ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Πτυχιακή Εργασία

Κρυπτογράφηση στο Ηλεκτρονικό Εμπόριο

Ονοματεπώνυμο Σπουδαστών: Κάρλος Χρίστος
Αργυρίου Σπυρίδων Νικόλαος

Εποπτεύων Καθηγητής: Παπαδόπουλος Δημήτριος

Πάτρα, 2014

Ευχαριστίες

Προτού προχωρήσω στην ανάπτυξη της εργασίας μου, επιθυμώ να αποδώσω ευχαριστίες στους καθηγητές μου οι οποίοι με τις γνώσεις τους και την εκπαιδευτική τους δεινότητα μου μετέδωσαν τα απαραίτητα εφόδια ώστε να ολοκληρώσω τις σπουδές μου. Ιδιαιτέρως θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Δημήτριο Παπαδόπουλο ο οποίος με καθοδηγούσε, με συμβούλευε και με διόρθωνε σε όλη την πορεία εκπόνησης της πτυχιακής μου εργασίας. Τέλος, ένα μεγάλο ευχαριστώ στην οικογένειά μου, η οποία με στήριξε ηθικά και υλικά σε όλη την πορεία της φοιτητικής μου ζωής.

Περιεχόμενα

Πρόλογος

Σκοπός της παρούσας εργασίας είναι να προσεγγίσει από πλευράς ασφάλειας το θέμα του ηλεκτρονικού εμπορίου. Ο ανταγωνισμός των τελευταίων ετών έχει οδηγήσει τις επιχειρήσεις στην εγκατάλειψη των κλασικών μεθόδων επιχειρηματικής λειτουργίας και στην ανάπτυξη σύγχρονων μεθόδων λειτουργίας και προβολής τους. Ωστόσο είναι και η ανάπτυξη των τεχνολογιών διαδικτύου, που επιβάλλει στις επιχειρήσεις την ανάπτυξη του ηλεκτρονικού εμπορίου. Πολλά είναι τα θέματα της ασφάλειας που ανακύπτουν στην όλη διαδικασία του ηλεκτρονικού εμπορίου. Με αυτά τα θέματα θα ασχοληθούμε στην παρούσα εργασία και θα δούμε την βασική μέθοδο που διασφαλίζει τις ηλεκτρονικές μας συναλλαγές: την κρυπτογραφία.

Στο πρώτο κεφάλαιο συγκεκριμένα δίνεται με σαφήνεια ο ορισμός της έννοιας του ηλεκτρονικού εμπορίου και περιγράφονται αναλυτικά οι κατηγορίες στις οποίες χωρίζεται. Ακόμα παραθέτονται τα βασικά πλεονεκτήματα και μειονεκτήματα που έχει, ενώ γίνεται και μια σύντομη ανασκόπηση του θεσμικού πλαισίου μέσα στο οποίο κινείται στην Ελλάδα. Τέλος οι τεχνολογίες του ηλεκτρονικού εμπορίου, όπως είναι η ηλεκτρονική ανταλλαγή πληροφοριών και τα πρωτόκολλα ασφάλειας που χρησιμοποιούνται, δεν θα μπορούσαν να μην αναλυθούν.

Στο δεύτερο κεφάλαιο γίνεται μια περαιτέρω ανάλυση στα θέματα ασφάλειας που αφορούν το ηλεκτρονικό εμπόριο και παρουσιάζονται με σαφήνεια οι κίνδυνοι που απειλούν σήμερα τις ηλεκτρονικές συναλλαγές, περισσότερο όμως από την πλευρά των καταναλωτών. Ένα από τα κυριότερα θέματα ασφάλειας είναι η υποκλοπή προσωπικών δεδομένων, κυρίως προσωπικών στοιχείων και στοιχείων πιστωτικών καρτών.

Στο τρίτο και σημαντικότερο κεφάλαιο κάνουμε εισαγωγή στην επιστήμη της κρυπτογραφίας και αναλύουμε διεξοδικά όλες εκείνες τις μεθόδους που έχουν προταθεί ανά τα χρόνια και θέλουν να δώσουν λύση στο πρόβλημα της ασφάλειας

των συναλλαγών. Οι κυριότερες κρυπτογραφικές μέθοδοι που αναλύουμε είναι η DES, η RSA, ενώ η σημαντικότερη κρυπτογραφική μέθοδος που χρησιμοποιείται ευρέως στις ηλεκτρονικές συναλλαγές είναι Υποδομή Δημόσιου Κλειδιού (PKI). Τέλος παραθέτονται αναλυτικά τα κρυπτογραφικά συστήματα που χρησιμοποιούνται όπως είναι το SET, το οποίο αποτελεί ένα πρωτόκολλο εμπορικών συναλλαγών για την χρήση πιστωτικών καρτών σε ανοικτά δίκτυα συναλλαγών.

Εισαγωγή

Στις μέρες μας η ευρεία διάδοση του διαδικτύου, το έχει καταστήσει ως ένα παγκόσμιο μέσο μεταφοράς και ανταλλαγής πληροφοριών. Οι δυνατότητες που παρέχει στους χρήστες του, ιδιώτες και επιχειρήσεις, είναι πολλαπλές. Μέσα σε αυτές τις δυνατότητες μπορούμε να αναγνωρίσουμε μια, η οποία είναι ιδιαίτερη σημαντική και αποτελεί την βάση για την διεκπεραίωση εμπορικών συναλλαγών: την άμεση επικοινωνία.

Στην επικοινωνία μεταξύ δύο χρηστών του διαδικτύου , ωστόσο δημιουργούνται διάφορα προβλήματα ασφάλειας πληροφοριών, τα οποία αφορούν την εξασφάλιση εμπιστευτικότητας-μυστικότητας-ακεραιότητας και διαθεσιμότητας των διακινούμενων πληροφοριών. Η εξασφάλιση και ταυτόχρονα διασφάλιση της ασφαλούς επικοινωνίας και ανταλλαγής δεδομένων μεταξύ δύο ατόμων θέτει ως κύρια απαίτηση την δυνατότητα αποστολής και λήψης πληροφοριών με τρόπο τέτοιο, ούτως ώστε οι πληροφορίες αυτές να μπορούν να ληφθούν και να διαβαστούν μόνο από τους παραλήπτες στους οποίους απευθύνονται. Την λύση στο πρόβλημα της ασφαλούς διακίνησης των πληροφοριών μεταξύ δύο η περισσότερων δικτύων έχει έρθει να δώσει εδώ και πολλά χρόνια η επιστήμη της κρυπτογραφίας.

Η κρυπτογραφία χρησιμοποιείται ευρέως σήμερα ως ένα πολύ χρήσιμο βοήθημα (εργαλείο) που συναινεί με τον ασφαλέστερο τρόπο στην μεταφορά δεδομένων και πληροφοριών, προκειμένου να προστατευτούν τα ανταλλασσόμενα δεδομένα σε διάφορα επίπεδα, δηλαδή ως προς την ακεραιότητα τους , την εμπιστευτικότητα τους, και τη διαθεσιμότητά τους. Ζητήματα προστασίας απορρήτου έχουν τεθεί εδώ και πολλά χρόνια, σε θέματα δικτυακών συναλλαγών όπως είναι η λήψη και αποστολή email, των χρηστών του διαδικτύου.

Ως Κρυπτογράφηση (encryption) ορίζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία με τέτοιο τρόπο ώστε αυτό να μην είναι δυνατό να διαβαστεί από κανέναν, παρά μόνο από τον νόμιμο παραλήπτη του. Η αντίστροφη διαδικασία κατά την οποία από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption). Υπάρχουν διάφοροι αλγόριθμοι κρυπτογράφησης και κρυπτογραφικά συστήματα τα οποία έχουν αναπτυχθεί τα τελευταία χρόνια, και με αυτά θα ασχοληθούμε ιδιαίτερα στην παρούσα εργασία.

Κεφάλαιο 1ο

Ηλεκτρονικό Εμπόριο

1.1. Ορισμός

Πολύ πρόσφατα, μέχρι και λίγα χρόνια πριν, οι συναλλαγές εμπόρων και καταναλωτών πραγματοποιούνταν αποκλειστικά με καθαρά συμβατικά μέσα. Οι καταναλωτές για να πραγματοποιήσουν μια αγορά ή να αγοράσουν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών . Στις μέρες μας, και ιδιαίτερα εν έτη 2014 ο τρόπος διεξαγωγής των συναλλαγών έχει τροποποιηθεί αρκετά, αφού το ηλεκτρονικό εμπόριο έχει κάνει την εμφάνιση του, προσφέροντας έναν εναλλακτικό, και με πολλά πλεονεκτήματα τρόπο πραγματοποίησης συναλλαγών. Το ηλεκτρονικό εμπόριο προοδεύει με μεγάλους ρυθμούς σε χώρες του εξωτερικού αλλά και στην Ελλάδα με πιο αργούς όμως ρυθμούς. Αιτία αυτής της όψιμης ανάπτυξης του στην Ελλάδα αποτελούν οι δύο υπουργικές αποφάσεις 3035/Β2-48.2001 και 7681/Β2-255.2001 οι οποίες προωθούν μια σειρά από ενέργειες δοκιμαστικής έρευνας για το ηλεκτρονικό εμπόριο. Η πρώτη απόφαση είναι του έτους 2001, της χρονιάς που σε άλλες χώρες του εξωτερικού είχε πλήρη ανάπτυξη το ηλεκτρονικό εμπόριο. Επίσης και οι υπουργικές αποφάσεις 4708/2003, 36/2003 και 10220/Γ3-571/2004 μας δείχνουν την ίδια ακριβώς κατάσταση.

Ο όρος ηλεκτρονικό εμπόριο αναφέρεται σε αυτό το είδος του εμπορίου το οποίο πραγματοποιείται με ηλεκτρονικά μέσα, δηλαδή βασίζεται αποκλειστικά στην ηλεκτρονική μετάδοση δεδομένων (Γκιούρδας, 2010). Σύμφωνα με το Προεδρικό Διάταγμα 39.2001 το ηλεκτρονικό εμπόριο έγκειται σε μια εμπορική συναλλαγή η οποία λαμβάνει χώρα στο διαδίκτυο δίχως να είναι αναγκαία η φυσική παρουσία του αγοραστή και του πωλητή, οι οποίοι είναι δυνατό να βρίσκονται ακόμα και σε διαφορετικές χώρες.

Διευρύνοντας ακόμα περισσότερο τον όρο του ηλεκτρονικού εμπορίου αναφέρουμε πως είναι μια οποιαδήποτε συναλλαγή η οποία περιέχει διαδικτυακή δέσμευση για αγοραπωλησία αγαθών ή υπηρεσιών. Επίσης στην έννοια του ηλεκτρονικού εμπορίου περιλαμβάνονται και οι συναλλαγές μέσω τηλεφώνου και φαξ.

Επιπλέον το ηλεκτρονικό εμπόριο διαχωρίζεται σε έμμεσο και άμεσο. Το έμμεσο ηλεκτρονικό εμπόριο σχετίζεται με την παραγγελία αγαθών ηλεκτρονικά, και τα αγαθά αυτά παραδίδονται στον αγοραστή με τους συμβατικούς τρόπους, όπως είναι το ταχυδρομείο. Από την άλλη το άμεσο ηλεκτρονικό εμπόριο πραγματοποιείται με την λήψη της παραγγελίας, την πληρωμή και την παράδοση άυλων αγαθών και υπηρεσιών. Η καταβολή του αντιτίμου των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα(Γκιούρδας, 2010).

1.2. Ιστορική Αναδρομή

Το 1970 ήταν η χρονιά που εμφανίστηκαν πρώτιστα τα συστήματα ηλεκτρονικής μεταφοράς χρηματικών πόρων τα γνωστά μας EFT (Emotional Freedom Techniques) που χρησιμοποιήθηκαν από όλες τις τράπεζες για τις μεταξύ τους συναλλαγές, η τεχνολογία των οποίων βασίστηκε σε ασφαλή ιδιωτικά δίκτυα και έτσι πραγματοποιούνταν οι συναλλαγές. Τα συστήματα EFT μετέβαλαν ριζικά την μορφή των αγορών εκείνη την εποχή. Λίγα χρόνια αργότερα, το 1980, έκαναν την εμφάνιση τους οι λεγόμενες τεχνολογίες ηλεκτρονικής επικοινωνίας οι οποίες στηρίζονταν στην τεχνολογία της ανταλλαγής μηνυμάτων, και οι οποίες είναι

γνωστές με το ακρωνύμιο EDI (Electronic Data Interchange). Η διάδοση τους ήταν εξαιρετικά σημαντική (Chaffey D. 2008).

Πολλές δραστηριότητες, που παραδοσιακά τότε εκτελούνταν με βασικό μέσο το χαρτί, είχαν την δυνατότητα πλέον με την χρήση των παραπάνω συστημάτων να πραγματοποιηθούν σε λιγότερο χρόνο αλλά και με μικρότερο κόστος. Οι συναλλαγές, που τα νωρίτερα χρόνια προϋπόθεταν έντυπα, όπως παραγγελίες για αγορές, άλλα έγγραφα και επιταγές πληρωμής, είχαν την δυνατότητα πλέον να πραγματοποιούνται εν μέρει ή ολικά με ηλεκτρονικό τρόπο χάρη στην ύπαρξη των συστημάτων EDI ή χάρη στο ηλεκτρονικό ταχυδρομείο.

Στο τέλος της δεκαετίας του 1980 τα δίκτυα υπολογιστών παρέχουν πλέον νέες μορφές επικοινωνίας, παρέχοντας δυνατότητες όπως:

1. το ηλεκτρονικό ταχυδρομείο (e-mail),
2. η ηλεκτρονική διάσκεψη (conferencing)
3. η ηλεκτρονική συνομιλία (IRC),
4. η δημιουργία ομάδων συζήτησης (newsgroups, forums),
5. η μεταφορά αρχείων ηλεκτρονικά (FTP) κτλ.

Η πρόσβαση στο δίκτυο έχει πλέον καταστεί οικονομικότερη στα πλαίσια της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών.

Στα μέσα της δεκαετίας του 1990, η εμφάνιση του Παγκόσμιου Ιστού (WWW) στο διαδίκτυο όπως επίσης και η υπερίσχυση των ηλεκτρονικών υπολογιστών (PC) –κυρίως προσωπικών – οι οποίοι έκαναν χρήση λειτουργικού συστήματος Windows, παρέχουν ευκολίες χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο Διαδίκτυο. Στην δεκαετία αυτή λοιπόν η τεχνολογία του ηλεκτρονικού εμπορίου είναι πλέον ένας πολύ οικονομικότερος και διαδεδομένος τρόπος προκειμένου να πραγματοποιηθούν όλων των ειδών οι συναλλαγές, ακόμα και οι μεγάλου όγκου, ενώ παράλληλα ενισχύει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων, δίνοντας την δυνατότητας σε μικρού μεγέθους επιχειρήσεις και οργανισμούς να ανταγωνιστούν τις μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις (Πασχόπουλος, 2006).

Μια πολύ σημαντική παράμετρος που ανέκυψε λοιπόν στην δεκαετία του 1990 ήταν το κατά πόσο ήταν ασφαλή τα ηλεκτρονικά μέσα για την πραγματοποίηση συναλλαγών, ανταλλαγής αρχείων, κ.α. Έτσι καθιερώθηκαν μέθοδοι κρυπτογράφησης του περιεχομένου αποστολής προκειμένου να μπορεί να γίνεται επαλήθευση της ταυτότητας αυτού που έστελνε τα ηλεκτρονικά μηνύματα, αλλά και η σχετική τροποποίηση και ρύθμιση της νομοθεσίας στον τομέα εισαγωγών-εξαγωγών και τον τομέα των επικοινωνιών, κάνουν ευκολότερη και οικονομικότερη την εκτέλεση ασφαλών διεθνών ηλεκτρονικών συναλλαγών(Σκιαδάς, 2001).

1.3. Νομοθεσία

Το ηλεκτρονικό εμπόριο παρά τις ιδιαιτερότητες του αποτελεί μια μορφή εμπορίου. Έτσι βρίσκουν εφαρμογή σε αυτό όλες οι κοινοτικές οδηγίες (το κοινοτικό δίκαιο) και οι εθνικές διατάξεις, περί προστασίας του καταναλωτή, οι οποίες αφορούν το εμπόριο γενικότερα. Πιο συγκεκριμένα (Ιγγλεζάκης 2008):

- Ο Ν. 2251/94, περί προστασίας των καταναλωτών στο άρθρο 4, ρυθμίζει τις συμβάσεις από απόσταση, στις οποίες υπόκειται και το ηλεκτρονικό εμπόριο.
- Ο Ν. 2472/97 που σχετίζεται και προφυλάσσει τα άτομα από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Ο Ν. 2174/99 άπτεται της προστασίας των ατομικών προσωπικών δεδομένων, στον τομέα των τηλεπικοινωνιών.
- Το Προεδρικό Διάταγμα 150/2001 (Φ.Ε.Κ. Α' 125) λίγα χρόνια αργότερα που αφορά τις ηλεκτρονικές υπογραφές, κάνει έκδηλη την προσπάθεια οι αρχές της Ελλάδας να προσφέρουν μια σωστή βάση νομοθετικών πλαισίων.
- Το Προεδρικό Διάταγμα 131/2003, που ψηφίστηκε για το ηλεκτρονικό εμπόριο αφορά μεν γενικότερες οδηγίες για την διεξαγωγή του εμπορίου, δίνει όμως βαρύτητα στα παρακάτω θέματα:
    - στην εξώδικη επίλυση διαφορών,

- σε θέματα συνεργασίασ των κρατών - μελών της Ευρωπαϊκής Ένωσης, για την επίλυση των προβλημάτων των καταναλωτών,
- στον ορισμό κανόνων δεοντολογίας, με υποχρεωτική ισχύ, για τους αποδέκτες τους,
- στην ευθύνη των ενδιάμεσων,
- στη σύναψη των ηλεκτρονικών συμβάσεων,
- στις πληροφορίες, που πρέπει να παρέχονται στις εμπορικές επικοινωνίες (διαφημιστικά, χορηγίες, προσφορές κ.λπ.),
- στον τόπο εγκατάστασης των φορέων παροχής υπηρεσιών.

Η νομοθεσία λοιπόν αυτή είχε να κάνει περισσότερο με την θέσπιση κανόνων για το ηλεκτρονικό εμπόριο το οποίο πραγματοποιούνταν μεταξύ των χωρών μελών της Ευρωπαϊκής Ένωσης. Σε περιπτώσεις που ο καταναλωτής πραγματοποιεί συναλλαγές με χώρες, που δεν είναι μέλη της Ευρωπαϊκής Ένωσης, είναι απαραίτητο να αποζητά τις πληροφορίες που παραχωρεί ο έμπορος στο ηλεκτρονικό του κατάστημα και οι οποίες σχετίζονται με το νομοθετικό κανονιστικό πλαίσιο, που θα διέπει τις αγορές του.

Επίσης η Σύμβαση των Βρυξελλών καθορίζει πως σε περιπτώσεις ύπαρξης διαφορών και διαφωνιών με έμπορο ή εταιρία που βρίσκονται σε άλλη χώρα, ο καταναλωτής, για τις χώρες που αποτελούν μέλη της Ευρωπαϊκής Ένωσης, θα πρέπει να απευθυνθεί στο δικαστήριο του τόπου κατοικίας του. Οι κανόνες δικαίου κάτω από τους οποίους θα πραγματοποιηθεί η δίκη στην περίπτωση αυτή ορίζεται από τη Σύμβαση της Ρώμης όπως επίσης και από τις Οδηγίες για την προστασία του Καταναλωτή. Αυτό είναι το ισχύον νομικό πλαίσιο, βάσει του οποίου οι αγοραστές και οι πωλητές έχουν την δυνατότητα να αξιοποιούν τις δυνατότητες του ηλεκτρονικού εμπορίου.

1.4. Κατηγορίες Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο σε πρακτικό επίπεδο μπορεί να διαχωριστεί σε τέσσερις πολύ βασικές κατηγορίες οι οποίες είναι οι παρακάτω:

Συναλλαγές μεταξύ επιχειρήσεων (Business-to-Business - B2B)

Αυτός το είδος του ηλεκτρονικού εμπορίου έγκειται στην διενέργεια ηλεκτρονικών εμπορικών συναλλαγών που λαμβάνουν χώρα μεταξύ επιχειρήσεων και οργανισμών παροχής προϊόντων και υπηρεσιών. Η διενέργεια αυτών των συναλλαγών αφορά κυρίως την αγορά προμηθειών. Πρόκειται στην ουσία για την προσομοίωση του χονδρικού εμπορίου που εφαρμόζεται μεταξύ επιχειρήσεων. Το είδος αυτό του ηλεκτρονικού εμπορίου προσφέρει σε επιχειρήσεις και οργανισμούς την δυνατότητα για βελτίωση της μεταξύ τους συνεργασία, κάνοντας πιο απλές τις διαδικασίες και το κόστος των προμηθειών, πιο γρήγορη την αποστολή των προμηθειών και πιο αποτελεσματικό τον έλεγχο του επιπέδου αποθεμάτων (Laudon, Traver, 2011). Επίσης γίνεται ευκολότερη η τήρηση του αρχείου των σχετικών εγγράφων και περισσότερο ποιοτική η εξυπηρέτηση των πελατών. Η αποτελεσματικότητα των δυνατοτήτων των επιχειρήσεων δύναται να γίνει ακόμα καλύτερη δεδομένης της ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς αλλά και μέσω της πραγματοποίησης ηλεκτρονικών πληρωμών. Ιδιαίτερα δε, οι ηλεκτρονικές πληρωμές συγκρατούν τα ποσοστά ανθρώπινου σφάλματος σε χαμηλά επίπεδα ενώ παράλληλα μειώνουν το κόστος των συναλλαγών και αυξάνουν την ταχύτητα ολοκλήρωσης τους. Το ηλεκτρονικό εμπόριο παρέχει τη δυνατότητα στον αγοραστή –καταναλωτή να γνωρίζει πληροφορίες σχετικά με τα προσφερόμενα προϊόντα - είτε μέσω των προμηθευτών είτε μέσω ενδιάμεσων οργανισμών οι οποίοι παρέχουν υπηρεσίες ηλεκτρονικού εμπορίου(Γκιούρδας, 2010).

Οι συναλλαγές μεταξύ επιχειρήσεων λειτουργούν εδώ και χρόνια στην Ελλάδα εδώ κάνοντας χρήση πληθώρας τεχνολογιών, μία από τις οποίες είναι και η Ηλεκτρονική Ανταλλαγή Εγγράφων (EDI – Electronic Data Interchange).

Λιανικές πωλήσεις - Ηλεκτρονικό εμπόριο μεταξύ επιχείρησης και καταναλωτών (Business-to-Consumer - B2C)

Η κατηγορία αυτή είναι η πιο διαδεδομένη στην Ελλάδα αλλά και το εξωτερικό. Πρόκειται για την κατηγορία στην οποία υπάγονται όλες οι εφαρμογές ηλεκτρονικού εμπορίου, οι οποίες αναπτύσσονται με αποκλειστικό σκοπό την απευθείας πώληση προϊόντων σε καταναλωτές. Ο καταναλωτής έχει απεριόριστη πρόσβαση σε μια μεγάλη ποικιλία προϊόντων μέσα από δικτυακά καταστήματα, και μπορεί να βλέπει, να επιλέγει, να συγκρίνει, ακόμα και να «δοκιμάζει» με την χρήση ειδικών προγραμμάτων, τα προϊόντα που θέλει καταλήγοντας εν τέλει στην αγορά. Η ενέργεια αυτή τον γλιτώνει από πολύ κόπο και χρόνο σε σχέση με τους συμβατικούς τρόπους πραγματοποίησης αγορών – υπηρεσιών(Γκιούρδας, 2010).

Εικόνα 1: Online Κατάστημα Ηλεκτρονικών Αγορών

Το εκάστοτε ηλεκτρονικό κατάστημα δεν γνωρίζει τον «ηλεκτρονικό» πελάτη, δεδομένου ότι αυτός μπορεί να είναι κάθε χρήστης του διαδικτύου. Το είδος αυτό του ηλεκτρονικού εμπορίου αναπτύχθηκε με ιδιαίτερα γρήγορους ρυθμούς με την ανάπτυξη και διάδοση του Παγκόσμιου Ιστού (www), όπως αναφέραμε και παραπάνω. Οι επιχειρήσεις και οργανισμοί πληροφορικής, ήταν οι πρώτοι που εφόρμησαν στην τεχνολογία του ηλεκτρονικού εμπορίου, και προώθησαν μια νέα αγορά μέσω του διαδικτύου, προσφέροντας online κάθε είδος προϊόντος και υπηρεσίας στους πελάτες τους.

Ηλεκτρονικό Εμπόριο Επιχείρησης προς Δημόσια Διοίκηση & Καταναλωτή προς Δημόσια Διοίκηση (B2G & C2G)

Οι δύο αυτές κατηγορίες ηλεκτρονικού εμπορίου τις οποίες συνενώσαμε σε μια αφορά τις ηλεκτρονικές συναλλαγές που πραγματοποιούνται μεταξύ επιχειρήσεων αλλά και μεταξύ καταναλωτών με φορείς της Δημόσιας Διοίκησης.

Στην Ελλάδα αυτή η μορφή ηλεκτρονικού εμπορίου είναι σε αρχικά στάδια, ενώ στα πλαίσια του προγράμματος Κοινωνίας της Πληροφορίας προγραμματίζεται μελλοντικά η ανάπτυξη πληθώρας εφαρμογών, οι οποίες θα ευνοούν και θα ενισχύουν τις συναλλαγές των Ελλήνων πολιτών όπως φυσικά και των επιχειρήσεων με την Δημόσια Διοίκηση (Καρανικόλας, 2006). Στην κατηγορία αυτή χαρακτηριστικό παράδειγαμ αποτελεί και το πρόγραμμα TAXIS το οποίο λειτουργεί εδώ και λίγα χρόνια στην Ελλάδα και μέσω του οποίου οι πολίτες μπορούν να κάνουν υποβολή των φορολογικών τους δηλώσεων, δηλώσεων ΦΠΑ, κ.α. Στην παρακάτω εικόνα βλέπουμε ένα στιγμιότυπο αυτής της εφαρμογής.

