική άποψη και ο στόχος τους είναι να περάσουν κάποιο μήνυμα προκαλώντας το ενδιαφέρον των μέσων μαζικής επικοινωνίας.

Υπάρχουν και οι hackers που έχουν ως στόχο το οικονομικό κέρδος, κάνουν ηλεκτρονικές επιθέσεις σε οικονομικούς οργανισμούς και αντιγράφουν παράνομα προγράμματα λογισμικού. Υπάρχουν βέβαια και οι επίσημοι hackers που εργάζονται νόμιμα για λογαριασμό κυβερνήσεων, κυρίως για κατασκοπευτικούς λόγους.

Μια άλλη κατηγορία hackers είναι οι ***meta-hackers,*** οι οποίοι παρακολουθούν τη δράση άλλων hackers χωρίς να γίνονται αντιληπτοί και προσπαθούν να εκμεταλλευτούν τις αδυναμίες των συστημάτων που οι άλλοι hackers ανακαλύπτουν.

Τέλος, η κατηγορία των hackers με την ονομασία ***darkdiders,*** είναι αυτοί που εκμεταλλεύονται τις αδυναμίες των συστημάτων υπολογιστών ώστε να αποκομίσουν οικονομικό όφελος για τους ίδιους προσωπικά ή και να προκαλέσουν καταστροφές.[50]

Το *hacking* είναι ποινικό αδίκημα σε πολλές χώρες καθώς η κοινωνία μας εξαρτάται όλο και περισσότερο από τους υπολογιστές και το Internet και πιο συγκεκριμένα τιμωρείται όποιος αποκτήσει χωρίς εξουσιοδότηση πρόσβαση σε συστήματα πληροφοριών, προκαλέσει ζημιά, αποκομίσει από τις ενέργειές του

[50] Βλέπε υποσημείωση 50.

οικονομικό όφελος ή αποδειχθεί ότι είναι μέλος ενός δικτύου οργανωμένου εγκλήματος.

II. CRACKERS

Οι ***crackers*** θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την καταστροφή ή και την αλλοίωση δικτυακών τόπων όπου αφήνουν περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους, την δημιουργία πειρατικών αντιγράφων προγραμμάτων ή τραγουδιών ή και βίντεο και άλλα.

Με απλά λόγια, πρόκειται για hackers οι οποίοι προβαίνουν σε πράξεις που παραβιάζουν διατάξεις του κοινού ποινικού κώδικα. Συνήθως πρόκειται για άτομα με έντονη ανάγκη για επίδειξη, οι οποίοι διεισδύουν σε συστήματα και προκαλούν ζημιές. Οι κυριότερες διαφορές τους από τους hackers είναι ότι δεν έχουν ιδιαίτερες γνώσεις για την πληροφορική και τον προγραμματισμό καθώς και το ότι δεν διέπονται από κανενός είδους ηθική αρχή. Για τους λόγους αυτούς μπορούν πολύ εύκολα να καταστρέψουν ολόκληρα συστήματα υπολογιστών απλά και μόνο για να κάνουν το κέφι τους, όταν βρουν βέβαια την κατάλληλη ευκαιρία.

3.3 FIREWALLS (Φράγματα Ασφαλείας)

Πρωτοεμφανίστηκε στις αρχές του 20ού αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους ούτως ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς. Σήμερα ο όρος αυτός έφτασε να σημαίνει το λογισμικό ή υλικό που παρεμβάλλεται μεταξύ δικτύων υπολογιστών ούτως ώστε να αποτρέψει την διάδοση ιών , δούρειων ίππων και τις επιθέσεις από κακόβουλους χρήστες. Πιο συγκεκριμένα το Firewalls παρέχει ένα είδος άμυνας του εσωτερικού του δικτύου π.χ. ενός LAN (Local Area Network) από διάφορους εισβολείς που βρίσκονται σε ένα εξωτερικό δίκτυο πχ Internet. Το Firewalls δρα ως

ένα σύνορο ασφαλείας για τα δεδομένα που μεταφέρονται από και προς το εσωτερικό του δικτύου . Το Firewalls (Φράγματα ασφαλείας) ταξινομούνται στις ακόλουθες κατηγορίες:

• Φράγματα ασφάλειας με φλιτάρισμα πακέτων (Packet-filtering firewalls): Το είδος αυτού του φράγματος ασφάλειας ελέγχει όλη την κίνηση που στέλνεται από ένα εξωτερικό δίκτυο στο εσωτερικό προστατευόμενο δίκτυο και απορρίπτει αυτόματα όποια πακέτα δεν επιτρέπονται εξετάζοντας τη διεύθυνση του αποστολέα ,του παραλήπτη και την θύρα βασιζόμενο σε ένα προκαθορισμένο σύνολο κανόνων . Εάν για παράδειγμα , ένας hacker από ένα εξωτερικό δίκτυο αποκτήσει με κάποιον τρόπο τη διεύθυνση ενός υπολογιστή που ανήκει στο εσωτερικό δίκτυο και προσπαθήσει να κάνει ζημία ,το φράγμα ασφάλειας θα απορρίψει όλα τα πακέτα δεδομένων που προέρχονται από τον 'εισβολέα' (hacker), από την στιγμή που έχουν μια εσωτερική διεύθυνση αλλά προέρχονται από ένα εξωτερικό δίκτυο.

• Πύλες επιπέδου εφαρμογής (Application-level gateways): Ένα πρόβλημα των φραγμάτων ασφάλειας με φιλτράρισμα πακέτων (packet-filtering firewalls) είναι ότι ελέγχουν τις διευθύνσεις των πακέτων δεδομένων που μεταδίδονται και όχι τα ιδία τα δεδομένα. Το μειονέκτημα έρχεται να καλύψει το δεύτερο είδος των φραγμάτων ασφάλειας. Μια πύλη επιπέδου εφαρμογής (Application-level gateways) περιορίζει την πρόσβαση μόνο σε συγκεκριμένες υπηρεσίες όπως είναι μια Web, Telnet ή FTP εφαρμογή. [51]

• Πύλες επιπέδου κυκλώματος (circuit level gateways): Λειτουργούν στο επίπεδο συνόδου(session layer) του προτύπου OSI, ή το επίπεδο TCP του TCP/ IP. Ελέγχουν το TCP handshaking (*Αρχική ανταλλαγή διδομένων του TCP πρωτοκόλλου για την επίτευξη της σύνδεση*) μεταξύ των πακέτων για να καθορίσουν εάν μια ζητούμενη σύνοδος είναι νόμιμη. Οι πληροφορίες που περνούν στον απομακρυσμένο υπολογιστή (remote computer) μέσω μιας πύλης επιπέδου κυκλώματος (circuit level gateway) εμφανίζονται να προέρχονται από την πύλη. Αυτό είναι χρήσιμο για την απόκρυψη

[51] *Πομπόρτσης, Ανδρέας Σ., Τσουλφάς, Ανέστης Γ.,2002 « Εισαγωγή στο ηλεκτρονικό εμπόριο» Εκδόσεις ΤΖΙΟΛΑ, Θεσσαλονίκη.*

πληροφοριών που αφορούν προστατευόμενα δίκτυα. Οι πύλες επιπέδου κυκλώματος (circuit level gateways) είναι σχετικά ανέξοδες και έχουν το πλεονέκτημα της απόκρυψης πληροφοριών για το ιδιωτικό δίκτυο που προστατεύουν.[52]

Εικόνα: 3.2

[52]http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/refeence/firewalls1.html*track=internαl

ΚΕΦΑΛΑΙΟ 4^0

ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΓΕΝΙΚΑ

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να είναι ασφαλή. Η ασφάλεια αποτελεί ίσως τον πιο κρίσιμο και καθοριστικό παράγοντα για την ευρεία διάδοση, χρήση και αποδοχή του εμπορίου πάνω από τα ανοιχτά συστήματα και δίκτυα. Η δημιουργία ασφαλούς περιβάλλοντος σημάνει προστασία των δικτυακών πόρων από ενδεχόμενες απειλές.[53] Σε αυτό το κεφάλαιο θα προσπαθήσουμε να αναπτύξουμε τις μεθόδους που διασφαλίζουν την ασφάλεια των ηλεκτρονικών συναλλαγών.

4.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

Κρυπτογραφία είναι η επιστήμη της προστασίας δεδομένων, η οποία παρέχει τρόπους και μεθόδους με την βοήθεια αλγορίθμων για μετατροπή των δεδομένων σε μια αναγνωρίσιμη μορφή έτσι ώστε να καθίσταται αδύνατη η επεξεργασία και η αναγνώριση τους από μη εξουσιοδοτούμενα άτομα. Την πληροφορία θα μπορεί να τη διαβάσει μόνο το άτομα για το οποίο προορίζεται. Η κρυπτογραφία λοιπόν είναι το τεχνολογικό μέσο που παρέχει ασφάλεια στη μετάδοση δεδομένων σε πληροφοριακά ή επικοινωνιακά συστήματα. Είναι ιδιαίτερα χρήσιμη σε περιπτώσεις αποστολής οικονομικών και προσωπικών δεδομένων και αποτελεί ένα χρήσιμο εργαλείο για την πιστοποίηση της αυθεντικότητας των εμπλεκόμενων στη συναλλαγή, αλλά και για τον προορισμό του ενόχου σε περίπτωση που η εμπιστευτικότητα και η ακεραιότητα των δεδομένων έχει παραβιαστεί. Εξαιτίας της ανάπτυξης του ηλεκτρονικού

[53] Κωνσταντίνος Μάρκελλος, Πηνελόπη Μάρκελλου, Μαρία Ρήγκου, Σπύρος Συρμακέσης, Αθανάσιος Τσακαληδης,2005,*Ε-Επιχειρηματικοτητα (από την ιδέα στην υλοποίηση)*, Ελληνικά Γράμματα , Αθήνα.

εμπορίου ,οι κρυπτογραφικές τεχνικές είναι ιδιαίτερα κρίσιμες για την ανάπτυξη και την χρήση καλά προστατευμένων πληροφοριακών και επικοινωνιακών δικτύων.

4.1.1 ΕΝΑ ΣΥΝΤΟΜΟ ΙΣΤΟΡΙΚΟ ΓΙΑ ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Η γνώση για την κρυπτογραφία μπορεί να εξακριβωθεί από τους αρχαίους χρόνους. Δεν είναι δύσκολο να καταλάβουμε γιατί: μόλις τρεις άνθρωποι χρησιμοποίησαν την ικανότητα της αναγνώρισης και της γραφής, υπήρχε η πιθανότητα οι δυο από αυτούς να θέλουν να ανταλλάξουν γράμματα χωρίς ένα τρίτος να μπορεί να το διαβάσει. Στην αρχαία Ελλάδα, οι Σπαρτιάτες στρατιώτες χρησιμοποιούσαν μια μορφή κρυπτογραφίας έτσι ώστε οι στρατιώτες να μπορούν να ανταλλάξουν μεταξύ τους μυστικά μηνύματα . Τα μηνύματα ήταν γραμμένα σε στενές ταινίες περγαμηνής, η οποία ήταν τυλιγμένη σε κυλινδρικές σκυτάλες. Αφού ξετύλιγαν την περγαμηνή, η γραφή μπορούσε να διαβαστεί μόνο από κάποιον που είχε μια σκυτάλη με το ίδιο ακριβός μέγεθος. Αυτό το πρωτόγονο σύστημα ήταν μια λογική διεργασία προστασίας μηνυμάτων από κλοπή και από τα περίεργα μάτια του ανθρώπου που τα μετέφερε επίσης. Σήμερα ο κύριος ρόλος της κρυπτογραφίας είναι να προστατεύει τις ηλεκτρονικές συναλλαγές. Αμέσως μετά που ο Samuel F. Morse δημόσια παρουσίασε τον τηλέγραφο το 1984 . Οι χρήστες του τηλεγράφου άρχισαν να ανησυχούν για το πόσο εμπιστευτικά ήταν τα μηνύματα τα οποία μετέφεραν. Τι θα γινόταν αν κάποιος ηχογραφούσε την γραμμή του τηλεγράφου. Τι θα εμπόδιζε τον ασυνείδητο τηλεγραφητή να κρατήσει ένα αντίγραφο του μηνύματος που θα το αναμετάδιδε και σε άλλους. Η απάντηση ήταν να κωδικοποιήσουν τα μηνύματα με ένα μυστικό κώδικα έτσι ώστε ο παραλήπτης να μπορούσε να αποκωδικοποιήσει. Η κρυπτογραφία έγινε ακόμα πιο σημαντική με την εφεύρεση της ραδιοτηλεφωνίας και την χρήση της τον πόλεμο. Χωρίς κρυπτογραφία, τα μηνύματα που μεταδίδονταν μεταξύ συμμάχων μπορούσαν να υποκλέπτονται από τον εχθρό.

4.1.2 ΣΤΟΙΧΕΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ- ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

Ακολουθεί η αποσαφήνιση ορισμένων εννοιών που θα χρησιμοποιηθούν παρακάτω και αποτελούν βασικά μέρη της λειτουργίας της κρυπτογράφησης.

- **Αρχικό κείμενο (*plain text*):** είναι το μήνυμα πριν γίνει σε αυτό οπουδήποτε παρέμβαση .

- **Κρυπτογραφημένο κείμενο (*cipher text):*** Είναι το μήνυμα αφού το έχουμε τροποποιήσει ώστε να το αποδώσουμε σε μη-αναγνώριση μορφή. Η διαδικασία μετατροπής του *plaintext* σε ciphertext λέγεται (encryption), ενώ η αντίστροφη διαδικασία είναι γνωστή ως αποκωδικοποίηση (decryption)

- **Κρυπτογραφικός αλγόριθμος (cipher)**: Είναι η μαθηματική διαδικασία που χρησιμοποιείται προκειμένου να μετατραπεί το plain text σε cipher text και αντιστρόφως.

- Α**λγόριθμος αποκρυπτογράφησης:** Αυτός είναι απαραίτητα ο αλγόριθμος κρυπτογράφησης εκτελεσμένος αντίστροφα . Παίρνει το κρυπτογραφημένο κείμενο και το μυστικό και παράγει το αρχικό κείμενο (plain text).

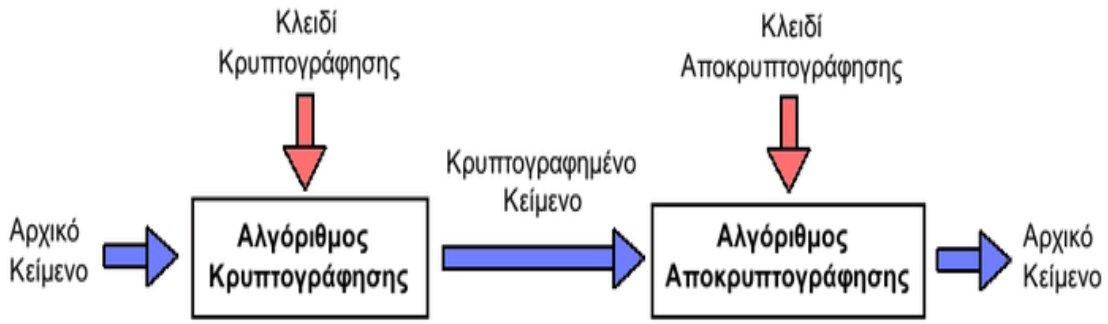
- **Κλειδί (*key*)** : Είναι ένα μυστικό κλειδί που χρησιμοποιείται για την κωδικοποίηση και/ή αποκωδικοποίηση του μηνύματος. Κάθε κλειδί μετατραπεί το ίδιο plain text σε διαφορετικό cipher text. Αν το σύστημα κρυπτογράφησης δουλεύει σωστά, μόνο όσοι γνωρίζουν το σωστό κλειδί μπορούν να αποκωδικοποιήσουν ένα κομμάτι του cipher text.[54]

4.1.3 Η ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΤΗΣ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης είναι η εξής: Ο αποστολέας του μηνύματος χρησιμοποιώντας ένα κλειδί κρυπτογράφησης και με

[54] Πομπόρτσης, Ανδρέας Σ., Τσουλφάς, Ανέστης Γ., 2002 « *Εισαγωγή στο ηλεκτρονικό εμπόριο»* Εκδόσεις ΤΖΙΟΛΑ, Θεσσαλονίκη.

την βοήθεια ενός αλγορίθμου κρυπτογράφησης μετατρέπει το αρχικό κείμενο (plain text) σε κρυπτογραφημένο κείμενο (cipher text). Στην συνέχεια ο παραλήπτης του κρυπτογραφημένο κείμενο (cipher text) χρησιμοποιεί έναν αλγόριθμο και ένα κλειδί αντίστοιχα και αποκτά το αρχικό κείμενο (plain text). Η όλη διαδικασία απεικονίζεται στην παρακάτω εικόνα.



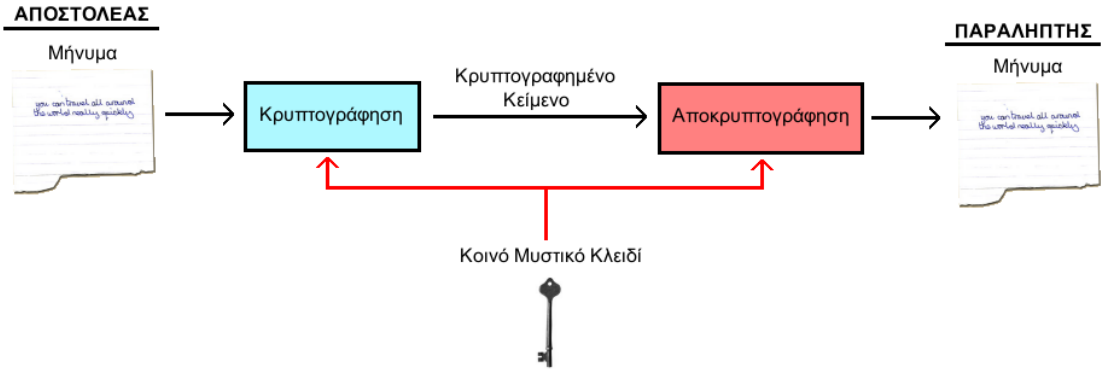
Εικόνα 4.1 :Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

4.2 ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

4.2.1 ΚΡΥΠΤΟΓΡΑΦΙΑ ΙΔΙΩΤΙΚΟΥ Ή ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Η Κρυπτογραφία ιδιωτικού κλειδιού ή συμμετρικού κλειδιού βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, γνωστό ως μυστικό κλειδί (secret key), με το οποίο γίνεται η κρυπτογράφηση και η αποκρυπτογράφηση της πληροφορίας . Ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν και χρησιμοποιούν το μυστικό κλειδί. Ειδικότερα, ακολουθούνται τα βήματα της διαδικασίας της κρυπτογράφησης και της αποκρυπτογράφησης που παρουσιάζεται παραπάνω με την διαφορά ότι αποστολέας και παραλήπτης χρησιμοποιούν ένα *κοινό* μυστικό κλειδί. Η Κρυπτογραφία ιδιωτικού κλειδιού ή συμμετρικού κλειδιού χρησιμοποιείται εδώ και χρόνια. Ένας από τους παλιότερους γνωστούς κώδικες κρυπτογραφίας είναι ο αλγόριθμος Καίσαρα, που αποτελεί έναν απλό κώδικα αντικατάστασης.

