Τ.Ε.Ι ΠΑΤΡΑΣ

ΤΕΧΝΟΛΟΓΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ: ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΙΟ, ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ-ΕΜΠΟΡΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΧΟΝΔΡΑΚΗΣ ΣΤΕΛΙΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΒΛΑΧΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ

ΠΑΤΡΑ 19 ΣΕΠΤΕΜΒΡΙΟΥ 2008

ΠΕΡΙΕΧΟΜΕΝΑ **ΣΕΛ.**

ΠΡΟΛΟΓΟΣ

Είναι κοινή παραδοχή ότι αν κάτι χαρακτηρίζει την εποχή την οποία ζούμε, αυτό είναι η έκρηξη τεχνολογίας και γνώσεων. «Έκρηξη» με ισχυρή τόσο την οριζόντια όσο και την κάθετη συνιστώσα: δεν μαζεύουμε απλά σαν κοινωνία περισσότερες γνώσεις, αλλά αυτές είναι τώρα σε πολύ μεγαλύτερο βαθμό διαθέσιμες, τόσο εν σχέση με την μερίδα του πληθυσμού η οποία έχει πρόσβαση στις πληροφορίες αυτές, όσο και ως προς την ταχύτητα διάδοσης της είδησης-γνώσης. Πολλοί είναι όμως οι παράγοντες που έχουν συμβάλλει στο «επίτευγμα» αυτό. Αν όμως θα πρέπει να αναφέρουμε κάποιον, αυτός θα ήταν τα τεχνικά μέσα αποθήκευσης και διάδοσης πληροφοριών, και ιδίως το διαδίκτυο.

Στις μέρες μας το διαδίκτυο (internet) αποτελεί την θεμέλια βάση για την παγκοσμίου κλίμακας επικοινωνία και πρόσβαση απομακρυσμένων πόρων, που απολαμβάνουν εκατομμύρια χρήστες των ηλεκτρονικών υπολογιστών. Αξίζει να επισημάνουμε ότι το διαδίκτυο είναι το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων, που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη .

Καθώς η τεχνολογία ανοίγει νέες λεωφόρους για τις ηλεκτρονικές επιχειρήσεις, όλο και περισσότερες εταιρίες χρησιμοποιούν το διαδίκτυο σαν την βασική μέθοδο επικοινωνίας και εμπορικών συναλλαγών τους εξαιτίας της άνεσης που υπάρχει σε ταχύτητα και πρόσβαση(*Γκλαβά, 2001*).Ωστόσο, με τις εξελίξεις της τεχνολογίας προκύπτει μια ανάγκη ασφάλειας, δηλαδή να

προστατεύονται τα ευαίσθητα δεδομένα των ηλέκτρονικων συναλλαγών, είτε αυτά προέρχονται από επικοινωνία, είτε από εμπορικές συναλλαγές

Η ανάγκη λοιπόν για ασφάλεια στο διαδίκτυο είναι ένα ζήτημα που έχει απασχολήσει και απασχολεί τον καθένα μας, αυτό με οδήγησε στο να ασχοληθώ με το εξής θέμα «Ασφάλεια ηλεκτρονικών συναλλαγών, μέθοδοι κρυπτογράφησης και ηλεκτρονικό εμπόριο» . Έτσι λοιπόν θα προσεγγίσουμε διεξοδικά την ανάγκη ύπαρξης ασφάλειας στις ηλεκτρονικές συναλλαγές, αναφέροντας αρχικά τους κινδύνους που ελλοχεύουν όταν συναλλασσόμαστε διαδικτυακά και στην συνέχεια θα προβάλλουμε λύσεις που διασφαλίζουν τις ηλεκτρονικές εμπορικές συναλλαγές. Τέλος καταλήγουμε σε κάποια συμπεράσματα για το πόσο ασφαλής είναι τελικά οι ηλεκτρονικές συναλλαγές.

ΕΙΣΑΓΩΓΗ

Η ευρεία διάδοση του διαδικτύου, ως ένα παγκόσμιο μέσο μεταφοράς και ανταλλαγής πληροφοριών επιτρέπει στους χρήστες του, καθώς και στις σύγχρονες επιχειρήσεις τη χρησιμοποίησή του για άμεση επικοινωνία, είτε με σκοπό την κοινωνική επαφή, είτε με συνεργάτες και προμηθευτές με σκοπό την διεκπεραίωση εμπορικών συναλλαγών. Είναι αντιληπτό ότι σ’ αυτήν την ραγδαία ανάπτυξή του οφείλονται διάφορα προβλήματα ασφάλειας πληροφοριών, που αφορούν την εξασφάλιση εμπιστευτικότητας- μυστικότητας- ακεραιότητας και διαθεσιμότητας των διακινούμενων δεδομένων. Συγκεκριμένα για αν γίνει αντιληπτή η φύση των προβλημάτων, αναπτύσσουμε τους παραπάνω όρους:

- **Εμπιστευτικότητα** (confidentiality): Είναι έννοια στενά συνδεδεμένη με την ιδιωτικότητα (privacy) και την μυστικότητα(secrecy). Αναφέρεται

στην μη αποκάλυψη των ευαίσθητων πληροφοριών σε χρήστες που δεν έχουν την κατάλληλη εξουσιοδότηση.

- **Ακεραιότητα** (integrity): Αφορά την δυνατότητα τροποποιήσεων (προσθήκες, διαγραφές και μεταβολές) των πληροφοριών. Το σύστημα θα πρέπει να επιτρέπει τέτοιες ενέργειες μόνο σε κατάλληλα εξουσιοδοτημένους χρήστες. Με αυτόν τον τρόπο διαφυλάσσεται η ακρίβεια και η πληρότητα των διακινούμενων δεδομένων.