Εικόνα 2: Πρόγραμμα TAXIS

Οι επιχειρήσεις ανάλογα με τον τομέα στον οποίο δραστηριοποιούνται, αλλά και με βάση τον τύπο και το είδος τους , μπορούν να επιλέξουν να εφαρμόσουν οποιαδήποτε μορφή ηλεκτρονικού εμπορίου θέλουν, η οποία σε κάθε περίπτωση και ανάλογα με τις ανάγκες της θα της προσφέρει τα επιθυμητά θετικά αποτελέσματα, ενώ δεν είναι αδύνατο αν εφαρμόσουν δύο ή και τρία είδη ηλεκτρονικού εμπορίου. Στην Ελλάδα το Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών (ΕΒΕΑ) είναι ο οργανισμός ο οποίος λειτουργεί προκειμένου να ωφελήσει τις επιχειρήσεις - οργανισμούς, οι οποίες επιθυμούν να μάθουν τις νέες τεχνολογίες καθώς και τους τρόπους ένταξης τους στην δραστηριότητά τους, προκειμένου να καταστούν ανταγωνιστικές στις αγορές τις οποίες ανήκουν.

1.5. Πλεονεκτήματα Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο παρέχει μια πληθώρα δυνατοτήτων και πλεονεκτημάτων σε αγοραστές και πωλητές (με την ευρύτερη έννοια) τα οποία είναι τα παρακάτω:

[1] Δίνει σε αγοραστές και πωλητές την δυνατότητα να συμμετέχουν σε μια διεθνή αγορά, άνευ χρονικών και γεωγραφικών περιορισμών. Πιο αναλυτικά τα όρια του ηλεκτρονικού εμπορίου δεν οροθετούνται βάσει γεωγραφικών συνόρων, αλλά έχουν να κάνουν περισσότερο με την κάλυψη των δικτύων του υπολογιστή. Από την μία πλευρά το ηλεκτρονικό εμπόριο δίνει την δυνατότητα σε μικρού μεγέθους επιχειρήσεις και οργανισμούς να περάσουν όχι μόνο στις τοπικές αγορές αλλά να συναλλάσσονται ηλεκτρονικά με τους εταίρους τους σε παγκόσμιο επίπεδο(Γκιούρδας, 2010). Τα αντίστοιχα οφέλη του καταναλωτή είναι ότι είναι σε θέση να διαλέξει μέσα από έναν μεγάλο αριθμό προμηθευτών, το προϊόν ή την υπηρεσία που χρειάζεται κάθε φορά, ανεξάρτητα από την γεωγραφική τους τοποθεσία.

[2] Το ηλεκτρονικό εμπόριο δίνει την δυνατότητα στις επιχειρήσεις να βελτιώσουν την ανταγωνιστικότητα τους, φτάνοντας την στο ίδιο επίπεδο με αυτή των μεγάλων πολυεθνικών εταιριών. Με αυτόν τον τρόπο μπορούμε να πούμε ότι οι επιχειρήσεις προσεγγίζουν περισσότερο τον πελάτη. Επιπλέον, δεδομένου ότι οι περιορισμοί για την είσοδό μιας επιχείρησης στην αγορά είναι ελάχιστοι, δίνεται η δυνατότητα για όλες να δραστηριοποιηθούν στο ηλεκτρονικό εμπόριο(Σκιαδάς, 2001). Πολλές είναι σήμερα οι εταιρείες που εφαρμόζουν ευρέως τις τεχνολογίες του ηλεκτρονικού εμπορίου, με σκοπό να προσφέρουν ένα αναβαθμισμένο επίπεδο στην στήριξη των πωλήσεων με αύξοντα επίπεδα πληροφόρησης για τα προϊόντα και τις υπηρεσίες τους, με ολοκληρωτική καθοδήγηση στην χρήση των προϊόντων τους και παράλληλα με ταχεία ανταπόκριση όταν οι καταναλωτές ζητούν επιπλέον πληροφορίες.

[3] Το ηλεκτρονικό προσφέρει μαζική προσαρμογή στις απαιτήσεις τους πελάτη φέρνοντας τα προϊόντα και υπηρεσίες που επιθυμεί στα μέτρα του. Με το παραπάνω εννοούμε ότι οι προμηθευτές είναι σε θέση να συλλέξουν λεπτομερείς και σημαντικές πληροφορίες σχετικά με το προφίλ των καταναλωτών και με αυτό τον τρόπο αυτομάτως να τους προσφέρουν προϊόντα και υπηρεσίες που είναι κοντά στις προτιμήσεις τους. Ένα πολύ απλό παράδειγμα των παραπάνω αποτελεί ένα ηλεκτρονικό περιοδικό το οποίο είναι ειδικά διαμορφωμένο ακόμα και για τον ιδιαίτερα απαιτητικό αναγνώστη και είναι συμβατό για να τονίσει τα άρθρα εκείνα που πιθανόν είναι ενδιαφέροντα αλλά και για να αποκλείσει τα αντίστοιχα άρθρα που έχουν ήδη διαβαστεί(Πασχόπουλος, 2006).

[4] Ένα ακόμα πλεονέκτημα του ηλεκτρονικού εμπορίου είναι πως μειώνει ή ακόμα και εξαλείφει τους προμηθευτικούς δεσμούς, προσφέροντας άμεση ικανοποίηση αναγκών(Πομπόρτσης, 2002). Ο προμηθευτής λοιπόν κάνοντας χρήση του ηλεκτρονικού εμπορίου φθάνει σε απευθείας επικοινωνία με τον πελάτη του δίχως να είναι απαραίτητη η παρέμβαση τρίτων προσώπων όπως για παράδειγμα η αποστολή προϊόντων χωρίς τη χρήση διαμεταφορέων, ενδιάμεσων αποθηκών κ.α.

[5] Ένα από τα πιο προφανή πλεονεκτήματα του ηλεκτρονικού εμπορίου είναι η ελαχιστοποίηση του κόστους και των τιμών. Τα έξοδα των επιχειρηματικών δραστηριοτήτων όπως το ενοίκιο, η διαφήμιση και προώθηση προϊόντων, η αποθήκευση και η διανομή κάνουν πολύ υψηλό κόστος στη πραγματική αγορά. Αντίθετα, τα έξοδα για μια επιχειρηματική ηλεκτρονική διεκπεραίωση είναι δυνατό να γίνει με πολύ μικρότερο κόστος αλλά και μέσα σε πολύ λιγότερο χρονικό διάστημα. Έτσι το ηλεκτρονικό εμπόριο και η καθιέρωση τους από τις επιχειρήσεις μπορεί να αποδώσει μείωση στα λειτουργικά τους έξοδα, και η μείωση αυτή μεταφέρεται στην τιμή του τελικού προϊόντος το οποίο πωλείται στους καταναλωτές. (Laudon, Traver, 2011).

[6] Μέσω του ηλεκτρονικού εμπορίου οι διευθυντές των επιχειρήσεων και οργανισμών έχουν την ικανότητα να αντιπαραβάλλουν προμηθευτές. Ο κόσμος του ηλεκτρονικού εμπορίου είναι από μόνος του ένας καινούργιος επιχειρηματικός κόσμος, στον οποίο οι δυνατότητες που παρέχονται βρίσκονται ακόμη σε χαμηλό επίπεδο. Έτσι προσφέρονται στις επιχειρήσεις-οργανισμούς σε συνεχή βάση, νέες επιχειρηματικές ευκαιρίες προκειμένου να αναπτύξουν νέα προϊόντα και υπηρεσίες.

1.6. Μειονεκτήματα Ηλεκτρονικού Εμπορίου

Σήμερα είναι κοινώς αποδεικτικό πως το διαδίκτυο κατέχει μεγάλο όγκο, προσφέροντας άκριτα μια πληθώρα πληροφοριών που καταιγίζει τους χρηστές του. Παρά τα πλεονεκτήματα που έχει το ηλεκτρονικό εμπόριο, μια μεγάλη μερίδα πληθυσμού αντιμάχεται σε αυτό για τους παρακάτω λόγους(Laudon, Traver, 2011):

[1] Πολλοί καταναλωτές δυσκολεύονται να εμπιστευθούν τις συναλλαγές μέσω διαδικτύου κυρίως για λόγους ασφάλειας. Είναι κοινή αλήθεια πως το διαδίκτυο είναι ένα μέσο που δεν παρέχει το επιθυμητό επίπεδο ασφάλειας στις συναλλαγές, με αποτέλεσμα και οι συναλλαγές να κρίνονται μη ασφαλείς. Πάνω στον τομέα αυτό, επειδή είναι ιδιαίτερα σημαντικός, γίνεται εκτεταμένη έρευνα ούτως ώστε οι συναλλαγές να

πραγματοποιούνται με όσο το δυνατόν περισσότερη ασφάλεια(Καρανικόλας, 2006). Ωστόσο, υπάρχουν και ηλεκτρονικά συστήματα πληρωμών τα οποία εφαρμόζονται τα τελευταία χρόνια και τα οποία έχουν λύσει εν μέρει τα περισσότερα και σημαντικότερα προβλήματα ασφάλειας ενώ ταυτόχρονα είναι και πιο ευέλικτα από τις παραδοσιακές μεθόδους πληρωμών.

[2] Δεν υπάρχει επαρκής έλεγχος σχετικά με την ποιότητα των παρεχόμενων προϊόντων/υπηρεσιών. Πολλά είδη επιχειρήσεων όπως εταιρίες πώλησης ρούχων και υποδημάτων, επιχειρήσεις διανομής ευαίσθητων τροφίμων, κοσμημάτων, κ.α. είναι πρακτικά αδύνατον, να ελεγχθούν ικανοποιητικώς για την ποιότητα των προϊόντων που παρέχουν στο καταναλωτικό κοινό, λόγω της απομακρυσμένης τοποθεσίας τους, αν και υπάρχουν εξαιρέσεις(Πολλάλης, Γιαννακόπουλος, 2007)..

[3] Οι τεχνολογίες που χρησιμοποιούνται στο ηλεκτρονικό εμπόριο είναι πολλές και διάφορες και θα τις δούμε αναλυτικά παρακάτω. Το κόστος για τη δημιουργία ενός απλού ηλεκτρονικού καταστήματος δύναται να μεταβληθεί δραματικά, από την χρήση των ήδη υπαρχουσών τεχνολογιών αλλά και από τις νέες τεχνολογίες που καθημερινά προστίθενται. Εκτός αυτού ακόμα και όταν οι τεχνολογίες εφαρμοστούν, οι επιχειρήσεις θα πρέπει να επενδύουν μεγάλα χρηματικά ποσά κάθε χρόνο για τη συντήρηση και βελτίωση των ηλεκτρονικών τους καταστημάτων.

[4] Υπάρχει έλλειψη επαφής μεταξύ του πωλητή και του καταναλωτή. Το φαινόμενο επιδρά συνήθως αρνητικά στον καταναλωτή με αποτέλεσμα να του δημιουργεί δυσπιστία αφού δεν έρχεται σε άμεση επαφή ούτε με το προϊόν αλλά ούτε και με τον πωλητή, και έτσι δεν μπορεί να είναι βέβαιος ότι το προϊόν που υπάρχει στην οθόνη του είναι και στην πραγματικότητα αυτό το οποίο θα παραλάβει, ή αν αυτά που ισχυρίζεται η εταιρία για το προϊόν είναι όντως αληθινά.

[5] Με το ηλεκτρονικό εμπόριο τίθενται προβλήματα βιωσιμότητας ορισμένων παραδοσιακών εμπορικών επιχειρήσεων, οδηγώντας σε μια σταδιακή έκλειψη των παραδοσιακών μορφών πώλησης, κάτι που με την σειρά του

επιφέρει μια πληθώρα άλλων μειονεκτημάτων με το κυριότερο τις απολύσεις εργαζομένων.

[6] Ακόμα όσο αφορά τους εργαζόμενους γνωρίζουμε ότι η παραδοσιακή απασχόληση ρυθμίζεται στην Ελλάδα από την αντίστοιχη εργατική νομοθεσία και τις συλλογικές συμβάσεις εργασίας. Ωστόσο είναι πιθανό η εργασία στο ηλεκτρονικό εμπόριο να μην προστατεύεται τοιουτοτρόπως και συνεπώς η μείωση του κόστους εργασίας θα αυξάνει την ανταγωνιστικότητα (Καρανικόλας, 2006). Αυτό σημαίνει ότι οι επιχειρήσεις θα απαιτούν από τους εργαζόμενους τους περισσότερα και καινούργια προσόντα, ικανότητες και δεξιότητες , γεγονός το οποίο ενδέχεται να δυσκολεύει την προσαρμογή τους στις νέες απαιτούμενες συνθήκες εργασίας.

[7] Η εξυπηρέτηση διαδικασιών b2c μεγάλης κλίμακας απαιτεί υψηλά αυτοματοποιημένα συστήματα και αποθήκες προϊόντων, αυξάνοντας ιδιαίτερα το κόστος της δημιουργίας ενός ηλεκτρονικού καταστήματος.

Συμπερασματικά μπορούμε να πούμε ότι το διαδίκτυο ως εμπορικό μέσο συνεπάγεται έναν αριθμό από σημαντικά ελαττώματα και κινδύνους που σχετίζονται με τις εμπορικές επικοινωνίες και συναλλαγές. Οι κίνδυνοι και τα μειονεκτήματα πηγάζουν κυρίως από τα δομικά χαρακτηριστικά του internet και περιλαμβάνουν την αλλαγή του επιχειρησιακού περιβάλλοντος, τεχνολογικά ζητήματα και ατέλειες του παροντικού επιπέδου τεχνολογίας, προβλήματα ασφάλειας, νομικά ζητήματα, δημόσιες και κοινωνικές τακτικές, μεγαλύτερο συναγωνισμό και φυσικά το κόστος. Αυτά τα μειονεκτήματα σχετίζονται με την δικτυακή τεχνολογία και την αλληλεπιδρούσα φύση του Δικτύου(Laudon, Traver, 2011).

Το σημαντικότερο πάντως μειονέκτημα του έγκειται αναμφίβολα σε θέματα ασφάλειας. Ένα αρκετά μεγάλο ποσοστό των χρηστών του διαδικτύου δεν εμπιστεύεται το Δίκτυο ως μέσο πληρωμής. Οι αγοραπωλησίες μέσω του Web και ιδιαίτερα αυτές που πραγματοποιούνται με τη χρήση πιστωτικής κάρτας συνεχίζουν ακόμα και σήμερα να παραμένουν μη ασφαλείς. Όσοι πραγματοποιούν συναλλαγές

μέσω διαδικτύου με την πιστωτικής του κάρτας στο Δίκτυο δεν θα μπορούν ποτέ να είναι σίγουροι για την ταυτότητα του ηλεκτρονικού πωλητή, ενώ και από την άλλη πλευρά ο πωλητής δεν θα είναι σε θέση να γνωρίζει την ταυτότητα του καταναλωτή. Καμία από τις δύο πλευρές (αγοραστές και πωλητές) δεν μπορεί να εγγυηθεί στην άλλη την ασφάλεια της συναλλαγής ούτε στον καταναλωτή πως ο αριθμός της κάρτας του με την οποία πραγματοποιεί τις ηλεκτρονικές συναλλαγές δεν θα καταλήξει κάπου στο internet και θα γίνει χρήση της για μοχθηρούς σκοπούς. Επιπλέον κανένας δεν βρίσκεται σε θέση να εγγυηθεί και στον πωλητή πως ο ιδιοκτήτης της πιστωτικής κάρτας θα αποδεχθεί την αγοραπωλησία(Σκιαδάς, 2001). Πρόκειται για ένα ιδιαίτερα σοβαρό ζήτημα το οποίο θα μας απασχολήσει ιδιαίτερα στην παρούσα εργασία.

1.7. Τα εργαλεία του Ηλεκτρονικού Εμπορίου

Τα εργαλεία του ηλεκτρονικού εμπορίου που θα παρουσιαστούν διαφοροποιούνται ως προς το εύρος των δυνατοτήτων που το κάθε ένα παρέχει, διευρυνόμενα σε εργαλεία για την κατασκευή μια ολοκληρωμένης δικτυακής παρουσίας μέχρι σουίτες για την παροχή ολοκληρωμένων λύσεων για το ηλεκτρονικό εμπόριο(Πομπόρτσης, 2002).

Ακόμα κάποια από αυτά είναι εμπορικά, ενώ κάποια άλλα είναι διαθέσιμα με τη μορφή Ανοικτού Κώδικα (OpenSource SoftWare) και κατά συνέπεια χωρίς ουσιαστική χρέωση. Εκτός από τα κυριότερα χαρακτηριστικά κάθε εργαλείου, παρατίθενται και μια σειρά από συνδέσμους σε δικτυακούς τόπους που έχουν υιοθετήσει με τον ένα ή τον άλλο τρόπο την συγκεκριμένη πλατφόρμα. Οι κυριότερες είναι(Laudon, Traver, 2011):

Microsoft Commerce Server

Πρόκειται για ένα λογισμικό που παρέχει η Microsoft για την ανάπτυξη ολοκληρωμένων λύσεων ηλεκτρονικού εμπορίου, εφαρμογή που είναι ιδιαίτερα

δημοφιλής καθώς δίνει την δυνατότητα χρήσης ευέλικτου συστήματος δημιουργίας προφίλ, κάτι το οποίο με την σειρά του παρέχει την δυνατότητα διατήρησης καταλόγων, τιμολόγησης και επεξεργασία επιχειρηματικών δεδομένων προσαρμοσμένων στις ανάγκες των χρηστών, ευέλικτο σύστημα καταλόγων προϊόντων, το οποίο παρέχει καθολικούς καταλόγους, με δυνατότητα παροχής προϊόντων/τιμών για πολλαπλές χώρες νομίσματα, εικονικούς καταλόγους οι οποίοι δίνουν τη δυνατότητα συνδυασμού καταλόγων από πολλαπλούς προμηθευτές, εισαγωγή/εξαγωγή StreamlinedXML καταλόγων και δυνατότητα συνεργασίας με τον MicrosoftBizTalkServer, αναζήτηση σε καταλόγους και εύκολη διαχείριση καταλόγων με το BusinessDesk.

Όσο αφορά την ασφάλεια των δεδομένων, αυτή εξασφαλίζεται με μονόπλευρο κατακερματισμό (one-wayhashing) και ασύμμετρη κρυπτογράφηση, μέθοδοι με τις οποίες θα ασχοληθούμε ιδιαίτερα σε επόμενο κεφάλαιο. Τέλος η παράμετρος της αποθήκευσης εναποτίθεται στον MicrosoftSQLServer, την εφαρμογή βάσεων δεδομένων της Microsoft.

Microsoft BizTalk Server

Ο BizTalkServer αποτελεί επίσης μια εφαρμογή της Microsoft η οποία διευκολύνει την αυτοματοποίηση της επικοινωνίας για την ανταλλαγή δεδομένων μεταξύ επιχειρήσεων αλλά και σε ενδοεπιχειρησιακό επίπεδο. Υποστηρίζονται όλα τα καθιερωμένα πρότυπα ανταλλαγής δεδομένων όπως EDI(EDIFACT), XML 1.0, SOAP 1.1. Επιπλέον η ασφαλής μεταφορά δεδομένων επιτυγχάνεται μέσω του προτύπου SecureMIME (S/MIME). Πρόκειται για ένα ισχυρό εργαλείο το οποίο διατείνεται στην συνεργασία με την πλατφόρμα CommerceServer.

Microsoft Exchange

Η εφαρμογή αυτή έχει σχεδιαστεί για να υποβοηθήσει την ανταλλαγή μηνυμάτων στις τάξεις της εταιρείας. Πιο συγκεκριμένα παρέχει μια πλατφόρμα για

την ανταλλαγή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου (e-mail) αλλά και την συνεργασία εντός του ενδοδικτύου (Intranet) της εταιρείας. Το Microsoft Exchange συνεργάζεται με την γνωστή εφαρμογή MicrosoftOutlook για την ανταλλαγή μηνυμάτων, ενώ έχει ενδιαφέρον να αναφερθεί ότι συνοδεύεται από χαρακτηριστικά που διευκολύνουν τη συνεργασία από απόσταση όπως, διεπαφή του Outlook μέσω διαδικτύου, επικοινωνία μέσω κινητών συσκευών που υποστηρίζουν XHTML φυλλομετρητές, μέσω υπολογιστών παλάμης της οικογένειας PocketPC και κινητών δικτύων IEEE 802.11. Τα ζητήματα ασφάλειας σε αυτήν την περίπτωση αντιμετωπίζονται και εδώ με τη χρήση SecureMIME.

Open Source Commerce

Πρόκειται για μία πλατφόρμα ηλεκτρονικού εμπορίου η οποία είναι αρκετά δημοφιλής. Αυτό συμβαίνει χάρη στο γεγονός ότι δίνεται δωρεάν και στηρίζεται σε τεχνολογίες ελευθέρου λογισμικού (Apache,MySql) και χάρη στο ότι η πλατφόρμα δύναται να παραμετροποιηθεί ολοσχερώς κατά περίπτωση αλλάζοντας τον κώδικα. Οι κυριότερες από τις λειτουργίες που παρέχει στους χρήστες της είναι λειτουργίες λογαριασμών πελατών, κατάλογος διευθύνσεων πελατών, ιστορικό παραγγελιών, κατάλογος προϊόντων (και αναζήτηση εντός των καταλόγων θέτοντας ορισμένα κριτήρια π.χ. αναζήτηση με βάση το είδος ή τον κατασκευαστή, κλπ), αξιολόγηση προϊόντων από πελάτες, ενημερώσεις μέσω e-mail, καλάθι αγορών και πλήρης επεξεργασία του, ασφαλείς επικοινωνία μέσω SSL, αριθμός διαθέσιμων προϊόντων (stock), παρουσίαση δημοφιλών προϊόντων, παρουσίαση εναλλακτικών αγορών και αγορών που έγιναν με ένα συγκεκριμένο προϊόν, εισαγωγή/ προσθήκη/ επεξεργασία/ διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών και αξιολογήσεων, στατιστικά για τα προϊόντα και τους πελάτες, δυναμική επεξεργασία χαρακτηριστικών προϊόντων, διατήρηση κατηγοριών φορολόγησης, και πολλά άλλα (Πασχόπουλος, 2006).

Yahoo Store

Πρόκειται για ένα διαδικτυακό σύστημα μέσω του οποίου μπορεί ο οποιοσδήποτε να σχεδιάσει και να διαχειρισθεί πλήρως ένα ηλεκτρονικό κατάστημα. Κύριο πλεονέκτημα αυτής της εφαρμογής είναι ότι το ηλεκτρονικό κατάστημα έχει την δυνατότητα να φιλοξενηθεί σε εξυπηρετητή του Yahoo γεγονός που κάνει το ανέβασμα του καταστήματος στο δίκτυο πιο γρήγορο. Μερικές από τις λειτουργίες που παρέχει έχουν να κάνουν με τον σχεδιασμός εμφάνισης του καταστήματος και τις παραμέτρους αυτού, όπως η εμφάνιση, το λογότυπο, τα χρώματα γραμματοσειρές, η διαχείριση από απόσταση, η λήψη των παραγγελιών είτε μέσω του web είτε μέσω email , fax. Επιπλέον παρέχει ασφαλή επικοινωνία μέσω SSL. Ακόμα επιτρέπει την εισαγωγή/ προσθήκη/ επεξεργασία/ διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών και αξιολογήσεων, ιστορικό παραγγελιών, κατάλογο προϊόντων, ενημερώσεις μέσω E-mail, καλάθι αγορών και πλήρης επεξεργασία του, αριθμό διαθέσιμων προϊόντων, παρουσίαση εναλλακτικών αγορών και αγορών που έγιναν με ένα συγκεκριμένο προϊόν και τέλος στατιστικά προϊόντων.

PHP Auction

Η εφαρμογή php auction θεωρείται μία από τις πιο πλήρης στην κατηγορία των ηλεκτρονικών δημοπρασιών, λόγω του χαμηλού κόστους απόκτησης της και του γεγονότος ότι στηρίζεται σε ελεύθερες αρχιτεκτονικές (Apache/MySql). Οι κύριες λειτουργίες της αφορούν την εγγραφή μέλους σε ένα ηλεκτρονικό κατάστημα, την δημιουργία καταλόγων δημοπρατούμενων προϊόντων-και την χρήση ευρετηρίου, αναζήτηση, πληροφορίες δημοπρασίας, ασφάλεια - χρήση προσωπικών κωδικών, πιστοποίηση, προφίλ πελάτη, προτάσεις – προτεινόμενες δημοφιλείς δημοπρασίες, προφίλ εταιρίας, πληροφορίες επικοινωνίας, φόρμα

επικοινωνίας, νέα και γεγονότα, Newsletter, χώροι συζήτησης, χάρτες, νομικό πλαίσιο, δημοπρασίες χρήστη, και πολλά άλλα.

PHP Shop

Πρόκειται για μια ακόμη πρόταση ελευθέρου λογισμικού, η οποία συνεχώς αυξάνεται και βελτιώνεται από την OpenSource κοινότητα. Η εφαρμογή δείχνει να είναι αρκετά δημοφιλής εξαιτίας παραγόντων όπως το μηδενικό της κόστος, η πληρότητα της αλλά και οι μεγάλες δυνατότητες παραμετροποίησης που εμφανίζει. Οι κύριες λειτουργίες που υποστηρίζει είναι κατάλογος προϊόντων (αναζήτηση με βάση το είδος ή τον κατασκευαστή), διαχείριση καταλόγου: εισαγωγή/ προσθήκη/ επεξεργασία/ διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών, κ.α., τήρηση λογαριασμών πελατών, κατηγορίες/ ομάδες αγοραστών, πολιτικές χρέωσης για κάθε ομάδα αγοραστών, αξιολόγηση προϊόντων από πελάτες, καλάθι αγορών και πλήρης επεξεργασία του ανά πάσα στιγμή, ασφαλής επικοινωνία μέσω SSL, αριθμός διαθέσιμων προϊόντων, παρουσίαση δημοφιλών προϊόντων, παρουσίαση εναλλακτικών αγορών και αγορών που έγιναν με ένα συγκεκριμένο προϊόν, στατιστικά προϊόντων και πελατών, διαχείριση των τρόπων πληρωμής και παράδοσης.