Η παραπάνω διαδικασία απεικονίζεται στην Εικόνα 4.2



Εικόνα 4.2 :Κρυπτογραφία ιδιωτικού κλειδιού ή συμμετρικού κλειδιού

Υπάρχουν δυο απαιτήσεις για την ασφαλή χρήση της κρυπτογραφίας ιδιωτικού ή συμμετρικού κλειδιού:

- Χρειαζόμαστε έναν ισχυρό αλγόριθμο κρυπτογράφησης. Κατ' ελάχιστο , θα θέλαμε ο αλγόριθμος να είναι τέτοιος ώστε ένας αντίπαλος, ο όποιος γνωρίζει τον αλγόριθμο και να έχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφημένα κείμενα , να μην είναι ικανός να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο ή να ανακαλύψει το κλειδί.

- Ο αποστολέας και ο παραλήπτης πρέπει να έχουν προμηθευτεί αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και πρέπει να κρατούν το κλειδί ασφαλές. Εάν κάποιος μπορεί να ανακαλύψει το κλειδί και γνωρίζει τον αλγόριθμο, κάθε επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνωρίσιμη.

Υπάρχουν δυο γενικές προσέγγισης προσβολής ενός συμμετρικού σχήματος κρυπτογράφησης. Η πρώτη επίθεση είναι γνωστή ως κρυπτοανάλυση. Οι επιθέσεις κρυπτοαναλυσής βασίζονται στη φύση του αλγορίθμου συν πιθανόν κάποιας γνώσης των γενικών χαρακτηριστικών του αρχικού κειμένου . Αυτός ο τύπος επίθεσης εκμεταλλεύεται τα χαρακτηριστικά του αλγορίθμου και επιχειρεί να εξαιρεί αφαιρετικά ένα συγκεκριμένο αρχικό κείμενο ή το κλειδί που χρησιμοποιείται. Εάν επιτύχει η επίθεση , το αποτέλεσμα είναι καταστροφικό. Όλα τα μελλοντικά και

παρελθοντικά μηνύματα κρυπτογραφημένα με εκείνο το κλειδί έχουν εκτεθεί. Η δεύτερη μέθοδος είναι γνωστή ως επίθεση ωμής ισχύος, είναι να δοκιμαστεί κάθε δυνατό κλειδί σε ένα κομμάτι κρυπτογραφημένου κειμένου μέχρι να ληφθεί μια κατανοητή μετάφραση σε αρχικό κείμενο.[55]

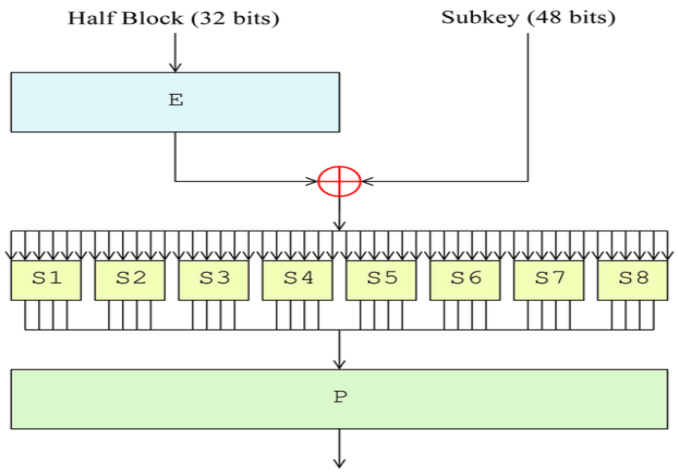
4.2.2 ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ Ή ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Η σύγχρονη κρυπτογραφία χρησιμοποιεί τις ίδιες βασικές ιδέες με την παραδοσιακή κρυπτογραφία (μετάθεση και αντικατάσταση), όμως η έμφαση δίνεται σε διαφορετικό σημείο. Παραδοσιακά οι κρυπτογράφοι χρησιμοποιούν απλούς αλγορίθμους. Σήμερα, ισχύει το αντίστροφο. Στόχος είναι να έχουμε έναν τόσο περίπλοκο και μπλεγμένο αλγόριθμο κρυπτογράφησης ώστε ακόμα και αν ο κρυπτοαναλυτής αποκτήσει τόνους κρυπτογραφημένου κειμένου της επιλογής του, να μην μπορεί να καταλάβει τίποτα από αυτά χωρίς να έχει το κλειδί. Οι αλγόριθμοι ιδιωτικού κλειδιού ή συμμετρικού κλειδιού μπορούν να χωριστούν σε δυο κατηγορίες. Σε αυτούς που κρυπτογραφούν ένα κομμάτι δεδομένων μόνο μιας ή αλγόριθμους "μπλοκ" (Block algorithms) και σε αυτούς που κάνουν την κρυπτογράφηση byte ανά byte σε δεδομένα συνεχής ροής ή αλγορίθμους "συρμού" (Stream algorithms). Στους αλγόριθμους ιδιωτικού κλειδιού ή συμμετρικού κλειδιού, συγκαταλέγονται οι εξής αλγόριθμοι : DES, Triple DES, DESX, GDES. RDES, IDEA, RC2, RC4, RC5 AES.

[55] William Stallings, 2004, *«ΕΠΙΚΟΙΝΩΝΙΕΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΕΔΟΜΕΝΩΝ»* έκτη έκδοση, Εκδόσεις ΤΖΙΟΛΑ.

4.2.2.1 Ο ΑΛΓΟΡΙΘΜΟΣ DES

Τον Ιανουάριο του 1977 η κυβέρνηση των Η.Π.Α υιοθέτησε μια κρυπτογραφία γινομένου που αναπτύχτηκε από την IBM (International Business Machines) ως το επίσημο πρότυπο της για τις μη απόρρητες πληροφορίες. Η κρυπτογραφία αυτή, δηλαδή , το Πρότυπο κρυπτογράφησης Δεδομένων ή DES υιοθετήθηκε ευρύτερα από την βιομηχανία για χρήση σε προϊόντα ασφάλειας. Το μήκος του κλειδιού που χρησιμοποιείται είναι 56 bits και θεωρείται μικρό για την επίτευξη προστασίας ανταλλασσόμενων μηνυμάτων από επιθέσεις . Το DES κρυπτογραφεί τα δεδομένα σε διακριτά μπλοκ των 64 bits και συχνά χρησιμοποιείται σε συνδυασμό με μια μέθοδο που ονομάζεται cipherblock chaining (CBC). Ο συνδυασμός και των δυο αυτών μεθόδων έχει σαν αποτέλεσμα, η κρυπτογράφηση καθενός μπλοκ να εξαρτάται από το περιεχόμενο του προηγούμενου, αυξάνοντας με αυτό τον τρόπο την ασφάλεια των κρυπτογραφημένων μνημάτων.[56]



Εικόνα:4.3

[56]Νικόλαος Β. Γεωργόπουλος ,Μαλαματένια –Άλμα Α. Πανταζή, Χαράλαμπος Θ. Νικολουράκος, Ιωσήφ Χ. Βαγγελατος,*2005, Ηλεκτρονικό Επιχειρείν, (προγραμματισμός και σχεδίαση), Ε*. Μπένου , Αθήνα

4.2.2.2 ΟΙ ΑΛΓΟΡΙΘΜΟΙ TRIPLE DES, DESX, GDES, RDES

Αυτοί οι αλγόριθμοι αποτελούν παραλλαγές του DES και μειώνουν τον κίνδυνο αποκρυπτογράφησης από εισβολής , χρησιμοποιώντας μεγαλύτερα μήκους κλειδιά . Συγκεκριμένα το triple Des κρυπτογραφεί τα μηνύματα με τρία μυστικά στην σειρά φθάνοντας με αυτό τον τρόπο την ασφάλεια των κρυπτογραφημένων μηνυμάτων. [57]

4.2.2.3 Ο ΑΛΓΟΡΙΘΜΟΣ AES

Καθώς το DES άρχιζε να πλησιάζει το τέλος της χρήσιμης ζωής του ακόμη και με το τριπλός DES, το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας ή NEST(National Institute of Standards and Technology) δηλαδή, η υπηρεσία του Υπουργείου Εμπορίου των Η.Π.Α αποφάσισε ότι η κυβέρνηση χρειαζόταν ένα νέο κρυπτογραφικό πρότυπο. Έτσι, τον Ιανουάριο του 1997 το NIST προσκάλεσε ερευνητές από όλο τον κόσμο να υποβάλουν προτάσεις για ένα νέο πρότυπο που θα ονομαζόταν Προηγμένο Πρότυπο Κρυπτογράφησης ή AES (Advanced Encryption Standard). Το πρότυπο που κυριάρχησε ήταν αυτό του εφευρέτη Rijndael.[58] Το πρότυπο AES περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plain text μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο

[57] Βλέπε υποσημείωση 57.
[58] Andrew S. Tanenbaum,2003 *«Δίκτυα Υπολογιστών»* Εκδόσεις Κλειδάριθμος. Αθήνα.

αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (cipher text). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plain text μπλοκ.[59]

4.2.2.4 Ο ΑΛΓΟΡΙΘΜΟΣ IDEA (international data encryption algorithm)

Ίσως ο πιο ενδιαφέρον και βασικός αλγόριθμος κρυπτογραφίας μετά το DES να είναι ο IDEA (international data encryption algorithm) . Ο IDEA σχεδιάστηκε από δύο ερευνητές στην Ελβετία, οπότε δεν έχει την καθοδήγηση της NSA. Προσφέρει πολύ δυνατή κρυπτογράφηση κάνοντας χρήση κλειδιού μεγέθους 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Έχει σχεδιαστεί για να εφαρμόζεται εύκολα τόσο σε υλικό όσο και σε λογισμικό . Μερικές από τις αριθμητικές διεργασίες που χρησιμοποιούν καθιστούν τις λογισμικές εφαρμογές αργές. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.[60]

4.2.2.5 ΟΙ ΑΛΓΟΡΙΘΜΟΙ RC2, RC4, RC5

Οι αλγόριθμοι RC2, RC4 και RC5 σχεδιάστηκαν από τον Ron Rivest (από εκεί προέρχεται το R στην RSA Data Security Inc.). Παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού κρυπτογράφησης, για πολύ γρήγορη και μεγάλου όγκου κρυπτογράφηση. Οι τρείς αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DES και μπορούν να γίνουν ακόμα πιο ασφαλείς εάν επιλέξουμε μεγαλύτερο μήκος κλειδιού. Πιο συγκεκριμένα ο αλγόριθμος RC2 βασίζεται σε κλειδιά μεταβλητούς μήκους για την κρυπτογράφηση και είναι σημαντικά πιο γρήγορος. Έχει την δυνατότητα να είναι περισσότερο η λιγότερο ασφαλής από το DES ανάλογα με το μήκος του κλειδιού που χρησιμοποιείται. Ο RC4 είναι ένα συμμετρικός αλγόριθμος ο οποίος χρησιμοποιεί κλειδιά μεταβλητού μήκους και είναι πολύ δημοφιλής στην κρυπτογράφηση των πληροφοριών κατά την επικοινωνία με web sites. Ο RC5 είναι

[59] http://students.ceid.upatras.gr/~mprokala/techarticles/cryptography/AES/aes.htm
[60] Κωνσταντίνος Μάρκελλος, Πηνελόπη Μαρκέλλου, Μαρία Ρήγκου ,Σπύρος Συρμακέσης, Αθανάσιος Τσακαλιδης,2005, *Ε-Επιχειρηματικότητα,* εκδόσεις Ελληνικά Γράμματα, Αθήνα.

ένας γρήγορος αλγόριθμος που υλοποιήθηκε το 1994, περιλαμβάνει πολλές παραμέτρους όπως μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος τμήματος κειμένου (block) και μεταβλητό αριθμός επαναλήψεων. Τυπικές επιλογές για το μέγεθος το block είναι 32bits (για πειραματικές εφαρμογές), 64bits (για αντικαταστεί του DES) και 128bits. Ο RC5 είναι πολύ απλός σε λειτουργιά, πράγμα που τον κάνει πολύ εύκολο στην ανάλυση. [61]

4.2.3 ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ Ή ΑΣΣΥΜΕΤΡΟΥ ΚΛΕΙΔΙΟΥ

Η κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρου κλειδιού επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης ιδιωτικού κλειδιού ή συμμετρικού κλειδιού αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Όπως υποδηλώνουν τα ονόματα ,το δημόσιο κλειδί από το ζεύγος κοινοποιείται για χρήση από άλλους , ενώ το ιδιωτικό κλειδί είναι γνωστό μόνον στον ιδιοκτήτη.

Βασικά βήματα υλοποίησης κρυπτογράφησης δημοσίου ή ασύμμετρου κλειδιού.

1. Κάθε χρήστης παράγει ένα ζεύγος κλειδιών για να χρησιμοποιηθούν για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.

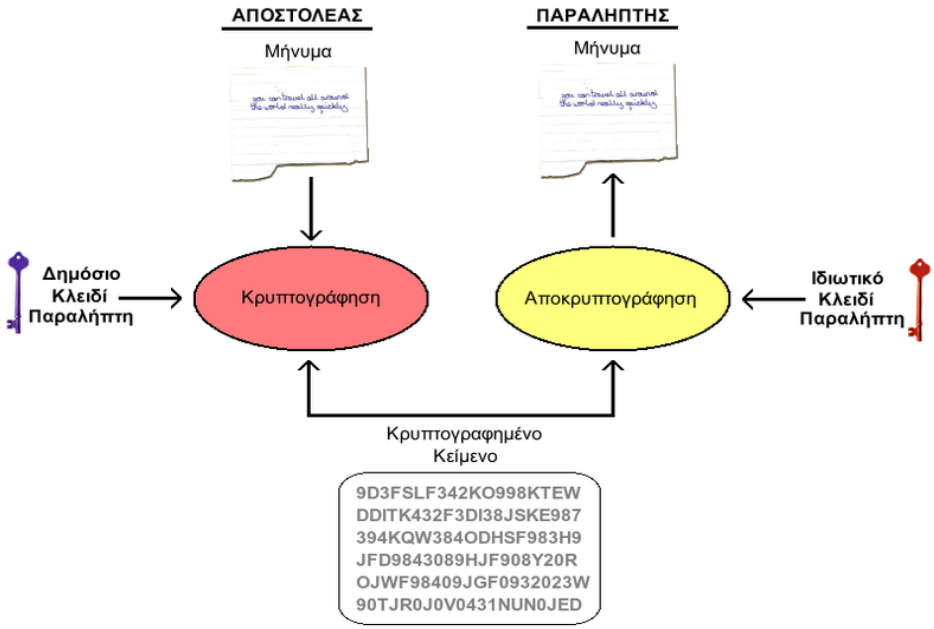
2. Κάθε χρήστης τοποθετεί το ένα από τα δυο κλειδιά σε ένα δημόσιο κατάλογο ή άλλο προσβάσιμο αρχείο . Αυτό είναι το δημόσιο κλειδί. Το αντίστοιχο δεύτερο κλειδί κρατιέται μυστικό.

[62]Βλέπε υποσημείωση 61

3. Εάν ο Χ επιθυμεί να στείλει ένα ιδιωτικό μήνυμα στον Ψ, ο Χ κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Ψ.

4. Όταν ο Ψ λάβει το μήνυμα , το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Κανένας άλλος παραλήπτης δε μπορεί να αποκρυπτογραφήσει το μήνυμα μόνο ο Ψ γνωρίζει το ιδιωτικό κλειδί του Ψ.

Όσο ένας χρήστης προστατεύει το ιδιωτικό του κλειδί , η εισερχόμενη επικοινωνία είναι ασφαλής. Οποιαδήποτε στιγμή , ένας χρήστης μπορεί να αλλάξει το ιδιωτικό του κλειδί και να δημοσιοποιήσει τι αντίστοιχο δημόσιο κλειδί για να αντικαταστήσει το παλιό δημόσιο κλειδί.



Εικόνα 4.4 :Κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρου κλειδιού

4.2.3.1 Ο ΑΛΓΟΡΙΘΜΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ Ή ΑΣΥΜΜΕΤΡΟΥ ΚΛΕΙΔΙΟΥ RSA

Ένα από τα πρώτα σχήματα δημόσιου κλειδιού αναπτύχτηκε το 1977 από τους Ron Rivest, Adi Shamir και Len Adleman και MIT και δημοσιεύτηκε για πρώτη φορά το 1978. Το σχήμα RSA έχει από τότε επικρατήσει στον υπέρτατο βαθμό ως η μοναδική ευρέως αποδεκτή και υλοποιημένη προσέγγιση της κρυπτογράφησης δημοσίου κλειδιού. Ο RSA είναι ένα κρυπτογράφημα τμήματος στο

οποίο το καθαρό κείμενο και το κρυπτογραφημένο κείμενο είναι ακέραιοι μεταξύ τους 0 και n-1 για κάποιο n. Η κρυπτογράφηση και αποκρυπτογράφηση είναι της ακόλουθης μορφής , για κάποιο καθαρό τμήμα κειμένου M και κρυπτογραφημένο τμήμα κειμένου C:

$C=M^e \bmod n$

$M=C^d \bmod n=(M^e)^d \bmod n = M^{ed} \bmod n$

Τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν τις τιμές των n και e και μόνο ο παραλήπτης να γνωρίζει την τιμή του d. Αυτός είναι ένας αλγόριθμος δημοσίου κλειδιού με δημόσιο κλειδί KU={e,n} και ιδιωτικό κλειδί KR={d,n}.Για να είναι ικανοποιητικός αυτός ο αλγόριθμος πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις.