- **Διαθεσιμότητα** (availability): Αναφέρεται στην δυνατότητα άμεσης πρόσβασης στις πληροφορίες, στις υπηρεσίες και γενικότερα σε όλους τους πόρους της πληροφορικής τεχνολογίας όταν ζητούνται, χωρίς αδικαιολόγητες καθυστερήσεις.

- ***Μη απάρνηση*:** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

- **Πιστοποίηση**: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Κατανοούμε λοιπόν ότι κάθε μεταφορά πληροφορίας, θα πρέπει σαφώς να είναι ασφαλής και αξιόπιστη, διαφορετικά οι χρήστες του διαδικτύου δεν θα έχουν την πεποίθηση ότι η επικοινωνία τους και τα δεδομένα που ανταλλάσσουν είναι ασφαλή από μη εξουσιοδοτημένη πρόσβαση ή παραποίηση, γεγονός που αποτελεί ανασταλτικό παράγοντα στο να χρησιμοποιούν το διαδίκτυο ευρύτερα ως μέσο διακίνησης σημαντικών πληροφοριών τους(αριθμοί πιστωτικών καρτών)(*Γεωργόπουλος 2001*)

ΚΕΦΑΛΑΙΟ 1^{Ο} ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΑΔΥΚΤΙΟ

Γενικά

Στην γενική του έννοια, **διαδίκτυο** είναι ένα δίκτυο ηλεκτρονικών υπολογιστών που (δια)συνδέει άλλα δίκτυα. Ο αντίστοιχος αγγλικός όρος *internet* προκύπτει από τη σύνθεση λέξεων *inter-network.*

1.1 Δίκτυα υπολογιστών

Είναι τα συστήματα στα οποία υπάρχει ένας μικρός ή μεγάλος αριθμός από ξεχωριστούς αλλά συνδεμένους μεταξύ τους υπολογιστές. Δύο υπολογιστές θεωρούνται συνδεμένοι σε δίκτυο, όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες. Ο αρχικός στόχος δημιουργίας των δικτύων ήταν η κοινή χρήση διαφόρων συσκευών (σκληροί δίσκοι, εκτυπωτές κλπ.) από όλους τους χρήστες του δικτύου.

Τα δίκτυα υπολογιστών χωρίζονται σε δύο βασικές κατηγορίες: Στα **Τοπικά Δίκτυα (LAN, Local Area Networks)** και στα **Δίκτυα Ευρείας Περιοχής (WAN, Wide Area Networks).** Για παράδειγμα, ένα δίκτυο υπολογιστών, στο ίδιο κτίριο, θεωρείται Τοπικό (LAN) ενώ ένα δίκτυο που χρησιμοποιείται απ' τα υποκαταστήματα μιας Τράπεζας σ' όλη τη χώρα, θεωρείται Δίκτυο Ευρείας Περιοχής (WAN).

1.1.1 Τοπικά δίκτυα

Οι υπολογιστές που είναι συνδεμένοι σε ένα τοπικό δίκτυο, ονομάζονται **σταθμοί εργασίας** και μπορούν να μοιράζονται πληροφορίες και πόρους του συστήματος. Δηλαδή, κάθε σταθμός εργασίας, μπορεί να βλέπει τους σκληρούς

δίσκους των υπόλοιπων υπολογιστών του δικτύου, σαν να είναι δικοί του δίσκοι. Μπορεί επίσης να κάνει εκτυπώσεις σε εκτυπωτή που είναι συνδεμένος σε κάποιον άλλο υπολογιστή. Επίσης μπορεί να μοιράζεται ένα modem με άλλους υπολογιστές του δικτύου. Τέλος, μπορεί να μοιράζεται προγράμματα, αρχεία δεδομένων κ.ά. με άλλους χρήστες. Με τον τρόπο αυτό, έχουμε εξοικονόμηση του κόστους, αφού ένας εκτυπωτής, ένα modem ή ένα πακέτο λογισμικού μπορεί να εξυπηρετεί περισσότερους από έναν υπολογιστές. Επίσης, μέσω του δικτύου, οι χρήστες μπορούν να επικοινωνούν μεταξύ τους και να ανταλλάσσουν μηνύματα, χωρίς να χρειάζεται να μετακινηθούν από το γραφείο τους.

1.1.1.1 Τοπολογία Τοπικών Δικτύων

Με τον όρο "**τοπολογία**" εννοούμε τον τρόπο με τον οποίο δύο ή περισσότεροι υπολογιστές (σταθμοί εργασίας) συνδέονται μεταξύ τους σε ένα τοπικό δίκτυο.

Τα κυριότερα είδη τοπολογίας είναι:

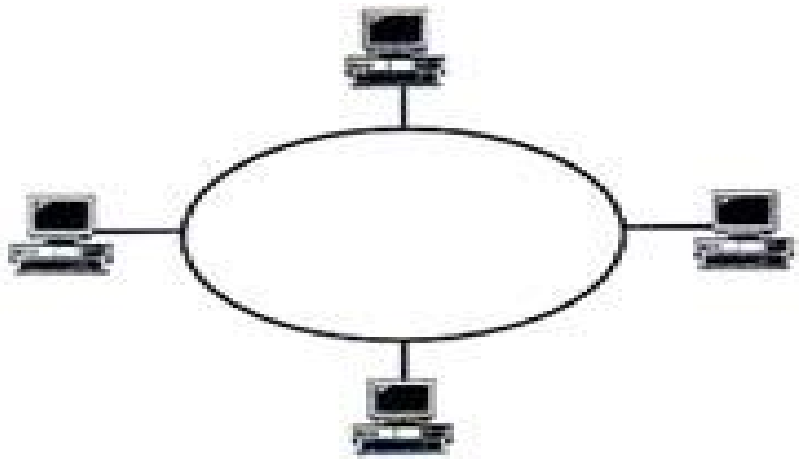
I. **Αστέρας(star)**

Οι υπολογιστές διατάσσονται σε μορφή αστεριού, γύρω από έναν κεντρικό υπολογιστή, ο οποίος ονομάζεται **διακομιστής (server)**. Ο διακομιστής ελέγχει την επικοινωνία μεταξύ των σταθμών και είναι υπεύθυνος για την παροχή των υπηρεσιών του δικτύου. Αν δημιουργηθεί πρόβλημα σ' ένα σταθμό εργασίας, το υπόλοιπο δίκτυο λειτουργεί κανονικά. Βλάβη όμως του διακομιστή, προκαλεί διακοπή της λειτουργίας όλου του δικτύου. (Στην περίπτωση αυτή, οι σταθμοί μπορούν να λειτουργήσουν σαν ανεξάρτητοι υπολογιστές και δεν μπορούν να κάνουν χρήση των υπηρεσιών του δικτύου). (Σχήμα 1.1)

Σχ. 1.1 Αστέρας

II. Δακτύλιος (ring)

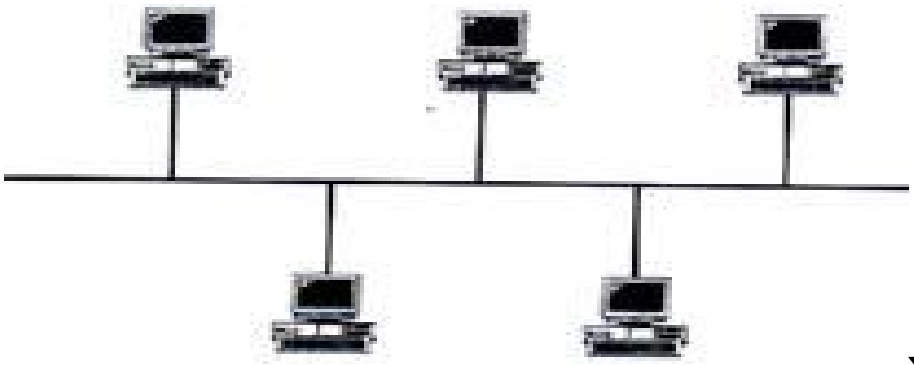
Οι υπολογιστές ενώνονται σε ένα καλώδιο και σχηματίζουν κλειστό δακτύλιο. Οι πληροφορίες που μεταδίδονται μέσω του καλωδίου, ακολουθούν πορεία μιας κατεύθυνσης, περνώντας διαδοχικά απ' όλους τους σταθμούς. Βλάβη σ' έναν σταθμό, προκαλεί διακοπή της λειτουργίας του δικτύου. (Σχήμα 1.2)



Σχ. 1.2 Δακτύλιος

III. Δίαυλος (bus)

Οι υπολογιστές ενώνονται μεταξύ τους σε σειρά, μέσω ενός και μόνο καλωδίου. Αν δημιουργηθεί πρόβλημα στο κεντρικό καλώδιο, τότε όλο το δίκτυο δεν μπορεί να λειτουργήσει. Το μικρό κόστος και η ευκολία εγκατάστασης καθιέρωσαν την τοπολογία αυτή στα μικρά δίκτυα. (Σχήμα 1.3)



Σχ. 1.3

1.1.2 Ευρεία δίκτυα

Τα δίκτυα ευρείας περιοχής χρησιμοποιούνται για να καλύψουν τις ανάγκες μεγάλων οργανισμών, πανεπιστημίων κλπ., οι οποίοι διαθέτουν υπολογιστές σε διαφορετικά κτίρια στην ίδια ή σε διαφορετικές πόλεις. Χαρακτηριστικό των δικτύων αυτών είναι ότι για τη μετάδοση των πληροφοριών από τη μια περιοχή στην άλλη, χρησιμοποιούν τα τηλεπικοινωνιακά δίκτυα (τηλεφωνικές γραμμές).

1.2 Τι είναι διαδίκτυο

Η σύνδεση τοπικών δικτύων μεταξύ τους αλλά και με δίκτυα ευρείας περιοχής, έτσι ώστε να είναι δυνατή η επικοινωνία μεταξύ τους, δημιουργεί ένα **διαδίκτυο**. Οι υπολογιστές που είναι συνδεμένοι σ' ένα διαδίκτυο, δεν έχουν όλοι το ίδιο λειτουργικό σύστημα. Επομένως, έπρεπε να βρεθεί ένας τρόπος ώστε οι υπολογιστές αυτοί να μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες. Η μέθοδος που βρέθηκε είναι γνωστή ως πρωτόκολλο IP (Internet Protocol). Έτσι, κάθε υπολογιστής ο οποίος διαθέτει το κατάλληλο λογισμικό για την υποστήριξη αυτού του πρωτοκόλλου, μπορεί να επικοινωνεί με οποιονδήποτε άλλο υπολογιστή που υποστηρίζει το πρωτόκολλο IP. Η εξέλιξη του πρωτοκόλλου IP είναι το **πρωτόκολλο TCP/IP** . Το IP στέλνει τα μικρά πακέτα δεδομένων, αποφασίζοντας για το δρομολόγιο το οποίο θα ακολουθήσουν. Κάθε πακέτο μπορεί να ακολουθήσει διαφορετικό δρόμο. Το **Internet** είναι ένα **διαδίκτυο** το οποίο ενώνει περισσότερους από 100 εκατομμύρια υπολογιστές σ' όλο τον κόσμο. Μια εταιρία η οποία διαθέτει την κατάλληλη υποδομή και μπορεί να μας προσφέρει τις κατάλληλες υπηρεσίες για να συνδεθούμε στο Internet, ονομάζεται **Παροχέας Υπηρεσιών Internet** (**ISP** = Internet Services Provider).