Web Sphere

Το WebSphere είναι εφαρμογή της εταιρείας IBM στον τομέα του ηλεκτρονικού εμπορίου. Η λογική της δημιουργίας αυτού του προϊόντος ξεφεύγει από το στενά όρια της δημιουργίας και υποστήριξης λειτουργιών ηλεκτρονικού καταστήματος καθώς στοχεύει και περαιτέρω στην υποστήριξη όσο το δυνατόν πιο ευρείας γκάμας επιχειρηματικών μοντέλων. Η πλατφόρμα του αποτελείται από άλλες μικρότερες εφαρμογές οι οποίες είναι:

- Application Developer: Είναι εκείνο το εργαλείο ανάπτυξης εφαρμογών για ηλεκτρονικό εμπόριο που συνοδεύει το WebSphere.

- Studio: εφαρμογή για ολοκληρωμένη ανάπτυξη και διαχείριση διαδικτυακών τόπων.
- Portal: Περιβάλλον για ανάπτυξη και διαχείριση δικτυακών πυλών, για σενάρια τόσο B2B όσο και B2C. Περιλαμβάνει δυνατότητες προσωποποίησης (personalization) και φιλτραρίσματος πληροφοριών για τους χρήστες και πρόσβαση σε portlets για την ενσωμάτωση στο επιχειρηματικό μοντέλο εφαρμογών ERP, CRM και Διαχείρισης Αλυσίδας Προμηθειών.
- Commerce: Αποτελεί το κύριο μέρος της εφαρμογής, το οποίο προσφέρει λύσεις για τις πωλήσεις, τις αγορές και την διαχείριση καναλιών

Οι κύριες λειτουργίες του Web Sphere είναι ο έλεγχος πρόσβασης και χαρακτηριστικά διαχείρισης χρηστών και δημιουργίας προφίλ, η διαχείριση καταλόγων, η συνεργασία σε συνεργατικούς χώρους εργασίας για την έκδοση Business και υποστήριξη χρηστών, διαχείριση αποθήκης, με τη βοήθεια του CommerceServer, αναζήτηση σε καταλόγους, σύμβουλο προϊόντων, διαχείριση password, με πρόνοια για την ακύρωση λογαριασμών που δεν χρησιμοποιούνται και καταγραφή προσβάσεων, διενέργεια διαφημιστικών εκστρατειών, διαχείριση εκπτώσεων και προώθησης προϊόντων, προσθήκη Business Intelligence με την εμπλοκή του IBM DB2 IBM Intelligent Miner for Data, παραγωγή αναφορών για κατηγορία, προϊόν, κατάσταση παραγγελίας, ανάλυση της κίνησης στο δικτυακό κατάστημα, υποστήριξη συστήματος πληρωμών με τεχνολογία paymentcassettes και σε συνεργασία με το πρωτόκολλο SSH και πολλές άλλες λειτουργίες.

1.8. Μοντέλα του Ηλεκτρονικού Εμπορίου

Η έννοια «μοντέλο» αποτελεί στην ουσία μία θεωρητική περιγραφή της πραγματικότητας. Ο δημιουργός ενός μοντέλου προσδιορίζει τις όψεις του πραγματικού συστήματος που τον αφορούν με άμεσο τρόπο και τα στοιχεία του υπό εξέταση συστήματος τα οποία σκοπεύει να μοντελοποιήσει (Πομπόρτσης, 2002).

Η έννοια του «Επιχειρησιακού Μοντέλου» ορίζεται ως μία συμβολική περιγραφή της επιχείρησης-οργανισμού καθώς επίσης και των θεμάτων που σχετίζονται άμεσα με αυτήν και απαρτίζεται από μεταξύ τους συμπληρωματικά μοντέλα των επιμέρους πλευρών της επιχείρησης. Το επιχειρησιακό μοντέλο ενέχει περιγραφές αποσπασματικών γεγονότων, αντικειμένων, σχέσεων και συναλλαγών οι οποίες λαμβάνουν χώρα στο εσωτερικό της επιχείρησης(Γκιούρδας, 2010).

Αναπτύξαμε την έννοια του επιχειρησιακού μοντέλου παραπάνω, προκείμενου να δούμε τις διάφορες όψεις που έχει λάβει σήμερα το ηλεκτρονικό εμπόριο. Στην παρούσα παράγραφο θα παραθέσουμε τις πιο σημαντικές και ευρέως χρησιμοποιούμενες οι οποίες είναι οι παρακάτω(Πολλάλης, Γιαννακόπουλος, 2007).:

e-business

Το ηλεκτρονικό επιχειρείν ή αλλιώς e-business είναι ένας όρος που χρησιμοποιείται ευρέως τα τελευταία χρόνια θεωρητικά αλλά και στην πράξη. Με τον όρο αυτό εννοούμε μια ευρύτερη έννοια του ηλεκτρονικού εμπορίου. Ως ηλεκτρονικό επιχειρείν (e-business) ορίζουμε ένα σύνολο από επιχειρηματικές στρατηγικές που στόχο έχουν να υποστηρίξουν και να μετασχηματίσουν τους τομείς εκείνους της επιχειρηματικής δραστηριότητας, κάνοντας χρήση νέων τεχνολογιών και διεκπεραιώνοντας συναλλαγές με ηλεκτρονικά μέσα. Πολύ συχνά οι όροι ηλεκτρονικό επιχειρείν και ηλεκτρονικό εμπόριο συγχέονται, ενώ ωστόσο πρόκειται για δύο διαφορετικά πράγματα. Ο όρος ηλεκτρονικό επιχειρείν περιλαμβάνει όλες τις οικονομικές κινήσεις και δραστηριότητες μιας επιχείρησης- οργανισμού που υποστηρίζονται κάνοντας χρήση ηλεκτρονικών μέσων. Το ηλεκτρονικό επιχειρείν περιλαμβάνει προμήθειες και εσωτερικές διεργασίες μιας επιχείρησης αλλά και τις συναλλαγές και όλες εκείνες τις επιχειρηματικές διαδικασίες οι οποίες προσφέρουν δράσεις πώλησης και αγοράς μέσω του διαδικτύου. Αντιθέτως, το ηλεκτρονικό εμπόριο συγκροτεί μια όψη του παραπάνω συνόλου, και στην ουσία πρόκειται για μία εφαρμογή η οποία απευθύνεται σε πιο ευρύ αγοραστικό κοινό με στόχο να συμβάλει στην επικοινωνία μεταξύ αγοραστών και επιχειρήσεων.

Μια επιχείρηση μπορεί να έχει εμπορική παρουσία στο διαδίκτυο μέσω ενός μεγάλου αριθμού διαφορετικών τρόπων, τους οποίους θα περιγράψουμε παρακάτω. Θα αναφερθούμε στις έννοιες των μοντέλου καταστήματος, μοντέλου δημοπρασιών, μοντέλου πύλης και μοντέλου δυναμικής τιμολόγησης. Κάθε επιχείρηση-οργανισμός που ενδιαφέρεται πραγματικά για την εμπορική της παρουσία στο διαδικτύου πρέπει να έχει υπόψη της και να μελετάει τα e-επιχειρείν μοντέλα αλλά και τον τρόπο με τον οποίο αυτά υλοποιούνται.

e-shop (Μοντέλο Καταστήματος)

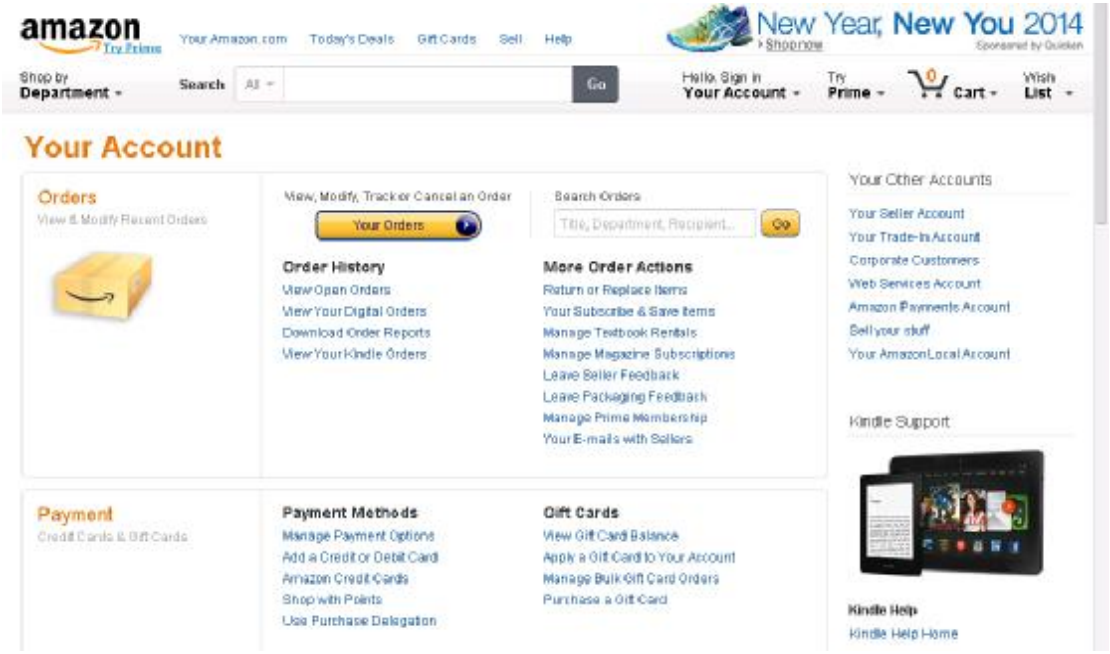
Το μοντέλο καταστήματος είναι ίσως ένα από τα πιο διαδεδομένο από όλα τα μοντέλα του ηλεκτρονικού εμπορίου. Ο έμπορος-προμηθευτής δίνει την δυνατότητα στους ενδιαφερόμενους να δούν έναν ηλεκτρονικό κατάλογο ο οποίος περιέχει τα παρεχόμενα προϊόντα και υπηρεσίες του, και ο πελάτης μπορεί να κάνει παραγγελίες μέσω του δικτυακού τόπου της εταιρείας του πωλητή. Το e-shop συνδυάζει πολλές παραμέτρους μαζί: την ασφάλεια, την επεξεργασία των εμπορικών συναλλαγών και την αποθήκευση όλων των πληροφοριών στη βάση δεδομένων του ηλεκτρονικού καταστήματος.

Επίσης αξίζει να αναφερθούμε και στο καλάθι αγορών (Shopping card ή basket) το οποίο αποτελεί ένα συστατικό στοιχεί του μοντέλου καταστήματος. Πρόκειται για μια τεχνολογία η οποία παρέχεται από το eshop και η οποία επεξεργάζεται τις παραγγελίες των καταναλωτών, δίνοντας τους την δυνατότητα να προσθέτουν τα επιθυμητά προς αγορά προϊόντα, κατά την διάρκεια επίσκεψης τους στο ηλεκτρονικό κατάστημα. Ολοκληρώνοντας ο καταναλωτής την παραγγελία του οι πληροφορίες του καλαθιού αποθηκεύονται σε μια βάση δεδομένων μαζί με τα προσωπικά στοιχεία του πελάτη, τα οποία ο ίδιος έχει παραθέσει προκειμένου να κάνει την παραγγελία του.

Ένα από τα ίσως πιο δημοφιλή eshops το οποίο υλοποιούν το μοντέλο καταστήματος είναι η Amazon (http://amazon.com), η λειτουργία της οποίας ξεκίνησε το 1994 με την πώληση αρχικά βιβλίων μέσω του διαδικτύου. Σήμερα πρόκειται ένα πανίσχυρο e-shop το οποίο συνεχίζει να επεκτείνει την ποικιλία των

προϊόντων της προσφέροντας πληθώρα καταναλωτικών αγαθών όπως ηλεκτρονικές συσκευές, μουσικά Cds, ταινίες video, DVDs, παιχνίδια, κ.α. Οι καταναλωτές του Amazon έχουν τη δυνατότητα μέσω της ιστοσελίδας αυτής να αφήνουν κριτικά σχόλια για τα προϊόντα που έχουν αγοράσει και τα οποία εμφανίζονται ανά συγκεκριμένο βιβλίο. Επιπλέον η ιστοσελίδα διαθέτει σύστημα καταγραφής των κινήσεων των πελατών το οποίο στηρίζεται στις προηγούμενες αγορές που έχουν κάνει αλλά και στις αναζητήσεις που έκανα για διάφορα προϊόντα στο παρελθόν. Έτσι κάθε φορά που κάποιος επισκέπτεται το ηλεκτρονικό κατάστημα της Amazon, του γίνονται αυτομάτως οι ανάλογες προτάσεις και εκθέσεις για προϊόντα που πιθανόν να τον ενδιαφέρουν περισσότερο.

Τα τελευταία χρόνια μάλιστα έκανε την εμφάνιση του στο Amazon ένα νέο διαφορετικό σύστημα, το λεγόμενο I-Click. Το σύστημα αυτό δίνει την δυνατότητα στους πελάτες της συγκεκριμένης ιστοσελίδας να χρησιμοποιήσουν τις ίδιες πληροφορίες τις οποίες εισήγαγαν στις προγενέστερες παραγγελίες τους, με πολύ απλό τρόπο. Έτσι από την στιγμή που εμπορεύονται συχνά με την ιστοσελίδα και πραγματοποιούν ηλεκτρονικά αγορές, δεν είναι υποχρεωμένοι να εισάγουν συνέχεια τα προσωπικά τους και άλλα στοιχεία προκειμένου να ολοκληρώσουν μια αγορά. Τα εμφανίζονται μόνα τους, ενώ φυσικά υπάρχει η δυνατότητα μεταβολής τους από τον χρήστη.



Εικόνα 3: Στιγμιότυπο Ιστοσελίδας Ηλεκτρονικού Εμπορίου Amazon

Ακόμα τα τελευταία χρόνια έχουν κάνει την εμφάνιση τους στο διαδίκτυο και τα ηλεκτρονικά εμπορικά κέντρα (Malls), που είναι στην ουσία ηλεκτρονικά πολυκαταστήματα, τα οποία προσφέρουν μια μεγάλη συλλογή από προϊόντα και υπηρεσίες. Το κυριότερο πλεονέκτημα που προσφέρουν στους καταναλωτές τους είναι η πραγματοποίηση αγοράς πολλών διαφορετικών προϊόντων μέσω μιας μόνο συναλλαγής.

E-Auction (μοντέλο δημοπρασιών)

Το e-auction εργάζεται ως ένα σημείο συναπαντήματος των χρηστών του διαδικτύου οι οποίοι έχουν είτε τον ρόλο του καταναλωτή που θέλει να πουλήσει είτε του εμπόρου που επιθυμεί να κάνει μια προσφορά. Η επιχείρηση Forrester Research που κάνει έρευνες πάνω σε θέματα τα οποία σχετίζονται άμεσα με το διαδίκτυο βρήκε πως μόνο κατά την διάρκεια του 2000 ξοδεύτηκαν περίπου 3,8 δισεκατομμύρια δολάρια σε δημοπρασίες μέσω του διαδικτύου (Σκιαδάς, 2001). Από τα πιο δημοφιλή e-shops τα οποία σήμερα που υλοποιούν αποκλειστικά και μόνο το μοντέλο δημοπρασιών είναι η εταιρία Fleamarket (http://www.emarket.gr) η οποία στην πράξη δίνει δωρεάν στα δύο μέρη (πωλητή-αγοραστή) το εφικτό εκτέλεσης αυτοματοποιημένων συναλλαγών για μια αγοραπωλησία. Ο τρόπος πώλησης ή αγοράς ενός προϊόντος προσομοιώνει κάπως την διαδικασία τοποθέτησης μικρών αγγελιών, με τη βασική διαφορά όμως ότι ο καταναλωτής ή ο έμπορος έχει τον πλήρη έλεγχο της αγγελίας ή της προσφοράς του.

Εικόνα 4: Στιγμιότυπο Ιστοσελίδας Διενέργειας Ηλεκτρονικών Δημοπρασιών Forrester

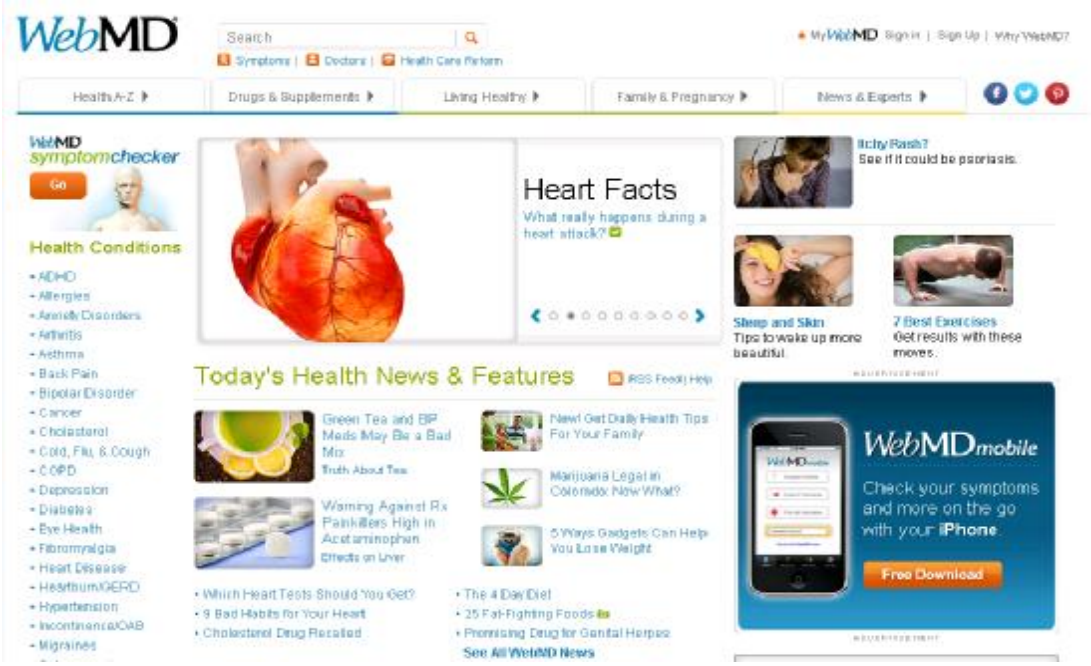
Μέσω του e-auction ο πωλητής φέρει την ικανότητα να παρουσιάζει το αντικείμενο ή τα αντικείμενα ενδιαφέροντος, συνοδευόμενα πάντα από λεπτομέρειες περιγραφής, όπως φωτογραφίες, αρχική τιμή και περίοδο διάθεσης τους ενώ αντίστοιχα στους υποψήφιους αγοραστές παρέχεται το εφικτό αναζήτησης σε ένα μεγάλο πλήθος κατηγοριών -ειδών, επισκόπησης των υποκείμενων υπό πώληση, συνεχής παρακολούθησης και ελέγχου των ήδη υποβληθέντων προσφορών τους και εισήγησης νέων προσφορών μέσω αυτοματοποιημένων ηλεκτρονικών συστημάτων. Οι χρήστες αξιολογούνται μεταξύ τους ηλεκτρονικά ώστε να διακρίνονται οι συνέπειες και αξιόπιστοι χρήστες από ασυνεπείς.

E-Portal (μοντέλο πύλης)

Το e-portal δίνει στους επισκέπτες της εκάστοτε ιστοσελίδας που επισκέπτονται οι χρήστες, το εφικτό αναζήτησης και εύρεσης πληροφοριών σχετικά με τα θέματα που τους ενδιαφέρουν. Οι περισσότεροι χρήστες του διαδικτύου έχουν

συνδυάσει τη λέξη πύλη με τις μηχανές αναζήτησης, χωρίς ωστόσο να πρόκειται για ίδιες εφαρμογές(Γκιούρδας, 2010). Οι μηχανές αναζήτησης είναι πύλες οι οποίες περικλείουν γενικού ενδιαφέροντος πληροφορίες για ένα πολύ σημαντικό πλάτος ζητημάτων τα οποία αναζητούνται σε τεραστίου όγκου βάσεις δεδομένων και ανήκουν στην κατηγορία των οριζόντιων πυλών. Η επόμενη κατηγορία πυλών είναι οι κάθετες πύλες, οι οποίες περικλείουν εκτενέστερες πληροφορίες πάνω σε ένα αναλυτικό θέμα και είναι τα λεγόμενα Portals, με τα οποία ασχολούμαστε στην παρούσα παράγραφο.

Επιπλέον, πληθώρα πυλών εντός του διαδικτύου περιέχουν και το μοντέλο δημοπρασιών, το οποίο αναφέραμε παραπάνω, καθώς επίσης και το μοντέλο καταστήματος δίνοντας έτσι ένα πιο ολοκληρωμένο περιβάλλον ηλεκτρονικών συναλλαγών. Ένα ακόμα πολύ σημαντικό πλεονέκτημα των Portals είναι η προσαρμογή τους στις βουλήσεις του κάθε επισκέπτη. Αυτό στην πράξη σημαίνει πως παρέχεται η δυνατότητα στους επισκέπτες της μόρφωσης της παρουσίασης και του περιεχομένου αυτών των ιστοτόπων με την πρόσθεση ή την αφαίρεση στοιχείων, ανάλογα με τα προσωπικά τους ενδιαφέροντα και τις προτιμήσεις τους. Έτσι την επόμενη φορά που ο ίδιος επισκέπτης πάει στον δικτυακό τόπο, αυτός θα έχει τη μορφή που του καθόρισε ο ίδιος. Οι πιο γνωστές οριζόντιες πύλες είναι οι www.google.gr, www.in.gr, κ.α. Ενώ μια γνωστή κάθετη πύλη είναι η http://webmd.com στιγμιότυπο της οποίας παρατίθεται παρακάτω.



Εικόνα 5: Στιγμιότυπο Ιστοσελίδας Κάθετης Πύλης (Portal)

Μοντέλο Δυναμικής Τιμολόγησης

Το μοντέλο δυναμικής τιμολόγησης παρέχει δυνατότητες στους χρήστες του εύρεσης επιθυμητών προϊόντων με βάση τη χαμηλότερη τιμή. Το μοντέλο μπορεί να διαχωριστεί σε τρείς υποκατηγορίες οι οποίες είναι οι παρακάτω:

- Το μοντέλο καθορισμού τιμής, το οποίο παρέχει στον χρήστη την δυνατότητα να διαλέξει μόνος του την τιμή των προϊόντων τα οποία επιθυμεί. Στην περίπτωση που η προτεινόμενη τιμή δεν κρίνεται συμφέρουσα για την επιχείρηση, ο πελάτης είναι υποχρεωμένος να προτείνει νέα προσφορά. Ολόκληρο το σύστημα της δυναμικής τιμολόγησης λειτουργεί μέσω ιστοτόπων - αντιπροσώπων, που αναζητούν μια σειρά από δικτυακούς τόπους ή βάσεις δεδομένων και συγκεντρώνουν και καταγράφουν τις τιμές σε συγκεκριμένα προϊόντα προκειμένου να είναι ευκολότερη από την χρήστη – αγοραστή η εύρεση οικονομικότερης τιμής.

Μια από τις πιο γνωστές εταιρείες που υλοποιούν αυτό το μοντέλο e-επιχειρείν είναι η Priceline (http://www.priceline.com). Οι προτάσεις συνήθως αφορούν αεροπορικά εισιτήρια, δωμάτια ξενοδοχείων, ενοικιάσεις αυτοκινήτων και απομακρυσμένες τηλεφωνικές συνδιαλέξεις. Παρακάτω μπορούμε να δούμε ένα στιγμιότυπο αυτής.

Εικόνα 6: Στιγμιότυπο Ιστοσελίδας Μοντέλου Δυναμικής Τιμολόγησης

- Το μοντέλο δυναμικής τιμολόγησης το οποίο δίνει την δυνατότητα στους καταναλωτές –αγοραστές της αναζήτησης μέσα από ένα εύρος εμπόρων – προμηθευτών των προϊόντων ή υπηρεσιών που τον ενδιαφέρουν στην χαμηλότερη δυνατή τιμή.
- Το μοντέλο ζήτησης τιμών στηρίζεται στην αρχή, βάσει της οποίας όσο περισσότεροι είναι οι καταναλωτές ενός προϊόντος, τόσο μικρότερη είναι η τιμή του ανά άτομο. Όταν πολλοί καταναλωτές οι οποίοι είναι συγκεντρωμένοι και οργανωμένοι σε ομάδες θέλουν να αγοράσουν το ίδιο προϊόν, τότε η τιμή του θα είναι σίγουρα πιο συμφέρουσα και για τους προμηθευτές αλλά και η τελική τιμή αγοράς πιο οικονομική για την ομάδα των καταναλωτών, από ότι θα ήταν αν το αγόραζαν μεμονομένοι πελάτες. Γνωστές εταιρείες που υλοποιούν αυτό το μοντέλο e-πιχειρείν είναι η Mercata (http://www.mercata.com) και η MobShop

(http://www.mobshop.com). Παρακάτω παραθέτουμε στιγμιότυπο της πρώτης.