- Είναι δυνατόν να βρεθούν οι τιμές των e,d,n τέτοιες ώστε $M^{ed}=M \bmod n$ για όλα τα $M<n$
- Είναι σχετικά εύκολο να υπολογιστούν τα C^d και M^e για όλες τις τιμές του $M<n$
- Είναι ανέφικτο να προσδιοριστεί το d όταν δοθούν τα e και n.

Οι δυο πρώτες απαιτήσεις ικανοποιούνται εύκολα. Η τρίτη απαίτηση μπορεί να ικανοποιηθεί για μεγάλες τιμές των e και n.[62]

Ακολούθως, απεικονίζεται η διαδικασία κρυπτογράφησης δημοσίου κλειδιού RSA συνοπτικά:

ΔΗΜΙΟΥΡΓΕΙΑ ΚΛΕΙΔΙΟΥ	
Επιλογή p, q	οι p και q είναι και οι δυο πρώτοι
Υπολογισμός $n=p \times q$	
Υπολογισμός $\varphi(n)=(p-1)(q-1)$	
Επιλογή ακέραιου e	$ged(\varphi(n),e)=1.\ 1<e<\varphi(n)$

[62] *William Stallings «ΕΠΙΚΟΙΝΩΝΙΕΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΕΔΟΜΕΝΩΝ» έκτη έκδοση, Εκδόσεις ΤΖΙΟΛΑ,* Θεσσαλονίκη.

Υπολογισμός d	d= e-1 mod φ (n)
Δημόσιο κλειδί	KU= (e, n)
Ιδιωτικό κλειδί	KR= (d ,n)
ΚΡΥΠΤΟΓΡΑΦΗΣΗ	
Μη κωδικοποιημένο κείμενο :	M <n
Κρυπτογραφημένο κείμενο :	C= Me (mod n)
ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ	
Μη κωδικοποιημένο κείμενο:	C
Κρυπτογραφημένο κείμενο :	M= C4 (mod n)

Εικόνα 4.5 :Ο Αλγόριθμος RSA

Όπως παρατηρούμαι ξεκινάει με την επιλογή των δυο πρώτων αριθμών p,q και υπολογίζει το γινόμενο τους n, το οποίο είναι ο διαιρέτης για την κρυπτογράφηση και την αποκρυπτογράφηση. Μετά, χρειαζόμαστε την ποσότητα φ(n), αναφερόμενη ως Euler totient του n, και αντίστοιχα πρώτων ως προς το n. Στην συνέχεια, επιλέγουμε ένα ακέραιο e που είναι πρώτος , ως προς το φ(n) , δηλαδή, ο μέγιστος κοινός διαιρέτης των e και φ(n) να είναι 1. Τελικά, υπολογίζεται το d ως το αντίστροφο πολλαπλάσιο του e και ακέραιο υπόλοιπο του φ(n). Μπορεί να δειχθεί πως τα d και e έχουν τις επιθυμητές ιδιότητες.

Παράδειγμα Αλγορίθμου RSA:

1. Επιλέγονται δυο πρώτοι αριθμοί p=7 και q=17
2. Υπολογίζεται το n =pxq =7x17=119
3. Υπολογίζεται το φ(n)=(p-1)(q-1)=96
4. Επιλέγεται e τέτοιοι ώστε ο e να είναι πρώτος ως προς το φ(n)=96 και μικτότερος από το φ(n). Σε αυτή την περίπτωση e=5
5. Προσδιορίζεται d τέτοιο ώστε de=1 mod 96 και d<96. Η σωστή τιμή είναι d=77, διότι 77x5=385=4x96+1.

Τα παραγόμενα κλειδιά είναι το δημόσιο κλειδί KU={5,119} και το ιδιωτικό κλειδί KR = {77, 119}. Το παράδειγμα δείχνει την χρήση αυτών των κλειδιών για ένα μη κωδικοποιημένο κείμενο εισόδου M=19. Για την κρυπτογράφηση, το 19 υψώνεται στην πέμπτη δύναμη, παράγοντας 2,476,099. Με την διαίρεση με το 119, το υπόλοιπο προσδιορίζεται να είναι 66.για τον λόγο αυτό, $19^5 = 19 \bmod 119$ και το κρυπτογραφημένο κείμενο είναι 66. Για την αποκρυπτογράφηση, προσδιορίζεται πως $66^{77} = 19 \bmod 199$.

4.2.4 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ Ή ΣΥΜΜΕΤΡΙΚΗΣ ΚΑΙ ΔΗΜΟΣΙΑΣ Ή ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Στην κρυπτογραφία ιδιωτικού ή συμμετρικού κλειδιού συγκαταλέγονται οι υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης, που μπορούν να υπερβούν τα 100 Mbps καθώς επίσης και οι απαιτήσεις της σε μνήμη και υπολογιστική ισχύ. Η ανάγκη της ανταλλαγής του μυστικού κλειδιού μεταξύ αποστολέα και παραλήπτη είναι ένας από τους βασικούς περιορισμούς της κρυπτογραφία ιδιωτικού ή συμμετρικού κλειδιού. Εάν τα δυο επικοινωνούντα μέρη βρίσκονται σε διαφορετικές τοποθεσίες, τότε θα πρέπει με κάποιον τρόπο να ανταλλάξουν το κοινό κλειδί που θα πρέπει να χρησιμοποιήσουν. Αυτό ενέχει τον κίνδυνο να υποκλαπεί το κλειδί από κάποιον τρίτο που παρακολουθεί τις γραμμές επικοινωνίας ή και να διαρρεύσει από το ένα από τα δυο μέρη. Ευνόητο επίσης είναι , ότι όσο ο αριθμός των χρηστών αυτού του συστήματος ασφάλειας μεγαλώνει,

μεγαλώνουν και τα προβλήματα της δημιουργίας ,της διανομής, της ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών. Άρα τα σχήματα αυτά δεν είναι εύκολα να επεκταθούν για την εξυπηρέτηση μεγάλου πληθυσμού και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή.

Το πρόβλημα της βασικής διανομής λύνεται από την κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρου κλειδιού. Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφόρα και έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί από κάποιον χρηστή, η κρυπτογραφία μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί , μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, και έτσι η γνώση του δημοσίου κλειδιού δεν αποτελεί πρόβλημα. Όπως γίνεται κατανοητό η κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρου κλειδιού προσφέρει μεγαλύτερη ασφάλεια από την κρυπτογραφία ιδιωτικού ή συμμετρικού κλειδιού. Ένα ακόμα σημαντικό όφελος κρυπτογραφίας δημοσίου κλειδιού ή ασύμμετρου κλειδιού είναι ότι μας δίνει την δυνατότητα να δημιουργήσουμε ψηφιακές υπόγραφες (η ψηφιακή υπογραφή θα αναλυθεί στην συνέχεια της πτυχιακής μας), οι οποίες δεν επιδέχονται πλαστογράφηση. Τέλος ,ένα τεράστιο μειονέκτημα της κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρου κλειδιού είναι σχετίζεται με την ταχύτητα της κωδικοποίησης , αφού δεν είναι γρήγορη στις περιπτώσεις μεγάλων μηνυμάτων.

4.3 Υποδομή Δημοσίου Κλειδιού (PKI)

Η υποδομή δημοσίου κλειδιού (Public Key Infastructure – PKI) είναι μια βάση ασφαλείας που βεβαιώνει ότι οι συναλλαγές μέσω του WEB μπορούν να είναι αξιόπιστες. Το PKI είναι το καθολικό όνομα που αναφέρεται στα ατομικά μέτρα ασφαλείας που βεβαιώνουν ότι οι συναλλαγές είναι εμπιστευτικές, που εξαναγκάζουν τους συνεργάτες μια επιχείρησης να αποδεικνύουν την ταυτότητά

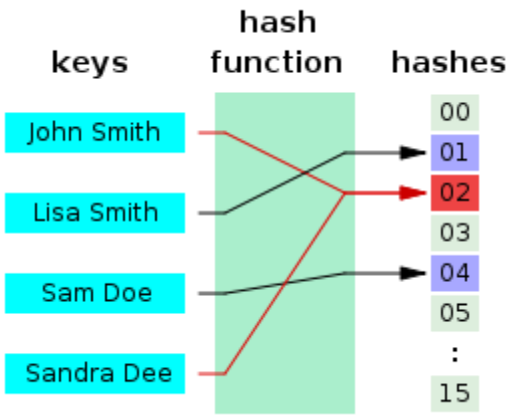
τους, που εμποδίζουν τροποποιήσεις ή αλλοιώσεις των συναλλαγών και εφαρμόζουν νομικά το αναμφισβήτητο των συναλλαγών. Συμπερασματικά λοιπόν το PKI επανακαθορίζει την εμπιστοσύνη των εταιριών όσον αφορά συναλλαγές που γίνονται στο Διαδίκτυο. Το PKI αποτελείτε από έξι(6) διαφορετικά μέρη που δουλεύουν μαζί για να δημιουργήσουν την βάση ασφαλείας τα οποία είναι:

- Κρυπτογράφηση Δημοσίου Κλειδιού (την έχουμε ανάλυση στην υποενότητα 4.2.3)
- Ψηφιακή Υπογραφή
- Συνάρτηση Κατακερματισμού
- Ψηφιακούς Φάκελους
- Αρχή Πιστοποίησης (Certificate Authority –CA)
- Αρχή Έκδοσης Εγγράφων (Registration Authority- RA)

4.3.1 ΣΥΝΑΡΤΗΣΗ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ(HASH FUNCTION)

Η συνάρτηση κατακερματισμού (hash function) του μηνύματος παρέχει ένα πραγματικά αξιόπιστο έλεγχο της ακεραιότητας του μηνύματος. Αυτή επιδίδεται στο να τεμαχίζει το απλό κείμενο σε μικρά κομμάτια και το μετατρέπει σε μια μορφή που δείχνει τυχαία. Τα μικρά αυτά κομμάτια του αρχικού μηνύματος, έχουν σταθερό μήκος και ονομάζονται hashes. Εξαιτίας του μικρού μήκους των hashes, η συνολική πληροφορία του μηνύματος χάνεται καθώς δεν υπάρχει τρόπος αποκωδικοποίησης του ενός hash. Η συνάρτηση κατακερματισμού (hash function) λειτουργεί σαν ψηφιακό δακτυλικό αποτύπωμα για το αρχικό μήνυμα, καθώς μια μικρή αλλαγή του απλού κειμένου συνεπάγεται την πλήρη μεταβολή της ταξινόμησής του. Η συνάρτηση κατακερματισμού (hash function) είναι η εξής: Η εκτέλεση της συνάρτησης κατακερματισμού για ένα μήνυμα θα δημιουργήσει το hash αυτού του μηνύματος, το hash υπογράφεται με το ιδιωτικό κλειδί του αποστολέα και στην συνέχεια το hash και το αρχικό μήνυμα στέλνεται στον

παραλήπτη. Τέλος, ο παραλήπτης αποκωδικοποιεί το hash χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα και συγκρίνει τα αποτελέσματα με αυτό που προκύπτει από την εκτέλεση της συνάρτησης κατακερματισμού για το παραπάνω μήνυμα, αν τα δύο αποτελέσματα είναι ίδια, τότε ο παραλήπτης επικυρώνει την ταυτότητα του αποστολέα αλλά και την αυθεντικότητα του μηνύματος. Τέτοιες συναρτήσεις είναι Sha & MD5.[63]



Εικόνα 4.5: Συνάρτηση κατακερματισμού

4.3.2 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Μπροστά στους κινδύνους της απάτης, της πλαστοπροσωπίας, της ασφάλειας των συναλλαγών και της φερεγγυότητας των συναλλασσομένων, ψηφίστηκε και στην Ελλάδα η σχετική νομοθεσία (ΠΔ.150/2001), όπου καθιερώνεται η νομική ισοτιμία της ψηφιακής υπογραφής με την κανονική (ιδιόχειρη) υπογραφή, όπως την γνωρίζαμε μέχρι σήμερα. Η ψηφιακή υπογραφή αντιπροσωπεύει ένα συγκεκριμένο γνωστό

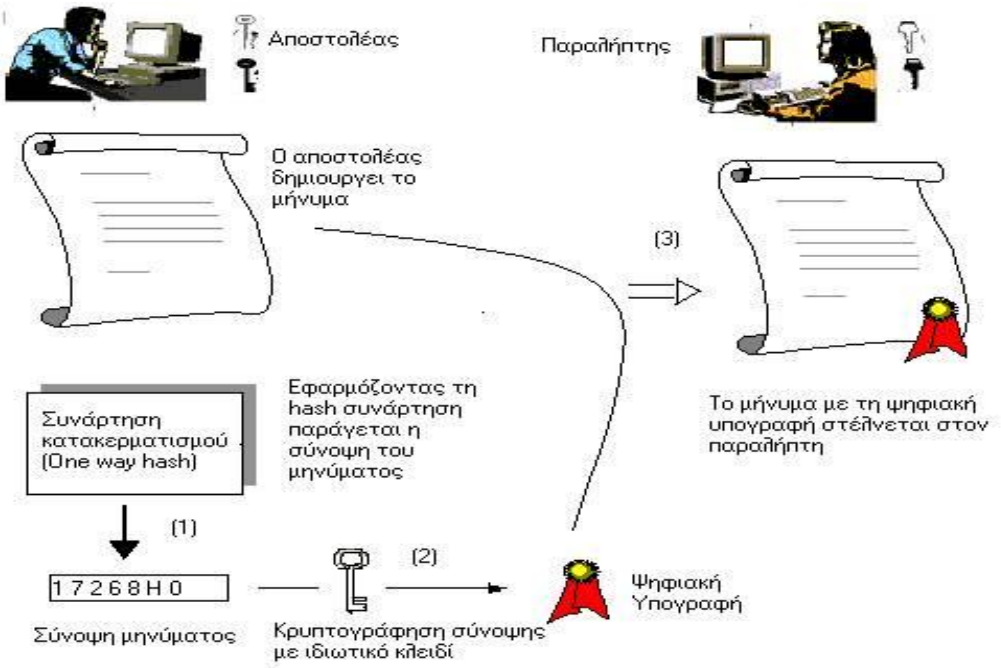
[63] Νικόλαος Β. Γεωργόπουλος ,Μαλαματένια –Άλμα Α. Πανταζή, Χαράλαμπος Θ. Νικολουράκος, Ιωσήφ Χ. Βαγγελατος,2005, *Ηλεκτρονικό Επιχειρείν, (προγραμματισμός και σχεδίαση),* Ε. Μπένου , Αθήνα

πρόσωπο ή υπηρεσία ή επιχείρηση και είναι μοναδική σε παγκόσμιο επίπεδο, ενώ η χρήση της έχει όλες τις γνωστές συνέπειες της κλασικής υπογραφής.

Για την δημιουργία μια ψηφιακή υπογραφή , ο αποστολέας πρώτα εφαρμόζει στο αρχικό μήνυμα (plaintext) την συνάρτηση κατακερματισμού (hash function). Μετά ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει την hash τιμή . Έτσι δημιουργείται μια ψηφιακή υπογραφή . Το αρχικό κείμενο το οποίο κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη ,η ψηφιακή υπογραφή και η συνάρτηση κατακερματισμού αποστέλλονται στον παραλήπτη. Ο παραλήπτης με την σειρά του ,χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την ψηφιακή υπογράφει και να πάρει την τιμή hash. Στην συνέχεια χρησιμοποιεί το διωκτικό του κλειδί για να αποκρυπτογραφήσει το αρχικό μήνυμα . Τέλος , ο παραλήπτης εφαρμόζει την συνάρτηση κατακερματισμού στο αρχικό μήνυμα . Εάν η τιμή που παίρνει είναι ιδία με αυτή που αποκρυπτογραφώ από την ψηφιακή υπογράφει , τότε η ακεραιότητα του μηνύματος είναι δεδομένη . Σε διαφορετική περίπτωση έχει παραποιηθεί από κάποιον τρίτο.[64]

Ένα βασικό πλεονέκτημα των ψηφιακών υπογράφων σε σχέση με τις χειρόγραφες υπογραφές που όλοι γνωρίζουμε είναι ότι οι χειρόγραφες υπογραφές είναι ανεξάρτητες από το έγγραφο το οποίο υπογραφούν . Εάν δηλαδή κάποιος πλαστογράφηση μια χειρόγραφη υπογραφή ,μπορεί στη συνέχεια να τη χρησιμοποίηση σε πολλά αλλά έγγραφα. Σε αντίθεση, μια ψηφιακή υπογραφή δημιουργείται με βάση το περιεχόμενο του εγγράφου έχοντας άμεση εξάρτηση από αυτά.

[64] Παναγιώτης Ε. Ναστου, Παύλος Γ. Σπυράκης, Γ Γιάννης Κ.Σταματιου,2003, *Σύγχρονη Κρυπτογραφία,* Εκδόσεις Ελληνικά Γράμματα ,Αθήνα .