1.2.1. Ιστορία του Internet

Τα θεμέλια του Διαδικτύου τα έθεσε ο Βάνεβαρ Μπους (Vannevar Bush) όταν στο κείμενό του "As We May Think" αναφέρθηκε σε ένα "γαλαξιακό δίκτυο" συνδεδεμένων υπολογιστών. Ο πυρήνας του Διαδικτύου ξεκίνησε το 1969 με την ονομασία ARPANET στην Υπηρεσία Προηγμένων Αμυντικών Ερευνών (Defense Advanced Research Projects Agency, *DARPA*) του υπουργείου Άμυνας των ΗΠΑ. Η αρχική έρευνα που συνέβαλε στο ARPANET περιελάμβανε εργασίες στα αποκεντρωμένα δίκτυα, τη Θεωρία ουρών (queueing theory) και την ανταλλαγή πακέτων packet switching. Στις 11

Ιανουαρίου 1983 το ARPANET άλλαξε το βασικό του δικτυακό πρωτόκολλο επικοινωνίας από το NCP στο **TCP/IP**, ξεκινώντας έτσι το Διαδίκτυο όπως το γνωρίζουμε σήμερα. Ένα σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο έχτισε την πρώτη Διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet , το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet. Ωστόσο, η τεράστια ανάπτυξη του Διαδικτύου επήλθε όταν ο Σύμβουλος του CERN Τιμ Μπέρνερς- Λι δημιούργησε τις υποδομές για την υπηρεσία του Παγκόσμιου Ιστού. Στη δεκαετία του 1990 το Διαδίκτυο γνώρισε τρομακτική ανάπτυξη, απορροφώντας επιτυχώς την πλειοψηφία των παλιότερων δικτύων υπολογιστών. (*Σακλαμπανάκης 1995*)

1.2.2 Το Διαδίκτυο σήμερα

Το Διαδίκτυο συγκροτείται από αμφί- ή πολύπλευρα εμπορικά συμβόλαια (π.χ. ομότιμες συμφωνίες) και από τεχνικές προδιαγραφές ή πρωτόκολλα που περιγράφουν την ανταλλαγή δεδομένων στο δίκτυο. **Πρωτόκολλο επικοινωνίας** ορίζουμε ένα σύνολο κανόνων που είναι συμφωνημένοι και από τα δυο επικοινωνούντα μέρη και που εξυπηρετούν τη μεταξύ τους ανταλλαγή πληροφοριών. Τα πρωτόκολλα αυτά μορφοποιούνται με συζητήσεις μέσα στο Internet Engineering Task Force (IETF) και τις ομάδες εργασίας του, οι οποίες είναι ανοιχτές για δημόσια συμμετοχή και κριτική. Αυτές οι επιτροπές παράγουν κείμενα που είναι γνωστά ως Αιτήματα για Σχολιασμό (ΑΓΣ). Ορισμένα ΑΓΣ εγείρονται από το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου (IAB). Μερικά από τα πιο γνωστά διαδικτυακά πρωτόκολλα είναι το IP, TCP, το UDP, το DNS, το PPP, το SLIP, το ICMP, το POP3, IMAP, το SMTP, το HTTP, το HTTPS, το SSH, το Telnet, το FTP, το LDAP και το SSL.

1.2.1.1Το πρωτόκολα **TCP/IP, UDP, DNS, ICMP, POP3 & IMAP, HTTP**

I. Το πρωτόκολλο **TCP/IP**

Το **TCP** ***(Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς)*** είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP Protocol *(πρωτόκολλο IP)*. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) Telnet (port 23), το FTP και πιο σημαντικό το HTTP (port 80).

II. Το πρωτόκολλο **UDP**

Το πρωτόκολλο **User Datagram Protocol (UDP)** είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι **Universal Datagram Protocol**. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών. Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Αντιθέτως, το πρωτόκολλο

TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία. Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές. Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου.

III. Το πρωτόκολλο **DNS**

Το **Domain Name System** ή **DNS** (Σύστημα Ονομάτων Τομέα) είναι ένα σύστημα με το οποίο αντιστοιχίζονται οι διευθύνσεις IP σε ονόματα τομέων