Εικόνα 7: Στιγμιότυπο Ιστοσελίδας Μοντέλου Δυναμικής Τιμολόγησης

1.9. Οι Τεχνολογίες του Ηλεκτρονικού Εμπορίου

Οι περισσότερες από τις τεχνολογίες του ηλεκτρονικού εμπορίου, χρησιμοποιούνται εδώ και αρκετά χρόνια και στην παρούσα παράγραφο θα παρουσιάσουμε τις σημαντικότερες οι οποίες είναι οι παρακάτω:

Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI - Electronic Data Interchange)

Η ηλεκτρονική ανταλλαγή δεδομένων εισήχθη στις ηλεκτρονικές τεχνολογίες στις αρχές της δεκαετίας του 1970. Πρόκειται για μια κοινή δομή αρχείων που σχεδιάστηκε έτσι ώστε να επιτρέψει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσω μεγάλων ιδιωτικών δικτύων. Είναι στην ουσία μια ηλεκτρονική ανταλλαγή δεδομένων εμπορικού και διοικητικού είδους μεταξύ

υπολογιστών, ελαχιστοποιώντας την χρήση διαδικασιών που πρέπει να είναι χειρόγραφες. Τα δεδομένα που μεταφέρονται είναι συστηματικά οργανωμένα σε αυτάρκη μηνύματα και το περιεχόμενο τους βασίζεται σε συγκεκριμένα και ολικώς αποδεκτά πρότυπα.

Τα δεδομένα τα οποία μεταφέρονται με EDI θα πρέπει να μπορούν να χρησιμοποιηθούν χρονικά άμεσα από το πληροφοριακό σύστημα του παραλήπτη, χωρίς να υπάρχει ανάγκη ανθρώπινης παρέμβασης. Επομένως, μεταξύ των υπολογιστών που ανταλλάσσονται τα δεδομένα θα πρέπει να χρησιμοποιείται μία κοινή «γλώσσα» επικοινωνίας(Σκιαδάς, 2001). Η ανάγκη αυτή οδήγησε στην θεμελίωση προτύπων EDI, από τα οποία τα κυριότερα είναι το UN/EDIFACT1 και το ANSI X122 που αναπτύχθηκαν στην Ευρώπη και Η.Π.Α. αντίστοιχα. Επίσης εκτός από τα προαναφερόμενα υπάρχουν και άλλα πρότυπα τα οποία χρησιμοποιούνται διεθνώς και παγκοσμίως και προέρχονται από τον Οργανισμό Ηνωμένων Εθνών. Τα πρότυπα αυτά καλύπτουν πληθώρα επικοινωνιακών αναγκών που έχουν οι εμπορικές εταιρείες. Παράδειγμα τέτοιου προτύπου είναι το EDIFACT (EDI For Administration, Commerce and Transportation).

Τα πρότυπα που προαναφέραμε έχουν τα εξής χαρακτηριστικά:

- Και τα δύο πρότυπα φέρουν ίδιους κανόνες σύνταξης όπως επίσης και ένα συγκεκριμένο είδος κωδικοποίησης για τον σχηματισμό μηνυμάτων των οποίων η δομή θα είναι ανεξάρτητη από το πληροφοριακό σύστημα.
- Και τα δύο πρότυπα κατέχουν ένα λεξικό δεδομένων. Αυτό το λεξικό ορίζει με αυστηρό τρόπο τα επιχειρησιακά δεδομένα όπως είναι η μορφή του νομίσματος, διευθύνσεων, ημερομηνίας κ.α.
- Και τα δύο πρότυπα διακρίνονται από σταθερά στοιχεία δεδομένων τα οποία όταν συνδυάζονται χρησιμοποιούνται σε σταθερά μηνύματα. Για παράδειγμα μπορούμε να φέρουμε ένα τιμολόγιο το οποίο αποτελείται από πολλά και διάφορα τμήματα όπως την αρχή του εγγράφου που περιλαμβάνει το όνομα και την διεύθυνση του πιστωτή αλλά και του χρεώστη, την ημερομηνία έκδοσης του τιμολογίου, κ.α. Μετά, ακολουθεί ένα τμήμα που αποτελείται από μια σειρά γραμμών (σαν πίνακας) που αναφέρουν λεπτομερείς πληροφορίες για το κάθε είδος προϊόντος που τιμολογείται,

όπως, την περιγραφή του, την ποσότητα, την τιμή μονάδας, κ.α. Εν τέλει υφίσταται και ακόμα ένα τμήμα του εγγράφου το οποίο παρέχει τα τελικά σύνολα.

Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)

Το SSl αποτελεί ένα πρωτόκολλο που λειτουργεί για την ασφάλεια των δεδομένων και σχεδιάστηκε με σκοπό την ασφαλή σύνδεση με τον εξυπηρετητή (server). Χρησιμοποιεί «κλειδί» δημόσιας κρυπτογράφησης – θα μιλήσουμε για αυτό σε επόμενο κεφάλαιο- έχοντας ως στόχο να προφυλάσσει τα δεδομένα κατά την διαδικασία της διακίνησης τους στο διαδίκτυο. Το SSL εκτός από την μέθοδο κρυπτογράφησης που αναφέραμε κάνει χρήση και άλλων μεθόδων. Επιπλέον το SSL χρησιμοποιεί το πρωτόκολλο TCP/IP για τη μεταφορά των δεδομένων. Έτσι έχει την δυνατότητα να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)

Το SET χρησιμοποιείται για να κωδικοποιεί τα ψηφία - αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Η εφαρμογή αυτή δημιουργήθηκε από τη Visa και τη MasterCard, και φαίνεται να απολαμβάνει σήμερα μεγάλης αποδοχής από την τραπεζική κοινότητα.

Γραμμωτός κώδικας (Barcode)

Η τεχνολογία του γραμμωτού κώδικα αποτελεί μέρος του ευρύτερου τομέα των τεχνολογιών αυτόματης αναγνώρισης. Είναι ένα διαχρονικό εργαλείο, το οποίο ωφελεί την φυσιολογική μετακίνηση και χρήση προϊόντων και υπηρεσιών, προβάλλοντας καταλυτικό ρόλο στην ολοκλήρωση της όλης διαδικασίας. Η ανάπτυξη του ξεκίνησε την δεκαετία του 1960, με κύριο σκοπό να εξυπηρετήσει πληρωμές προϊόντων σε καταστήματα τροφίμων. Η χρήση του τα μετέπειτα χρόνια έγινε πιο εκτενής, μετά την εξάπλωση των πρώτων προτύπων στο τέλος της δεκαετίας του 1970. Λίγα χρόνια μετά , λόγω της σταδιακής εξάπλωσης του εξοπλισμού, αυξήθηκαν κατ' επέκταση και οι τρόποι χρήσης της τεχνολογίας γραμμωτού κώδικα (Ince, 2007),.

Κεφάλαιο 2ο

Ασφάλεια και Κρυπτογράφηση

2.1. Η Ασφάλεια στο Ηλεκτρονικό Εμπόριο

Σε ένα συνεχώς αναπτυσσόμενο επικοινωνιακό μέσο όπως είναι το διαδίκτυο με συνεχή καταβολή κεφαλαίων για επενδύσεις, και ιδιαίτερα στην ιδέα του ηλεκτρονικού επιχειρείν, υπάρχουν μεγάλα περιθώρια κέρδους αλλά και «ζημιάς». Μέσα σ’ αυτό το κλίμα, πληθαίνουν συνεχώς και οι αφορμές για ηλεκτρονική απάτη και για να αποφευχθούν ή και να εξαλειφθούν τέτοιου είδους καταστάσεις καλό είναι να λαμβάνονται τα απαραίτητα μέτρα ασφαλείας. Αυτά τα μέτρα έχουν κάποιους στόχους οι οποίοι είναι οι παρακάτω:

[1] Την εμπιστευτικότητα της πληροφορίας: διασφαλίζοντας πως η πληροφορία είναι προσπελάσιμη από τους σωστούς χρήστες (π.χ. τα σχέδια για το νέο προϊόν είναι προσπελάσιμα σε ορισμένους μόνο χρήστες)

[2] Την πιστοποίηση αυθεντικότητας: επαληθεύοντας την αυθεντικότητα ενός χρήστη ή υπολογιστικού συστήματος (π.χ. πως είναι πράγματι ο χρήστης που ζητά προσπέλαση)

[3] Την αποφυγή άρνησης πράξεων: εξασφαλίζοντας πως οι χρήστες δεν μπορούν να αρνηθούν τις ηλεκτρονικές πράξεις τους (π.χ. ότι αντέγραψαν ένα αρχείο)

[4] Την ακεραιότητα των δεδομένων: διασφαλίζοντας πως τα δεδομένα δεν έχουν αλλάξει και είναι τα ίδια με αυτά που αρχικά τοποθετήθηκαν (π.χ. τα περιεχόμενα της μελέτης δεν έχουν αλλάξει από κάποιο τρίτο)

[5] Τον έλεγχο προσπέλασης: διασφαλίζοντας πως οι πόροι βρίσκονται κάτω από τον αποκλειστικό έλεγχο εξουσιοδοτημένων χρηστών, βεβαιώνοντας πως ο χρήστης που ζητά την προσπέλαση έχει την άδεια να το κάνει (π.χ. η αλλαγή στο αρχείο ενός υπαλλήλου επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα)

[6] Την διαθεσιμότητα των πόρων: εξασφαλίζοντας πως τα δεδομένα οι υπηρεσίες και οι εξυπηρετητές είναι διαθέσιμα όποτε ζητηθούν (π.χ. άμεση αποκατάσταση δεδομένων και υπηρεσιών μετά από επίθεση).

Η ανάγκη για την διασφάλιση της ασφάλειας στα τοπικά δίκτυα και άλλα και στα δίκτυα ευρείας ζώνης, κάνει όλο και πιο εκτεταμένη την ανάγκη για δημιουργία των εμποδίων εκείνων που είναι απαραίτητα στην φυσική προσπέλαση του εξοπλισμού, το δίκτυο, αλλά και τις εφαρμογές. Την δεδομένη χρονική στιγμή δεν υπάρχει κάποιο σύστημα ασφαλείας δικτύων το οποίο είναι στο 100% και το πιο πιθανό μάλιστα είναι ένα τέτοιο σύστημα να μην κατασκευαστεί λόγω του ασύμφορου κόστους που εσωκλείει (Κομνηνός, Σπυράκης 2002).

Για το λόγο αυτό οι περισσότεροι επιδιώκουν να κατασκευάσουν απλώς ένα ασφαλές σύστημα του οποίου το κόστος υλοποίησης θα είναι οριακά μεγαλύτερο από το κόστος μια κακόβουλης επίθεσης. Για την κατασκευή ενός τέτοιου συστήματος όποιο και αν είναι το κόστος του απαιτούνται μια σειρά από ενέργειες, οι οποίες είναι οι ενέργειες για την δημιουργία ενός λογισμικού ή μιας μονάδας υλικού. Οι ενέργειες αυτές είναι η ανάλυση απαιτήσεων, ο σχεδιασμός, η υλοποίηση, η δοκιμή και η τελική λειτουργία. Πιο αναλυτικά λοιπόν έχουμε τις παρακάτω ενέργειες:

[1] Πρέπει να γίνει ανάλυση απαιτήσεων , δηλαδή από την μία λεπτομερής ανάλυση των κινδύνων οι οποίοι είναι πιθανό να εμφανιστούν στην πορεία και από την άλλη η καταγραφή των πόρων τους οποίους θέλουμε να διαφυλάξουμε από επιθέσεις. Όσο αφορά την καταγραφή των κινδύνων είναι αναγκαία η καλή γνώση των εργαλείων και των μεθόδων με τις οποίες πραγματοποιούνται οι κακόβουλες επιθέσεις.

[2] Πρέπει να προσδιοριστεί και να οριοθετηθεί η πολιτική ασφαλείας που θα επιλέξουμε να ακολουθήσουμε.

[3] Πρέπει να γίνει σχεδιασμός του συστήματος ασφάλειας που θα φτιάξουμε. Μιλώντας για σχεδιασμό , εννοούμε την αρχιτεκτονική

[4] Το λογισμικό ή υλικό που θα κατασκευαστεί θα πρέπει να περιέχει και υπηρεσίες ασφαλείας οι οποίες θα πρέπει να αποφασισθούν εξαρχής και πριν την υλοποίηση του.

[5] Να έχουμε σχεδιάσει τον τρόπο αντιμετώπισης ενός περιστατικού επίθεσης να ενημερώνουμε τους χρήστες μας

[6] Να ήμαστε πάντα ενημερωμένοι για τα πιο πρόσφατα νέα σε σχέση με την ασφάλεια.

Το Διαδίκτυο, όπως υποδηλώνει και η φύση της έννοιας του, αποτελεί το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων μεταξύ τους, τα οποία είναι συνήθως διαφορετικής τεχνολογίας, που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε όλη την υφήλιο. Αυτή η ετερογένεια των δικτύων που συνιστούν το διαδίκτυο, καθιστούν δύσκολο το γεγονός να αντιμετωπιστεί αποτελεσματικά, σε όλο του το εύρος από άποψη ασφάλειας. Βέβαια πολύ σημαντικό είναι και το γεγονός ότι οι μηχανισμοί που στηρίζουν και συντηρούν την λειτουργικότητά του διαδικτύου σχεδιάστηκαν αρχικώς με στόχο την βελτιστοποίηση των διαφόρων δυνατοτήτων διασύνδεσης ετερογενών δικτύων και όχι για να παρέχουν ασφάλεια. Συμπερασματικά λοιπόν, η ασφάλεια ενός δικτύου επιτυγχάνεται ως επιπρόσθετο χαρακτηριστικό του δικτυακού σχεδίου και όχι ως βασικό συστατικό του. Οι κύριοι λόγοι που κάνουν το Διαδίκτυο ένα μη ασφαλές μέσο για την πραγματοποίηση ηλεκτρονικών είναι οι παρακάτω:

[1] Η ετερογένεια των δικτύων όπως αναφέραμε με δεδομένο επιπλέον το απέραντο μέγεθος τους, έχει ως αποτέλεσμα οι διαδικασίες που διασφαλίζουν ένα σύστημα συναλλαγών σε ένα τέτοιο περιβάλλον, να απαιτούν έναν μεγάλο αριθμό περίπλοκων ρυθμίσεων και διαμορφώσεων ασφάλειας.

[2] Η εύκολη και χωρίς περιορισμούς πρόσβαση που παρέχει στα εκατομμύρια χρήστες του διαδικτύου, το κάνει αυτόματο πιο ευάλωτο σε σχέση με άλλα είδη δικτύων.

[3] Η μη ύπαρξη πολιτικής ελέγχου προσπέλασης. Δεν υπάρχει κατάλληλη υποδομή στους υπάρχοντες κόμβους του δικτύου εξαιτίας κυρίως του κόστους ή ακόμα και της άγνοιας, κάτι το οποίο έχει ως αποτέλεσμα να δημιουργείται μεγάλος κίνδυνος από την ευρέως ανοικτή σύνδεσή τους στο διαδίκτυο.

[4] Η φύση των πρωτοκόλλων ασφαλείας TCP/IP και συναφών υπηρεσιών που υπερασπίζει το διαδίκτυο, δεν δύναται να εκμηδενίσουν τους κινδύνους

ασφαλείας. Και έτσι σε πολλές περιπτώσεις επιδέξιοι εισβολείς μπορούν με σχετική ευκολία και άνεση να παραβιάσουν την ασφάλεια των παρεχόμενων TCP/IP υπηρεσιών, με δεδομένο πως το μεγαλύτερο μέτος του διακινούμενων μέσω διαδικτύου δεδομένων βρίσκεται σε μη κρυπτογραφημένη μορφή.

[5] Η αυξημένη πολυπλοκότητα των διαδικασιών, η οποία μετριάζει το αίσθημα αξιοπιστίας, αφού όσο πιο δυσκολονόητο είναι κάτι τόσο μείζονα είναι και η δυσπιστία που περνάει για αυτό.

[6] Το εφικτό της διατήρησης της ανωνυμίας ενός χρήστη κατά την περιήγησή του στο Διαδίκτυο.

2.2. Κίνδυνοι Ηλεκτρονικών Συναλλαγών

Προκειμένου να αναπτύξουμε τους κίνδυνους που απειλούν το ηλεκτρονικό εμπόριο, πρέπει να αναφέρουμε ότι κίνδυνος αποτελεί κάθε εξωτερική απειλή που έχει ως σκοπό να βλάψει την ακεραιότητα των ηλεκτρονικών συναλλαγών και μέσω της παραβίασης της ιδιωτικότητας να εκμεταλλευτεί οποιαδήποτε πληροφορία που μπορεί να αποκομίσει. Οι κίνδυνοι που αντιμετωπίζουν οι ηλεκτρονικές συναλλαγές παρουσιάζονται παρακάτω.

2.2.1. Υποκλοπή Δεδομένων

Υποκλοπή προσωπικών δεδομένων στο διαδίκτυο αποτελεί η διαδικασία της εξαπάτησης ενός χρήστη με σκοπό να δώσει τις προσωπικές του πληροφορίες σε έναν «πλαστό» διαδικτυακό τόπο όπως είναι η διεύθυνση του, ο αριθμό ταυτότητας του, οι αριθμοί τραπεζικών λογαριασμών κ.α..μια τέτοια δραστηριότητα επιτρέπει σε έναν απατεώνα να υποκλέψει ή ακόμα και να πλαστογραφήσει τα στοιχεία ενός χρήστη προκειμένου να κερδίσει παράνομη πρόσβαση στα δεδομένα του, όπως

προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς ασφαλείας, κ.λπ (Γκριτζάλης ,Γκριτζάλης., Κάτσικας, 2007). Σε αυτήν την κατηγορία μπορούμε να εντάξουμε και τις Απάτες (Scams), αν και συνήθως αυτοί που τις επιδιώκουν δεν ενδιαφέρονται για τις προσωπικές πληροφορίες των χρηστών όπως αυτές που αναφέραμε παραπάνω, αλλά προσπαθούν να προκαλέσουν τον οίκτο για τον ανθρώπινο πόνο ώστε να κάνουν τους χρήστες να προσφέρουν χρήματα για να συνδράμουν σε ένα δήθεν καλό σκοπό. Ενδεικτικό παράδειγμα εδώ είναι το γεγονός ότι σχεδόν σε κάθε μεγάλη καταστροφή όπως σεισμός, πλημμύρες, πείνα, πόλεμος, έχουν προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες τους να προσφέρουν χρηματικά ποσά προκειμένου να βοηθήσουν για κάποιο καλό σκοπό. Όλα τα παραπάνω παραβιάζουν την ιδιωτική ζωή των χρηστώ του διαδικτύου και επίσης εκμεταλλεύονται δεδομένα που έχουν υποκλαπεί όπως συνθηματικά ή στοιχεία από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά (Κόκοτος, 2009).

Η υποκλοπή προσωπικών δεδομένων μπορεί να πραγματοποιηθεί μέσω ηλεκτρονικών μηνυμάτων (e-mail) που εξαπατούν έναν χρήστη ώστε να στην συνέχεια να επισκεφτεί πλαστές ιστοσελίδες, ή κατά την διάρκεια του φυλλομετρήματος οποιασδήποτε ηλεκτρονικής ιστοσελίδας, η οποία είναι μολυσμένη από ίο. Ακόμα μέσω της περιήγησης σε ιστότοπους με αναληθή προϊόντα και πληροφορίες. Επιπλέον σε πιο εξειδικευμένες περιπτώσεις υποκλοπή προσωπικών δεδομένων μπορεί να πραγματοποιηθεί κατά την περιήγηση ενός χρήστη σε έναν ισότοπο, που είναι μολυσμένος με προγράμματα που καταγράφουν προσωπικές και οικονομικές πληροφορίες, τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν.

2.2.2. Κακόβουλος Κώδικας

Ο κακόβουλος κώδικας έγκειται σε ειδικά προγράμματα τα οποία επιτίθενται σε άλλα προγράμματα και υπολογιστικά συστήματα και συνήθως αποτελούνται από δύο συστατικά στοιχεία. Το πρώτο είναι το λεγόμενο φορτίο που είναι το μέρος

τους αυτό που προκαλεί την ζημιά. Το δεύτερο είναι ο μηχανισμός εξάπλωσης ο οποίος είναι υπεύθυνος για τη διάδοση των προγραμμάτων αυτών.

Τα είδη του κακόβουλου κώδικα είναι πολλά και στην παρούσα παράγραφο θα παρουσιάσουμε τα πιο σημαντικά τα οποία είναι τα παρακάτω:

Ιοί (Viruses)

Οι Ιοί αποτελούν τα πιο γνωστά μέσα επίθεσης στην ασφάλεια του διαδικτύου. Οι τεχνικές που χρησιμοποιούν είναι ως επι το πλείστον πονηρές και δόλιες. Σκοπός τους είναι να εγκατασταθούν σε υπολογιστικά συστήματα χωρίς φυσικά την συγκατάβαση του ιδιοκτήτη και να πλήξουν την ακεραιότητα του συστήματος. Οι τρόποι που χρησιμοποιούν για να το πετύχουν είναι άλλες φορέα ανώδυνοι, αλλα στις περισσότερες περιπτώσεις είναι επώδυνοι αφού προκαλούν απώλεια δεδομένων, ή οδηγούν το όλο σύστημα σε διαμόρφωση.

Σκουλήκια (Worms)

Τα «σκουλήκια» (worms) είναι προγράμματα που δρουν αυτόνομα και «σέρνονται» (έτσι προκύπτει το όνομα «σκουλήκι») από site σε site εκμεταλλευόμενα τρύπες του συστήματος. Σε κάθε ιστοσελίδα τα σκουλήκια δρούν αυτόνομα και χωρίς την χρήση ή την ενσωμάτωση τους σε άλλα προγράμματα. Το πιο «διάσημο» σκουλήκι όλων των εποχών ήταν το Internet Worm, το οποίο το 1988, μπόρεσε να διασπάσει το Διαδίκτυο στην Αμερική, προκαλώντας αντιδράσεις πανικού σε όλο τον κόσμο.

Δούριοι Ίπποι (Trojan Horses)

Οι Δούρειοι Ίπποι (trojan horses) αποτελούν κακόβουκα προγράμματα τα οποία προσποιούνται ότι διαθέτουν διαφορετικές λειτουργίες από αυτές που πραγματικά

έχουν –από εκεί άλλωστε προκύπτει και το όνομα τους. Συνήθως αποτελούν μέρος άλλων προγραμμάτων, αλλά είναι δυνατό να δρούν και μεμονωμένα.

2.2.3. Ηλεκτρονικό Ψάρεμα (Phishing)

Το Phishing αποτελεί μια ενέργεια εξαπάτησης των χρηστών του παγκόσμιου ιστού, κατά την οποία ο ειδικός (χάκερ) που το πραγματοποιεί υποδύεται μία αξιόπιστη οντότητα, ο οποίος εκμεταλλεύεται την ελλειπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του θύματος, με σκοπό την μη νόμιμη απόκτηση των προσωπικών του δεδομένων, τα οποία συνήθως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί. Σε περιπτώσεις δε που το ηλεκτρονικό ψάρεμα πραγματοποιείται σε δικτυακούς τόπους που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου, στόχος είναι η απόκτηση των προσωπικών αριθμών των πιστωτικών καρτών. Μία επιτυχημένη επίθεση phishing στηρίζεται σε τρεις βασικούς παράγοντες, την έλλειψη συγκεκριμένων γνώσεων του ατόμου που θα εξαπατηθεί, την έλλειψη προσοχής του θύματος και την οπτική εξαπάτηση. Έτσι είναι δύσκολο να αναγνωρίσει τα ίχνη του phishing. Ακόμα και σε περιπτώσεις που ο χρήστης διαθέτει τις απαραίτητες γνώσεις για να αναγνωρίσει τα κακόβουλα στοιχεία, πολλές φορές μπορεί να μην προσέξει τα σημάδια. Άλλωστε η σωστή τεχνική phishing κρύβει τα περισσότερα από τα σημάδια.

2.2.3. Hacking

Το hacking είναι η ενέργεια που πραγματοποιεί ο hacker προκειμένου να βλάψει έναν ηλεκτρονικό υπολογιστή και με αυτόν τον τρόπο να ανακτήσει ευαίσθητα προσωπικά δεδομένα του ανυποψίαστου χρήστη. Στις μέρες μας όμως, οι ηλεκτρονικές επιθέσεις έχουν αλλάξει τον σκοπό τους έχοντας ξεκάθαρα οικονομικά κίνητρα ενώ θύματα τους αποτελούν κυρίως μεγάλοι εμπορικοί οργανισμοί, όπως τράπεζες και επιχειρήσεις οι οποίες καταπιάνονται με το ηλεκτρονικό εμπόριο, τα ηλεκτρονικά συστήματα των δημόσιων υπηρεσιών, κ.α.

2.2.3. Απάτες Πιστωτικών Καρτών

Όταν πραγματοποιούνται απάτες σε πιστωτικές κάρτες, συνήθως κάποιος κακόβουλος χρήστης κατασκευάζει έναν ψεύτικο ιστότοπο καταφέρνοντας έτσι να μαζεύει στοιχεία κι αριθμούς πιστωτικών καρτών άλλων χρηστών του διαδικτύου, οι οποίοι κρίνουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους. Επιπλέον, δεν είναι λιγοστές και οι περιπτώσεις στις οποίες κάποιοι πετυχαίνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών χρηστών του διαδικτύου τα οποία εν συνεχεία μεταχειρίζονται σε άλλες διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

Όταν κάποιος χρήστης συνδέεται στο διαδίκτυο, είτε αυτός ανήκει σε κάποια ηλεκτρονική εταιρεία, είτε πρόκειται για απλό χρήστη, συνδέεται με έναν μεγάλο αριθμό άλλων δικτύων και συνεπώς μεγάλο αριθμό χρηστών. Η σύνδεση αυτή επιτρέπει να γίνεται κοινός ένας μεγάλος όγκος πληροφοριών. Το πρόβλημα αυτό δημιουργείται, διότι υπάρχουν πληροφορίες οι οποίες κατ’ ανάγκη πρέπει να είναι εμπιστευτικές και να μην υπάρχει τρόπος να είναι ορατές σε μη εξουσιοδοτημένους χρήστες. Παρ’ όλα αυτά πολλοί χρήστες βρίσκουν τρόπους για να καρπώνονται την οποιαδήποτε πληροφορία , ακόμα και όταν αυτή είναι απόρρητη, και αυτό αποτελεί ένα πολύ μελανό σημείο του ηλεκτρονικού εμπορίου (Κόκοτος, 2009). Η ανάγκη για ασφάλεια της μεταφερόμενης πληροφορίας οδήγησε στην ανάπτυξη της κρυπτογράφησης, την οποία θα δούμε αναλυτικά στο επόμενο κεφάλαιο.