Εικόνα 4.6: Ψηφιακές υπογραφές

4.3.2.1 ΠΑΡΑΔΕΙΓΜΑ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

Ας υποθέσουμε ότι δύο οντότητες Α και Β, που μπορεί να είναι ιδιώτες, υπηρεσίες, εταιρείες ή και άλλοι φορείς, επιθυμούν να επικοινωνήσουν με τη χρήση ψηφιακών υπογραφών. Η ψηφιακή υπογραφή της οντότητας Α αποτελείται από το ζεύγος κλειδιών ΙΑ (ιδιωτικό κλειδί) και ΔΑ (δημόσιο κλειδί). Αντίστοιχα, η ψηφιακή υπογραφή της οντότητας Β αποτελείται από το ζεύγος κλειδιών ΙΒ (ιδιωτικό κλειδί) και ΔΒ (δημόσιο κλειδί). Τα ιδιωτικά κλειδιά ΙΑ και ΙΒ είναι γνωστά μόνο στις οντότητες Α και Β αντίστοιχα, ενώ τα δημόσια κλειδιά τους ΔΑ και ΔΒ είναι γνωστά σ' όλον τον κόσμο. Η οντότητα Α πριν στείλει το μήνυμά της, το κρυπτογραφεί κάνοντας χρήση του ιδιωτικού της κλειδιού ΙΑ και έτσι θα μπορεί ο καθένας να χρησιμοποιήσει το αντίστοιχο δημόσιο κλειδί ΔΑ για να το αποκρυπτογραφήσει. Η οντότητα Β είναι έτσι σίγουρη ότι το μήνυμα προέρχεται όντως από την οντότητα Α και όχι από κάποιον τρίτο που προσποιείται ότι είναι η οντότητα Α, καθώς το δημόσιο κλειδί ΔΑ μπορεί να αποκρυπτογραφήσει μόνο το αντίστοιχο ιδιωτικό κλειδί ΙΑ, το οποίο μόνο η οντότητα Α κατέχει. Επίσης, η οντότητα Β είναι σίγουρη ότι το

μήνυμα δεν έχει αλλοιωθεί καθ' οδόν προς τον προορισμό του από κάποιον τρίτο, καθώς κανείς δεν είναι σε θέση να γνωρίζει το ιδιωτικό κλειδί ΙΑ που χρησιμοποιήθηκε για την κρυπτογράφησή του, αλλά ακόμα και στην περίπτωση που το κείμενο τροποποιηθεί, η οντότητα Β θα διαπιστώσει ότι το δημόσιο κλειδί δεν θα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα και έτσι θα γνωρίζει ότι το μήνυμα είναι παραποιημένο. Το παραπάνω είναι ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο με ψηφιακή υπογραφή, πρόκειται δηλαδή για ένα μήνυμα για το οποίο είμαστε σίγουροι για την ταυτότητα του αποστολέα του καθώς και για το ότι το μήνυμα αυτό είναι γνήσιο και όχι παραποιημένο. Στην περίπτωση τώρα που η οντότητα Α θελήσει να στείλει ένα μήνυμα στην οντότητα Β που να είναι όμως και κρυπτογραφημένο, δηλ. μόνο η οντότητα Β να μπορεί να το διαβάσει και κανένας άλλος, τότε θα πρέπει να κρυπτογραφήσει το μήνυμα και με το δημόσιο κλειδί ΔΒ της οντότητας Β. Έτσι, μόνο η οντότητα Β θα μπορέσει να αποκρυπτογραφήσει το μήνυμα καθώς μόνο αυτή διαθέτει το αντίστοιχο ιδιωτικό κλειδί ΙΒ. Θα πρέπει επιπλέον να εφαρμόσει και το δημόσιο κλειδί ΔΑ της οντότητας Α για να μπορέσει να επαναφέρει το αρχικό μήνυμα. Το παραπάνω είναι ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο και κρυπτογραφημένο με ψηφιακή υπογραφή, πρόκειται δηλαδή για ένα μήνυμα για το οποίο όχι μόνο είμαστε σίγουροι για την ταυτότητα του αποστολέα του και για το ότι το μήνυμα είναι γνήσιο και όχι παραποιημένο αλλά και ότι κανείς άλλος δεν μπορεί να το δει και να το αποκρυπτογραφήσει εκτός από αυτόν για τον οποίο προορίζεται.

Για να μπορέσουν να έχουν εφαρμογή οι παραπάνω διαδικασίες, θα πρέπει να είμαστε σίγουροι ότι η ψηφιακή υπογραφή έχει εκδοθεί νόμιμα στο όνομα κάποιου χρήστη και ότι αυτός ο χρήστης έδωσε τα πραγματικά του στοιχεία όταν ζήτησε να εκδοθεί η ψηφιακή υπογραφή του. Η λύση είναι η ύπαρξη ενός αξιόπιστου οργανισμού, ο οποίος θα αναλάβει να εκδίδει και να πιστοποιεί τις ψηφιακές υπογραφές.

4.3.3 ΨΗΦΙΑΚΟΣ ΦΑΚΕΛΟΣ (digital envelope)

Η κρυπτογράφηση δημοσίου κλειδιού, όπως έχει ήδη αναφερθεί, είναι ιδανική για την ασφαλή ανταλλαγή μηνυμάτων μέσω του Διαδικτύου, όμως το μειονέκτημα

της μικρής ταχύτητας εκτέλεσης των απαραίτητων αλγορίθμων σε σχέση με αυτή των συμμετρικών αλγορίθμων καθιστά την ασύμμετρη κρυπτογράφηση ακατάλληλη για την μεταφορά μεγάλων μηνυμάτων. Η λύση στο πρόβλημα είναι ο ψηφιακός φάκελος, ο οποίος συνδυάζει τα δυο συστήματα κρυπτογράφησης προκειμένου να χρησιμοποιηθούν τα καλύτερα χαρακτηριστικά τους. Το σύστημα ψηφιακού φακέλου χρησιμοποιείται για την εγκατάσταση μια διπλής κατεύθυνσης επικοινωνίας.

Ο αποστολέας για να εκμεταλλευτεί το σύστημα του ψηφιακού φακέλου πρέπει αρχικά να παράγει ένα τυχαίο μυστικό κλειδί, το οποίο ονομάζεται session key γιατί απορρίπτεται μετά το τέλος της επικοινωνίας του αποστολέα και του παραλήπτη. Στη συνέχεια, το μήνυμα κρυπτογραφείται με τη βοήθεια του session key και του συμμετρικού αλγορίθμου. Το session key κωδικοποιείται με το δημόσιο κλειδί του παραλήπτη μορφοποιώντας το ψηφιακό φάκελο. Ο αποστολέας προωθεί στο παραλήπτη το κρυπτογραφημένο μήνυμα και το ψηφιακό φάκελο.

Ο παραλήπτης με τη σειρά του χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το ψηφιακό φάκελο και να αποκτήσει το session key, με τη βοήθεια του όποιου αποκωδικοποιείται το μήνυμα. Τέλος, τόσο το μήνυμα όσο και το session key είναι ασφαλή, αφού το μήνυμα κρυπτογραφήθηκε με το συμμετρικό session key που γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης, ενώ το session key κρυπτογραφήθηκε με τη βοήθεια της μεθόδου κρυπτογράφησης του δημοσίου κλειδιού.[65]

Ας υποθέσουμε ότι ο χρήστης Β θέλει να στείλει μήνυμα στον χρήστη Β. Ο Α διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με την δημόσια κλείδα του Β. Στέλνει στον Β το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο Β θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με την δημόσια κλείδα του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα

[65] Νικόλαος Β. Γεωργόπουλος ,Μαλαματένια –Άλμα Α. Πανταζή, Χαράλαμπος Θ. Νικολουράκος, Ιωσήφ Χ. Βαγγελατος,2005, *Ηλεκτρονικό Επιχειρείν, (προγραμματισμός και σχεδίαση),* Ε. Μπένου , Αθήνα

κρυπτογραφημένο μήνυμα. Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία.

4.3.4 ΑΡΧΕΣ ΕΚΔΟΣΕΙΣ ΠΙΣΤΟΠΟΙΗΣΗΣ (CERTIFIACATION AUTHORITIES – CA)

Τα ψηφιακά πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποίησης (Certification Authorities CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός ικανός να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Ουσιαστικά, είναι ένα εμπορικός οργανισμός ο οποίος βεβαιώνει υπεύθυνα τις ταυτότητες οργανισμών και μεμονωμένων ατόμων . Αντί, λοιπόν να κρατάμε στον σκληρό μας δίσκο τα δημόσια κλειδιά όλων, κρατάμε τα δημόσια κλειδιά ορισμένων γνωστών και έμπιστων CAs.Πριν στείλουμε μήνυμα σε κάποιον ζητάμε από αυτές τις CAs να μας δώσει ένα Ψηφιακό Πιστοποιητικό (Digital Certificate). Από αυτό το πιστοποιητικό μπορούμε να επαληθεύσουμε την ταυτότητα του παραλήπτη και να αποκαλύψουμε το δημόσιο κλειδί του.[66] .Οι αναγνωρισμένες και έμπιστες εταιρείες που εκδίδουν ψηφιακά πιστοποιητικά είναι κατά κύριο λόγο τρεις, η VeriSign, GoDaddy και η Comodo για αυτό και αποτελούν ένα από τα μεγαλύτερα δικτυακά ολιγοπώλια.

4.3.4.1 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ(digital certificate)

Τα ψηφιακά πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν την σχέση μεταξύ ενός δημοσίου κλειδιού και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον

[66] Πομπόρτσης, Ανδρέας Σ., Τσουλφάς, Ανέστης Γ., 2002 «Εισαγωγή στο ηλεκτρονικό εμπόριο» Εκδόσεις ΤΖΙΟΛΑ

άλλο με την χρήση ψεύτικου κλειδιού ,συνεπώς δεν επιδέχονται πλαστογράφηση και οποιαδήποτε παραβίαση.

Παρακάτω θα δώσουμε ένα παράδειγμα:

Ας υποθέσουμε ότι ο Α χρειάζεται το δημόσιο κλειδί του Β για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον Β να του στείλει το δημόσιο κλειδί του μπορεί να θέσει την όλη επικοινωνία σε ρίσκο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης του δημοσίου κλειδιού του Β με το δημόσιο κλειδί κάποιου άλλου (επίθεση man -in -the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικός με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας ένα ψεύτικο δημόσιο κλειδί . Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί το δημόσιο κλειδί που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

Ένα ψηφιακό πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.[67]

Η διαδικασία δημιουργίας ενός ψηφιακού πιστοποιητικού είναι η ακόλουθη : Καταρχήν παράγουμε ένα ζευγάρι δημοσίου/ιδιωτικού κλειδιού. Κρατάμε το ιδιωτικό κλειδί και στέλνουμε το δημόσιο κλειδί σε μια Αρχή Πιστοποίησης(CAs) μαζί με τις πληροφορίες πιστοποιήσεις ,με την μορφή ενός ¨πιστοποιητικού αίτησης¨, πληρώνουμε το ποσό που απαιτείται από την Αρχή Πιστοποίησης(CAs) . Στην συνεχεία, η Αρχή Πιστοποίησης(CAs) πιστοποιεί ότι είμαστε αυτοί που έχουμε δηλώσει. Η πιστοποιήσει μπορεί να είναι λεπτομερής η επίπλοα, ανάλογα με την

[67] http://el.wikipedia.org/wiki/ Ψηφιακό_πιστοποιητικό

Αρχή Πιστοποίησης(CAs). Εφόσον έχουν ελέγχει όλα , η Αρχή Πιστοποίησης(CAs) δημιουργεί ένα πιστοποιητικό στο οποίο περιέχεται το δικό μας δημόσιο κλαδί μαζί με πληροφορίες πιστοποίησης. Τέλος η Αρχή Πιστοποίησης(CAs) παράγει μια σύνοψη του μηνύματος από το πιστοποιητικό και υπογραεί το hash με το ιδιωτικό κλειδί, δημιουργώντας έτσι ένα υπογεγραμμένο πιστοποιητικό και επιστρεπτέοι σε εμάς.[68]

4.3.5 ΑΡΧΕΣ ΕΚΔΟΣΗΣ ΕΓΓΡΑΦΩΝ (REGISTRATION AUTHORITIES-RA)

Η αρχή έκδοσης εγγράφων (REGISTRATION AUTHORITIES-RA) είναι μια αρχή στο διαδίκτυο η όποια λαμβάνει τις αιτήσεις των χρηστών για έκδοση ψηφιακών πιστοποιητικών, πιστοποιεί την ταυτότητα του χρηστή και εν συνεχεία έρχεται σε επαφή με την αρχή έκδοσης πιστοποίησης (certification authorities –CA) για την έκδοση των πιστοποιητικών .[69]Στην ουσία είναι ένας συνδετικός κρίκος που ενώνει τον χρηστή με την αρχή έκδοσης πιστοποίησης (certification authorities –CA.

Η χρησιμότητα της RA έγκειται στο γεγονός ότι απελευθερώνει χρόνο από την CA ,αφού αναλαμβάνει την χρονοβόρα διαδικασία του ελέγχου της ταυτότητας του χρήστη και έτσι η CA έχει την δυνατότητα να επικεντρωθεί στην διαχείριση της PKI. Επίσης, οι ενέργειες της αίτησης και της πιστοποίησης της ταυτότητας του χρήστη μπορούν να διαχωριστούν τελείως από τις ενέργειες που δίνουν το πιστοποιητικό. Πρόκειται επομένως για ένα επιπλέον βήμα ασφάλειας που διαχωρίζει τις ιδιωτικές πληροφορίες από το ιδιωτικό πιστοποιητικό.

4.4 ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Τα πρωτόκολλα που θα παρουσιαστούν στην συνεχεία κατηγοριοποιούνται σύμφωνα με το αν παρέχουν ασφάλεια σύνδεσης ή ασφάλεια εφαρμογών . Για παράδειγμα, το Secure Sockets Layer(SSL) στοχεύει στην ασφάλεια επικοινωνίας στο διαδίκτυο ,ενώ το Secure HTTP(S-HTTP) και το Secure MIME (S-MIME), από την άλλη προσφέρουν αυθεντικοποίηση και εμπιστευτικότητα στις εφαρμογές. Το SET

[68] Πομπόρτσης, Ανδρέας Σ., Τσουλφάς, Ανέστης Γ. *«Εισαγωγή στο ηλεκτρονικό εμπόριο»* Εκδόσεις ΤΖΙΟΛΑ.
[69] http://searchsecurity.techtarget.com/definition/registration-authority

προχώρα ένα βήμα παραπάνω προσφέροντας ασφάλεια στις συναλλαγές ηλεκτρονικού εμπορίου.

4.4.1 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL (Secure Socket Layer)

Το SSL (Secure Socket Layer), είναι ένα αναγνωρισμένο πρωτόκολλο ασφαλούς επικοινωνίας στο διαδίκτυο. Πρωτοεμφανίστηκε το 1994 και χρησιμοποιείται για την αποστολή εμπιστευτικών δεδομένων. Πιο συγκεκριμένα χρησιμοποίει τεχνικές ασύμμετρης κρυπτογράφησης στην αρχική επαφή, ώστε να επιτεχθούν οι ακόλουθοι στόχοι.

- Ο εξυπηρετητής ή και ο πελάτης αυθεντικοποιουνται μέσω ψηφιακών πιστοποιητικών.
- Εξυπηρετητής και ο πελάτης συμφωνούν στην χρήση ενός συγκεκριμένου κλειδιού συνόδου (session key) με το όποιο θα κρυπτογραφηθεί το υπόλοιπο της συναλλαγής . Όσο πιο μεγάλο είναι το μήκος του κλειδιού τόσο πιο δύσκολο είναι η αποκρυπτογραφήσει του[70]

4.4.2 ΤΟ ΠΡΩΤΟΚΟΛΛΟ S-HTTP

ΤΟ HTTP λειτουργεί σε ανώτερο επίπεδο από το SSL, καθώς το πρώτο προσφέρει ασφάλεια σε επίπεδο κειμένου ,το οποίο διαχειρίζεται ο τελικός χρήστης, ενώ το δεύτερο σε επίπεδο σύνδεσης μεταξύ υπολογιστών .Στην πραγματικότητα το Ασφαλές Πρωτόκολλο Υπερκείμενου S-HTTP(Secure Hypertext Transfer Protocol) της εταιρείας Commerce Net αποτελεί μια επέκταση του δημοφιλούς πρωτοκόλλου HTTP με επιπλέον χαρακτηριστικά ασφαλείας. Προσφέρει διάφορες τεχνικές για την προστασία των δεδομένων, όπως κρυπτογράφηση με χρήση αλγορίθμων RSA. Οι αλγόριθμοι αυτοί χρησιμοποιούνται κυρίως στις ΗΠΑ. Τα κλειδιά αυτά παράγονται με την χρήση δυο πολύ μεγάλου μήκους πρώτων αριθμών, οι οποίοι είναι σχεδόν

[70] Κωνσταντίνος Μάρκελλος, Πηνελόπη Μαρκέλλου, Μαρία Ρήγκου ,Σπύρος Συρμακέσης, Αθανάσιος Τσακαλιδης,2005*, Ε-Επιχειρηματικότητα,* Ελληνικά Γράμματα, Αθήνα .

αδύνατον να υπολογιστούν. Οι αλγόριθμοι αυτοί προβλέπεται να αποτελέσουν τη βάση για πολλές μεθόδους πληρωμών μέσω δικτύου υπολογιστών.

4.4.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ S/MIME (SECURE/MIME)

Το S/MIME (SECURE/MIME) αναπτύχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων. Το S / MIME (συντόμευση για το "Ασφαλής / MIME") είναι μια έκδοση του πρωτοκόλλου MIME που υποστηρίζει την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου και το περιεχόμενό τους μέσω του δημόσιου κλειδιού κρυπτογράφησης τεχνολογία της RSA. Το S / MIME δημιουργήθηκε το 1995 από μια ομάδα των προμηθευτών λογισμικού για την πρόληψη και την αναχαίτιση πλαστογραφία e-mail, και δεδομένου ότι στηρίζεται στο υπάρχον πρότυπο MIME πρωτόκολλο, μπορεί να ενσωματωθεί εύκολα σε υπάρχοντα προϊόντα e-mail και μηνυμάτων. Σκοπός του είναι η καταπολέμηση της πλαστογραφίας και της υποκλοπής ηλεκτρονικών μηνυμάτων καθώς και η ευκολία στην χρήση.

4.4.4 ΤΟ ΠΡΩΤΟΚΟΛΛΟ PGP (Pretty Good Privacy)

Το PGP (Pretty Good Privacy) το οποίο παρουσιάστηκε το 1991,είναι ένα πλήρες πακέτο ασφάλειας ηλεκτρονικού ταχυδρομείου που παρέχει προστασία απορρήτου πιστοποίηση ταυτότητας ,ψηφιακές υπογραφές ,όλα σε μια εύκολη στη χρήση μορφή. Με λίγα λόγια το PGP (Pretty Good Privacy) επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

Διασφάλιση του απορρήτου: σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.

Πιστοποίηση της ταυτότητας: σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.