(Domain Names). Τα ονόματα τομέων όπως και οι διευθύνσεις IP που αναπαριστούν είναι μοναδικά, έχουν μια ιεραρχία και διαβάζονται από αριστερά προς τα δεξιά. Η σχέση μεταξύ ενός ονόματος και της διεύθυνσης IP δεν είναι 1 προς 1. Δηλαδή σε ένα όνομα μπορούν να αντιστοιχούν πολλές IP διευθύνσεις. Για παράδειγμα η διεύθυνση www.google.gr αντιστοιχεί σε τρεις IP διευθύνσεις, την 66.102.9.99 την 66.102.9.104 και την 66.102.9.147 . Σε αυτή την περίπτωση έχουμε τρεις εξυπηρετητές που λειτουργούν ταυτόχρονα εκτελώντας την ίδια δουλειά αλλά μοιράζονται τον φόρτο εργασίας δια τρία. Σε αυτή την περίπτωση ο διακομιστής DNS εκτελεί εξισορρόπηση φορτίου μεταξύ των τριών άλλων διακομιστών. Το σύστημα DNS επιτρέπει την ανεύρεση ενός διακομιστή (server) με βάση το όνομα του. Ο διακομιστής μπορεί να υποστηρίζει ένα αριθμό από υπηρεσίες όπως http, ftp, smtp κλπ δίνοντας μας τη δυνατότητα να συνδεθούμε σε μια ιστοσελίδα(http), σε μια αποθήκη αρχείων(ftp), η να πάρουμε το mail μας(smtp). Έτσι είναι ευκολότερο να θυμόμαστε την ιστοσελίδα www.google.gr παρά τη διεύθυνση 66.102.9.99

IV. Το πρωτόκολλο **ICMP**

Το πρωτόκολλο **Internet Control Message Protocol (ICMP)** είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο. Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί το εργαλείο ping, το οποίο στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο

υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.

V. Το πρωτόκολλο **POP3 & IMAP**

Το POP3 αποτελεί εξέλιξη των προηγούμενων μορφών του πρωτοκόλλου, τα οποία ονομαζόταν ανεπίσημα POP1 και POP2. Ο όρος **Post Office Protocol** είναι πλέον συνώνυμος με το POP3, καθώς οι προηγούμενες μορφές του πρωτοκόλλου έχουν πλέον καταργηθεί στην πράξη.Το POP3 είναι σχεδιασμένο με τέτοιον τρόπο ούτως ώστε να επιτρέπει στους χρήστες του διαδικτύου που έχουν προσωρινές συνδέσεις (πχ dial-up) να παραλαμβάνουν την ηλεκτρονική τους αλληλογραφία, να την αποθηκεύουν στον τοπικό σκληρό δίσκο και στην συνέχεια να την διαβάζουν χωρίς να χρειάζεται να παραμένουν συνδεδεμένοι στο διαδίκτυο. Παρόλο που υπάρχει η δυνατότητα τα μηνύματα να παραμείνουν στον server ηλεκτρονικού ταχυδρομείου, οι περισσότερες εφαρμογές POP3 συνδέονται με τον server, λαμβάνουν όλα τα ηλεκτρονικά μηνύματα, τα αποθηκεύουν στον υπολογιστή του χρήστη, τα σβήνουν από τον server και αποσυνδέονται. Σε αντίθεση με το POP3, το πρωτόκολλο **Internet Message Access Protocol (IMAP)** που εμφανίστηκε αργότερα υποστηρίζει τόσο την online όσο και την offline ανάγνωση μηνυμάτων. Επίσης αφήνει τα μηνύματα στον server έως ότου ο χρήστης αποφασίσει να τα διαγράψει. Η τακτική αυτή δίνει την δυνατότητα σε έναν χρήστη να διαβάζει τα email του από διάφορους υπολογιστές. Αντίθετα, το POP3 επιτρέπει την ανάγνωση των email μονάχα από τον υπολογιστή στον οποίο έχουν κατέβει. Τα περισσότερα προγράμματα διαχείρισης ηλεκτρονικής αλληλογραφίας (Mozilla Thunderbird, Microsoft Outlook κοκ) υποστηρίζουν και τα δύο πρωτόκολλα και δίνουν στον χρήστη την δυνατότητα να επιλέξει ποιό ταιριάζει καλύτερα στις ανάγκες του. Παρόλα αυτά

όμως, το πρωτόκολλο IMAP υποστηρίζεται από λιγότερους servers σε σχέση με το πρωτόκολλο POP3.

Το POP3 χρησιμοποιεί την πόρτα 110 για να εγκαθιδρύσει μία σύνδεση TCP με τον mail server. Πολλά προγράμματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν κρυπτογράφηση ούτως ώστε τα δεδομένα που διακινούνται στην σύνδεση αυτή να μην είναι αναγνώσιμα από άλλους. Για να αποδεχθεί ο mail server την σύνδεση, θα πρέπει ο χρήστης να δώσει το όνομα χρήστη και τον κωδικό πρόσβασής του. Η αρχική έκδοση του POP3 μετέδιδε τα ευαίσθητα αυτά δεδομένα σε μορφή απλού κειμένου, οπότε οποιοσδήποτε μπορούσε να τα διαβάσει. Στην συνέχεια όμως το πρωτόκολλο βελτιώθηκε και πλέον παρέχει την δυνατότητα κρυπτογραφημένης μετάδοσης του ονόματος χρήστη και του κωδικού. Παρόλα αυτά όμως, πολλοί χρήστες δεν γνωρίζουν αυτήν την δυνατότητα και συνεπώς δεν την χρησιμοποιούν.

VI. Το πρωτόκολλο **HTTP**

Κάθε υπηρεσία στο Internet έχει το δικό της πρωτόκολλο. Το πρωτόκολλο του Web λέγεται **HTTP** (Hypertext Transfer Protocol) και είναι ένα σύνολο από κανόνες που ελέγχουν και καθορίζουν την διακίνηση των ιστοσελίδων από τους Web servers στους υπολογιστές των χρηστών. Όταν πληκτρολογείτε την ηλεκτρονική διεύθυνση μίας ιστοσελίδας, ξεκινάτε πάντα με http . Με αυτό τον τρόπο καθορίζεται τον τρόπο με τον οποίο θα πραγματοποιηθεί η συνδιαλλαγή μεταξύ του υπολογιστή σας και του server στον οποίο φυλάσσετε η ιστοσελίδα που σκοπεύετε να κατεβάσετε.