2.3. Άλλοι Κίνδυνοι Ηλεκτρονικών Συναλλαγών

Στην παρούσα παράγραφο θα αναλύσουμε άλλου είδους κινδύνων εκτός τους προαναφερόμενους, που έχουν να κάνουν με επιθέσεις σε ηλεκτρονικά καταστήματα:

Επιθέσεις σε Ιστοσελίδες

Οι ιστοσελίδες του διαδικτύου αποτελούσαν πάντα τον εύκολο στόχο για επιθέσεις από hackers. Αυτό συνέβαινε γιατί οι δικλείδες ασφαλείας που είχαν και έχουν δεν ήταν πάντα αρκετά ικανοποιητικές ώστε να απωθήσουν τέτοιου είδους εισβολές. Η επίθεση σε αυτή την περίπτωση πραγματοποιείται αλλάζοντας το λινκ της κεντρικής σελίδας και ορίζοντας το να δείχνει σε κάποια άλλη κακόβουλη τοποθεσία. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί έχουν δει την φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρίες, κυβερνητικοί οργανισμοί, στρατιωτικά προγράμματα είναι οι κύριοι στόχοι.

Επίθεση στην υπηρεσία ονοματολογίας (DNS)

Ένας άλλος τρόπος για να τροποποιηθούν σι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (Domain Name Service) ο κόμβος. Για παράδειγμα αν η IP διεύθυνση του κόμβου www.victim.com μεταφραζόταν σε 13.42.111.33, η επίθεση θα είχε ωα αποτέλεσμα την αλλαγή των κατάλληλων στοιχείων της βάσης δεδομένων του DomainNameServer και η σελίδα να παραπέμπει σε μια άλλη ιστοσελίδα, κακόβουλη, όπως π.χ. πορνογραφικού περιεχομένου. Ο Eugene Kashpureff, στέλεχος της AlterNIC, άλλαξε τα στοιχεία της βάσης δεδομένων που κρατά τα Domain Names και τις IP διευθύνσεις, έτσι ώστε όσοι προσπαθούσαν να πάνε στην σελίδα του InterNIC, οδηγούνταν στις σελίδες του AlterNIC. Από εκεί οι χρήστες μπορούσαν με ένα κλικ να πάνε στην πραγματική σελίδα (Macavinta, 1997). Η επίθεση έγινε ένα Σαββατοκύριακο του Ιουλίου του 1997, σαν διαμαρτυρία για το μονοπώλιο που πέτυχε το InterNIC για την διαχείριση του DNS πρώτου επιπέδου για τους δημοφιλείς κόμβους .com, .org, .net αποφέροντάς του έτσι κέρδη των $78 εκατομμυρίων. Ο Kashpureff τελικά συνελήφθη στον Καναδά με ένταλμα του FBI και δικάστηκε σε 2 χρόνια επιτήρηση και $100 (εκατό

δολάρια) πρόστιμο μετά από συμφωνία με την Network Solutions που είχε την διαχείριση του InterNIC και την δημόσια συγγνώμη του.

Επίθεση με «Ανιχνευτές»

Οι ανιχνευτές δικτυακής κίνησης συνήθως αποτελούν προγράμματα τα οποία χρησιμοποιούνται προκειμένου να επιτευχθεί ο έλεγχος της ασφάλειας των υπολογιστικών συστημάτων. Το όνομα τους προκύπτει από το γεγονός ότι έχουν γνώση για όλα τα πιθανά εξωτερικά σημεία τα οποία θα μπορούσε να εκμεταλλευτεί ένας hacker προκειμένου να πλήξει την ασφάλεια του συστήματος. Παρ΄ότι λοιπόν αρχικά η δημιουργία τους συντελέστηκε για καλό σκοπό, αργότερα ο τρόπος λειτουργίας τους έγινε αντικείμενο εκμετάλλευσης από τους επίδοξους hacker. Τέτοιου είδους προγράμματα είναι το ISS, το TCPdump, το Nmap, το SATAN αλλά και πολλά άλλα. Το ποσοστό της χρήσης τους είναι 14.3% του συνολικού των εργαλείων.

Επίθεση στο πρωτόκολλο TFTP

Το πρωτόκολλο TFTP (Trivial File Transfer Protocol) σχεδιάστηκε εξαρχής για την άνευ δίσκου εκκίνηση «πελατών». Παρ' όλα αυτά, δεν δόθηκε η απαραίτητη προσοχή στα σημεία πρόσβασης συγκεκριμένων καταλόγων του συστήματος, κάτι το οποίο είχε ως αποτέλεσμα κάποιος να είναι σε θέση αντιγράψει κι άλλα αρχεία, όπως για παράδειγμα, το αρχείο κωδικών πρόσβασης.

Επίθεση σιη Δικτυακή Υπηρεσία Πληροφοριών (NIS)

Πρόκειται για την υλοποίηση της Sun Microsystems «Κίτρινων Σελίδων» (Yellow Pages) για κατανεμημένη διαχείριση δικτυακών πληροφοριών (όπως αρχεία κωδικών πρόσβασης, χάρτες του δικτύου κλπ.). Παρ' όλα αυτά, αυτές οι πληροφορίες διέρχονταν πάνω από το δίκτυο και έτσι ο οποιοσδήποτε ήταν σε θέση να τα παρακολουθήσει και να τα υποκλέψει. Το NIS (Network Information Service) στην συνέχει αντικαταστάθηκε από το NIS+ (από την Sun Microsystems και πάλι) το οποίο πλέον έκανε χρήση κρυπτογραφικών μεθόδων για την εκτέλεση της ασφαλούς μεταφοράς ευαίσθητων πληροφοριών.

Επίθεση στο πρωτόκολλο μεταφοράς αρχείων (FTP)

Το FTP είναι το πρωτόκολλο ασφαλούς μεταφοράς αρχείων μέσω του διαδικτύου όπως προκύπτει και από το όνομα του (File Transfer Protocol). Μέσω αυτού του πρωτόκολλου μεταφοράς αρχείων και συνάμα μιας λανθασμένης διαμόρφωσης ο οποιοσδήποτε είναι σε θέση να υποκλέψει αρχεία ενός υπολογιστικού συστήματος.

Επίθεση στο Σύστημα Δικτυακής Αρχειοθέτησης (NFS)

Το NFS (Network File System) είναι ένα σύστημα δικτυακής αρχειοθέτησης και αποτέλεσε πρωτοποριακή υλοποίηση από την Sun Microsystems. Ωστόσο, κάνοντας χρήση λάθος διαμόρφωσης, μπορεί να «μοιράσει» τα δικτυακός αποθηκευμένα αρχεία σε κακόβουλους χρήστες που δεν έχουν την απαραίτητη εξουσιοδότηση.

Επίθεση στο πρωτόκολλο ηλεκτρονικού ταχυδρομείου (SMTP)

Το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) πρόκειται για το TCP/IP πρωτόκολλο επικοινωνίας των MTA (Mail Transfer Agents) της υπηρεσίας του

ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος (10.4%) είναι το sendmail (σε Berkeley UNIX συστήματα). Πιο πρόσφατα, νέα προγράμματα με μεγαλύτερη ασφάλεια έχουν εμφανιστεί, τόσο για πλατφόρμες UNIX (π.χ. qmail) όσο και για πλατφόρμες Windows (Exchange Server).

Επίθεση στο ηλεκτρονικό ταχυδρομείο

Πρόκειται για ένα ακόμα είδος πολύ συχνά εμφανιζόμενων επιθέσεων, τα οποία ανακύπτουν λόγω της προβληματικής και ελλιπούς χρήσης του SMTP. Τέτοια είναι το mail spoofing (απόκρυψη αποστολέα ή αλλαγή διεύθυνσής του), mail bombs (μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), binmail, mailrace, mail abuse. Ένα πιο σύγχρονο δε είδος επίθεσης σε λογαριασμούς ηλεκτρονικού ταχυδρομείου είναι το πολύ γνωστό σε όλους μας spamming, δηλαδή η μαζική μηνυμάτων ηλεκτρονικού ταχυδρομείου με περιεχόμενο ακατάλληλο ή ασήμαντο.

Επίθεση με «έμπιστους υπολογιστές»

Το πρόβλημα της επίθεση με έμπιστους υπολογιστές αρχικά παρουσιάζεται σε υπολογιστικά συστήματα με λογισμικό UNIX. Ο όρος των «έμπιστων υπολογιστών» (trusted hosts) έγκειται στη διευκόλυνση των χρηστών οι οποίοι διατηρούσαν πολλούς λογαριασμούς σε διαφορετικά υπολογιστικά συστήματα και έπρεπε να έχουν άμεση πρόσβαση δίχως την καθυστέρηση για ταυτοποίηση μέσω κωδικών πρόσβασης.

Επίθεση από εύρεση των κωδικών πρόσβασης

Η αδυναμία και ευαισθησία των κωδικών πρόσβασης αποτελεί την πιο συχνή μορφή επίθεσης σε ασφάλεια από όλες όσες μελετήσαμε μέχρι τώρα. Η αποκάλυψη του κωδικού πρόσβασης ενός χρήστη σε τρίτους είναι δυνατό να πραγματοποιηθεί με πολλούς και διάφορους τρόπους οι πιο γνωστοί από τους οποίους είναι οι παρακάτω:

[1] Αρχικά αντιγραφή του αρχείου διατήρησης κωδικού και στην συνέχεια επεξεργασία αυτού,

[2] «Σπάσιμο» του κωδικού πρόσβασης (password cracking) κάνοντας χρήση ειδικών προγραμμάτων τα οποία προσπαθούν να μαντέψουν τους κωδικούς χρησιμοποιώντας σύνηθες λέξεις,

[3] «Αδύνατοι κωδικοί» (weak passwords). Εδώ έχουμε τους κωδικούς τους οποίους κάποιος μπορεί να βρει με ευκολία, δεδομένου ότι γνωρίζει το άτομο στο οποίο ανήκει ο λογαριασμός (χρήση του ονόματος, διεύθυνσης, τηλεφώνου κλπ.).

Επίθεση με «σπαστήρια» κωδικών

Τα «σπαστήρια κωδικών» (password cracks) είναι προγράμματα τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης (password file) και με χρήση ενός λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται για κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Ενδεικτικά εδώ μπορούμε να πούμε σε ένα υπολογιστικό σύστημα με λειτουργικό Unix το οποίο έχει 1000 περίπου χρήστες, και με την προϋπόθεση ότι οι χρήστες του συστήματος δεν είναι εκπαιδευμένοι στο να επιλέγουν δύσκολους

κωδικούς, ένα «σπαστήρι» κωδικών είναι σε θέση να προσπελάσει με ευκολία ένα ποσοστό 40% των συνολικών κωδικών.

Επίθεση με «ωτακουστές»

Οι «Ωτακουστές» πακέτων (packet sniffers) αποτελούν ειδικά προγράμματα τα οποία δύναται να παρακολουθούν την κίνηση μέσα σε ένα δίκτυο σε επίπεδο IP πακέτων. Με τις τεχνικές που αναπτύσσουν τους δίνεται η δυνατότητα να διαφοροποιούν τα μηνύματα που λαμβάνουν αλλά ταυτόχρονα να κάνουν αναγνώριση των πρωτοκόλλων που περνούν διαμέσω του δικτύου. Οι packet sniffers χρησιμοποιούνται για επιθέσεις συνήθως σε τοπικά δίκτυα και σπάνε κωδικούς πρόσβασης, μέσω παρακολούθησης της πληκτρολόγησης του ατόμου από εκάστοτε συγκεκριμένους σταθμούς εργασίας.

Με του ειδικούς μηχανισμούς που διαθέτουν διαφοροποιούν τα πακέτα μηνυμάτων τα οποία τις περισσότερες φορές περιέχουν χρήσιμη πληροφορία δίχως ωστόσο να επηρεάζουν το περιεχόμενο τους.

Από την άλλη βέβαια η χρήση των ωτακουστών μπορεί να έχει και θετικά αποτελέσματα για την διαχείριση δικτύου και υπολογιστικών συστημάτων, όμως και σε αυτήν την περίπτωση είναι σημαντικό τέτοιες τεχνολογίες να μην χρησιμοποιούντα με κακόβουλο τρόπο. Η χρήση ενός ωτακουστή τις περισσότερες φορές απαιτεί προνόμια διαχειριστή , αν και σήμερα, ο καθένας είναι «διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο. Για τον λόγο αυτό. η ασφάλεια από τα sniffers θα πρέπει να εξασφαλίζεται στο επίπεδο παρόχου υπηρεσιών δικτύου (ISP).

Επίθεση με πλαστογράφηση της IP διεύθυνσης

Η τεχνική της πλαστογράφησης της IP διεύθυνσης στηρίζεται στη δυνατότητα που δύναται να έχει ένας κόμβος και να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Από την στιγμή που πληθώρα συστημάτων καθορίζουν ποια είναι τα πακέτα τα οποία επιτρέπονται και ποια όχι να εισέλθουν σε ένα δίκτυο ανάλογα με την IP διεύθυνση του αποστολέα, αυτό αποτελεί μία χρήσιμη τεχνική στα χέρια ενός hacker. Έτσι είναι εφικτό να διασφαλιστεί η προσπέλαση σε υπηρεσίες που επιτρέπονται σε κόμβους με συγκεκριμένες IP διευθύνσεις. Επίσης μπορεί να σταλεί από ένα εξωτερικό δίκτυο ένα πακέτο δεδομένων που να φαίνεται πως έχει σταλεί από εσωτερικό κόμβο ενός προφυλαγμένου δικτύου, δίνοντας έτσι την δυνατότητα να εκτελεστούν εντολές, που επιτρέπονται να εκτελεστούν μόνο από εσωτερικούς κόμβους.

Η πλαστογράφηση της IP διεύθυνσης αποτελεί μια σημαντική τεχνική επίθεσης σε δικτυωμένους υπολογιστές. Για να αποκτήσουν πρόσβαση, οι hackers δημιουργούν πακέτα με πλαστές IP διευθύνσεις. Αυτό εκμεταλλεύεται τις εφαρμογές που χρησιμοποιούν ταυτοποίηση (authentication) που βασίζεται στην IP διεύθυνση του αποστολέα και μπορεί να οδηγήσει ακόμα και στην απόκτηση πρόσβασης διαχειριστή στο σύστημα στόχο (για παράδειγμα στις περιπτώσεις χρήσης του /etc/hosts.equiv ή .rhosts). Οι επιθέσεις αυτές μπορούν να εμποδιστούν μέσω τείχων προστασίας τα οποία τσεκάρουν τις διευθύνσεις IP πρωτού μπουν στο τοπικό, έμπιστο (trusted) δίκτυο.

Κεφάλαιο 3ο

Κρυπτογράφηση στο Ηλεκτρονικό Εμπόριο

3.1. Εισαγωγή στην Κρυπτογραφία

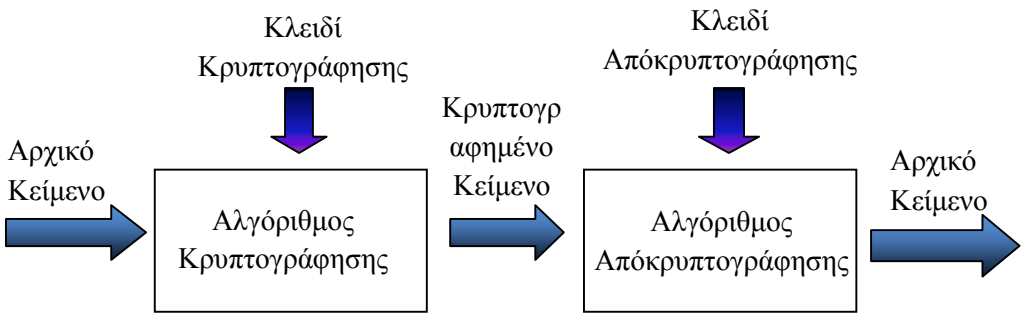
Η κρυπτογραφία χρησιμοποιείται ευρέως σήμερα ως ένα πολύ χρήσιμο εργαλείο στην ασφάλεια της μεταφοράς πληροφοριών, προκειμένου να προστατευτούν προσωπικά δεδομένα ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Σε νομικό και κοινωνικό επίπεδο, εδώ και πολλά χρόνια θέτονται ζητήματα προστασίας απορρήτου σε όλες τις δυνατές εκδοχές μιας δικτυακής συναλλαγής όπως είναι η λήψη και αποστολή email, οι διαφόρων ειδών εμπορικές συναλλαγές, η τήρηση του τραπεζικού και ιατρικού απορρήτου, κ.α. και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων των χρηστών του διαδικτύου.

Από την στιγμή που ξεκίνησαν να μεταδίδονται δεδομένα μέσω διαδικτύου, γεννήθηκε η κρυπτογράφηση με σκοπό να ασφαλιστούν όλα τα μεταφερόμενα μηνύματα. Με άλλα λόγια η κρυπτογράφηση εξασφαλίζει, με τρόπους που θα δούμε στην συνέχεια το απόρρητο των μεταφερόμενων προσωπικών πληροφοριών εντός διαδικτύου. Σκόπιμο είναι προτού αναφερθούμε σε αυτές τις μεθόδους να δώσουμε κάποιους βασικούς ορισμούς, ξεκινώντας από αυτόν της κρυπτογράφησης.

Κρυπτογράφηση (encryption) λοιπόν καλείται η διαδικασία μεταβολής ενός μηνύματος με τέτοιο τρόπο ώστε αυτό να μην είναι δυνατό να αναγνωστεί από κανέναν, εκτός από τον νόμιμο παραλήπτη του. Η αντίστροφη από την παραπάνω διαδικασία καλείται αποκρυπτογράφηση και σε αυτήν από το κρυπτογραφημένο κείμενο ανακύπτει το αρχικό μήνυμα. Το αρχικό μήνυμα είναι η είσοδος στην διαδικασία της κρυπτογράφησης και το κρυπτογραφημένο η έξοδος. Αντίστροφα έχουν τα πράγματα στην διαδικασία της αποκρυπτογράφησης.

Κλειδί είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης το μετράμε σε αριθμό bits. Γενικά ισχύει ότι όσο πιο μεγάλο είναι το κλειδί κρυπτογράφησης, τόσο πιο δύσκολα μπορεί να αποκρυπτογραφηθεί η κρυπτογραφημένη πληροφορία από επιδέξιους εισβολείς. Ανόμοιοι αλγόριθμοι κρυπτογράφησης προϋποθέτουν διαφορετικά μήκη κλειδιών για να καταφέρουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Την διαδικασία της κρυπτογράφησης μπορούμε να δούμε στο παρακάτω σχήμα:



Εικόνα 8: Διαδικασία Κρυπτογράφησης

3.2. Η Λειτουργία της Κρυπτογράφησης

Τα διάφορα κρυπτογραφικά συστήματα, ανάλογα με τον τρόπο που λειτουργούν μπορούν να χωριστούν σε δύο μεγάλες ομάδες οι οποίες είναι τα stream και τα block ciphers. Τα block chippers κρυπτογραφούν την αρχική πληροφορία ανά τμήμα τα οποία ονομάζονται blocks –από εκεί προκύπτει και η ονομασία τους – συνήθως μεγέθους 64 και 128 bits. Στην αντίπερα όχθη τα stream ciphers κρυπτογραφούν το κάθε bit ξεχωριστά.

Στην διάρκεια της κρυπτογράφησης τα block ciphers κάνουν χρήση διάφορων τεχνικών**.** Προκειμένου να γίνει χρήσιμο ένα mode πρέπει να είναι

αποδοτικό και ασφαλές στον ίδιο βαθμό που είναι και το block cipher. Οι διάφορες τεχνικές που χρησιμοποιούνται για το σκοπό αυτό και τις οποίες θα δούμε αναλυτικά είναι οι παρακάτω:

Electronic Code Book (ECB)

Όταν χρησιμοποιείται αυτός ο τρόπος λειτουργίας ECB, το κάθε block που μεταφέρεται κρυπτογραφείται ξεχωριστά. Αυτό σημαίνει ότι δύο ίδια blocks, είτε ανήκουν στην ίδια αρχική πληροφορία, είτε σε διαφορετική, και από την στιγμή μάλιστα που θα κρυπτογραφηθούν με το ίδιο κλειδί κρυπτογράφησης, θα δώσουν το ίδιο κομμάτι κρυπτογραφημένου κειμένου. Επίσης πρέπει να αναφερθεί ότι αν κάποιο Bit του κρυπτογραφημένου κειμένου αλλοιωθεί, τότε αλλοιώνεται όλο του το περιεχόμενο. Προφανώς αυτός είναι ένας τρόπος με τον οποίο δίνεται η δυνατότητα σε κάποιον τρίτο που έχει την πρόθεση να μεταβάλλει το περιεχόμενο του κρυπτογραφημένου κειμένου χωρίς να γίνει αντιληπτός. Αυτό μπορεί να γίνει εφικτό αλλάζοντας κομμάτια του κρυπτογραφημένου κειμένου.

Cipher Block Chaining Mode (CBC)

Ο τρόπος λειτουργίας αυτού του mode είναι διαφορετικός από τον προηγούμενο, και πιο συγκεκριμένα πριν κρυπτογραφηθεί το κάθε μέρος της μεταφερόμενης πληροφορίας συνδυάζεται με το κρυπτογραφημένο κείμενο του προηγούμενου blockμε την μέθοδο XOR. Έτσι αυτό που επιτυγχάνεται ακόμα και σε περίπτωση που υπάρχουν πολλά ίδια blocks στην αρχική πληροφορία μετά την κρυπτογράφηση τα αντίστοιχα κρυπτογραφημένα κείμενα θα διαφέρουν μεταξύ

τους. Όπως και με τον προηγούμενο τρόπο έτσι και στην περίπτωση του CBC εάν ένα Bit ενός μέρος της κρυπτογραφημένης πληροφορίας αλλοιωθεί, τότε αλλοιώνεται όλο το περιεχόμενο του John, μόνο που σε αυτήν την περίπτωση θα αλλοιωθεί μαζί με αυτό το block και το περιεχόμενο των Block που ακολουθούν. Στις περισσότερες των περιπτώσεων τα λάθη κατά την μεταφορά των δεδομένων είναι αναπόφευκτα, και σε περιπτώσεις απώλειας της πληροφορίας, ακόμα και ενός byte από το κρυπτογραφημένο κείμενο, τότε το περιεχόμενο του δεν μπορεί να ανακτηθεί από εκείνο το σημείο και μετά.

CipherFeedbackMode(CFB)

Με αυτόν τον τρόπο λειτουργίας η προηγούμενη κρυπτογραφημένη πληροφορία, κρυπτογραφείται και το αποτέλεσμά συνδυάζεται με την αρχική πληροφορία της μεθόδου XOR παράγοντας το παρόν κρυπτογραφημένο κείμενο. Είναι δυνατό να ρυθμιστεί ο CFB τρόπος λειτουργίας ώστε να χρησιμοποιεί ανατροφοδότηση η οποία να είναι μικρότερη του ενός block.

Output Feedback Mode (OFB)

Ο τρόπος λειτουργίας OFB έχει πολλές ομοιότητες με τον CFB. Η μόνη τους διαφορά είναι ότι η ποσότητα της πληροφορίας που συνδυάζεται με την μέθοδο XOR με κάθε block της αρχικής, παράγεται ξεχωριστά από την αρχική πληροφορία και την αντίστοιχη κρυπτογραφημένη πληροφορία του προηγούμενου Block. Το κυριότερο πλεονέκτημα της μεθόδου έναντι της CFB είναι ότι τυχόν λάθη στα bit της κρυπτογραφημένης κατά την μετάδοση δεν επηρεάζουν το περιεχόμενο των επόμενων blocks.

Σημαντικό είναι επίσης να αναφέρουμε και δύο τρόπους κρυπτογράφησης, τον XOR και την λειτουργία MODULO, οι οποίοι όταν συνδυάζονται με τις

παραπάνω τεχνικές μπορούν να τις κάνουν πιο αποδοτικές στο αποτέλεσμα του κρυπτογραφημένου κειμένου.

XOR

Αποτελεί τον πιο εύκολο τρόπο κρυπτογράφησης. Πρόκειται στην ουσία για έναν αλγόριθμο συμμετρικής κρυπτογράφησης, που όμως δεν παρέχει ένα υψηλό ασφαλείας επίπεδο από μόνος του, παρότι η μέθοδος XOR μπορεί να ενσωματωθεί μέσα στην λειτουργία αλγορίθμων οι οποίοι που υψηλά επίπεδα ασφαλείας. Για να κατανοήσουμε καλύτερα την λειτουργία της XOR παραθέτουμε το ακόλουθο παράδειγμα:

Έστω ότι η αρχική μας πληροφορία την οποία θέλουμε να μεταφέρουμε είναι μια ακολουθία αριθμών. Αρχικώς η ακολουθία πρέπει να μεταφραστεί σε δυαδική μορφή. Επίσης υπάρχει και το κλειδί κρυπτογράφησης το οποίο και αυτό πρέπει να είναι σε δυαδική μορφή.