Ευκολία: σημαίνει ότι η διασφάλιση του απόρρητου και η πιστοποίησης της

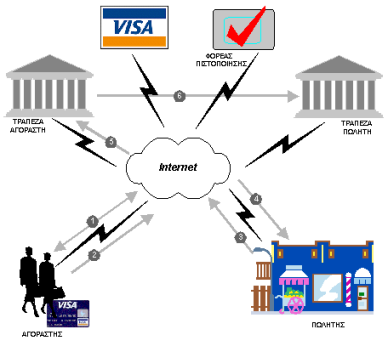
ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία.[71]

Εν συνεχεία, θα προσπαθήσουμε να εξηγήσουμε πως λειτουργεί το πρωτόκολλο PGP μέσω ενός παραδείγματος. Ας υποθέσουμε ότι ένας χρήστης Α θέλει να στείλει μήνυμα Ρ στο ηλεκτρονικό ταχυδρομείου του χρήστη Β. Η διαδικασία είναι η ακόλουθη: Οι δυο χρήστες έχουν τα δικά τους ιδιωτικά κλειδιά (Dx) και δημόσια (Ex) κλειδιά RSA.Θεωρούμε ότι ο ένας γνωρίζει το δημόσιο κλειδί του άλλου εκ των προτέρων. Αρχικά, το πρόγραμμα PGP στον υπολογιστή του Α περνάει το μήνυμα, Ρ, από τη συνάρτηση hash MD5. Στη συνέχεια, το hash κρυπτογραφείται με το ιδιωτικό RSA κλειδί του Α, DA. Όταν ο Β τελικά λάβει το μήνυμα τότε θα μπορέσει να αποκρυπτογραφήσει το hash με το δημόσιο κλειδί, ΕΑ, και να επιβεβαιώσει ότι είναι σωστό. Το κρυπτογραφημένο hash και το αρχικό μήνυμα κατόπιν, διατάσσονται σε ένα νέο μήνυμα Ρ1 και συμπιέζονται ώστε να παραχθεί το Ρ1.Z. Στη συνέχεια, παράγεται τυχαία ένα κλειδί για τον αλγόριθμο IDEA, ΚΜ, το οποίο ισχύει μόνο για την συγκεκριμένη αποστολή ηλεκτρονικού ταχυδρομείου. Το κλειδί αυτό χρησιμοποιείται για τη κρυπτογράφηση του *Ρ*1.*Z* με το IDEA. Επιπλέον, το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του Β. Τα δύο αυτά τμήματα διατάσσονται και αποστέλλονται στο δίκτυο. Όταν ο Β λάβει το μήνυμα, αποκρυπτογραφεί το κλειδί χρησιμοποιώντας το ιδιωτικό του κλειδί RSA (DB). Χρησιμοποιώντας το ΚΜ αποκρυπτογραφεί το μήνυμα που είναι κρυπτογραφημένο με τον αλγόριθμο IDEA και λαμβάνει το *Ρ*1.*Z*. Μετά την αποσυμπίεση ο Β ξεχωρίζει το hash από το καθαρό μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Α. Αν το hash συμφωνεί με τον υπολογισμό MD5 που εκτελεί ο ίδιος τότε γνωρίζει ότι το μήνυμα είναι αυτό που έστειλε ο Α.

[71] *http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/pgp.htm*

4.4.5 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SET (Secure Electronic Transaction)

Οι δυο μεγαλύτεροι οργανισμοί πιστωτικών καρτών, VISA και Mastercard, σε συνεργασία με έναν αριθμό μεγάλων επιχειρήσεων από τον χώρο της πληροφορικής τεχνολογίας, έχουν αναπτύξει το πρωτόκολλο SET, για την ασφαλή πραγματοποίηση συναλλαγών μέσα από ψηφιακά δίκτυα. Το πρωτόκολλο SET χρησιμοποιείται μόνο για την ασφαλή συναλλαγή μέσω πιστωτικών καρτών και επιταγών ανάμεσα στους πελάτες και τους έμπορους .Το πρωτόκολλο SET προσφέρει τις εξής υπηρεσίες: πιστοποίηση, εμπιστευτικότητα, ακεραιότητα του μηνύματος, διασύνδεση του μηνύματος. Στο πρωτόκολλο SET εμπλέκονται τέσσερις φορείς. Ο κάτοχος της κάρτας , ο έμπορος ,η τράπεζα που εκδίδει την πιστωτική κάρτα και η τράπεζα του εμπόρου. Όπως και με αλλά πρωτοκολλά κρυπτογραφήσεις , το SET χρησιμοποιεί ένα δημόσιο/ιδιωτικό ζεύγος κλειδιών και υπογεγραμμένων πιστοποιητικών για να δημιουργήσει κάθε ταυτότητα των μελών που παίρνουν μέρος στην συναλλαγή και για να τους επιτρέψει να στείλουν ιδιωτικά μηνύματα μεταξύ τους.[72]



Κατά τη διάρκεια μιας συναλλαγής πώλησης ενός προϊόντος , το πρωτόκολλο SET λειτούργει ως εξής: Τα πρώτα βήματα, αφορούν ασφαλώς την επιλογή των προϊόντων που θα αγοραστούν . Αυτή μπορεί να γίνεται είτε on-line μέσω κάποιου περιηγητή που τρέχει στον υπολογιστή του αγοραστή ή και σε ειδικής χρήσης υπολογιστή. Όταν ο αγοραστής επιλέξει τα προς αγορά είδη, συμπληρώνει μια φόρμα που περιέχει την περιγραφή των ειδών, τις τιμές τους, τυχόν δαπάνες αποστολής και φόρους. Ο χειρισμός αυτής της φόρμας γίνεται από ειδικό λογισμικό ηλεκτρονικών αγορών, το οποίο δύναται να επιτρέπει ακόμα και τη διαπραγμάτευση εκπτώσεων με βάση το πόσο "καλός πελάτης" είναι ο αγοραστής, το πόσο φτηνότερα έχει κάποιος ανταγωνιστής το ίδιο προϊόν, ειδικές προσφορές, κλπ. Ακολούθως επιλέγεται ο τρόπος πληρωμής. Δεν είναι υποχρεωτικό να χρησιμοποιηθεί πιστωτική κάρτα και Δίκτυο, μπορεί κανείς να διαλέξει μια πιο παραδοσιακή μέθοδο όπως η αντικαταβολή. Ο αγοραστής, λοιπόν, στέλνει στον πωλητή μια εντολή αγοράς μαζί με οδηγίες πληρωμής. Σύμφωνα με το SET, τόσο η εντολή αγοράς (που περιέχει τον

[72] Πομπόρτσης, Ανδρέας Σ., Τσουλφάς, Ανέστης Γ., 2002«*Εισαγωγή στο ηλεκτρονικό εμπόριο»* Εκδόσεις ΤΖΙΟΛΑ, Θεσσαλονίκη.

ακριβή προσδιορισμό των ειδών που αγοράζονται) όσο και οι λεπτομέρειες του τρόπου πληρωμής (αριθμός πιστωτικής κάρτας, αριθμός δόσεων κλπ) αποστέλλονται με κρυπτογράφηση με ψηφιακή υπογραφή που έχει εκδοθεί από κάποιον οργανισμό πιστοποίησης. Όταν ο πωλητής λάβει την εντολή, ζητά επαλήθευση της πληρωμής από το πιστωτικό ίδρυμα του αγοραστή. Όταν αυτή ληφθεί, μια επιβεβαίωση της παραγγελίας αποστέλλεται στον αγοραστή, με όλα τα σχετικά δεδομένα να διακινούνται στο δίκτυο ασφαλώς κρυπτογραφημένα. Παράλληλα, η αίτηση πληρωμής φτάνει στην τράπεζα του αγοραστή η οποία μεταφέρει το ποσό της συναλλαγής σε λογαριασμό του πωλητή, ενώ ξενικά και η εκτέλεση της παραγγελίας (αποστολή των ειδών, εκτέλεση των υπηρεσιών, κλπ). Τέλος, ο πωλητής απευθύνεται στο πιστωτικό του ίδρυμα για την λήψη της πληρωμής και η συναλλαγή έχει ολοκληρωθεί. Το SET εξασφαλίζει ότι όλη η παραπάνω διαδικασία έχει γίνει με πλήρη "ηλεκτρονική εχεμύθεια".[73]

4.4.6 ΤΟ ΠΡΩΤΟΚΟΛΛΟ IPsec (Internet Protocol Security)

Όπως ήδη έχουμε αναφέρει το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος της IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων, προσφέροντας υπηρεσίες πιστοποίησης ταυτότητας και εξασφάλισης απορρήτου σε επίπεδο IP. Ακόμα σημαντικότερο είναι ότι το σύστημα είναι ευέλικτο και επεκτάσιμο. Για παράδειγμα, μια εφαρμογή που χρησιμοποιεί IPsec μπορεί να επιλέξει αν θα χρησιμοποιεί μια βοηθητική λειτουργία πιστοποίησης ταυτότητας που θα επικυρώνει τον αποστολέα, ή αν θα χρησιμοποιεί μια βοηθητική λειτουργία κρυπτογράφησης η οποία θα εξασφαλίζει επίσης το απόρρητο για το ωφέλιμο φορτίο, οι επιλογές αυτές μπορεί να είναι ασύμμετρες (για παράδειγμα, πιστοποίηση ταυτότητας προς τη μια κατεύθυνση, αλλά όχι προς την άλλη). Επιπλέον, το IPsec δεν περιορίζει το χρήστη σε ένα συγκεκριμένο αλγόριθμο κρυπτογράφησης ή πιστοποίησης ταυτότητας. Αντίθετα, παρέχει ένα γενικό πλαίσιο που επιτρέπει σε οποιοδήποτε ζεύγος επικοινωνούντων ακραίων σημείων να

[73] http://conta.uom.gr/conta/ekpaideysh/seminaria/thlematikes/security/SET_buying.htm

διαλέξουν αλγορίθμους και παραμέτρους (π.χ. το μέγεθος του κλειδιού) που αυτοί θεωρούν ότι παρέχουν την καταλληλότερη ασφάλεια για την επικοινωνία τους.[74]

4.4.7 ΤΟ ΠΡΩΤΟΚΟΛΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΚΕΡΒΕΡΟΣ (Kerberos Authentication System)

Ένα πρωτόκολλο πιστοποίησης ταυτότητας που χρησιμοποιείτε σε πολλά πραγματικά συστήματα είναι το Kerberos, το οποίο βασίζεται σε μια παραλλαγή του αλγορίθμου Needham- Schoeder. Το πρωτόκολλο πήρε το όνομα του από το πολυκέφαλο σκύλο της Ελληνικής μυθολογίας που φύλαγε την είσοδο του Άδη .Το Kerberos σχεδιάστηκε στο M.I.T για να επιτρέπει τους χρήστες των σταθμών εργασίας να προσπελάζουν με ασφάλεια τους πόρους του δικτύου.[75] Οι εκδόσεις 1 έως και 3 του KERBEROS χρησιμοποιούνταν μόνο εσωτερικά στο MIT. Η έκδοση 4 (V4) διατέθηκε δημόσια και χρησιμοποιήθηκε ευρύτατα. Η ανάπτυξη της έκδοσης 5 (V5) ξεκίνησε το 1989, ως αποτέλεσμα συζητήσεων μεταξύ διαχειριστών συστημάτων, χρηστών και της ομάδας ανάπτυξης, και προδιαγράφηκε για χρήση στο Internet το Σεπτέμβριο του 1993. Σήμερα, τόσο η έκδοση 4 όσο και η έκδοση 5 Kerberos του διανέμονται από διάφορους κατασκευαστές.

Το Kerberos επιτρέπει στις δικτυακές εφαρμογές να αναγνωρίζουν με ασφάλεια την ταυτότητα του χρήστη που ζητά εξυπηρέτηση, χωρίς να στέλνει στο δίκτυο δεδομένα που μπορούν να επιτρέψουν σε ένα πιθανό εισβολέα να προσποιηθεί ότι είναι ο χρήστης και χωρίς να βασίζεται στις διευθύνσεις των μηχανών του δικτύου. Πιο συγκεκριμένα, λειτουργεί παρέχοντας "εισιτήρια" τα οποία οι συμμετέχοντες μπορούν να χρησιμοποιήσουν για να αποδείξουν την ταυτότητά τους, και μυστικά κλειδιά για ασφαλείς επικοινωνίες μεταξύ των συμμετεχόντων. Οι αποδείξεις εκδίδονται από ένα αφιερωμένο υπολογιστή που καλείται authentication server (AS). Ο AS αυθεντικοποιεί τους χρήστες κατά τη σύνδεσή τους και τους εφοδιάζει με ένα εισιτήριο. Αυτό το εισιτήριο μπορεί να χρησιμοποιηθεί για την έκδοση εισιτηρίων από έναν

[74] DOUGLAS E. COMER,2010 «*ΔΙΑΔΙΚΤΥΟ με TCP/IP ΑΡΧΕΣ, ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ*»,4Η Αμερικάνικη έκδοση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, Αθήνα.
[75] Andrew S. Tanenbaum, 2003 *«Δίκτυα Υπολογιστών»* Εκδόσεις Κλειδάριθμος, Αθήνα.

εξυπηρετητή έκδοσης εισιτηρίων τα οποία στη συνέχεια μπορούν να χρησιμοποιηθούν ως διαπιστευτήρια για την επαφή με άλλους εξυπηρετητές. Τέλος, να πούμε ότι κάθε απόδειξη έχει περιορισμένη διάρκεια ζωής και όταν το χρονικό αυτό διάστημα περάσει τότε είναι άχρηστο.[76] Το Kerberos βασίζεται στην κρυπτογραφία συμμετρικού κλειδιού και προαιρετικά μπορεί να χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού , χρησιμοποιώντας ασύμμετρη κρυπτογράφηση κατά τη διάρκεια ορισμένων φάσεων της ταυτότητας. Για την ανταλλαγή των μηνυμάτων ο Kerberos εκμεταλλεύεται το IP επίπεδο σε συνδυασμό με το UDP πρωτόκολλο.[77]

[76] http://www.scribd.com/doc/36358788/8/Kerberos

[77] http://translate.google.gr/translate?hl=el&langpair=en|el&u=http://en.wikipedia.org/wiki/Kerberos_(protocol)

ΚΕΦΑΛΑΙΟ 5

ΘΕΣΜΙΚΟ ΠΛΑΣΙΟ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΓΕΝΙΚΑ

Η αυξανομένη χρήση του διαδικτύου ως μέσο διεξαγωγής συναλλαγών και αγοραπωλησιών έχει προκαλέσει σημαντικές αλλαγές στη μορφή των αγορών και έχει δημιουργήσει νέους τομείς στους οποίους χρειάζεται η παρέμβαση του κράτους. Οι απόφαση για το τι είδους προϊόντα και υπηρεσίες θα προσφερθούν μέσω του διαδικτύου εναπόκειται στους ίδιους τους καταναλωτές και τις επιχειρήσεις. Καθήκον των κυβερνήσεων είναι η διασφάλιση ενός ρυθμιστικού πλαισίου για τις ηλεκτρονικές συναλλαγές το οποίο να είναι ευέλικτο και προσαρμόσιμο στις συνεχείς μεταβολές του τομέα των ηλεκτρονικών συναλλαγών και το οποίο να επιτρέπει την ελεύθερη διαμόρφωση των συμβάσεων.[78] Όμως η νομοθεσία βρέθηκε απροετοίμαστη σε παγκόσμιο επίπεδο στην απότομη τεχνολογική ανάπτυξη και στην αρχική ραγδαία εξάπλωση του ηλεκτρονικού εμπορίου και αποδείχτηκε ελλιπής και αδύναμη να προσαρμοστεί γρήγορα στα νέα δεδομένα.

Ο βασικός λόγος που οδήγησε στην ύπαρξη του νομικού κενού είναι η ίδια η φύση του διαδικτύου. Τα χαρακτηριστικά είναι τέτοια που δεν επιτρέπουν η προϋπάρχουσα νομολογία αναφορικά με τις συναλλαγές και όλα τα συναφή νομικά ζητήματα ,να εφαρμοστεί στις ηλεκτρονικές συναλλαγές .Επίσης, τα χαρακτηριστικά του διαδικτύου εμποδίζουν την καθολική εφαρμογή της ισχύουσας νομοθεσίας. Το διαδίκτυο εξαπλώνεται σε όλο τον κόσμο και καταλύει τα σύνορα. Δημιουργεί μια νέα αγορά στην οποία μπορεί να έχουν πρόσβαση και να είναι υποψήφιοι συναλλασσόμενοι, άνθρωποι από κάθε γωνία του πλανήτη. Στο συγκεκριμένο κεφάλαιο θα εξετάσουμε το νομικό πλαίσιο σε επίπεδο Ευρωπαϊκής Ένωσης αλλά και της ελληνικής νομοθεσίας που σχετίζονται άμεσα ή έμμεσα με τον ευρύτερο χώρο των ηλεκτρονικών συναλλαγών.

[78] Γιάννης Κατσουλάκος, 2001 *« Νέα οικονομία, Διαδίκτυο και Ηλεκτρονικό εμπόριο»* Εκδόσεις ΚΕΡΚΥΡΑ.

5.1 ΕΥΡΩΠΑΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Δεδομένων των προβλημάτων που δημιουργεί η ίδια η φύση του Διαδικτύου στις όποιες προσπάθειες νομοθετικής ρύθμισης των εμπορικών πράξεων που μετέρχονται ηλεκτρονικών μέσων προκειμένου να υλοποιηθούν, η Ευρωπαϊκή Ένωση προχωρά σταδιακά σε μια συντονισμένη προσπάθεια αντιμετώπισης του προβλήματος με την σταδιακή δημιουργία ενός νομικού πλαισίου που θα θέσει τις βάσεις για μια ολοκληρωμένη ρύθμιση των ηλεκτρονικών συναλλαγών σε κάθε επίπεδο αλλά και για τη σταδιακή αποδοχή του από το καταναλωτικό κοινό.

5.1.1 ΕΥΡΩΠΑΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗ ΡΥΘΜΙΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Κανονισμός (ΕΚ) αριθ. 2560/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19ης Δεκεμβρίου 2001 σχετικά με τις διασυνοριακές πληρωμές σε ευρώ.