1.3 Διευθυνσιοδότηση στο Internet

Το Internet όπως προείπαμε, αποτελείται από χιλιάδες δίκτυα στα οποία είναι συνδεδεμένοι εκατομμύρια υπολογιστές. Πως μπορεί να προσδιοριστεί λοιπόν με ακρίβεια ο υπολογιστής για τον οποίο προορίζονται κάποια δεδομένα; Με άλλα λόγια πως ξεχωρίζει ένας υπολογιστής του Internet από ένα άλλο;

1.3.1 Διευθύνσεις **IP(Internet protocol)**

Σε κάθε υπολογιστή αντιστοιχίζεται μια μοναδική διεύθυνση, που ονομάζεται διεύθυνση IP(Internet Protocol Address) και η οποία αποτελεί την «ταυτότητά» του στο διαδίκτυο. Μια διεύθυνση IP αποτελείται από 4 αριθμούς χωρισμένους σε τελείες. Π.χ. ένας υπολογιστής που βρίσκεται στο Α.Τ.Ε.Ι ΠΑΤΡΑΣ έχει διεύθυνση 195.251.8.35, ένας άλλος έχει διεύθυνση 195.251.8.10

Στην πραγματικότητα μια IP Διεύθυνση είναι ένας δυαδικός αριθμός 32-bit που για να γίνει περισσότερο κατανοητός στους ανθρώπους, χωρίζεται σε 4 ομάδες των 8-bit και κατόπιν κάθε ομάδα μεταφράζεται στον αντίστοιχο δεκαδικό αριθμό. Π.χ. 00010010 01001011 00000000 00001010 (δυαδικός αριθμός 32-bit) 18.75.0.10 (4 δεκαδικοί αριθμοί χωρισμένοι με τελείες). Μια διεύθυνση IP περιέχει δύο κομμάτια πληροφορίας. Το πρώτο είναι ο αριθμός δικτύου (network id) στο οποίο ανήκει ο υπολογιστής. Κάθε δίκτυο χαρακτηρίζεται από ένα μοναδικό αριθμό που αποτελεί την «**ταυτότητά**» του στο Internet. Το δεύτερο είναι ένας τοπικός αριθμός υπολογιστή που τον προσδιορίζει μέσα στο συγκεκριμένο δίκτυο(Host id). Οι Διευθύνσεις στο Internet ανήκουν σε έναν από τους παρακάτω τέσσερις τύπους, ανάλογα με το πλήθος των συστημάτων που περιλαμβάνει το δίκτυο:

Κλάση Α: Η μορφή των διευθύνσεων της κατηγορίας αυτής διαμορφώνεται από το πρώτο Bit που είναι το 0, τα επόμενα 7 bit αποτελούν το id του δικτύου και

τα υπόλοιπα 24 το host id. Οι διευθύνσεις αυτής της μορφής είναι κατάλληλες για ένα τοπικό δίκτυο με πολλά συστήματα(hosts).

Κλάση Β: Εδώ η μορφή των διευθύνσεων αρχίζει με τα bits 10 και ακολουθούν τα 14 bits του network id και τα 16 bits του host id.

Κλάση C: Εδώ τα χαρακτηριστικά bits είναι 110, μετά ακολουθούν τα υπόλοιπα 21 τα οποία δηλώνουν το network id και τέλος 8 bits για το host id.

Κλάση D: Εδώ οι διευθύνσεις σχηματίζονται από τα bits 1110 στην αρχή, και ακολουθούν τα υπόλοιπα 28 bits. Αυτή η κατηγορία απευθύνεται σε περιπτώσεις μετάδοσης multicast.

Κάθε οργανισμός που θέλει να συνδέσει στο Internet τους υπολογιστές του ζητά έναν αριθμό δικτύου από κάποιον επίσημο οργανισμό που ασχολείται με την κατανομή των διευθύνσεων στο Internet, έτσι ώστε να εξασφαλίζεται η μοναδικότητά τους.(Κομνηνός 2002)

1.3.2 **Dynamic** και **static** διευθύνσεις **IP**

Οι διευθύνσεις IP ορίζονται είτε μόνιμα (για παράδειγμα, σε ένα διακομιστή ο οποίος βρίσκεται πάντα στην ίδια διεύθυνση) είτε προσωρινά από ένα πλήθος διαθέσιμων διευθύνσεων.