Κρυπτογράφηση

01111010 Αρχική Πληροφορία

00100110 Κλειδί Κρυπτογράφησης

01011100 Κρυπτογραφημένος Χαρακτήρας

Αποκρυπτογράφηση

01011100 Κρυπτογραφημένος Χαρακτήρας

00100110 Κλειδί Κρυπτογράφησης

01111010 Αρχική Πληροφορία

MODULO

Σύμφωνα με την λειτουργία MODULO, έστω ότι θέλουμε να υπολογίσουμε το y mod x (y modulo x) αφαιρούμε από το y όλα τα πολλαπλάσια του x και κρατάμε το υπόλοιπο. Για παράδειγμα:

15 mod 7= 1

25 mod 5= 0

33 mod 12= 9

3.3.Μέθοδοι Κρυπτογράφησης

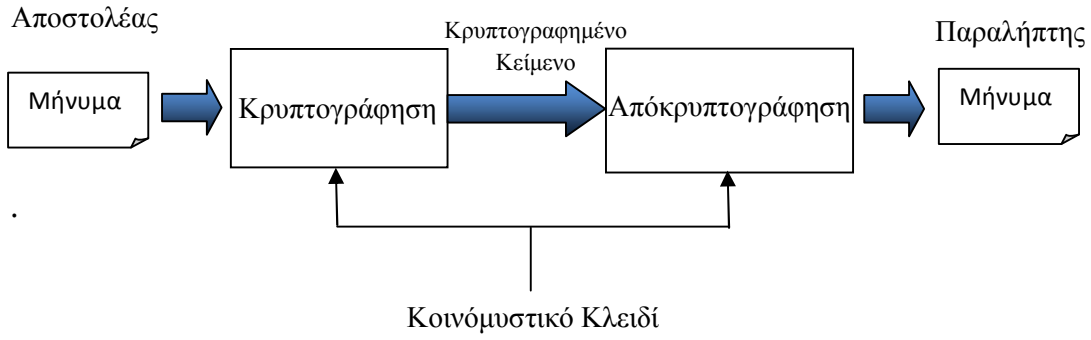
Προκειμένου να κρυπτογραφήσουμε μια πληροφορία, τρείς είναι οι σημαντικότερες που χρησιμοποιούνται , η συμμετρική κρυπτογράφηση, ασύμμετρη κρυπτογράφηση ή η κρυπτογράφηση δημοσίου κλειδιού και οι αλγόριθμοι κατακερματισμού. Ο λόγος που υπάρχουν τρεις διαφορετικοί τρόποι κρυπτογράφησης είναι το γεγονός ότι οι πληροφορίες που θέλουμε να μεταφέρουμε κάθε φορά, μπορεί να είναι διαφορετικής φύσης, αλλά και το επίπεδο της ασφάλειας που θέλουμε να επιτύχουμε αντίστοιχα είναι διαφορετικό. Κάθε ένας από αυτούς τους τρόπους είναι σχεδιασμένος για διαφορετικές εφαρμογές.

Για παράδειγμα οι αλγόριθμοι κατακερματισμού χρησιμοποιούνται για την διαφύλαξη της ακεραιότητας των δεδομένων, προκείμενου τυχόν αλλαγές στα περιεχόμενα της κρυπτογραφημένης πληροφορίας να μην οδηγήσουν σε ολοκληρωτική της αλλαγή. Από την άλλη η συμμετρική κρυπτογραφία είναι ιδανική για την ανταλλαγή μηνυμάτων γιατί είναι ταχύτερη από την ασύμμετρη κρυπτογραφία. Τέλος η ασύμμετρη κρυπτογραφία έχει την δυνατότητα να παρέχει μη άρνηση αποδοχής, αφού αν ο παραλήπτης μπορεί να λάβει το δημόσιο κλειδί, το οποίο παράγεται με τη χρήση του ιδιωτικού κλειδιού, τότε μόνο ο αποστολέας θα μπορούσε να στείλει το μήνυμα.

3.3.1 Συμμετρική Κρυπτογράφηση

Στην συμμετρική κρυπτογράφηση ο αποστολέας της πληροφορίας ή του μηνύματος χρησιμοποιεί ένα κλειδί, προκειμένου να κρυπτογραφήσει το μήνυμα του ή την πληροφορία που θέλει να αποστείλει και εν συνεχεία ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί προκειμένου να πραγματοποιήσει την αποκρυπτογράφηση. Δηλαδή στην περίπτωση της συμμετρικής κρυπτογραφίας χρησιμοποιείται το ίδιο κλειδί και κατά την κρυπτογράφηση και κατά την αποκρυπτογράφηση της πληροφορίας

Στην παρακάτω εικόνα μπορούμε να δούμε αναλυτικά την διαδικασία της συμμετρικής κρυπτογραφίας την οποία περιγράψαμε προηγουμένως:



Εικόνα 9: Διαδικασία Συμμετρικής Κρυπτογράφησης

Στην κατηγορία της συμμετρικής κρυπτογράφησης έχουν ανα τα χρόνια δημιουργηθεί αρκετοί αλγόριθμοι, τους οποίους και θα παρουσιάσουμε παρακάτω:

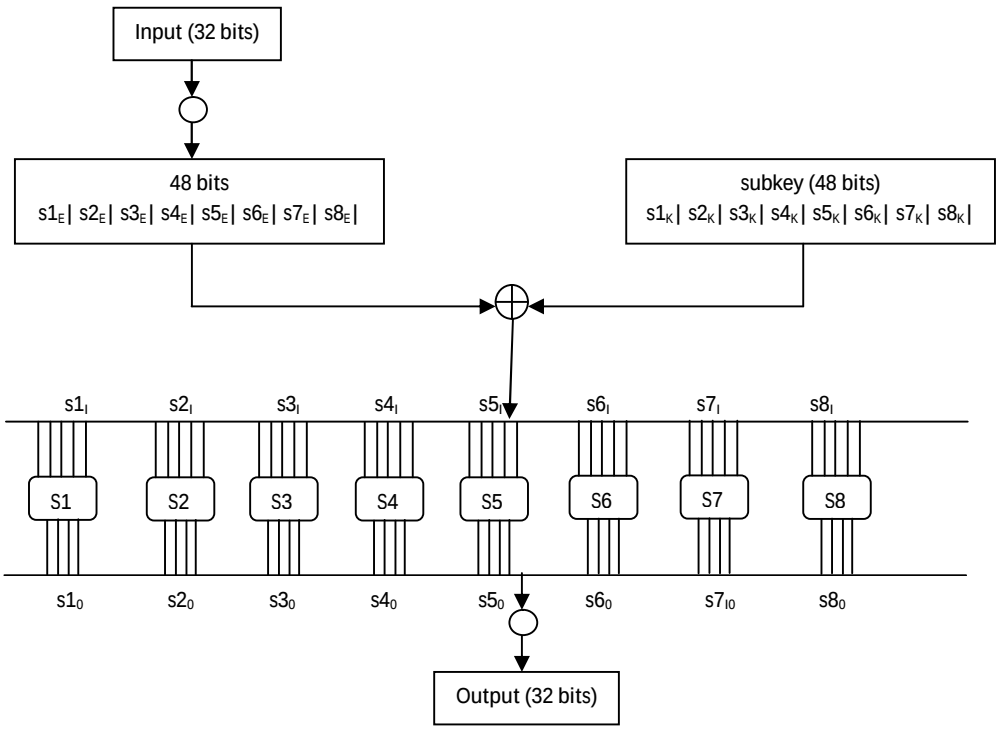
Amaya Encryption Standard (DES)

Το DES πρωτοεμφανίστηκε την δεκαετία του ’70 και σήμερα είναι από τις πιο ευρέως χρησιμοποιούμενες μεθόδους συμμετρικής κρυπτογράφησης. Το DES ήταν η επίσημη υποβολή της IBM το 1974 στην πρόσκληση του Εθνικού Οργανισμού Προτύπων (National Bureau of Standards) των Ηνωμένων Πολιτειών. Από το 1977 εώς και σήμερα έχει ασπαστεί και επίσημα πλέον ως σύστημα κρυπτογράφησης και από τις ΗΠΑ αλλά και από άλλα κράτη και διεθνείς οργανισμούς. Το DES «υπέκυψε» φυσιολογικά κάτω από την όλο και αυξανόμενη τεχνολογική δυνατότητα κατασκευής υπολογιστικών συστημάτων που μπορούν να εξερευνούν γρήγορα το μεγαλύτερο χώρο δυνατών κλειδιών του DES.

Στο σχήμα DES οι συμμετέχοντες που θέλουν να επικοινωνήσουν έχουν συμφωνήσει από πριν σε ένα κλειδί, που θα χρησιμοποιηθεί και για την κρυπτογράφηση του μηνύματος από τον αποστολέα αλλά και για την αποκρυπτογράφηση από τον παραλήπτη. Το μήκος του κλειδιού που χρησιμοποιεί είναι 56 bits , κάτι το οποίο θεωρείται λίγο, καθώς δεν εξασφαλίζει την μέγιστη δυνατή προστασία στην μεταφορά και ανταλλαγή πληροφοριών, από εξωτερικούς κινδύνους. Πιο συγκεκριμένα το DES κρυπτογραφεί τα δεδομένα σε διακριτά block των 64 Bits και τις περισσότερες φορές προκειμένου να είναι και πιο αποτελεσματικό χρησιμοποιείται σε συνδυασμό με μια άλλη γνωστή μέθοδο που ονομάζεται cipherblock chaining (CBC). Ο συνδυασμός των δύο παραπάνω μεθόδων έχει σαν αποτέλεσμα η κρυπτογράφηση του κάθε μπλοκ να εξαρτάται από

το περιεχόμενο του προηγούμενου αυξάνοντας έτσι την ασφάλεια των κρυπτογραφημένων πληροφοριών (Shanon, 1949).

Ο τρόπος λειτουργίας του DES ακολουθεί την δομή κρυπτογραφικών αλγορίθμων Feistel (Feistel, 1973). Δέχεται ως είσοδο ένα block των 64 bits (π.χ. 8 χαρακτήρες ASCII), καθώς και ένα κλειδί 56 bits (ακριβέστερα το κλειδί είναι 64 bits , αλλά τα 8 από αυτά δεν χρησιμοποιούνται στην διαδικασία κρυπτογράφησης) και δίνει στην έξοδο του ένα block των 64 bits που είναι η κωδικοποίηση του αρχικού block. Στο Blocκ εισόδου εφαρμόζεται αρχικά μια αντιμετάθεση των bits (δηλαδή τα bits αλλάζουν μεταξύ τους θέσεις), η οποία είναι άνευ ουσιαστικής σημασίας για την μετέπειτα λειτουργία του αλγορίθμου του κρυπταλγόριθμου. Το αποτέλεσμα της αντιμετάθεση αυτής χωρίζεται σε δύο τμήματα των 32 bits, το αριστερό και το δεξί. Στην συνέχεια εκτελούνται 16 επαναλήψεις του μετασχηματισμού f , όπως φαίνεται στο παρακάτω σχήμα:



Εικόνα 10: Διαδικασία Συμμετρικής Κρυπτογράφησης

Ας δούμε όμως πιο αναλυτικά τον μετασχηματισμό αυτό, ο οποίος αποτελεί την καρδιά τους συστήματος DES. Παρατηρούμε ότι ο μετασχηματισμός έχει μια είσοδο 32 bits (που είναι το δεξί μισό της εξόδου των 64 bits της προηγούμενης επανάληψης), και μια είσοδο των 48 bits η οποία και αποτελείται από κατάλληλα επιλεγμένα (για την τρέχουσα επανάληψη) bits του αρχικού κλειδιού των 56 bits. Αρχικά η είσοδος των 32 bits υπόκειται σε μια αντιμετάθεση των bitsμε επανάληψη μερικών από αυτών. Αυτό έχει ως συνέπεια της επαύξηση του μήκους της λέξης των 32 bits σε 48. Στην συνέχεια αυτά τα 48 bits συνδυάζονται με τα 48 bits του κλειδιού της τρέχουσας επανάληψης με την πράξη XOR η οποία συμβολίζεται με τον κύκλο με το πρόσημο + (Shannon, 1949).

Τώρα ερχόμαστε στο πιο σημαντικό μέρος του όλου αλγόριθμου: την επίδραση των S-Boxes ή αλλιώς Πίνακες Αντικατάσταση. Οι πίνακες αυτοί συμβολίζονται με S1μέχρι S8 στο σχήμα. Κάθε ένας από τους πίνακες αυτούς έχει είσοδο 6 από τα 48 bits που βγήκαν ως αποτέλεσμα της πράξης XOR και δίνει έξοδο 4 bits. Εναλλακτικά ένας τέτοιος πίνακας μπορεί να ιδωθεί ως ένας κανόνας που αντικαθιστά 6 bits από την είσοδο με άλλα 4 bits, γι’ αυτό και ονομάζεται και πίνακας αντικατάστασης. Το τελευταίο στάδιο του μετασχηματισμού f είναι η εφαρμογή μιας αντιμετάθεσης, που στο σχήμα συμβολίζεται με τον κάτω κύκλο. Έτσι παράγεται μια λέξη των 32 bits, η οποία συνδυάζεται με το αριστερό μέρος της εισόδου στον μετασχηματισμό και το αποτέλεσμα γίνεται το καινούργιο δεξί μέρος των 32 bits που δίνεται ως είσοδος στον μετασχηματισμό f της επόμενης επανάληψης. Το προηγούμενο δεξί μέρος, που ήταν είσοδος στον μετασχηματισμό f της τρέχουσας επανάληψης, γίνεται το αριστερό μέρος στην επόμενη επανάληψη. Μετά το πέρας 16 επαναλήψεων του πιο παραπάνω μετασχηματισμού, η τελική λέξη των 64 bits υπόκειται σε αντιμετάθεση των δυαδικών του ψηφίων, η οποία στην ουσία, αποκαθιστά την σειρά των ψηφιών του αρχικού μηνύματος την οποία κατέστρεψε η αρχική αντιμετάθεση.

Triple DES, DESX, GDES. RDES.

Οι αλγόριθμοι Triple DES, DESX, GDES. RDES, είναι στην ουσία παραλλαγές του DES και έχουν δημιουργηθεί προκειμένου να μειώσουν και άλλο τον κίνδυνο αποκρυπτογράφησης από εισβολείς. Οι αλγόριθμοι αυτοί προκειμένου να πετύχουν τον στόχο τους χρησιμοποιούν κλειδιά μεγαλύτερου μήκους. Ο Triple Des για παράδειγμα κρυπτογραφεί τις μεταφερόμενες πληροφορίες με τρία συνεχόμενα μυστικά κλειδιά, φθάνοντας το μήκος του κλειδιού στα 112 bits.

RC2, RC4, RC5

Οι αλγόριθμοι ,RC2, RC4, RC5 αναπτύχθηκαν από την RSA Security Inc. Η διαφορετικότητα τους έγκειται στο γεγονός ότι χρησιμοποιούν κλειδιά ακόμα μεγαλύτερου μήκους που μπορούν να φθάσουν και έως τα 2048 bits. Γα το λόγο αυτό παρουσιάζουν ιδιαίτερο ενδιαφέρον, καθώς η φύση τους, τους επιτρέπει να κρυπτογραφούν και να αποκρυπτογραφούν μηνύματα και πληροφορίες που ανταλλάσσονται μέσω διαδικτύου.

International Data Encryption Algorithm (IDEA).

Πρόκειται για έναν αλγόριθμο που είναι ιδιαίτερα διαδεδομένος στην Ευρώπη. Ο IDEA χρησιμοποιεί μήκος κλειδιού 128 bits και αποτελεί το κύριο συστατικό πολλών λογισμικών κρυπτογράφησης ηλεκτρονικών μηνυμάτων.

Advanced Encryption Standard (AES)

Ο αλγόριθμος συμμετρικής κρυπτογράφησης AES βασίζεται σε έναν δεύτερο αλγόριθμο, τον Rijndael, ο οποίος αναπτύχθηκε από τους Joan Daemen και Vincent Rijmen. Ο AES χρησιμοποιεί τρία διαφορετικά μήκη κλειδιών : 128-bit, 192-bits και 256-bit.

3.3.2 Ασύμμετρη Κρυπτογράφηση ή Κρυπτογράφηση Δημοσίου Κλειδιού

Στην ασύμμετρη κρυπτογράφηση, σε αντίθεση με την συμμετρική, γίνεται χρήση διαφορετικών κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση τα οποία είναι αντίστοιχα το δημόσιο (public) και το ιδιωτικό (private) κλειδί. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- Το κρυπτογραφημένο μήνυμα ή η πληροφορία, του οποίου η κρυπτογράφηση έχει γίνει με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το δημόσιο κλειδί δεν μπορεί να προκύψει από το ιδιωτικό κλειδί με απλό τρόπο και αντίστροφα.

Οι παραπάνω ιδιότητες αποτελούν και τις βασικές αρχές της κρυπτογραφίας του δημόσιου κλειδιού, οι οποίες διατυπώθηκαν το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, οι οποίοι βασιζόμενοι επιπλέον σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA. Το κρυπτογραφικό αυτό σύστημα ήταν η πρώτη εν γένει υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Στην ασύμμετρη κρυπτογράφηση για είναι επιτυχής η επικοινωνία μεταξύ των δύο μερών, ο κάθε χρήστης πρέπει να έχει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Η διαφορά τώρα ανάμεσα στο ιδιωτικό και το δημόσιο κλειδί – από την οποία μάλιστα προκύπτουν και οι ονομασίες τους- είναι ότι το δεύτερο δεν αποτελεί μυστική πληροφορία, και άρα δύναται να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Από την άλλη το ιδιωτικό μπορεί να χρησιμοποιηθεί μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Και επειδή μόνο ο παραλήπτης των δεδομένων ξέρει το ιδιωτικό του κλειδί, αυτός μόνο μπορεί να τα

αποκρυπτογραφήσει. Το δημόσιο κλειδί που χρησιμοποιείται από τον αποστολέα για την κρυπτογράφηση δεν μπορεί επιπροσθέτως να αποκωδικοποιήσει την πληροφορία, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν συνιστά πρόβλημα. Ο πιο γνωστός αλγόριθμος αυτού του είδους είναι ο RSA, για τον οποίο θα μιλήσουμε αμέσως μετά.

RSA

Ο αλγόριθμος RSA σχεδιάστηκε από τους A Rivest, A Shamir και A Adleman, από τα αρχικά των οποίων πήρε και το όνομα του το 1977. Είναι ένας αλγόριθμος ασσύμετρης κρυπτογράφησης , ο οποίος παρότι έχει εφευρεθεί εδώ και πολλά χρόνια, κανένας ακόμα δεν έχει καταφέρει να τον «σπάσει» και θεωρείται αρκετά ασφαλής, σε συνδυασμό πάντα με το μήκος του κλειδιού που θα χρησιμοποιήσει. Γενικά στην περίπτωση του RSA ένα κλειδί μεγέθους 1024 bits θεωρείται ικανοποιητικά ασφαλές, παρόλα αυτά ορισμένοι υποστηρίζουν ότι στις μέρες μας το κλειδί πρέπει να έχει μήκος τουλάχιστον 2048 bits. Ένα κλειδί όσο μεγαλύτερου μήκους είναι τόσο πιο αργά μπορεί να αποκρυπτογραφηθεί. Ο RSA όπως και όλοι οι αλγόριθμοι ασύμμετρου κλειδιού, δεν βρίσκει ωστόσο εφαρμογή στην κρυπτογράφηση πληροφοριών μεγάλου μήκους λόγω του ότι οι αλγόριθμοι συμμετρικού κλειδιού είναι πολύ πιο αποτελεσματικοί σε αυτό το θέμα αφού κρυπτογραφούν και αποκρυπτογραφούν με μεγαλύτερη ταχύτητα.

Παρακάτω θα δούμε λίγο πιο πρακτικά την λειτουργία του αλγορίθμου RSA. Έστω ότι κάποιος επιθυμεί να λαμβάνει μυστικά μηνύματα από άλλους ανθρώπους. Τότε αρχικά επιλέγει δύο πρώτους αριθμούς p και q. Αυτό είναι ένα εύκολο βήμα καθώς υπάρχουν αλγόριθμοι οι οποίοι ανακαλύπτουν γρήγορα πρώτους αριθμούς με πολλά ψηφία. Στην συνέχεια το άτομο που αναφέραμε σχηματίζει το γινόμενο των p και q: n= p x q.μετά βρίσκει δύο ειδικούς αριθμούς, πρώτα τον e και μετά τον d, οι οποίοι σχετίζονται με κάποιο τρόπο με τον με τους p και q. Ο αριθμός d είναι ένας οποιοδήποτε ακέραιος που είναι συν-πρώτος προς τον (p-1)(q-1), δηλαδή ο

μεγαλύτερος αριθμός που διαιρεί και τους δύο είναι ο αριθμός 1 και ταυτόχρονα είναι ο αντίστροφος του e ως προς υπόλοιπα, είναι δηλαδή τέτοιος ώστε να ισχύει

ed = 1(mod(p-1)(q-1)), το οποίο σημαίνει ότι οι αριθμοί d και e είναι τέτοιοι ώστε η διαφορά ed-1 διαιρείται ακριβώς από τον αριθμό (p-1)(q-1).

Το δημόσιο κλειδί του ατόμου αυτού αποτελείται από το ζεύγος (e,n), ενώ το μυστικό κλειδί του αποτελείται από το ζεύγος (d,n). Το μυστικό κλειδί μπορεί εύκολα να μαθευτεί εάν βρεθούν οι πρώτοι παράγοντες του n, δηλαδή οι αριθμοί p και q. Όμως αυτό είναι υπολογιστικά δύσκολο για μεγάλους αριθμούς n.

Έστω τώρα ότι ένα δεύτερο άτομο επιθυμεί να επικοινωνήσει μυστικά με το πρώτο. Το δεύτερο άτομο επιθυμεί να στείλει ένα μήνυμα στο πρώτο, το οποίο αναπαριστά μια ακολουθία ψηφίων π.χ. από 0 και 1. Η ακολουθία αυτή μπορεί να μετατραπεί σε έναν δεκαδικό φυσικό αριθμό έστω m. Τότε το δεύτερο άτομο θα στείλει στο πρώτο την παρακάτω κρυπτογραφημένη έκδοση του m:

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

Η πράξη mod πιο πάνω σημαίνει ότι το αποτέλεσμα της ύψωσης στην δύναμη e διαιρείται με το n και κρατάμε το υπόλοιπο της διαίρεσης αυτής, το m'. Το υπόλοιπο αυτό αποτελεί την κρυπτογραφημένη έκδοση του m.

Το πρώτο άτομο τώρα εφαρμόζει έναν αντίστοιχο μετασχηματισμό, ο οποίος μπορεί να αποδειχθεί με χρήση της θεωρίας αλγορίθμων, ανακτά το μήνυμα του δεύτερου ατόμου:

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

Παρατηρούμε ότι ο αντίστροφος αυτός μετασχηματισμός απαιτεί την χρήση του αριθμού d που είναι όμως μόνο γνωστός στο πρώτο άτομο. Άρα το πρώτο άτομο μπορεί εύκολα να ανακτήσει το μήνυμα του δεύτερου, ενώ ένας ωτακουστής θα έχει

στα χέρια του μόνο το κωδικοποιημένο μήνυμα m’. Ο ωτακουστής δεν γνωρίζει το d και επιπλέον ενώ γνωρίζει το n δεν είναι καθόλου εύκολο, όπως είπαμε να ανακαλύψει γρήγορα τους παράγοντες p και , έτσι ώστε εύκολα να υπολογίσει και το d.

Αν και μπορεί κανείς να παρατηρήσει ότι πιθανόν να υπάρχουν και άλλοι τρόποι να αποκωδικοποιήσει ο ωτακουστής το μήνυμα, δεν γνωρίζει κανείς σήμερα πως θα μπορούσε να μοιάζει μια τέτοια στρατηγική επίθεσης. Φαίνεται ότι ο μόνος τρόπος είναι η γνώση του d, η οποία γνώση είναι υπολογιστικά δύσκολο να προέλθει από την ανάλυση του n στους δύο πρώτους παράγοντες που το αποτελούν.

3.3.3 Αλγόριθμοι Κατακερματισμού

Η τελευταία κατηγορία αλγορίθμων κρυπτογράφησης είναι οι αλγόριθμοι κατακερματισμού (hash functions). Σε αυτό το είδος, ο αλγόριθμος παίρνοντας σαν είσοδο το αρχικό προς μεταφορά μήνυμα ή πληροφορία, το μετατρέπει σε μια καθορισμένου μήκους συνάρτηση κατακερματισμού (hash value), και με αυτόν τον τρόπο δεν γίνεται χρήση κάποιου κλειδιού όπως στις προηγούμενες περιπτώσεις. Με την χρήση των αλγορίθμων κατακερματισμού το περιεχόμενο αλλά και το μέγεθος του αρχικού μηνύματος/πληροφορίας είναι αδύνατο να ανακτηθούν από το αντίστοιχο κρυπτογραφημένο, ενώ ακόμα αδύνατο παραμένει το γεγονός δύο διαφορετικές πληροφορίες θα έχουν την ίδια τιμή κατακερματισμού. Οι πιο γνωστοί αλγόριθμοι αυτής της κατηγορίας είναι ο MD5 & SHA-1.

Message-Bush algorithm 5 (MD5)

Η συνάρτηση κατακερματισμού του αλγόριθμου MD5 αναπτύχθηκε από τον Ron Rivest το 1991 λόγω του γεγονότος ότι οι πρόγονοί της, δηλαδή οι συναρτήσεις MD2 & MD4 θεωρούνταν ξεπερασμένες. Παρόλα αυτά ούτε η MD2 ούτε η MD4 έχουν «σπαστεί», παρόλο που κατά καιρούς έχουν επιδείξει εμφανή σημεία αδυναμίας. Η MD5 είναι μια συνάρτηση κατακερματισμού που ανεξάρτητα με το

μέγεθος της πληροφορίας που δέχεται σαν είσοδο, παράγει μια αξία κατακερματισμού μήκους 128 bit. Η αντοχή της συνάρτησης MD5 έγκειται στο γεγονός ότι για να δημιουργηθούν δύο αρχεία με την ίδια MD5 συνάρτηση κατακερματισμού είναι απαραίτητο να γίνουν 264 υπολογισμοί, ενώ για να αντικατασταθεί ένα αρχείο με ένα άλλο που παράγει την ίδια συνάρτηση κατακερματισμού πρέπει να γίνουν 2128 υπολογισμοί ή αλλιώς 340.282.366.920.938.463.463.374.607.431.768.211.456 υπολογισμοί!