Ο παρών κανονισμός θεσπίζει κανόνες σχετικά με τις διασυνοριακές πληρωμές σε ευρώ προκειμένου να εξασφαλιστεί ότι το κόστος για τις πληρωμές αυτές είναι ίδιο με το κόστος των πληρωμών σε ευρώ που πραγματοποιούνται στο εσωτερικό κράτους μέλους. Ως διασυνοριακές πληρωμές ο παρόν ορισμός θεωρεί τις διασυνοριακές μεταφορές πίστωσης, τις διασυνοριακές επιταγές και τις διασυνοριακές πράξεις ηλεκτρονικής πληρωμής. Ειδικότερα, οι διασυνοριακές πράξεις ηλεκτρονικής πληρωμής στις οποίες και επικεντρώνεται η παρούσα ανάλυση ορίζονται ως:

- οι διασυνοριακές μεταφορές χρηματικών ποσών με μέσο ηλεκτρονικής πληρωμής, εκτός από εκείνες τις οποίες εντέλλονται και εκτελούνται από ιδρύματα, και

- οι διασυνοριακές αναλήψεις μετρητών με μέσο ηλεκτρονικής πληρωμής καθώς και η φόρτιση (και αποφόρτιση) υποθέματος ηλεκτρονικού χρήματος σε μηχανήματα αυτόματης ανάληψης και σε αυτόματες ταμειολογιστικές μηχανές στα καταστήματα του εκδότη ή ενός ιδρύματος που έχει συμβατική υποχρέωση να αποδέχεται το μέσο πληρωμής.

Είναι επομένως προφανές ότι οι διατάξεις του συγκεκριμένου κανονισμού δεν αφορούν μόνο στα τραπεζικά ιδρύματα αλλά και σε άλλες ατομικές ή εταιρικές επιχειρήσεις που εκτελούν διασυνοριακές πληρωμές καθώς με βάση την Οδηγία 200/46/ΕΚ, που αναλύουμε στη συνέχεια, στην έννοια του πιστωτικού ιδρύματος εμπίπτουν και τα ιδρύματα ηλεκτρονικού χρήματος. Ο Κανονισμός ορίζει τα έξοδα που επιβάλλονται από τα πιστωτικά ιδρύματα κατά την πραγματοποίηση διασυνοριακών πληρωμών ενώ ορίζονται και οι πληροφορίες που πρέπει να παρέχονται στους καταναλωτές. Έτσι, κάθε ίδρυμα παρέχει εκ των προτέρων στους πελάτες του, με άμεσα κατανοητή μορφή, γραπτώς, καθώς και κατά περίπτωση, βάσει των εθνικών κανόνων, με ηλεκτρονικά μέσα, πληροφορίες σχετικά με τα έξοδα που επιβάλλει για διασυνοριακές πληρωμές και για πληρωμές στο εσωτερικό του κράτους μέλους στο οποίο είναι εγκατεστημένο.

Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις. Η παρούσα οδηγία έχει ως αντικείμενο την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών, οι οποίες αφορούν τις εξ αποστάσεως συμβάσεις μεταξύ καταναλωτών και προμηθευτών. Ως εξ αποστάσεων σύμβαση ορίζεται κάθε σύμβαση μεταξύ ενός προμηθευτή και ενός καταναλωτή που αφορά αγαθά ή υπηρεσίες, η οποία συνάπτεται στα πλαίσια ενός συστήματος πωλήσεων ή παροχής υπηρεσιών εξ αποστάσεως, που οργανώνεται από τον προμηθευτή, ο οποίος, με τη σύμβαση αυτή, χρησιμοποιεί αποκλειστικά ένα ή περισσότερα μέσα επικοινωνίας εξ αποστάσεως έως τη σύναψη της συμβάσεως, συμπεριλαμβανομένης και αυτής καθεαυτής της σύναψης της συμβάσεως.

Τα κίνητρα για τη ρύθμιση των εξ αποστάσεων συμβάσεων εντοπίζονται στο γεγονός ότι η διασυνοριακή πώληση εξ αποστάσεως μπορεί να είναι μια από τις

κυριότερες εκδηλώσεις της ολοκλήρωσης της εσωτερικής αγοράς για τους καταναλωτές καθώς και στο γεγονός ότι η καθιέρωση νέων τεχνολογιών συνεπάγεται πολλαπλασιασμό των μέσων που τίθενται στη διάθεση των καταναλωτών για να γνωρίσουν τις προσφορές που γίνονται σε ολόκληρη την Κοινότητα. Δεδομένου ότι ορισμένα κράτη μέλη έχουν ήδη λάβει διαφορετικά ή αποκλίνοντα μέτρα προστασίας των καταναλωτών στον τομέα της πώλησης εξ αποστάσεως με αρνητικές συνέπειες για τον ανταγωνισμό μεταξύ των επιχειρήσεων στην ενιαία αγορά κρίθηκε αναγκαίο να θεσπιστεί ελάχιστο σύνολο κοινών κανόνων σε κοινοτικό επίπεδο στον τομέα αυτόν. Η Οδηγία 97/7/ΕΚ ρυθμίζει τις πληροφορίες που πρέπει να παρέχονται πριν και μετά τη σύναψη της σύμβασης καθώς και τους τρόπους με τους οποίους μπορεί να προστατευθεί ο καταναλωτής όταν έχει πληρώσει με τη πιστωτική του κάρτα ή όταν του παρέχονται υπηρεσίες και αγαθά που δεν έχει ζητήσει.

Οδηγία 2000/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαρτίου 2000 σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων.

Οδηγία 2000/28/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την τροποποίηση της οδηγίας 2000/12/ΕΚ σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων. Η Οδηγία 2000/28/ΕΚ τροποποιεί την οδηγία 2000/12/ΕΚ σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων προσθέτοντας διατάξεις σχετικά με το ηλεκτρονικό χρήμα.

Ειδικότερα: στον ορισμό «Πιστωτικό ίδρυμα» αναφέρει ότι είναι:

- επιχείρηση της οποίας η δραστηριότητα συνίσταται στην αποδοχή από το κοινό καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων και στη χορήγηση πιστώσεων για ίδιο λογαριασμό, ή
- ίδρυμα ηλεκτρονικού χρήματος κατά την έννοια της οδηγίας 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Σεπτεμβρίου 2000, για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.

Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική αγορά «Οδηγία για το ηλεκτρονικό εμπόριο». Η Οδηγία ορίζει ως «ίδρυμα ηλεκτρονικού χρήματος» μια επιχείρηση ή άλλου τύπου νομικό πρόσωπο εκτός του πιστωτικού ιδρύματος κατά την έννοια του άρθρου 1, σημείο 1, πρώτο εδάφιο στοιχείο α) της οδηγίας 2000/12/ΕΚ, η οποία εκδίδει μέσα πληρωμής υπό μορφή ηλεκτρονικού χρήματος. Επίσης, η Οδηγία αυτή ορίζει και την έννοια του ηλεκτρονικού χρήματος ως νομισματική αξία, η οποία αντιστοιχεί σε απαίτηση έναντι του εκδότη και:

α) είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα,

β) έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού και

γ) γίνεται δεκτή ως μέσο πληρωμής από επιχειρήσεις άλλες, πέραν της εκδότριας.»

Επίσης, με βάση την συγκεκριμένη Οδηγία ρυθμίζεται πότε και πώς μπορεί ο κομιστής ηλεκτρονικού χρήματος να ζητήσει την εξαργύρωση του στην ονομαστική αξία σε κέρματα και χαρτονομίσματα ή με μεταφορά σε τραπεζικό λογαριασμό. Ρυθμίζονται οι περιορισμοί στην έκδοση ηλεκτρονικού χρήματος καθώς και οι κυρώσεις που συνεπάγεται η παραβίαση του νόμου. Ενώ ρυθμίζονται και οι όροι και προϋποθέσεις ίδρυσης και λειτουργίας ιδρυμάτων ηλεκτρονικού χρήματος

Σύσταση της Επιτροπής 87/598/ΕΟΚ της 8ης Δεκεμβρίου 1987 για ευρωπαϊκό κώδικα δεοντολογίας σε θέματα ηλεκτρονικών πληρωμών (Σχέσεις μεταξύ χρηματοπιστωτικών οργανισμών, εμπόρων ή άλλων παρεχόντων υπηρεσίες και καταναλωτών). Ο κώδικας συνοψίζει τους όρους που πρέπει να πληρούνται για να

καταστεί δυνατή η ανάπτυξη των νέων μέσων ηλεκτρονικής πληρωμής προς όφελος των οικονομικών εταίρων, να εξασφαλιστεί ασφάλεια και ευκολία χρήσης στους καταναλωτές, μεγαλύτερη παραγωγικότητα και αυξημένη ασφάλεια στους παρέχοντες υπηρεσίες και τους εκδότες των καρτών πληρωμής. Οι βασικές αρχές του κώδικα σχετίζονται με:

- τους όρους των συμβάσεων που καταρτίζονται μεταξύ εκδοτών και καταναλωτών,
- τη διαλειτουργικότητα του συστήματος προκειμένου οι κάρτες που εκδίδονται σε ένα κράτος να μπορούν να χρησιμοποιηθούν σε άλλα,
- τον εξοπλισμό που απαιτείται από τους παρόχους υπηρεσιών ηλεκτρονικών πληρωμών
- Την προστασία των δεδομένων τα οποία διαβιβάζονται, τη στιγμή της πληρωμής, στην τράπεζα του παρέχοντος υπηρεσίες και στη συνέχεια στον εκδότη. Τα δεδομένα αυτά δεν πρέπει σε καμία περίπτωση να θέσουν σε κίνδυνο την προστασία της ιδιωτικής ζωής και περιορίζονται αυστηρά στα στοιχεία που προβλέπονται συνήθως για τις επιταγές και τις μεταφορές ποσών από λογαριασμό σε λογαριασμό.
- Τη δίκαιη πρόσβαση στο σύστημα ηλεκτρονικών πληρωμών σε όσους παρέχονται υπηρεσίες, όποια και αν είναι η οικονομική τους σημασία. Ο αποκλεισμός από την πρόσβαση δεν είναι δυνατός παρά μόνο για νομικούς λόγους.

Σύσταση της Επιτροπής 88/590/ΕΟΚ της $17_{ης}$ Νοέμβριου 1988 που αφορά τα συστήματα πληρωμών και ιδίως τις σχέσεις μεταξύ κατόχου και εκδότη κάρτας.

Σύσταση 97/489/ΕΚ καλύπτει τις συναλλαγές που διενεργούνται με ηλεκτρονικά μέσα πληρωμής . Τα μέσα αυτά περιλαμβάνουν εκείνα που επιτρέπουν την (εξ΄ αποστάσεως) πρόσβαση στο λογαριασμό ενός πελάτη ιδίως τις κάρτες πληρωμής και τις μέσω τηλεφώνου ή κατ οίκον τραπεζικές εργασίες. [79]

[79] Το νομικό πλαίσιο που αφορά τις ηλεκτρονικές συναλλαγές και την ηλεκτρονική υπογραφή στην Ευρωπαϊκή Ένωση βρίσκεται αναρτημένο στον επίσημο διαδικτυακό κόσμο της Ευρωπαϊκής Ένωσης http://europa.eu/index_el.htm

5.1.2 ΕΥΡΩΠΑΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ

Κανονισμός 44/2001 ΕΚ για την διεθνή δικαιοδοσία (σε αντικατάσταση της Σύμβασης των Βρυξελλών), που αναγνωρίζει το κύρος της ηλεκτρονικής υπογραφής σε συμφωνίες παρέκτασης της διεθνούς δικαιοδοσίας.

Στόχος της οδηγίας είναι η θέσπιση νομικού πλαισίου για τις ηλεκτρονικές υπογραφές και υπηρεσίες πιστοποίησης και η διευκόλυνση της χρήσης σε κοινοτικό επίπεδο των ηλεκτρονικών υπογραφών. Ανοίγει νέους ορίζοντες δραστηριοποίησης για τους παρόχους υπηρεσιών οι οποίοι δρώντας σε διασυνοριακό επίπεδο θα μπορούν να αυξήσουν την ανταγωνιστικότητά τους και να προσφέρουν έτσι στους καταναλωτές και στις επιχειρήσεις νέες ευκαιρίες ασφαλούς ανταλλαγής πληροφοριών και ηλεκτρονικών συναλλαγών, ανεξαρτήτως συνόρων.

Απόφαση της Επιτροπής (2001) για έγκριση ενός παγκοσμίου δικτύου για την πιστοποίηση των ηλεκτρονικών υπογραφών και άλλων συναλλαγών ηλεκτρονικού εμπορίου

Απόφαση 2000/709 της Επιτροπής για τους φορείς ελέγχου και συμμόρφωσης των διατάξεων δημιουργίας της ηλεκτρονικής υπογραφής στους όρους ασφάλειας του Παραρτήματος ΙΙΙ της Οδηγίας 99/93/ΕΚ

Προεδρικό διάταγμα 150/2000 της 25ης Ιουνίου 2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές [80]

5.2 ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΣΤΗΝ ΕΛΛΑΔΑ

Στην Ελλάδα, οι αρμόδιες αρχές έχουν περιοριστεί στην συμμόρφωση του εσωτερικού δικαίου προς τα ευρωπαϊκά νομοθετήματα που ήδη ισχύουν. Πέραν δε

[80] *Βλέπε υποσημείωση 79*

της νομολογίας που έχει ρυθμίσει ειδικότερα πρακτικά ζητήματα δεν υπάρχουν νομοθετήματα προσαρμοσμένα στις ιδιαιτερότητες της ελληνικής αγοράς. Παρακάτω γίνεται εκτενέστερη ανάλυση του νομοθετικού πλαισίου.

5.2.1 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΡΥΘΜΙΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Νόμος Υπ΄ Αριθμό 3148/2003 Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων: Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων, αντικατάσταση και συμπλήρωση των διατάξεων για τα ιδρύματα ηλεκτρονικού χρήματος και άλλες διατάξεις.

Προεδρικό Διάταγμα 33/2000: Προσαρμογή της Ελληνικής νομοθεσίας προς την Οδηγία 27.1.1997 για τις διασυνοριακές μεταφορές πιστώσεων.

Υπουργική απόφαση Ζ1-178/2001: Συναλλαγές που γίνονται με κάρτες-Εναρμόνιση με τις διατάξεις της Σύστασης 97/489/ΕΚ της Επιτροπής-Καταναλωτική Πίστη – Προσαρμογή της Κοινής Υπουργικής Απόφασης Φ1-983/91 προς τις διατάξεις της Οδηγίας 98/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου. Η υπουργική αυτή απόφαση αναφέρεται στις συναλλαγές που γίνονται με κάρτες. Εναρμονίζει την ελληνική νομοθεσία με ορισμένες διατάξεις της σύστασης 97/489/ΕΚ. Ορίζει την κάρτα, τον εκδότη και τον κάτοχο αυτής. Καταγράφει τις υποχρεώσεις του κατόχου της κάρτας, όπως αυτήν της ασφαλής φύλαξης της κάρτας και των μέσων που επιτρέπουν τη χρησιμοποίησή της καθώς και τις ευθύνες του. Προβλέπει ότι ο κάτοχος, από το χρόνο που γνωστοποιεί στον εκδότη απώλεια ή κλοπή της κάρτας, δεν φέρει ευθύνη για τις επακόλουθες ζημίες, εκτός εάν έχει ενεργήσει με δόλο.

Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: Καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών. Ειδικότερα περιλαμβάνονται οι ορισμοί των εννοιών ηλεκτρονική πληρωμή, ηλεκτρονικό χρήμα, πιστωτικός κίνδυνος, διαχειριστής συστημάτων πληρωμών καθώς και άλλες βασικές έννοιες. Στην Πράξη αυτή ορίζεται το σύστημα πληρωμών ως σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα

με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μία περιοχή, συνήθως σε μία χώρα. Υπό την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει: (ί) τα πιστωτικά ιδρύματα και τους χρηματοδοτικούς οργανισμούς, (ίί) τα μη πιστωτικά ιδρύματα που παρέχουν υπηρεσίες για τη διενέργεια πληρωμών, (ίίί) την τεχνική υποδομή, (ίν) το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, (ν) τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και (νί) τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος.

Επιπλέον, η Πράξη Αριθ. 50/31.7.2002 προσδιορίζει τις γενικές αρχές λειτουργίας των συστημάτων ηλεκτρονικού χρήματος καθώς και την σκοπιμότητα της άσκησης εποπτείας από μέρους της Τράπεζας της Ελλάδος. Τέλος, η Πράξη προσδιορίζει τα στοιχεία που πρέπει να υποβάλλονται από τους διαχειριστές συστημάτων πληρωμών και ηλεκτρονικού χρήματος στην Τράπεζα της Ελλάδος, Διεύθυνση Νομισματικής Πολιτικής και Τραπεζικών Εργασιών, Γραφείο Επίβλεψης Συστημάτων Πληρωμών πριν από την έναρξη λειτουργίας τους, σε εξαμηνιαία βάση, σε ετήσια βάση, και σε περιπτώσεις έκτακτων περιστατικών.

Πράξη Διοικητή Αριθ. 2501/31.10.2002: Ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους.[81]

5.2.2 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ

Προεδρικό διάταγμα 150/2001 της 25ης Ιουνίου 2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. Το Προεδρικό Διάταγμα ενσωματώνει στην ελληνική νομοθεσία την οδηγία 99/93/ΕΚ. Η οδηγία υποχρεώνει τα κράτη μέλη για σύσταση φορέων επιτήρησης. Η Ελλάδα συμμορφώθηκε με την υποχρέωση και όρισε την ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και

[81] E-business forum ‚Ε' κύκλος εργασιών :ομάδα εργασίας Ε3, Ηλεκτρονικές Πληρωμές: Προβλήματα και προοπτικές http://www.ebusinessforum.gr/

Ταχυδρομείων) ως την αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα παροχών υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, και για τη διαπίστωση της συμμόρφωσης προς τις «ασφαλείς διατάξεις δημιουργίας υπογραφής». Ακόμη, η ΕΕΤΤ είναι αρμόδια για τον ορισμό και την εποπτεία ιδιωτικών ή δημόσιων φορέων για τη διαπίστευση των παρόχων πιστοποίησης όσο και για τη διαπίστωση της συμμόρφωσης προς τις «ασφαλείς διατάξεις δημιουργίας υπογραφής». Στους παρόχους που παρανομούν ενεργώντας ως διαπιστευμένοι ενώ δεν είναι, η ΕΕΤΤ επιβάλλει πρόστιμα που μπορεί να φτάσουν έως και τις 300.00 ευρώ. Το προεδρικό διάταγμα ορίζει τους τύπους των ηλεκτρονικών υπογραφών.