Dynamic IP

Οι Dynamic διευθύνσεις IP δίνονται για να αναγνωρίζονται προσωρινές συσκευές όπως προσωπικοί υπολογιστές ή προγράμματα πελάτες (clients). Οι ISPs χρησιμοποιούν δυναμική κατανομή (οι διευθύνσεις IP κατανέμονται δυναμικά) για να ορίσουν διευθύνσεις από ένα μικρό πλήθος διαθέσιμων σε ένα μεγαλύτερο αριθμό πελατών. Αυτή η μέθοδος χρησιμοποιείται για σύνδεση μέσω τηλεφώνου (dial-up), Wi-Fi και άλλες προσωρινές συνδέσεις, επιτρέποντας σε χρήστες φορητών υπολογιστών να συνδέονται αυτόματα σε μια ποικιλία υπηρεσιών χωρίς να χρειάζεται να γνωρίζουν λεπτομέρειες σχετικά με το routing του κάθε δικτύου. Οι χρήστες με dynamic διευθύνσεις IP πιθανόν να έχουν προβλήματα στο να τρέχουν δικό τους mail servers (διακομιστή ηλεκτρονικού ταχυδρομείου) καθώς τα τελευταία χρόνια υπηρεσίες όπως το mail-abuse.org έχουν συλλέξει λίστες από διαστήματα (ranges) διευθύνσεων IP (διευθύνσεις δηλαδή που έχουν ίδια κάποια αρχικά ψηφία) και τις έχουν μπλοκάρει. Η δυναμική κατανομή διευθύνσεων IP απαιτεί έναν κεντρικό διακομιστή (server) για να ακούει τα αιτήματα και να ορίσει έπειτα μια διεύθυνση. Οι διευθύνσεις μπορούν να οριστούν τυχαία ή να βασιστούν σε μια προκαθορισμένη πολιτική (policy). Το πιο συνηθισμένο πρωτόκολλο που χρησιμοποιείται για τον ορισμό διευθύνσεων δυναμικά είναι το Dynamic host Configuration Protocol (DHCP). Το DHCP περιλαμβάνει ένα lease time που καθορίζει πόσο καιρό μπορεί αυτός που κάνει την αίτηση να χρησιμοποιήσει μια διεύθυνση πριν ζητήσει την ανανέωσή της, επιτρέποντας σε διευθύνσεις να παίρνονται, εάν όποιος τις ζήτησε αποσυνδεθεί. Είναι σύνηθες να χρησιμοποιείται δυναμική κατανομή για ιδιωτικά δίκτυα. Δεδομένου ότι τα ιδιωτικά δίκτυα σπάνια παρουσιάζουν έλλειψη διευθύνσεων, είναι δυνατό να οριστεί η ίδια διεύθυνση στον ίδιο υπολογιστή με κάθε request ή να καθοριστεί ένας παρατεταμένος lease time. Αυτές οι δύο μέθοδοι μιμούνται την ανάθεση static IP address.

Static IP

Οι static διευθύνσεις IP χρησιμοποιούνται για να αναγνωρίζονται ημι-μόνιμες συσκευές με σταθερές διευθύνεις IP. Οι εξυπηρετητές (servers) τυπικά χρησιμοποιούν static διευθύνσεις IP. Η static διεύθυνση μπορεί να διαμορφωθεί άμεσα (να γίνει configured) επάνω στη συσκευή η ως μέρος της κεντρικής διαμόρφωσης DHCP που συσχετίζει τη MAC address της συσκευής με μια στατική διεύθυνση.

Υπάρχουν κάποιες υπηρεσίες που ορίζουν την πολιτική που ακολουθείται στο Internet. Η ανάπτυξη του Internet κατευθύνεται από τον Internet Society ο οποίος περιγράφεται ως ένας μη κυβερνητικός, διεθνής οργανισμός που έχει ω σκοπό την καθολική συνεργασία και το συντονισμό του internet και των τεχνολογιών και εφαρμογών του. Η καταγραφή των ονομάτων τομέα και η διαχείρισή τους γίνεται από τον Internet Corporation For Assigned Names and Numbers (ICANN) και του Network Solutions Incorporated. Οι περισσότερες εταιρίες παροχής Internet (ISPs) παρέχουν επίσης υπηρεσίες καταγραφής ονομάτων τομέων. Το κέντρο πληροφοριών δικτύου Internet(Internet Network Information Center, InterNIC) παρέχει το τμήμα της διεύθυνσης που προσδιορίζει την διεύθυνση του τοπικού δικτύου και δίνει στον διαχειριστή του δικτύου μια περιοχή διευθύνσεων.(Bennett falk 1996)

1.4 Υπηρεσίες Διαδικτύου

Μερικές από τις πιο γνωστές ιντερνετικές υπηρεσίες που χρησιμοποιούν τα προαναφερθέντα πρωτόκολλα είναι το ηλεκτρονικό ταχυδρομείο (e-mail), οι ομάδες συζητήσεων (newsgroups), η διαμοίραση αρχείων (file sharing) και ο Παγκόσμιος Ιστός (World Wide Web). Επίσης υπάρχουν και άλλες υπηρεσίες όπως Telnet, Ftp κτλ.

I. Ηλεκτρονικό Ταχυδρομείο (**e-mail**)

Υποστηρίζει την ανταλλαγή μηνυμάτων μεταξύ των χρηστών χάρη στην προσωπική ηλεκτρονική διεύθυνση του καθενός. Το περιεχόμενο μπορεί να είναι κείμενο, ήχος, εικόνα Video κτλ. Χρησιμοποιεί τα πρωτόκολλα IMAP & POP3

II. Ομάδες συζητήσεων(**news group**)

Είναι κατά βάση ηλεκτρονικές συζητήσεις. Οι χρήστες του διαδικτύου ανταλλάσουν ιδέες και συζητούν για διάφορα θέματα.

III. Διαμοίραση αρχείων(**P2P file sharing**)

Το Peer-to-peer (P2P) ανταλλαγής αρχείων είναι ένα σύστημα επιμερισμού αρχείων απευθείας μεταξύ των χρηστών του δικτύου, χωρίς τη βοήθεια η την παρεμβολή ενός κεντρικού server. Η αποκεντρωμένη φύση του peer-to-peer file sharing καταργεί την ανάγκη για ένα κεντρικό server, και καταργεί τη δυνατότητα κεντρικού έλεγχου. Υπάρχουν πολλά peer-to-peer δίκτυα ανταλλαγής αρχείων σε λειτουργιά. Η κύρια peer-to-peer file sharing δικτύων είναι το Gnutella, Direct Connect, eDonkey2000, Fast Track, και Open Nap.