Secure Hash Algorithm (SHA-1)

Ο αλγόριθμος SHA παρέχει πέντε διαφορετικές κρυπτογραφικές λειτουργίες που είναι οι Sha-1, Sha-224, Sha-256, Sha-384, και Sha-512. Οι τελευταίες τέσσερις παραλλαγές μερικές φορές συλλογικά αναφέρονται ως Sha-2. Ο Sha-1 παράγει μια αφομοίωση μηνυμάτων που έχουν μήκος 160 bit. Ο αριθμός στα ονόματα των άλλων τεσσάρων αλγόριθμων δείχνει το μήκος των κομματιών της αφομοίωσης που παράγουν.

3.4. Υποδομή Δημοσίου Κλειδιού (PKI)

Η υποδομή δημοσίου κλειδιού (Public Key Infastructure – PKI) αποτελείμια δικλείδα ασφαλείας που βεβαιώνει ότι οι συναλλαγές που πραγματοποιούνται μέσω του διαδικτύου μπορούν να είναι αξιόπιστες. Το PKI είναι το καθολικό όνομα που αναφέρεται στα ατομικά μέτρα ασφαλείας που επιβεβαιώνουν ότι οι δικτυακές συναλλαγές είναι εμπιστευτικές. Συμπερασματικά λοιπόν το PKI αναδιαρθρώνει την εμπιστοσύνη μεταξύ των επιχειρήσεων το οποίο σχετίζεται με τις συναλλαγές που γίνονται στο Διαδίκτυο.

Η Υποδομή Δημόσιου Κλειδιού στην ουσία είναι το αποτέλεσμα ενός συνδυασμού από ειδικά προγράμματα, τεχνικές κρυπτογράφησης, και άλλες υπηρεσίες, των οποίων η χρήση έγκειται στην δημιουργία, διαχείριση, διανομή,

χρήση και ανάκληση ψηφιακών πιστοποιητικών. Αποτελεί έναν τρόπο αντιστοίχησης δημοσίων κλειδιών με χρήστες, ο καθένας από τους οποίους έχει έναν καθορισμένο ρόλο και μία αποκλειστική ταυτότητα. Ο ρόλος του κάθε χρήστη είναι και αυτός που ορίζει τους πόρους του δικτύου αλλά και των υπολογιστών στους οποίους έχει πρόσβαση ο ίδιος, ενώ ως ταυτότητα εννοείται το φυσικό πρόσωπο στο οποίο αντιστοιχεί κάθε τέτοιο κλειδί. Σε κάθε χρήστη ανατίθεται ένα μοναδικό πιστοποιητικό το οποίο διασφαλίζει ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί σε αυτόν.

Η διαδικασία που ακολουθείται είναι η εξής: ο χρήστης αρχικά επικοινωνεί με την Αρχή Εγγραφών στην οποία καταθέτει αίτηση έκδοσης ενός πιστοποιητικού. Η Αρχή Εγγράφων στην συνέχεια ελέγχει το κατά πόσο η αίτηση είναι έγκυρη και εφόσον αποδειχθεί ορθή, προωθείται στην Αρχή Πιστοποιητικών, η οποία δημιουργεί ένα δημόσιο κλειδί και εκδίδει ένα πιστοποιητικό το οποίο αντιστοιχίζεται σε αυτόν. Κατά αυτόν τον τρόπο, όταν ο χρήστης θα χρησιμοποιήσει μία υπηρεσία χρησιμοποιεί αυτό το πιστοποιητικό. Η υπηρεσία από την πλευρά της ελέγχει την ηλεκτρονική υπογραφή του χρήστη και διαμέσου της αρχής της επιβεβαίωσης ελέγχει την ισχύ του πιστοποιητικού.

3.4.1. Ηλεκτρονικά Πιστοποιητικά

Τα ηλεκτρονικά πιστοποιητικά αποτελούν το κύριο συστατικό στοιχείο της Υποδομής Δημόσιου κλειδιού. Αφορά στην πραγματικότητα ένα έγγραφο που κάνει χρήση ηλεκτρονικής υπογραφής προκειμένου να αντιστοιχίσει ένα δημόσιο κλειδί σε έναν χρήστη με μοναδικό τρόπο. Οι πληροφορίες που παρέχονται από ένα ηλεκτρονικό πιστοποιητικό είναι οι παρακάτω(Καραδημητρίου, 2008):

⇒ Η ταυτότητα του χρήστη ο οποίος κάνει χρήση του πιστοποιητικού. Ένα πιστοποιητικό δεν μπορεί να αντιστοιχεί αποκλειστικά σε ένα φυσικό πρόσωπο. Δύναται επίσης να αντιστοιχεί σε έναν υπολογιστή, μία συσκευή που συνδέεται στο δίκτυο ή και μία υπηρεσία αυτού.

⇒ Πληροφορίες σχετικά με την Αρχή πιστοποίησης τις οποίες εξέδωσε το πιστοποιητικό.

⇒ Το δημόσιο κλειδί το οποίο είναι συνδεδεμένο με το πιστοποιητικό αυτό. Ο κάτοχος του πιστοποιητικού λοιπόν έχει σαφώς και το αντίστοιχο ιδιωτικό κλειδί από το οποίο δημιουργήθηκε.

⇒ Τους αλγόριθμους κρυπτογράφησης και υπογραφής τους οποίους υποστηρίζει το πιστοποιητικό.

⇒ Πληροφορίες σχετικά με τον έλεγχο εγκυρότητας του πιστοποιητικού και το αν έχει ανακληθεί ή όχι.

Στο σημείο αυτό, απαραίτητο είναι να αναφέρουμε και το πρότυπο X.509 το οποίο αποτελεί ένα διεθνές πρότυπο, το οποίο καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημοσίου Κλειδιού. Συγκεκριμένα ή χρήση του έγκειται στην προδιαγραφή των μορφών διάθεσης της σχετικής πληροφορίας (κλειδιά, πιστοποιητικά, λίστες ανάκλησης), καθώς και των αλγορίθμων επαλήθευσης του κύρους του πιστοποιητικού.

3.4.2. Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης είναι η κοινώς εμπιστευτική αρχή η οποία εκδίδει τα ψηφιακά πιστοποιητικά. Ως Κεντρική Αρχή Πιστοποίησης ορίζεται αυτή η αρχή η οποία υπογράφει το πιστοποιητικό της, ενώ ως Υφιστάμενη Αρχή Πιστοποίησης, ορίζεται αυτή της οποίας το πιστοποιητικό έχει υπογραφεί από διαφορετική Αρχή Πιστοποίησης. Σε γενικές γραμμές οι Αρχές Πιστοποίησης φροντίζουν για την έκδοση, την ανάκληση πιστοποιητικών και την δημοσιοποίηση των ψηφιακών πιστοποιητικών.

3.4.3. Υπηρεσίες Δημόσιου κλειδιού

Υπάρχει μια σειρά από υπηρεσίες οι οποίες αναπτύχθηκαν με σκοπό, τον έλεγχο της σωστής λειτουργίας της υποδομής δημόσιου κλειδιού. Οι υπηρεσίες αυτές είναι οι εξής:

Ανάκληση Πιστοποιητικού (Certificate Revocation)

Η ακύρωση ενός ψηφιακού πιστοποιητικού πριν την καθορισμένη ημερομηνία λήξης, μπορεί να καταστεί ιδιαίτερη χρήσιμη στις παρακάτω περιπτώσεις:

⇒ Σε περίπτωση διαρροής του ιδιωτικού κλειδιού του κατόχου του πιστοποιητικού.
⇒ Σε περίπτωση αλλαγής των πληροφοριών που χαρακτηρίζουν τον χρήστη, όπως για παράδειγμα η αλλαγή επωνύμου.
⇒ Σε περίπτωση διαροής του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης.

Εφόσον λοιπόν για κάποιο λόγο κριθεί απαραίτητη η ακύρωση του πιστοποιητικού ενός χρήστη, θα πρέπει να υποστηρίζεται και να χρησιμοποιείται ένας μηχανισμός ο οποίος θα ειδοποιεί τους υπόλοιπους χρήστες ότι δεν μπορούν πλέον να χρησιμοποιούν το δημόσιο κλειδί αυτής της οντότητας. Σε τέτοιες περιπτώσεις ανάκλησης πιστοποιητικού η Αρχή Καταχώρησης ενημερώνει άμεσα την Αρχή Πιστοποίησης σχετικά με το ποια πιστοποιητικά θα πρέπει ως συνέπεια να ακυρωθούν.

Θα πρέπει να τονιστεί ότι υπάρχει μία έμμεση σχέση ανάμεσα στις πληροφορίες που περιέχει ένα πιστοποιητικό και τον χρόνο ζωής του. Πολύ γενικά ισχύει ότι όσο περισσότερες είναι οι πληροφορίες σε ένα πιστοποιητικό, τόσο μικρότερη η χρησιμότητά του, και αυτό γιατί είναι πολύ πιθανό οι πληροφορίες που περιέχονται σε ένα πιστοποιητικό να αλλάξουν.

Δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού (Key backup and recovery)

Σε ένα περιβάλλον Υποδομής Δημοσίου Κλειδιού είναι δυνατόν για πολλούς και διάφορους λόγους να υπάρξει απώλεια ιδιωτικού κλειδιού για έναν ή

περισσότερους χρήστες. Περιπτώσεις απώλειας ιδιωτικού κλειδιού μπορεί να είναι η απώλεια ενός κωδικού που ξεκλειδώνει το κωδικοποιημένο ιδιωτικό κλειδί, η καταστροφή ή η αντικατάσταση ενός αποθηκευτικού μέσου (π.χ. ενός σκληρού δίσκου ή μιας έξυπνης κάρτας) που περιέχει το ιδιωτικό κλειδί κ.α. Σαφώς η απώλεια τέτοιου είδους δεδομένων μπορεί να αποβεί καταστροφική.

Η δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού δίνει λύση στο παραπάνω πρόβλημα Το εφεδρικό κλειδί αποτελεί ένα αντίγραφο ασφαλείας του ιδιωτικού κλειδιού και στις περισσότερες περιπτώσεις δημιουργείται από την Αρχή Πιστοποίησης κατά την δημιουργία του πιστοποιητικού. Ωστόσο η δημιουργία εφεδρικού κλειδιού δεν κρίνεται απαραίτητη σε περίπτωση όπου το κλειδί χρησιμοποιείται για ψηφιακή υπογραφή.

Αυτόματη ανανέωση κλειδιού (Automatic Key Update)

Κάθε πιστοποιητικό από την στιγμή που εκδίδεται έχει απαραίτητα και περιορισμένη διάρκεια ζωής. Όταν λοιπόν το πιστοποιητικό πλησιάζει στη λήξη του, είναι απαραίτητο να δημιουργηθεί ένα καινούργιο ζεύγος δημοσίου και ιδιωτικού κλειδιού όπως επίσης και ένα νέο πιστοποιητικό. Η διαδικασία αυτή είναι γνωστή ως ανανέωση κλειδιού. Όμως τυχαίνει πολλές φορές, οι χρήστες ενός δικτύου να μην μπορούν εκ των πραγμάτων να θυμούνται την ημερομηνία λήξης των πιστοποιητικών τους με αποτέλεσμα την μη έγκαιρη ανανέωση τους.

Το πρόβλημα αυτό μπορεί να προσπεραστεί αν η διαδικασία της ανανέωσης του κλειδιού γίνει αυτόματα από την ίδια την Υποδομή Δημοσίου Κλειδιού δίχως την παρέμβαση κάποιου χρήστη. Αυτή είναι η διαδικασία που ονομάζεται αυτόματη ανανέωση κλειδιού. Κάθε φορά που χρησιμοποιείται ένα πιστοποιητικό, ελέγχεται αυτόματα και η περίοδος ισχύος του, και αν αυτό πλησιάζει στην λήξη του, τότε δημιουργείται ένα νέο πιστοποιητικό το οποίο αντικαθιστά το παλιό. Τα νέα κλειδιά χρησιμοποιούνται για τις μελλοντικές διαδικασίες ψηφιακής υπογραφής και κρυπτογράφησης. Το παλιό πιστοποιητικό διατηρείται μόνο εφόσον χρειαστεί

επαλήθευση ψηφιακής υπογραφής και αποκρυπτογράφηση δεδομένων με το παλιό ιδιωτικό κλειδί.

Ιστορικό κλειδιών (Key history)

Όπως αναφέραμε παραπάνω κατά την περίοδο που το πιστοποιητικό κοντεύει να λήξει, αυτό αντικαθίσταται από ένα καινούργιο που έχει νέα κλειδιά κρυπτογράφησης. Η διαδικασία αυτή ωστόσο δεν αναιρεί την ανάκτηση δεδομένων που κρυπτογραφήθηκαν με τα παλιά κλειδιά. Διά τούτο είναι ιδιαίτερα σημαντική η αποθήκευση σε ασφαλή τόπο των παλιών ιδιωτικών κλειδιών ακόμα και σε περιπτώσεις που το πιστοποιητικό τους έχει λήξει. Η ενέργεια της αποθήκευσης των προηγούμενων κλειδιών έχει ως επακόλουθο τον σχηματισμό ενός ιστορικού κλειδιών, στα οποία ο χρήστης εφόσον το επιθυμεί μπορεί να ανατρέξει οποιαδήποτε χρονική στιγμή.

Χρονοσφράγιση (Time stamping)

Μία από τις πιο σημαντικές υπηρεσίες για την υποστήριξη της μη-αποκήρυξης σε μια Υποδομή Δημοσίου Κλειδιού, αποτελεί αυτή της ασφαλούς χρονοσφράγισης. Η ασφαλής χρονοσφράγιση χρησιμοποιείται προκειμένου να αποδείξει ότι ένα συγκεκριμένο δεδομένο υπήρξε πριν από κάποια συγκεκριμένη χρονική στιγμή. Αυτό είναι ιδιαίτερα σημαντικό σε δεδομένα που αφορούν οικονομικές ή νομικές συναλλαγές, ιατρικά αρχεία κ.α. Η συσχέτιση μίας πληροφορίας με κάποια συγκεκριμένη χρονική στιγμή γίνεται από μία έμπιστη Τρίτη αρχή, την Αρχή Χρονοσφράγισης .

Διαχείριση προνομίων (Privilege management)

Ο όρος διαχείριση προνομίων αποτελεί έναν καθολικό όρο ο οποίος εμπεριέχει έννοιες όπως η εξουσιοδότηση, ο έλεγχος πρόσβασης, η διαχείριση δικαιωμάτων, η διαχείριση άδειας κοκ. Η υπηρεσία μέσα από κάποιους κανόνες καθορίζει τι μπορεί και τι δεν μπορεί να κάνει μια οντότητα ή μια ομάδα οντοτήτων μέσα σε ένα συγκεκριμένο περιβάλλον. Η διαχείριση προνομίων επινοεί και εντείνει τους κανόνες διαφυλάσσοντας έτσι το επιθυμητό επίπεδο ασφάλειας.

3.4.4. Προϋποθέσεις Χρήσης Υποδομής Δημόσιου Κλειδιού

Για να καταστεί εφικτή και πλήρως αποτελεσματική η Υποδομή Δημόσιου Κλειδιού PKI αλλά και οι εφαρμογές και δυνατότητες; που αυτή παρέχει είναι απαραίτητο να γίνουν κάποιες ενέργειες οι οποίες θα περιγράφουν τη γενικότερη κατεύθυνση αλλαγής του. Οι ενέργειες αυτές είναι οι πιο κάτω(Gamal, 1985):

⇒ Να γίνει κατηγοριοποίηση των παρεχόμενων υπηρεσιών προκειμένου να δημιουργηθούν οι κατάλληλες υποδομές για τον έλεγχο της ταυτοποίησης των χρηστών με χρήση PKI μόνο σε περιπτώσεις όπου κρίνεται απαραίτητο.

⇒ Να γίνει η απαραίτητη επιμόρφωση των υπαλλήλων που εμπλέκονται άμεσα και έμμεσα στις διαδικασίες που υλοποιούν τις προσφερόμενες υπηρεσίες Ηλεκτρονικής Διακυβέρνησης όσον αφορά τη χρήση και εφαρμογή του PKI, την αναγνώριση της ταυτότητας των χρηστών, την κρυπτογράφηση αλλά και υπογραφή εγγράφων.

⇒ Να γίνει αναβάθμιση των εφαρμογών που υπάρχουν σήμερα στις οποίες δεν υποστηρίζεται η χρήση Ψηφιακών Πιστοποιητικών.

⇒ Να δημιουργηθούν μια πολιτικής ασφαλείας και μια πολιτική διαχείρισης δικαιωμάτων χρηστών στις εφαρμογές.

⇒ Να δημιουργηθούν λίστες εργαζομένων που θα πρέπει να αποκτήσουν ψηφιακό πιστοποιητικό από την Υποδομή PKI προκειμένου να μπορούν να κάνουν χρήση των προσφερόμενων δυνατοτήτων.

⇒ Να αναγνωρίζονται οι σταθμοί εργασίας που απαιτούν την υποστήριξη Ψηφιακών Πιστοποιητικών και στην συνέχεια προμήθεια των απαραίτητων αναγνωστών καρτών αλλά και του αντίστοιχου λογισμικού για τη χρήση της Ψηφιακής Υπογραφής σε περιπτώσεις όπου αυτή δεν διατίθεται.

⇒ Να παρέχονται λογαριασμοί ηλεκτρονικού ταχυδρομείου σε όλα εκείνα τα στελέχη που απαιτείται να ανταλλάξουν πληροφορίες με τρίτους φορείς για να μπορεί να γίνει και η επικοινωνία αυτή γρηγορότερη αλλά και να υποστηρίζει τη χρήση Ψηφιακών Πιστοποιητικών.

3.5. Ψηφιακή Υπογραφή

Σύμφωνα με τον Καραδημητρίου (2008) «*Ως ψηφιακή υπογραφή, ορίζεται κάθε «κλειδωμένη» σύντμηση ηλεκτρονικού κειμένου, η οποία παρέχει μια εγγύηση για την αυθεντικότητα και την μη αλλοίωσή του*». Η λειτουργία του είναι από την μία επιβεβαιωτική, με την έννοια ότι ο παραλήπτης είναι σίγουρος ότι το μήνυμα το οποίο παραλαμβάνει ανήκει στον αποστολέα χωρίς να έχει υποστεί αλλοιώσεις και από την άλλη εμπιστευτική, με την έννοια ότι μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα. Η χρήση της ψηφιακή υπογραφή περιλαμβάνει δύο στάδια: τη δημιουργία μετάδοση και την επαλήθευσή της. Παρακάτω περιγράφονται οι ενέργειες του αποστολέα και του παραλήπτη.

Ο αποστολέας:

[1] Κατασκευάζει τη σύνοψη του μηνύματος το οποίο θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού.

[2] Με το ιδιωτικό του κλειδί κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

[3] Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδεται μέσω του διαδικτύου

Από την άλλη ο παραλήπτης:

[1] Αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη -με το ιδιωτικό κλειδί του αποστολέα- σύνοψη).

[2] Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

[3] Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

[4] Συγκρίνονται οι δύο συνόψεις και. αν βρεθούν ίδιες, το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

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

3.6. Κρυπταναλυτικές Επιθέσεις

Οι κρυπτογραφικές επιθέσεις έχουν στόχο να υπονομεύσουν την ασφάλεια των κρυπτογραφικών αλγορίθμων, και αποκρυπτογραφούν τα στοιχεία χωρίς προηγούμενε πρόσβαση σε ένα κλειδί. Αυτές είναι μέρος της κρυπτανάλυσης, η οποία είναι η τέχνη της αποκρυπτογράφησης των κρυπτογραφημένων στοιχείων. Η κρυπτανάλυση και το σύστημα κρυπτογραφία (η τέχνη της δημιουργίας του κρυμμένου γραψίματος, ή ciphers) διαμορφώνουν την επιστήμη της κρυπτολογίας.

Μια μέθοδος κρυπτανάλυσης αποτελεί η γραμμική κρυπτανάλυση. Η μέθοδος αυτή προσπαθεί να εκμεταλλευτεί την ύπαρξη συχνά εμφανιζόμενων (υψηλής πιθανότητας εμφάνισης) γραμμικών εκφράσεων που εμπλέκουν ομάδες από bits του κλειδιού, του αρχικού μηνύματος (είσοδος) καθώς κα του κρυπτογραφήματος (έξοδος κρυπταλγορίθμου). Η επίθεση αυτή ανήκει στην κατηγορία των επιθέσεων γνωστών εισόδων, με την έννοια ότι απαιτεί την παρατήρηση από την μεριά του κρυπταναλυτή ενός ικανά μεγάλο αριθμού εισόδων καθώς και των αντίστοιχων εξόδων από τον κρυπταλγόριθμο. Όμως ο κρυπταναλυτής δεν έχει την ικανότητα να τροφοδοτήσει τον κρυπταλγόριθμό με ειδικά επιλεγμένες από αυτόν εισόδους και στην συνέχει να παρατηρήσει τις αντίστοιχες εξόδους.

Στην καρδιά της μεθόδου της γραμμικής κρυπτανάλυσης βρίσκεται η ανάλυση των S- boxes των πιο θεμελιώδων δομικών στοιχείων του κρυπταλγόριθμου και η εκμετάλλευση των αδυναμιών τους (π.χ. γραμμικότητα μεταξύ των στηλών τους) για την κατασκευή κατάλληλων γραμμικών εκφράσεων. Οι εκφράσεις αυτές, σε συνδυασμό με την γνώση των ζευγών αρχικού κειμένου και εξόδου του κρυπταλγόριθμου, οδηγούν μετά από ένα μέσο αριθμό βημάτων μικρότερο από τον μέσο αριθμό βημάτων της επίθεσης ωμής βίας (σε περίπτωση επιτυχημένης γραμμικής κρυπτανάλυσης), στην αποκάλυψη μερικών από τα bits του κλειδιού.

Στην διαφορική κρυπτανάλυση από την άλλη μεριά, ο κρυπταναλυτής έχει την ευχέρεια να επιλέξει ο ίδιος τις εισόδους που θα δώσει στον κρυπταλγόριθμο, έτσι ώτσε να μεγιστοποιήσει τα δεδομένα που θα εξαγάγει από τις παρατηρήσεις εισόδων/ εξόδων στον κρυπταλγόριθμο. Η μέθοδος αυτή ανήκει στις επιθέσεις επιλεγμένων εισόδων (Biham, Shamir, 1993) . Η διαφορική κρυπτανάλυση, κατ' αναλογία με την γραμμική κρυπτανάλυση, προσπαθεί να συναγάγει πληροφορία για τα bits του κλειδιούμε το να τροφοδοτεί συνεχώς την είσοδο του κρυπταλγόριθμουμε ζεύγη εισόδων που διαφέρουν σε συγκεκριμένες θέσεις bits, έτσι ώστε να προκαλούνται ενδιάμεσες τιμές που έχουν διαφορές πάλι σε συγκεκριμένες θέσεις υψηλής πιθανότητας. Η συσσώρευση παρατηρήσεων μετά από ικανά μεγάλο αριθμό τέτοιων ζευγών εισόδων οδηγεί, στην αποκάλυψη ορισμένων bits του κλειδιού.

Από τα πιο πάνω γίνεται φανερή η σπουδαιότητα της σχεδίασης των βασικών δομών ενός block κρυπταλγόριθμου βασισμένου στην δομή Feistel και ιδιαίτερα των S- boxes του. Όσο μεγάλο μήκος κλειδιού και να προσδώσουμε στον κρυπταλγόριθμό μας, μόνο η προσεκτική ανάλυση της σχεδίασης του και των δομικών του στοιχείων μπορεί να μας πείσει ότι ο κρυπταλγόριθμος δεν υποκύπτει σε επιθέσεις που ακολουθούν συντομότερη οδό από το να δοκιμάσουν όλα τα τεράστια σε αριθμό ομολογουμένως, δυνατά κλειδιά (Feistel, 1973).

Και εδώ ερχόμαστε στον DES. Η αλήθεια είναι ότι οι πολλές αναλύσεις που έχει υποστεί ο DES και τα δομικά του στοιχεία έχουν αποκαλύψει ότι η παραμικρή μεταβλή των S-boxes του έχουν γραμμικές προσεγγίσεις αρκετά υψηλής πιθανότητας με αφορμή τα παραπάνω, τα τελευταία χρόνια έχουν αναπτυχθεί πολλές μεθοδολογίες κατασκευής «καλών» S-boxes, έτσι ώστε να έχουν συγκεκριμένες ιδιότητες που δυσκολεύουν την εφαρμογή της γραμμικής και της διαφορικής κρυπτανάλυσης (Biham, Shamir, 1993).

Φυσικά αν και τα S-boxes αποτελούν το βασικό δομικό λίθο ενός κρυπταλγορίθμου, δεν θα πρέπει να ξεχνάμε ότι υπάρχουν και άλλα πράγματα που πρέπει να προσεχθούν, όπως η συνάρτηση επανάληψης, η δρομολόγηση κλειδιού,

κλπ. Το σημαντικό είναι ότι γενικά είναι δύσκολο να μπορέσει να σχεδιάσει κανείς κάτι που, ιδανικά να είναι ανθεκτικό απέναντι σε όλες τις γνωστές επιθέσεις. Για παράδειγμα ακόμα και αν οι σχεδιαστές του DES είχαν επιχειρήσει να κάνουν τον κρυπταλγόριθμο τους ανθεκτικό και απέναντι στην γραμμική κρυπτανάλυση, πιθανότατα να μην το είχαν καταφέρει, καθώς οι ιδιότητες αντοχής απέναντι στην διαφορική και γραμμική κρυπτανάλυση μπορεί να είναι αντικρουόμενες για τα μεγέθη του DES και τα μεγέθη των S-boxes που χρησιμοποιήθηκαν (Coppersmith, 1992).