Στο Προεδρικό Διάταγμα ρητώς αναφέρεται ο τύπος της αναγνωρισμένης ηλεκτρονικής υπογραφής και για τις έννομες συνέπειές αυτής, αναφέρει ότι η προηγμένη η-υπογραφή με αναγνωρισμένο πιστοποιητικό και δημιουργημένη από ασφαλή διάταξη επέχει θέση ιδιόχειρης, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο. Επίσης, δεν αποκλείει τη νομική ισχύ η-υπογραφών οι οποίες δε διαθέτουν τα παραπάνω χαρακτηριστικά. Σχετική νομολογία αποτελεί ότι ένα ηλεκτρονικό μήνυμα (e-mail), το οποίο βεβαιώνει την αναγνώριση ενός χρέους, μπορεί να θεωρηθεί ισοδύναμο χειρόγραφης υπογραφής. Σε ότι αφορά την ευθύνη των παρόχων υπηρεσιών πιστοποίησης υπάρχει πιστή μεταφορά της οδηγίας. Το ίδιο συμβαίνει και με την προστασία δεδομένων, όπου όμως υπάρχουν και πρόσθετοι κανόνες για τους παρόχους, όπως η υποχρέωσή τους να αναφέρουν σε ετήσια βάση στην ΕΕΤΤ τα μέτρα που λαμβάνουν για την προστασία αρχειοθετημένων, αποθηκευμένων πληροφοριών. Οι ισχύοντες όροι για αναγνωρισμένα πιστοποιητικά, οι ισχύοντες όροι για παρόχους υπηρεσιών πιστοποίησης που τα εκδίδουν, οι απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής και οι συστάσεις για την ασφαλή επαλήθευση της υπογραφής έχουν αντιγραφεί πιστά από τα παραρτήματα της οδηγία. Η εκ των προτέρων αδειοδότηση παροχών απαγορεύεται ρητά (η καταχώρηση υπηρεσιών πιστοποίησης στην ΕΕΤΤ κοστίζει 300 ευρώ).

Κανονισμοί Ε.Ε.Τ.Τ 248/71 για την παροχή Πιστοποίησης ηλεκτρονικής υπογραφής

Προεδρικό διάταγμα 342/2002 για την διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ δημοσίων υπηρεσιών, ΝΠΔΔ, ΟΤΑ, ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων. Το ΠΔ 342/2002 καθιστά τα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) νόμιμα μέσα συναλλαγής και πληροφόρησης. Όμως, μόνο αν αυτά φέρουν ψηφιακή υπογραφή μπορούν να συνδέονται με την παραγωγή έννομων αποτελεσμάτων ή με την άσκηση δικαιώματος. Αλλιώς, τα διακινούμενα έγγραφα (μεταξύ Δημοσίου, ΝΠΔΔ , ΟΤΑ και ιδιωτών) με ηλεκτρονικό ταχυδρομείο περιορίζονται σε έγγραφα που έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, στατιστικές μελέτες, οδηγίες, αιτήσεις παροχής πληροφοριών και απαντήσεις.

Προεδρικό διάταγμα 39/2001 για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας σε συμμόρφωση προς τις Οδηγίες 98/34/ΕΚ&98/48/ΕΚ.[82]

[82] E-business forum ‚Ε' κύκλος εργασιών :ομάδα εργασίας Ε3, Ηλεκτρονικές Πληρωμές: Προβλήματα και προοπτικές http://www.ebusinessforum.gr/

ΚΕΦΑΛΑΙΟ 6^0 ΠΛΑΙΣΙΟ ΕΡΕΥΝΑΣ

6.1 ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΕΜΠΕΙΡΙΚΗ ΕΦΑΡΜΟΓΗ

Είναι γνωστό ότι η μεθοδολογία που θα ακολουθείται κάθε φορά προσδιορίζεται, κυρίως, από τις ιδιαιτερότητες και τους επιμέρους στόχους της εκάστοτε έρευνας. Στην προκειμένη περίπτωση ο προσανατολισμός σε αποκλειστικά ποσοτική κατεύθυνση δεν θα μπορούσε να δώσει μια εικόνα βάθους ως προς τις μεθόδους ασφάλειας των ηλεκτρονικών συναλλαγών που χρησιμοποιούν επιλεγμένες επιχειρήσεις. Προκειμένου να καταστεί δυνατή η διείσδυση στην καθημερινότητα των επιχειρήσεων που προωθούν τα προϊόντα τους μέσω ιντερνέτ επιλέχτηκε μικρός αριθμός επιχειρήσεων για μια σε βάθος μελέτη. Το ερευνητικό - μεθοδολογικό πλαίσιο για τη μελέτη είναι η μελέτη περίπτωσης των επιχειρήσεων.

6.2 ΠΕΡΙΠΤΩΣΗΣ ΜΕΛΕΤΗΣ

$1^η$ Περίπτωση

MULTIRAMA

Η Multirama ήταν το πρώτο εξειδικευμένο Δίκτυο Καταστημάτων Πληροφορικής που παρουσιάστηκε στην Ελληνική αγορά. Η εξέλιξη της εταιρίας συμπορεύτηκε με την ανάπτυξη και τις εξελίξεις στις αγορές της Πληροφορικής και της Υψηλής Τεχνολογίας με στόχο την πλήρη κάλυψη του πελάτη σε προϊόντα πληροφορικής και ψηφιακής τεχνολογίας.

Ασφάλεια συναλλαγών & Προσωπικά δεδομένα

Η Εταιρία αναγνωρίζει τη σημασία του θέματος της ασφαλείας των Προσωπικών Δεδομένων, καθώς και των ηλεκτρονικών συναλλαγών και έχει λάβει όλα τα απαραίτητα μέτρα, με τις πιο σύγχρονες και προηγμένες μεθόδους, ώστε να εξασφαλίζεται η μέγιστη δυνατή ασφάλεια. Όλες οι πληροφορίες, οι οποίες

σχετίζονται με τα προσωπικά στοιχεία των χρηστών, διασφαλίζονται ως απόρρητες.

Η Multirama χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128-bit (την πιο ισχυρή σήμερα), για ασφαλείς online εμπορικές συναλλαγές. Με αυτόν τον τρόπο κρυπτογραφούνται όλες οι προσωπικές πληροφορίες του πελάτη, συμπεριλαμβάνοντας τον αριθμό της πιστωτικής κάρτας, το όνομα και την διεύθυνση του, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχτούν κατά την μεταφορά τους στο Internet. Τα στοιχεία των χρηστών (όνομα, επάγγελμα, ηλεκτρονική διεύθυνση, διεύθυνση κατοικίας, κλπ.) και των συναλλαγών των χρηστών του ηλεκτρονικού καταστήματος θεωρούνται απόρρητα, όπως και στις συνήθεις συναλλαγές σε εμπορικό κατάστημα.

Μόνο εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση στις πληροφορίες των συναλλαγών και μόνο όποτε αυτό είναι αναγκαίο, π.χ. για τη διεκπεραίωση των παραγγελιών. Κατά τα λοιπά, η Multirama δεσμεύεται να μην αποκαλύψει τα στοιχεία των πελατών και των συναλλαγών τους, εκτός αν έχει έγγραφη εξουσιοδότηση από τους ίδιους, ή αυτό επιβάλλεται από δικαστική απόφαση ή απόφαση άλλης δημόσιας αρχής. Τα προσωπικά δεδομένα που δηλώνονται στο ηλεκτρονικό κατάστημα με το εμπορικό σήμα Multirama χρησιμοποιούνται αποκλειστικά από αυτό ή συνεργαζόμενες με αυτό επιχειρήσεις, με σκοπό την υποστήριξη, προώθηση και εκτέλεση της συναλλακτικής σχέσης. Το σύνολο των εγγράφων και ηλεκτρονικών στοιχείων που θα ανταλλαχθούν μεταξύ των μερών στα πλαίσια της πώλησης θα τηρούνται από την Multirama . Ο πελάτης μπορεί να έχει πρόσβαση σε αυτά εφόσον το επιθυμεί.

2η Περίπτωση

ΕΥΡΩΓΝΩΣΗ

Το ηλεκτρονικό κατάστημα www.eurognosibooks.com είναι ένα ηλεκτρονικό κατάστημα πώλησης προϊόντων και υπηρεσιών μέσω του Διαδικτύου που δημιούργησε η ανώνυμη εταιρεία με τον διακριτικό τίτλο «ΕΥΡΩΠΑΪΚΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΣ ΟΜΙΛΟΣ ΕΥΡΩΓΝΩΣΗ Α.Ε.»

Ασφάλεια

Το ηλεκτρονικό κατάστημα www.eurognosibooks.com χρησιμοποιεί το

πρωτόκολλο SSL, με κρυπτογράφηση 40-256bit, για ασφαλείς online εμπορικές συναλλαγές. Με το πρωτόκολλο αυτό κρυπτογραφούνται όλες οι πληροφορίες της συναλλαγής και προστατεύονται. Όταν η πληρωμή γίνεται με πιστωτική κάρτα, γίνεται επεξεργασία της πληρωμής από το site της τράπεζας Alpha που χρησιμοποιεί τα πιστοποιητικά SSL της Geotrust εξασφαλίζοντας την μέγιστη προστασία των δεδομένων.

Η ασφάλεια του Ηλεκτρονικού καταστήματος της εταιρείας επιτυγχάνεται με τις ακόλουθες μεθόδους:

- Για την εξασφάλιση του απορρήτου της μεταφοράς των δεδομένων, χρησιμοποιεί το πρωτόκολλο κρυπτογράφησης SSL 40-256bit. Το σύστημα έχει πιστοποιηθεί από την εταιρία Verisign, η οποία ειδικεύεται σε θέματα ασφαλείας συναλλαγών.
- Από την έναρξη έως τη λήξη της σύνδεσή (on-line session) με το ηλεκτρονικό κατάστημα της εταιρείας, όλες οι πληροφορίες και τα προσωπικά στοιχεία κρυπτογραφούνται με βάση το πρωτόκολλο κρυπτογράφησης SSL 40-256-bit. Η κρυπτογράφηση είναι ουσιαστικά ένας τρόπος κωδικοποίησης της πληροφορίας μέχρι αυτή να φτάσει στον ορισμένο αποδέκτη της, ο οποίος θα μπορέσει να την αποκωδικοποιήσει με χρήση του κατάλληλου κλειδιού. Κάθε φορά που συνδέετε ο χρήστης με το ηλεκτρονικό κατάστημα της εταιρείας, όλη η επικοινωνία ανάμεσα στον υπολογιστή του και τα συστήματα της εταιρείας κρυπτογραφείται με χρήση κλειδιού 40-256 bits. Δηλαδή, κάθε φορά που στέλνει πληροφορίες προς το σύστημα, ο browser του τις κρυπτογραφεί πρώτα με χρήση κλειδιού 40-256 bits και στη συνέχεια τις στέλνει στο σύστημα. Το σύστημα της εταιρείας αποκρυπτογραφεί πρώτα τις πληροφορίες που λαμβάνει χρησιμοποιώντας το ίδιο κλειδί (που προκαθορίζεται με την έναρξη της σύνδεσή του χρήστη με την υπηρεσία) και στη συνέχεια τις επεξεργάζεται. Τα συστήματα της εταιρείας, αποστέλλει πληροφορίες ακολουθώντας την ίδια διαδικασία κρυπτογράφησης.

- Όλες οι πληροφορίες που διαβιβάζονται είναι εμπιστευτικές. Μόνο εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση στις πληροφορίες των συναλλαγών και μόνο όταν είναι αναγκαίο. Η εταιρεία δεν αποκαλύπτει τα στοιχεία των πελατών και των συναλλαγών της, εκτός αν έχει έγγραφη εξουσιοδότηση. Τέλος, τα προσωπικά δεδομένα που δηλώνονται στο ηλεκτρονικό κατάστημα με το εμπορικό

σήμα ΕΥΡΩΓΝΩΣΗ & EUROLAB χρησιμοποιούνται αποκλειστικά από αυτό, με σκοπό την υποστήριξη, προώθηση και εκτέλεση της συναλλακτικής σχέσης.

3η Περίπτωση

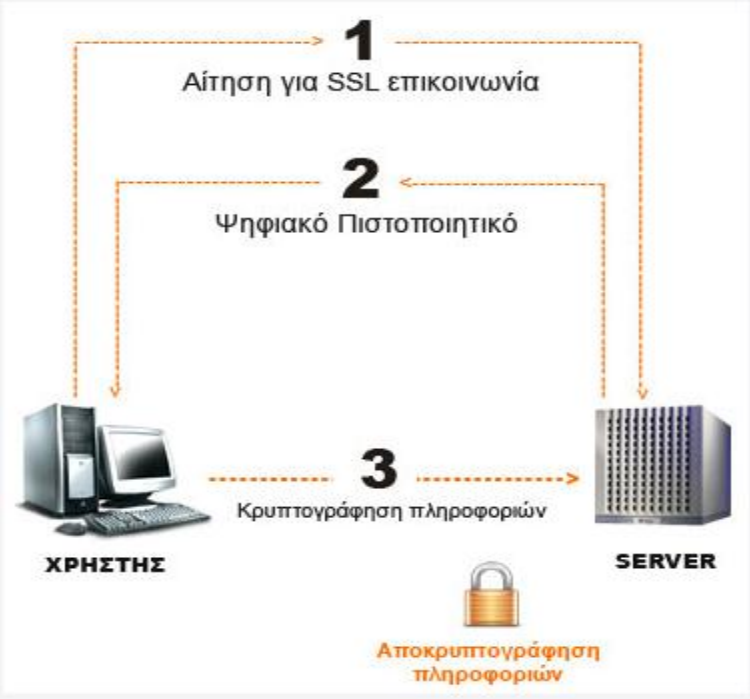
E-shop.gr

Η e-shop.gr αποτελεί ανώνυμη εταιρεία ηλεκτρονικού εμπορίου και παροχής υπηρεσιών διαδικτύου. Μετά από μια δεκαετή περίοδο έντονης ανάπτυξης είναι πλέον κυρίαρχη στην αγορά ηλεκτρονικού εμπορίου διαθέτοντας ολοκληρωμένα συστήματα υπολογιστών με το σήμα Innovator™ καθώς και ότι άλλο χρειάζεται ο καταναλωτής από hardware, software, περιφερειακά, ήχο και εικόνα, κινητή τηλεφωνία, βιβλία, παιχνίδια κτλ. Οι καταναλωτές έχουν την δυνατότητα να πραγματοποιήσουν τις παραγγελίες τους ηλεκτρονικά.

Ασφάλεια

Το e-shop.gr δεσμεύεται όσον αφορά στην εξασφάλιση της ασφάλειας και της ακεραιότητας των δεδομένων που συλλέγει σχετικά με τους χρήστες της ιστοσελίδας του. Το e-shop.gr έχει υιοθετήσει διαδικασίες, οι οποίες προφυλάσσουν τα προσωπικά δεδομένα που οι χρήστες προσκομίζουν στην ιστοσελίδα του ή του παρέχουν με οποιοδήποτε άλλο μέσο (πχ. τηλεφωνικά). Αυτές οι διαδικασίες προστατεύουν τα δεδομένα των χρηστών από οποιαδήποτε μη επιτρεπόμενη πρόσβαση ή αποκάλυψη, απώλεια ή κακή χρήση, και αλλαγή ή καταστροφή. Βοηθούν επίσης στο να πιστοποιείται ότι τα στοιχεία αυτά είναι ακριβή και χρησιμοποιούνται σωστά. Η σύνδεσή σε αυτό είναι ασφαλής διότι χρησιμοποιεί τεχνολογία SSL (Secure Socket Layer). Η τεχνολογία SSL στηρίζεται σε ένα κωδικό κλειδί για κρυπτογράφηση των δεδομένων πριν αποσταλούν μέσω της (SSL) σύνδεσης. Ο έλεγχος ασφαλείας μεταξύ των δεδομένων και του Server γίνεται με βάση το μοναδικό κωδικό κλειδί διασφαλίζοντας στο ακέραιο την επικοινωνία. Οι

φυλλομετρητές (browsers) Netscape Navigator, Internet Explorer, Mozilla Firefox, Opera, Safari υποστηρίζουν το πρωτόκολλο SSL και προτείνεται η χρήση τους για την σύνδεση στην ιστοσελίδα του e-shop.gr.



4η Περίπτωση

Η υπηρεσία Live-Pay της Eurobank

Δραστηριότητα της Live-Pay της Eurobank

Μία νέα πρωτοποριακή υπηρεσία ηλεκτρονικών πληρωμών το Live-Pay της Eurobank EFG παρέχει τη δυνατότητα στους ιδιώτες πελάτες της Τράπεζας να εξοφλούν τις υποχρεώσεις τους προς οργανισμούς ή επιχειρήσεις στο internet, από τον υπολογιστή ή το κινητό τους τηλέφωνο, με τη χρήση πιστωτικής κάρτας οποιασδήποτε τράπεζας. Ειδικότερα, μέσω του Live-Pay οι καταναλωτές έχουν τη δυνατότητα να εξοφλούν online μια σειρά από υποχρεώσεις, όπως οφειλές

προς το Δημόσιο, λογαριασμούς τηλεφώνου και internet, ασφαλιστικές υπηρεσίες, συνδρομές σε εφημερίδες και περιοδικά, διαμονή σε ξενοδοχεία και πολλές άλλες, με τη χρέωση πιστωτικής ή προπληρωμένης κάρτας οποιασδήποτε Τράπεζας (Visa, Mastercard, Prepaid Visa). Επίσης, τα εγγεγραμμένα μέλη του Live-Pay απολαμβάνουν πρόσθετες λειτουργίες που τους διευκολύνουν στην παρακολούθηση και εκτέλεση των πληρωμών τους, όπως πρόσβαση στο ιστορικό των συναλλαγών τους, η αποθήκευση των τακτικών πληρωμών τους, η τήρηση ηλεκτρονικού αρχείου πληρωμών/αποδείξεων κλπ. Η υπηρεσία είναι διαθέσιμη 24ώρες το 24ωρο και ένας εκπρόσωπός του Live-Pay βρίσκεται πάντα διαθέσιμος να εξυπηρετήσει είτε μέσω Live chat, είτε μέσω τηλέφωνου χωρίς κόστος και χωρίς αναμονή.