Τέλος θα αναφερθούμε στην επίθεση ωμής βίας με την χρήση υλικού. Δω δεν μπορούμε να πούμε τίποτα περισσότερο πέρα από ότι η μόνη άμυνα είναι το μεγάλο μήκος κλειδιού. Η τεχνολογία τρέχει με απίστευτους ρυθμούς. Η ταχύτητα των σημερινών επεξεργαστών έχει πλέον υπερβεί το 1 GHz, το οποίο αποτελεί ασύλληπτη ταχύτητα για τα δεδομένα της δεκαετίας του 70, όταν προτάθηκε ο DES. Και αν προσθέσουμε και την δυνατότητα διασύνδεσης πολλών από αυτούς τους επεξεργαστές, φτάνουμε σε δραματικές κρυπταναλυτικές επιθέσεις, όπως αυτή του Mike Weinerμε τους χιλιάδες ειδικά κατασκευασμένους απλούς επεξεργαστές και μάλιστα σε πολλαπλάσια επίπεδα ταχύτητας.

Όλα όσα εκθέσαμε παραπάνω οδηγούν στο συμπέρασμα ότι η σχεδίαση ενός κρυπταλγόριθμου είναι μια εξαιρετικά λεπτή διαδικασία που απαιτεί να ληφθούν υπόψη, πέρα από την καλή σχεδίαση, τα τρέχοντα και τα προβλεπόμενα οικονομικό-τεχνολογικά δεδομένα του χρονικού ορίζοντα, στον οποίο απαιτείται ο κρυπταλγόριθμος να μένει ασφαλής. Σήμερα υπάρχει μια όλο και αυξανόμενη, διεθνώς δραστηριότητα στον τομέα της σχεδίασης και υλοποίησης αλγορίθμων κρυπτογράφησης δεδομένων. Πιστεύουμε ότι η ολοένα και μεγαλύτερη εξάρτηση της σημερινής κοινωνίας από την ηλεκτρονική πληροφορία, την διαφύλαξη της και την διακίνηση της, καθιστά την ανάπτυξη εγχώριας τεχνογνωσίας στον τομέα αυτό αναπόσπαστο μέρος της μακροπρόθεσμης στρατηγικής βασικής έρευνας για κάθε χώρα, αν μη τι άλλο για να μπορεί τουλάχιστον να αντιμετωπιστεί πιθανή προσπάθεια επιβολής επικίνδυνης ή κακής ποιότητας έξωθεν τεχνογνωσίας (Coppersmith, 1992).

3.7. Κρυπτογραφικά Συστήματα

3.7.1.Mime

Το ηλεκτρονικό ταχυδρομείο, αρχικώς ήταν σχεδιασμένο ώστε να μην υποστηρίζει αποστολή αρχείων, παρα μόνο απλού κειμένου . Πολλές μέθοδοι αναπτύχθηκαν ανά τα χρόνια με σκοπό να αναπτυχθεί αυτή η τάση αποστολής αρχείων. Οι πρώτες από τις μεθόδους που εμφανίστηκαν κωδικοποιούσαν τα δεδομένα σε μορφή κειμένου και έτσι αυτά στέλνονταν μέσω του ηλεκτρονικού ταχυδρομείου. Το 1992 όμως η Internet Engineering Task Force (IEFT) επινόησε το Multipurpose Internet Extensions (mime) το οποίο είχε σαν σκοπό την ενοποίηση και τον συντονισμό όλων των προηγούμενων μεθόδων που είχαν αναπτυχθεί. Το mime δεν υποστηρίζει ένα και μοναδικό πρότυπο για την κωδικοποίηση των δεδομένων αλλά επιτρέπει στους χρήστες του να συνδυάσουν τις κωδικοποιήσεις που επιθυμούν αυτοί.

Το mime ωστόσο δεν παρέχει κάποιο είδος ασφαλείας. Για το λόγο αυτό επινοήθηκε το s/mime (secure mime), το οποίο, θα μπορούσαμε να πούμε ότι καλύπτει το κενό αυτό της ασφάλειας. Το s/mime χρησιμοποιεί μεθόδους ασύμμετρης κρυπτογραφίας κατά την μεταφορά των αρχείων. Έτσι όταν κάποιος θέλει να στείλει ένα μήνυμα χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει τα δεδομένα και τα αποστέλλει στον κατάλληλο εξυπηρετητή. Για να ανακτηθεί το αρχικό μήνυμα τα δεδομένα αποκρυπτογραφούνται στον e-mail server ή στον e-mail client.

Εν έτη 2013 δεν υπάρχουν πολλοί e-mail clients που να υποστηρίζουν αποκρυπτογραφήσαμε το σύστημα s/mime, αλλά σε περίπτωση που αυτή μπορεί να είναι εφικτή δύναται να προκύψουν διάφορα προβλήματα. Για παράδειγμα είναι δυνατόν μελλοντικά να υπάρξει η ανάγκη αλλαγής του ζεύγους των κλειδιών του. Στην περίπτωση αυτή προκύπτει ένα πρόβλημα το οποίο είναι το εξής: από την στιγμή που τα μηνύματα αποθηκεύονται στον e-mail server τα μηνύματα που έχουν κρυπτογραφηθεί με το παλιό κλειδί δεν θα είναι πλέον διαθέσιμα.

Αντίθετα κατά την αποκρυπτογράφηση στον email server, αυτός πρέπει να κατέχει όλα τα δημόσια κλειδιά και ιδιωτικά όλων των χρηστών και να αποκρυπτογραφεί όλα τα μηνύματά τους. Και σε αυτήν την περίπτωση προκύπτουν προβλήματα που έχουν να κάνουν από την μία με τον φόρτο εργασίας του mail server και από την άλλη με το γεγονός ότι αν κάποιος καταφέρει να αποκτήσει πρόσβαση σε αυτόν θα μπορεί να αποκτήσει το περιεχόμενο οποιουδήποτε e-mail και οποιουδήποτε χρήστη.

3.7.2.SSL – Secure Sockets Layer

Το πρωτόκολλο SSL (Secure Sockets Layer ή ασφαλές στρώμα υποδοχών) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε με σκοπό για να προσδώσει ασφάλεια στην διαδικασία της μετάδοσης ευαίσθητων δεδομένων στο διαδίκτυο, όπως είναι αυτά που μεταδίδονται κατά την εκτέλεση ηλεκτρονικών συναλλαγών. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL.

Το SSl υποστηρίζει πλήθος κρυπτογραφικών αλγορίθμων τους οποίους αναπτύξαμε σε προηγούμενα κεφάλαια και οι οποίοι είναι:

- DES - Data Encryption Standard, DSA - Digital Signature Algorithm,
- KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA,
- SHA-1 - Secure Hash Algorithm, SKIPJACK, Triple-DES.

3.7.3. TSL – Transport Layer Security

Η ασφάλεια στρώματος μεταφορών (TLS) ο οποίος αποτελεί προκάτοχο του πρωτοκόλλου SSL, είναι επίσης κρυπτογραφικό πρωτόκολλο που παρέχει ασφαλείς ανακοινώσεις σχετικά με το διαδίκτυο για θέματα όπως η πλοήγηση στον παγκόσμιο ιστό, το ηλεκτρονικό ταχυδρομείο, η αποστολή με φαξ Διαδικτύου, το στιγμιαίο μήνυμα και άλλες μεταφορές δεδομένων.

Υπάρχουν μικρές διαφορές μεταξύ της SSL και TLS, αλλά είναι ουσιαστικά οι ίδιες. Το πρωτόκολλο TLS επιτρέπει τις εφαρμογές για να επικοινωνήσει μέ ένα δίκτυο με σκοπό με τέτοιο τρόπο ώστε να αποτρέψει να κρυφακούσει κάποιος, να πειράξει, η ακόμα και να παραποιήσει μηνύματα. Το επόμενο επίπεδο ασφάλειας στο οποίο και οι δύο χρήστες της «συνομιλίας» είναι σίγουρες με ποιους επικοινωνούν είναι γνωστό ως αμοιβαία επικύρωση. Η αμοιβαία επικύρωση απαιτεί κρυπτογράφηση δημοσίου κλειδιού (PKI), την οποία περιγράψαμε σε προηγούμενο κεφάλαιο, στους πελάτες εκτός αν τα tls-PSK(pre-shared key) ή το ασφαλές μακρινό πρωτόκολλο κωδικού πρόσβασης (SRP-Secure Remote Password Protocol) χρησιμοποιούνται, τα οποία παρέχουν την ισχυρή αμοιβαία επικύρωση χωρίς να πρέπει να επεκταθεί ένα PKI.

Το TLS περιλαμβάνει τρεις βασικές φάσεις. Στην πρώτη φάση, ο client και ο server διαπραγματεύονται τις cipher ακολουθίες, που καθορίζουν οι ciphers που χρησιμοποιούνται, οι βασικοί αλγόριθμοι ανταλλαγής και επικύρωσης, καθώς επίσης και οι κώδικες επικύρωσης μηνυμάτων (MACs-message authentication codes). Οι βασικοί αλγόριθμοι ανταλλαγής και επικύρωσης είναι χαρακτηριστικά δημόσιοι βασικοί αλγόριθμοι, ή σε tls-PSK κλειδιά θα μπορούσαν να χρησιμοποιηθούν. Οι κώδικες επικύρωσης μηνυμάτων αποτελούνται από τις κρυπτογραφικές hash λειτουργίες χρησιμοποιώντας την κατασκευή HMAC(hash) για TLS, και μια μεταβλητή ψευδοτυχαίας λειτουργίας για τη SSL.

Τέλος οι αλγόριθμοι που χρησιμοποιούνται από τον TSL είναι οι παρακάτω ανάλογα και με την λειτουργία που εκτελούν.

- ⇒ Για ανταλλαγή κλειδιών: RSA, Diffie-Hellman, ECDH, SRP, PSK
- ⇒ Για πιστοποίηση: RSA, DSA, ECDSA
- ⇒ Συμμετρικοί Ciphers Αλγόριθμοι: RC4, Triple DES, AES, IDEA, DES
- ⇒ Αλγόριθμοι κατακερματισμού: MD2, MD4, MD5

3.7.4.SET – Secure Electronic Trnasactions

Το SET που στα ελληνικά αποδίδεται ως ασφαλείς ηλεκτρονικές συναλλαγές είναι ένα πρωτόκολλο εμπορικών συναλλαγών για την χρήση πιστωτικών καρτών σε ανοικτά δίκτυα. Αναπτύχθηκε από την MasterCard και την Visa σαν μια μέθοδος εξασφάλισης των συναλλαγών με τη χρήση καρτών διαμέσου του Internet.

Σε αντίθεση με το SSL που περιγράψαμε προηγουμένως που αποτελεί σύστημα κρυπτογραφίας γενικού σκοπού, το SET χρησιμοποιείται αποκλειστικά και μόνο για την διενέργεια μόνο χρεωστικών και πιστωτικών συναλλαγών καρτών μεταξύ εμπόρων και πελατών. Το SET παρέχει Πιστοποίηση, μη άρνηση αποδοχής, Εμπιστευτικότητα και Ακεραιότητα.

Όσο αφορά τον τρόπο λειτουργίας του το SET κάνει χρήση ενός ασφαλούς αλγόριθμου κατακερματισμού που παράγει ένα κατακερματισμό 160 δυαδικών ψηφίων. Για το ζευγάρι δημοσίου- ιδιωτικού κλειδιού χρησιμοποιεί τον αλγόριθμο RSA μήκους 1024 δυαδικών ψηφίων. Για την συμμετρική κρυπτογράφηση το SET χρησιμοποιεί σαν προεπιλογή τον αλγόριθμο DES μήκους 56 δυαδικών, αλλά παρόλα αυτά μπορεί να χρησιμοποιήσει μια ποικιλία διαφορετικών αλγόριθμων συμμετρικού
κλειδιού. Το SET χρησιμοποιεί ζευγάρια Ιδιωτικών- Δημοσίων κλειδιών και ψηφιακά πιστοποιητικά για να πιστοποιήσουν την ταυτότητα του κάθε συμβαλλόμενου και να τους επιτρέψει την εμπιστευτική επικοινωνία μεταξύ τους.

Το SET ακόμα κρυπτογραφεί πληροφορίες σχετικές με την παραγγελία με την χρήση ενός τυχαίου συμμετρικού κλειδιού συνόδου και τις «πακετάρει» σε ένα ψηφιακό φάκελο χρησιμοποιώντας το δημόσιο κλειδί του εμπόρου.

Κατ’ αυτό τον τρόπο οι πληροφορίες που αφορούν την πληρωμή της παραγγελίας κρυπτογραφούνται παρόμοια αλλά σε αυτήν την περίπτωση με το δημόσιο κλειδί της τράπεζας του εμπόρου. Το λογισμικό στην συνέχεια υπολογίζει από κοινού κατακερματισμό της παραγγελίας και των πληροφοριών πληρωμής και τον υπογράφει με το ιδιωτικό κλειδί του πελάτη. Με αυτόν τον τρόπο ο έμπορος και η τράπεζα του δεν μπορούν να έχουν πρόσβαση σε πληροφορίες που δεν πρέπει, και

παράλληλα επικυρώνεται η ακεραιότητα του μηνύματος. Πρέπει να σημειωθεί ότι με την χρήση του SET η τράπεζα που εξέδωσε πιστωτική κάρτα συν τοις άλλοις αποκρυπτογραφεί τις πληροφορίες πληρωμής του πελάτη, τον πιστοποιεί και ελέγχει την εγκυρότητα του αριθμού της πιστωτικής κάρτας. Ο λόγος που κάνει το SET καταλληλότερο από το SSL είναι ότι με το SET γίνεται έλεγχος της εγκυρότητας της πιστωτικής κάρτας και ότι ο έμπορος δεν έχει πρόσβαση στον αριθμό της ενώ ταυτόχρονα βεβαιώνεται για την εγκυρότητά της. Επίσης το SET διαθέτει δύο ζεύγη κλειδιά για συγκεκριμένα μέρη του πρωτοκόλλου, σε αντίθεση με το SSL το οποίο χρησιμοποιεί το ίδιο ζεύγος κλειδιών τόσο για την κρυπτογράφηση όσο και για τις ψηφιακές υπογραφές. Συγκεκριμένα στο SET, το ψηφιακό κατάστημα, η τράπεζα του καταστήματος και η τράπεζα έκδοσης της πιστωτικής κάρτας κατέχουν δύο ζεύγη κλειδιών, το ένα χρησιμοποιείται για την κρυπτογράφηση και το άλλο για τις ψηφιακές υπογραφές.

3.7.5. Secure HyperText Transfer Protocol (HTTPS)

Το ασφαλές πρωτόκολλο HTTPS χρησιμοποιείται στην επιστήμη των υπολογιστών προκειμένου να πιστοποιήσει μια ασφαλή http σύνδεση. Ένας σύνδεσμος (URL) στο internet ο οποίος αρχίζει με τους χαρακτήρες https δηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το σύστημα αυτό αρχικώς αναπτύχθηκε από την Netscape Communications Corporation με σκοπό να χρησιμοποιηθεί σε ιστοτόπους όπου η διαδικασία της αυθεντικοποίησης των χρηστών και η κρυπτογραφημένη επικοινωνία ήταν ενέργειες ζωτικής σημασίας.

3. 7.6. Domain Name System Security (DNS)

Το DNS σχεδιάστηκε πολύ πριν εμφανιστούν τα πρώτα προβλήματα ασφαλείας στο διαδίκτυο, και όταν λίγοι είχαν προβλέψει για αυτά. Λόγω του ότι αποτελεί μια υπηρεσία βασιζόμενη στο πρωτόκολλο UDP ανακύπτουν διάφορα

προβλήματα ασφαλείας. Σε αντίθεση με το TCP το UDP δεν έχει κάποιο μηχανισμό ώστε να πιστοποιούνται οι αποστολείς των πακέτων που λαμβάνονται. Έτσι το UDP και κατά συνέπεια το DNS μπορεί να επιτρέψει την εξαπάτηση ως προς τον αποστολές κάθε πακέτου, κάτι που μπορεί να ξεκινήσει μια σειρά επιθέσεων ασφαλείας.

Σαν απάντηση στα παραπάνω προβλήματα του DNS αναπτύχθηκε ένα νέο ασφαλές πρωτόκολλο, το DNSSEC, το οποίο προσπαθεί με την χρήση ενός διανομέα δημοσίων κλειδιών να εμποδίσει την εξαπάτηση, ως προς τον αποστολέα, των πακέτων και να εξασφαλίσει ακεραιότητα των δεδομένων.

3. 7.7. Internet Protocol Security (IP)

Η ασφάλεια πρωτοκόλλου Διαδικτύου αποτελεί μια ακολουθία πρωτοκόλλων για την εξασφάλιση και ορθή διεξαγωγή των επικοινωνιών πρωτοκόλλου Διαδικτύου (IP)με την επικύρωση ή/και την κρυπτογράφηση κάθε πακέτου IP σε ένα ρεύμα στοιχείων. Το IPsec περιλαμβάνει ακόμα τα πρωτόκολλα για την κρυπτογραφική βασική καθιέρωση. Η υπάρχουσα έκδοση του IP πρωτοκόλλου είναι η IPv4 και η οποία φαίνεται να έχει μεγάλη λειτουργικότητα στις μέρες μας. Παρ' όλα αυτά δεν παύουν να προκύπτουν διάφορα προβλήματα από την χρησιμοποίησή του.

Έτσι το Internet Engineering Task Force (IEFT) ίδρυσε το IP Security Protocol Working Group το οποίο στην συνέχεια ανέπτυξε το IPsec. Το IPsec δεν είναι από μόνο του ένα πρωτόκολλο αλλά μια ομάδα πρωτοκόλλων με σκοπό την εξασφάλιση της σωστής χρήσης του πρωτοκόλλου IP. Αν και αρχικά το IPsec προοριζόταν για το IPv6 μπορεί να χρησιμοποιηθεί και πάνω από το πρωτόκολλο IPv4.Τα πρωτόκολλα IPsec λειτουργούν στο στρώμα δικτύων, στρώμα 3 του προτύπου της OSI. Άλλα πρωτόκολλα ασφάλειας Διαδικτύου σε διαδεδομένη χρήση, όπως η SSL,TLS και SSH, λειτουργούν από το στρώμα μεταφορών επάνω.

Αυτό καθιστά το IPsec πιο εύκαμπτο, δεδομένου ότι μπορεί να χρησιμοποιηθεί για την προστασία του στρώματος 4 πρωτόκολλα, και συμπεριλαμβανομένου του TCP και UDP, τα πιο συνηθέστερα χρησιμοποιημένα πρωτόκολλα στρώματος μεταφορών. Το IPsec έχει ένα πλεονέκτημα πέρα από τη SSL και άλλες μεθόδους που αναπτύσσουν δραστηριότητες στα υψηλότερα στρώματα: μια εφαρμογή δεν πρέπει να έχει ως σκοπό να χρησιμοποιήσει IPsec, ενώ η δυνατότητα να χρησιμοποιηθεί η SSL ή ένα άλλο πρωτόκολλο υψηλός-στρώματος πρέπει να ενσωματωθεί στο σχέδιο μιας εφαρμογής. Το IPsec είναι ένα πλαίσιο των ανοιχτών προτύπων που παρέχει την εμπιστευτικότητα στοιχείων, την ακεραιότητα στοιχείων, και την επικύρωση στοιχείων μεταξύ των συμμετεχόντων. Το IPsec παρέχει αυτές τις υπηρεσίες ασφάλειας στο στρώμα IP χρησιμοποιεί IKE (Internet Key Exchange) για να χειριστεί τη διαπραγμάτευση των πρωτοκόλλων και των αλγορίθμων βασισμένων στην τοπική πολιτική και για να παραγάγει τα κλειδιά κρυπτογράφησης και επικύρωσης που χρησιμοποιούνται από IPsec. Το IPSec μπορεί να χρησιμοποιηθεί για να προστατεύσει μια ή περισσότερες ροές στοιχείων μεταξύ ενός ζευγαριού των οικοδεσποτών, μεταξύ ενός ζευγαριού των πυλών ασφάλειας, ή μεταξύ μιας πύλης ασφάλειας και ενός οικοδεσπότη.

Συμπεράσματα

Οι δικτυακές συναλλαγές δεν θα μπορέσουν ποτέ να είναι 100% ασφαλής. Επιτήδειοι θα υπάρχουν πάντα, αλλά και η κρυπτογράφηση και τα συστήματα ασφαλείας θα αναπτύσσονται συνεχώς. Μολονότι θεωρείται ότι οι συναλλαγές μέσω πιστωτικής κάρτας στο διαδίκτυο δεν είναι ασφαλείς, οι ειδικοί υποστηρίζουν ότι το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές συναλλαγές εν γένει είναι ασφαλέστερες από τις αγορές με πιστωτικές κάρτες σε «φυσικά» καταστήματα. Κάθε φορά που ο πελάτης πληρώνει με πιστωτική κάρτα σε ένα κατάστημα ή εστιατόριο και κάθε φορά που πετά την απόδειξη μιας πιστωτικής κάρτας γίνεται περισσότερο ευάλωτος στην απάτη.

Η ποσότητα της γνώσης γύρω από τα τεχνικά θέματα του διαδικτύου είναι σταθερή, ωστόσο το ίδιο το διαδίκτυο συνεχίζει να διογκώνεται, με αποτέλεσμα να αυξάνονται καθημερινά και οι κίνδυνοι των συναλλαγών. Με άλλα λόγια, συνεχίζουν να υπάρχουν πολλοί χρήστες του διαδικτύου με λίγη ή ακόμα και ανύπαρκτη γνώση για τους δυνητικούς κινδύνους που διατρέχουν, πόσο μάλλον για τα διαθέσιμα μέτρα προστασίας. Την ίδια στιγμή, το διαδίκτυο με τον μεγάλο όγκο των δικτυακών τόπων που περιέχει, γίνεται ευάλωτο στο «κράκινγκ» (cracking).μάλιστα τα κακόβουλα αυτά προγράμματα - εργαλεία είναι με τέτοιον τρόπο σχεδιασμένα, ώστε να μπορούν να χρησιμοποιηθούν ακόμα και από χρήστες με λίγες γνώσεις.

Από την άλλη μεριά, η κρυπτογράφηση αποτελεί τον κυριότερο μηχανισμό που προστατεύει τόσο τα στοιχεία όσο και την ομαλή και ασφαλή διεξαγωγή μίας ηλεκτρονικής συναλλαγής, χρησιμοποιείται για να διασφαλίσει την ιδιωτικότητα (privacy), την ακεραιότητα (integrity) και την εμπιστευτικότητα (confidentiality) των επιχειρηματικών συναλλαγών και μηνυμάτων και αποτελεί τη βάση για αρκετά από τα on—line συστήματα πληρωμών, όπως πχ το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές. Η κρυπτογραφία χρησιμοποιείται ευρέως σήμερα ως ένα πολύ χρήσιμο εργαλείο στην ασφάλεια της μεταφοράς πληροφοριών, προκειμένου

να προστατευτούν προσωπικά δεδομένα ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους.

Βιβλιογραφία

ΕΛΛΗΝΙΚΗ

[1] Γκιούρδας Μ. (2010), Ηλεκτρονικό Εμπόριο 2010, Εκδ. Γκιούρδας, Αθήνα

[2] Ιγγλεζάκης Ι.(2008), Δίκαιο της πληροφορικής, 2η έκδοση, Εκδ. Σάκκουλα, Αθήνα

[3] Καραδημητρίου Κ. (2008), Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο Εκδόσεις Σάκκουλα Α.Ε.

[4] Καρανικόλας Ν. (2006), Τεχνολογίες Διαδικτύου και Ηλεκτρονικό Εμπόριο, Εκδόσεις Νέων Τεχνολογιών, Αθήνα

[5] Κόκοτος Χ. (2009), Πρόβλεψη ενεργειών και υποστήριξη λήψης αποφάσεων στο ηλεκτρονικό επιχειρείν, Εκδόσεις Σταμούλη

[6] Πασχόπουλος Α. (2006), Ηλεκτρονικό Εμπόριο – Επιχειρηματική Στρατηγική καιμάρκετινγκ στο διαδίκτυο, Εκδ. Κλειδάριθμος, Αθήνα

[7] Πασχόπουλος Α., Σκαλτσας Π. (2000), Ηλεκτρονικό Εμπόριο, Εκδ. Κλειδάριθμος, Αθήνα

[8] Πολλάλης Γ., Γιαννακόπουλος Δ., (2007), Ηλεκτρονικό Επιχειρείν, Εκδ. Σταμούλη, Αθήνα

[9] Πομπόρτσης Α. (2002), Εισαγωγή στο Ηλεκτρονικό Εμπόριο, Εκδ. Τζιόλα, Αθήνα

[10] Σκιαδάς Χ. (2001), Γενικές Αρχέςμάρκετινγκ και Ηλεκτρονικού Εμπορίου, Εκδ. Παπασωτηρίου, Αθήνα

ΞΕΝΗ

[1] Biham E. Shamir A.,(1993), Differential cryptanalysis of the Data Encryption Standard, Springer – Verlag.

[1] Chaffey D. (2008), Ηλεκτρονικό Επιχειρείν και Ηλεκτρονικό Εμπόριο, Εκδ. Κλειδάριθμος, Αθήνα

[2] Coppersmith D.(1992), The data encryption standard and its strength against attacks, IBM Journal and Development

[3] Feistel H. (1973), Cryptography and Computer Privacy, Scientific American

[4] Gamal T. (1985), A public key cryptosystem and a signature scheme based on discrete Logarithms, IEEE Transactions on Information Theory, 1985

[5] Ince D. (2007), Κατανεμημένες Εφαρμογές και Ηλεκτρονικό Εμπόριο, Εκδόσεις Πανεπιστημίου μακεδονίας

[6] Laudon K., Traver C. (2011), Ηλεκτρονικό Εμπόριο, 7η έκδοση, Εκδ. Παπασωτηρίου, Αθήνα

[7] Shannon C.E (1949), Communication theory of secrecy systems, Bell System Technical Journal