Ασφάλεια

Για τη Eurobank αποτελεί ζήτημα υψίστης σημασίας η προστασία των ηλεκτρονικών συναλλαγών των πελατών της. Για το σκοπό αυτό, οι μηχανισμοί ασφάλειας των συναλλαγών που χρησιμοποιούνται στην υπηρεσία Live-Pay ανταποκρίνονται στις αυστηρότερες προδιαγραφές ασφάλειας. Το Live-Pay χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128bit, για ασφαλείς online εμπορικές συναλλαγές. Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2^{128} πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από τον φυλλομετρητή παγκοσμίου ιστού στον server της τράπεζας. Για αυτόν τον λόγο, η κρυπτογράφηση στα 128bit θεωρείται πρακτικά αδύνατο να παραβιαστεί. Με αυτό τον τρόπο κρυπτογραφούνται και προστατεύονται όλες οι προσωπικές πληροφορίες, συμπεριλαμβανομένων των στοιχείων της πιστωτικής κάρτας, του ονόματος και της διεύθυνσής, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχτούν κατά τη μεταφορά τους στον παγκόσμιο ιστό. Το SSL ξεκινά την κωδικοποίηση από τα 40bit. Στο Live-Pay χρησιμοποιείται κρυπτογράφηση στα 128bit η οποία είναι ένα τρισεκατομμύριο φορές πολυπλοκότερη, και άρα ασφαλέστερη για την προστασία των προσωπικών δεδομένων των πελατών από την αντίστοιχη των 40bit.

Πιστοποίηση της υπηρεσίας Live-Pay από τη Verisign

Το σύστημα ασφαλούς επικοινωνίας του Live-Pay είναι πιστοποιημένο από την εταιρεία Verisign, μια διεθνώς αναγνωρισμένη ως ηγέτιδα εταιρεία, στον τομέα

της παροχής προστασίας συναλλαγών και δεδομένων μέσω Internet. Κάθε στοιχείο που καταχωρείτε στο site της κωδικοποιείται πριν βγει online και σε συνέχεια διερευνάτε η αυθεντικότητα του μηνύματος και του server. Η Verisign κάθε φορά που εισέρχεται ο χρήστης σε ασφαλή σελίδα στην οποία πρόκειται να γίνει συναλλαγή στοιχείων, παρουσιάζει ένα μικρό εικονίδιο με τη μορφή λουκέτου στο κάτω μέρος των σελίδων, το οποίο δείχνει και παράλληλα βεβαιώνει ότι η συναλλαγή προστατεύεται. Επιπλέον, ο χρήστης είναι σίγουρος ότι έχει μεταφερθεί σε μια ασφαλή (secure) σελίδα ενός δικτυακού τόπου γιατί η διεύθυνση του δικτυακού τόπου ξεκινά με "https" αντί για "http" (το "s" σημαίνει "secure"). Τα παραπάνω αποδεικνύουν πως η μετάδοση προσωπικών στοιχείων (όνομα, διεύθυνση, πιστωτική κάρτα, κ.λπ.) γίνεται με κρυπτογράφηση, ώστε να μην μπορεί να γίνει αντιληπτή από τρίτους.

Ελεγχόμενη πρόσβαση στα συστήματα της τράπεζας

Η πρόσβαση στα συστήματα της Eurobank (servers) προστατεύεται από τελευταία τεχνολογία Firewall, η οποία επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών απαγορεύοντας, παράλληλα, την πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Τράπεζας σε μη αναγνωρισμένους χρήστες.

5η Περίπτωση

Hellas Pay

Hellas Pay προσφέρει ένα σύνολο από καινοτόμες υπηρεσίες πληρωμών σε Ιδιώτες, ατή ασφάλεια και ταυτόχρονα Επιχειρήσεις και Επαγγελματίες, παρέχοντας τη μέγιστη δυνατή ευελιξία που χρειάζονται για την πραγματοποίηση πληρωμών με Κάρτα (πιστωτική, χρεωστική, προπληρωμένη) μέσω διαδικτύου ή/και μέσω τηλεφώνου. Παράλληλα, ως πιστοποιημένος φορέας εκκαθάρισης της Κάρτας Αποδείξεων, η Hellas Pay παρέχει τη δυνατότητα καταχώρησης των συναλλαγών στη Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών, με

την οποία είναι διασυνδεδεμένη. Η εταιρεία λειτουργεί με επίσημη άδεια από την Τράπεζα της Ελλάδος.

Ασφάλεια των συναλλαγών

Η Hellas Pay αναγνωρίζοντας τη σημασία της ασφάλειας των ηλεκτρονικών συναλλαγών, έχει λάβει όλα τα απαραίτητα μέτρα ώστε να παρέχει υπηρεσίες πληρωμών με τη μέγιστη δυνατή ασφάλεια. Η Hellas Pay ως ίδρυμα πληρωμών, ακολουθεί όλες τις διαδικασίες του PCI DSS[83] που απευθύνονται στον κλάδο, ώστε να:

- Προστατεύει τα προσωπικά δεδομένα των πελατών της.
- Ενισχύει την εμπιστοσύνη των πελατών μέσω ενός υψηλότερου επιπέδου ασφαλείας δεδομένων
- Οχυρώνει τους πελάτες της από οικονομικές απώλειες και έξοδα 'επανόρθωσης'
- Διατηρεί την εμπιστοσύνη και να προστατεύει τη φήμη του ονόματός των πελατών της

Στο πλαίσιο των παραπάνω, η Hellas Pay έχει λάβει πιστοποίηση PCI-DSS και εφαρμόζει την προβλεπόμενη πολιτική ασφάλειας η οποία αξιολογείται με συνεχόμενους ελέγχους από πιστοποιημένο υπεύθυνο ασφαλείας (security auditor).

Εξασφάλιση του Απορρήτου της Μεταφοράς των Δεδομένων

Από την έναρξη έως τη λήξη της σύνδεσή (on-line session), όλες οι πληροφορίες και τα προσωπικά στοιχεία του χρήστη κρυπτογραφούνται με βάση το πρωτόκολλο κρυπτογράφησης 128-bit (Secure Sockets Layer - SSL). Η κρυπτογράφηση είναι ουσιαστικά ένας τρόπος κωδικοποίησης της πληροφορίας μέχρι αυτή να φτάσει στον ορισμένο αποδέκτη της, ο οποίος θα μπορέσει να την αποκωδικοποιήσει με χρήση του κατάλληλου κλειδιού. Κάθε φορά που ο πελάτης πληρώνει με την Hellas Pay,

[83] Payment Card Industry Data Security Standard (PCI DSS) είναι ένα διεθνές πρότυπο το οποίο απευθύνεται σε κάθε Οργανισμό ή Εταιρία που συμμετέχει σε μια αλυσίδα συναλλαγής, ένα σύνολο τεχνικών και λειτουργικών απαιτήσεων που τίθενται από το PCI Security Standards Council (PCI SSC) για την προστασία των δεδομένων καρτών.

όλη η επικοινωνία ανάμεσα στον υπολογιστή του και τα συστήματα της Hellas Pay κρυπτογραφείται με χρήση κλειδιού 128 bits της Verisign (της πιο αναγνωρισμένης εταιρίας έκδοσης κρυπτογραφικών κλειδιών για τραπεζικές υπηρεσίες).

Ελεγχόμενη Πρόσβαση

Η πρόσβαση στα συστήματα της Hellas Pay ελέγχεται από Firewall, το οποίο επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών από τους πελάτες/επισκέπτες απαγορεύοντας, την πρόσβαση τους όμως σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Hellas Pay. Για τη μέγιστη προστασία των δεδομένων και όπως επιβάλει το πρότυπο PCI-DSS, η Hellas Pay χρησιμοποιεί τελευταίας τεχνολογίας συστήματα εντοπισμού κακόβουλων επιθέσεων .

6.3 ΣΥΜΠΕΡΑΣΜΑΤΑ ΜΕΛΕΤΗΣ

Με την μελέτη των παραπάνω εταιριών συμπεραίνουμε ότι όλες οι εταιρίες δίνουν μεγάλη έμφαση στην ασφάλεια των ηλεκτρονικών συναλλαγών που πραγματεύονται. Οι εταιρείες λαμβάνουν όλα τα απαραίτητα αλλά και ποιο σύγχρονα μέσα για την εξασφάλιση της προστασίας των ηλεκτρονικών συναλλαγών. Παρατηρούμε ότι όλες οι εταιρείες χρησιμοποιούν το πρωτόκολλο ασφάλειας SSL κυρίως με κρυπτογράφηση 128 bit. Αυτό το πρωτόκολλο είναι απαραίτητο σε ιστοσελίδες οι οποίες ανταλλάσουν σημαντικές πληροφορίες όπως, προσωπικά δεδομένα ή κωδικούς πιστωτικών καρτών, σε ηλεκτρονικά καταστήματα όπου οι συναλλαγές – πληρωμές γίνονται μέσω πιστωτικών καρτών, σε ιστοσελίδες που επιτρέπεται η πρόσβαση σε αυτές μέσω κωδικού αλλά και σε ιστοσελίδες που αποθηκεύουν ή ανταλλάσουν προσωπικά δεδομένα γιατί προσφέρει αξιοπιστία και ασφαλής μετακίνηση δεδομένων. Εν κατακλείδι, η επισκεψιμότητα των ιστοσελίδων των εταιρειών έχει αυξηθεί, όπως και οι ηλεκτρονικές αγορές καθώς οι επισκέπτες αυτών των ιστοσελίδων κοινοποιούν πιο άνετα στοιχεία πληρωμών και προσωπικά στοιχεία για να προβούν σε ηλεκτρονικές συναλλαγές.

ΣΥΜΠΕΡΑΣΜΑΤΑ-ΕΠΙΛΟΓΟΣ

Σε μια εποχή που χαρακτηρίζεται από την ανάπτυξη της τεχνολογίας και από την διείσδυση του ιντερνέτ στην καθημερινότητα μας όλο και περισσότεροι είναι αυτοί που αποφασίζουν να πραγματοποιήσουν αγορές ηλεκτρονικά χρησιμοποιώντας ως μέσο την μεγάλη γκάμα ηλεκτρονικών μεθόδων που έχει δημιουργηθεί. Οι συναλλαγές μέσω Internet χαρακτηρίζονται από ακαταμάχητα πλεονεκτήματα, με αποτέλεσμα να αποτελούν ολοένα και μεγαλύτερο τμήμα της σύγχρονης ψηφιακής ζωής μας. Όπως κάθε αγορά όμως, έτσι και η ψηφιακή δεν είναι άμοιρη κινδύνων. Λαμβάνοντας υπόψη ότι η τεχνολογία είναι κάτι άγνωστο για τους περισσότερους είναι φυσικό αυτό που απασχολεί περισσότερο τους καταναλωτές να είναι το κατά πόσο αυτές οι συναλλαγές είναι ασφαλείς. Για την ασφάλεια ενός συστήματος ηλεκτρονικών πληρωμών και ειδικότερα ηλεκτρονικού χρήματος είναι απαραίτητη μια σειρά από τεχνικές και εργαλεία όπως οι αλγόριθμοι, τα πιστοποιητικά και τα πρωτόκολλα. Ένα ασφαλές σύστημα δεν είναι κάτι απλό, χρειάζονται γνώσεις και απαιτείται ο σωστός σχεδιασμός ολόκληρου του συστήματος και φυσικά η σωστή διαχείριση των διαδικασιών ασφαλείας από εξουσιοδοτημένα άτομα, η εκπαίδευση προσωπικού είναι απαραίτητη. Βέβαια, οι καταναλωτές θα πρέπει και αυτοί με την σειρά τους να είναι αρκετά προσεχτικοί για παράδειγμα, να μην δίνουν τα στοιχεία τους σε τρίτους. Με τον συνδυασμό των παραπάνω, μπορεί να επιτευχθεί η ασφάλεια συνεπάγοντας μια μεγαλύτερη άνθιση των συναλλαγών, έτσι ώστε τέλος να εξυπηρετούνται τα συμφέροντα και των εμπόρων και των καταναλωτών.

ΒΙΛΙΟΓΡΑΦΙΑ

Έγγραφη:

1. Tanenbaum, Andrew S. 2000*, «Δίκτυα Υπολογιστών»*, Τρίτη Έκδοση, Πρώτη Ελληνική Έκδοση, Εκδόσεις Παπασωτηρίου, Αθήνα.

2. Stallings William , 2007 «*Ασύρματες Επικοινωνίες και Δίκτυα»,* Εκδόσεις Τζιόλα, Θεσσαλονίκη.

3. *Pa*trick Ciccarelli, Christina Faulkner, 2005 «Δίκτυα υπολογιστών, Εισαγωγή στη Σύγχρονη Τεχνολογία», Εκδόσεις Μ. Γκιούρδας, Αθήνα.

4. *DOUGLAS E. COMER, 2010 «ΔΙΑΔΙΚΤΥΑ με TCP/IP ΑΡΧΕΣ, ΠΡΩΤΟΚΟΛΛΑ, ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ»,* 4η Αμερικάνικη έκδοση, Εκδόσεις κλειδάριθμος, Αθήνα.

5. Andrew S. Tanenbaum, 2003 *«Δίκτυα Υπολογιστών»,* Εκδόσεις Κλειδάριθμος, Αθήνα.

6. Γ. Πάγκαλος, Ι. Μαυρίδης, 2003 *«Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων»,* Εκδόσεις ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη.

7. Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν.,1998 «Ηλεκτρονικό Εμπόριο», Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

8. Πασχόπουλος Α, Σκαλτσάς Π.,2009 «Ηλεκτρονικό Εμπόριο», 3η έκδοση, εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ.

9. Turban, E. Lee, J. King, D.& Chung, H. M., 2003 «Electronic commerce: A managerial perspective» international edition, Upper Saddle River: Prentice Hall

10. Πομπόρτσης Ανδρέας Σ., Τσουλφάς, Ανέστης Γ. 2002, « Εισαγωγή στο ηλεκτρονικό εμπόριο» Εκδόσεις ΤΖΙΟΛΑ.

11. Κομνηνός θ. - Σπυράκης Π. ,2002 «Ασφάλεια δικτύων υπολογιστικών συστημάτων, αναχαιτίστε τους εισβολείς», Εκδόσεις Ελληνικά Γράμματα.

12. Γ. Πολλάλης - Δ. Γιαννακόπουλος,2007 «Ηλεκτρονικό επιχειρείν», Εκδόσεις Σταμούλη.

13. Παυλίδης Γ, 2003 «Ολοκληρωμένη Τεχνολογία Πληροφορικής», εκδόσεις Gutenberg.

14. Κάτσικας Σ., Γκριτζάλης Δ., Γκριτζάλης Σ.,2004 *«Ασφάλεια πληροφοριακών συστημάτων»,* εκδόσεις Νέων Τεχνολογιών.

15. Γιάννης Κατσουλάκος, 2001 «*Νέα οικονομία, Διαδίκτυο και Ηλεκτρονικό εμπόριο»* Εκδόσεις ΚΕΡΚΥΡΑ.

16. Κωνσταντίνος Μάρκελλος, Πηνελόπη Μάρκελλου, Μαρία Ρήγκου, Σπύρος Συρμακέσης, Αθανάσιος Τσακαληδης,2005, *Ε-Επιχειρηματικοτητα* (από την ιδέα στην υλοποίηση), Ελληνικά Γράμματα Αθήνα.
17. Νικόλαος Β. Γεωργόπουλος ,Μαλαματένια –Άλμα Α. Πανταζή, Χαράλαμπος Θ. Νικολουράκος, Ιωσήφ Χ. Βαγγελατος,2005, *«Ηλεκτρονικό Επιχειρείν»,* (προγραμματισμός και σχεδίαση), Ε. Μπένου , Αθήνα
18. Παναγιώτης Ε. Ναστου, Παύλος Γ. Σπυράκης, Γ Γιάννης Κ. Σταματίου,(2003) *«Σύγχρονη Κρυπτογραφία*», Εκδόσεις Ελληνικά Γράμματα, Αθήνα.
19. Παπαδόπουλος Δ, εργαστηριακές σημειώσεις στο μάθημα Ηλεκτρονικό Εμπόριο, section 3-ηλεκτρονικές πληρωμές.
20. Αναγνώστου Παναγιώτης(2008):Εισαγωγή στα Διαδίκτυα Η/Υ και Internet (Εργαστηριακές σημειώσεις) .

ΙΣΤΟΤΟΠΟΙ:

http://el.wikipedia.org/wiki/Διαδίκτυο
http:/ /www.mediamarkt.gr
http://www.cnc.uom.gr/services/pdf/section1(2).pdf
http://www.ea.gr/ep/agroweb/htmls/lessons/commerce1gr/21d.htm
http://users.sch.gr/mntoumos/erkef76.htm
http://el.wikipedia.org/wiki/IP
http://www2.uth.gr/main/help/help-desk/internet/internet4.html
http://el.wikipedia.org/wiki/TCP
http://el.wikipedia.org/wiki/Ηλεκτρονικό_εμπόριο
http://www.ebusinessforum.gr
http://en.wikipedia.org/wiki/Digital_wallet
http://el.wikipedia.org
http://www.nbg.gr/
http://www.atebank.gr
http://users.uom.gr/~kaklaman/book/Chapters/C11/
http://el.wikipedia.org/wiki/

http://support.google.com/chrome/

http://www.sch.gr/sch-portlets/static/manual/aboutSpam/

http://el.wikipedia.org/wiki/IP_spoofing

http://el.wikipedia.org/wiki/Rootkit

http://www.e-crime.gr/crime.htm

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html

http://students.ceid.upatras.gr/~mprokala/techarticles/cryptography/AES/aes.htm

http://el.wikipedia.org/wiki/ Ψηφιακό_πιστοποιητικό

http://searchsecurity.techtarget.com/definition/registration-authority

http://conta.uom.gr/conta/ekpaideysh/seminaria/thlematikes/security/SET_buying.htm

http://www.scribd.com/doc/36358788/8/Kerberos

http://translate.google.gr/translate?hl=el&langpair=en|el&u=http://en.wikipedia.org/wiki/Kerberos_(protocol)

http://europa.eu/index_el.htm

http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/firewalls1.html*track=internal