IV. Ο Παγκόσμιος Ιστός (**World Wide Web**)

Το World Wide Web (Παγκόσμιος Ιστός) ή WWW ή απλά Web είναι μια από τις πιο συχνά χρησιμοποιούμενες υπηρεσίες του Internet. Ο Ιστός βασίζεται στην έννοια του **Υπερκειμένου** (**Hypertext**). Το υπερκείμενο είναι δεδομένα

που περιέχουν **υπερσυνδέσμους** (**HyperLinks**) ή απλά Links (συνδέσμους) για άλλα δεδομένα. Τα δεδομένα του ιστού ονομάζονται σελίδες (Sites). Τα προγράμματα που χρησιμοποιούνται για την προσπέλαση των σελίδων του ιστού ονομάζονται **browsers** (φυλλομετρητές). Καθώς ακολουθούμε τον ένα σύνδεσμο μετά τον άλλον μέσα στις σελίδες λέμε ότι περιδιαβαίνουμε (navigate) τον ιστό. Αρχικά οι σελίδες του ιστού περιείχαν μόνο κείμενο. Σήμερα μπορεί να περιέχουν οτιδήποτε πληροφορίες όπως εικόνες, γραφικά, ήχο και οποιαδήποτε άλλη μορφή ψηφιακής πληροφορίας γι' αυτό χρησιμοποιείται ο όρος **Hypermedia** (Υπερμέσα). Οι σελίδες του ιστού μπορεί να βρίσκονται οπουδήποτε μέσα στο Internet.

V. FTP

Παρέχει στον χρήστη την δυνατότητα να πάρει αρχεία από άλλους υπολογιστές

VI. TELNET

Επιτρέπει την άμεση σύνδεση με κάποιον από τους υπολογιστές του δικτύου μέσω ενός προγράμματος που ονομάζεται Telnet. Μέσω αυτού του προγράμματος ένας απομακρυσμένος υπολογιστής(telnet server) συνδέεται με έναν άλλο υπολογιστή (telnet client) και ο χρήστης μπορεί να κάνει login στον απομακρυσμένο υπολογιστή, να τρέξει προγράμματα κτλ.

ΚΕΦΑΛΑΙΟ 2^{Ο} ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

2.1 Λόγοι ανασφάλειας στο διαδίκτυο

Το Διαδίκτυο όπως είναι γνωστό αποτελεί το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων, όχι κατά ανάγκη ίδιας τεχνολογίας, που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε όλη την Γη. Είναι λοιπόν αντιληπτό ότι είναι πολύ δύσκολο να αντιμετωπιστεί ολικά από άποψη ασφάλειας, εξαιτίας της ετερογένειας που το χαρακτηρίζει. Βέβαια πολύ σημαντικό είναι το γεγονός ότι οι μηχανισμοί που στηρίζουν την λειτουργικότητά του σχεδιάστηκαν με σκοπό την βελτιστοποίηση των διαφόρων δυνατοτήτων διασύνδεσης ετερογενών δικτύων και εκμετάλλευσης πόρων – πληροφοριών και όχι για να παρέχουν ασφάλεια. Συμπερασματικά, η ασφάλεια επιτυγχάνεται ως πρόσθετο χαρακτηριστικό του δικτυακού σχεδίου και όχι ως κομμάτι του. Οι λόγοι που κάνουν το Διαδίκτυο ανασφαλές είναι:

- Η **ετερογένεια των δικτύων** που τα συνδέει με δεδομένο το απέραντο μέγεθός του, έχει ως συνέπεια οι διαδικασίες που διασφαλίζουν ένα σύστημα σε ένα τέτοιο περιβάλλον, να απαιτούν έναν μεγάλο αριθμό περίπλοκων ρυθμίσεων και διαμορφώσεων.
- Η **εύκολη και απεριόριστη πρόσβαση** που παρέχει σε εκατομμύρια χρήστες, το τρέπει πιο ευάλωτο από κάθε άλλο δίκτυο.
- Η **μη ύπαρξη συνολικής πολιτικής ελέγχου προσπέλασης**. Δεν υπάρχει κατάλληλη υποδομή στους υπάρχοντες κόμβους εξαιτίας κόστους ή ακόμα και άγνοιας, με αποτέλεσμα να υπάρχει μεγάλος κίνδυνος από την ευρέως ανοικτή σύνδεσή τους στο διαδίκτυο.
- Η **φύση των πρωτοκόλλων TCP/IP** και των περισσότερων υπηρεσιών που υποστηρίζουν δεν μπορούν να εκμηδενίσουν τους κινδύνους ασφαλείας. Το γεγονός ότι δεν επιτρέπονται τα πακέτα των δεδομένων να περνούν από μια σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και

επιμέρους δικτύων μέχρι να φθάσουν στον τελικό τους προορισμό, δίνει την δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διάφορους τρόπους στην επικοινωνία των δύο νόμιμων μερών. Επιδέξιοι εισβολείς μπορούν σχετικά εύκολα να παραβιάσουν την ασφάλεια των TCP/IP υπηρεσιών, με δεδομένο και ότι η πλειοψηφία των δεδομένων που διακινούνται είναι σε μη κρυπτογραφημένη μορφή.

- Η **αυξημένη πολυπλοκότητα διαδικασιών**, η οποία περιορίζει το αίσθημα εμπιστοσύνης, μιας και όσο πιο δυσνόητο είναι κάτι τόσο μεγαλύτερη είναι και η δυσπιστία που επικρατεί για αυτό.
- Η **δυνατότητα ανωνυμίας ενός χρήστη** κατά την διάρκεια της περιήγησής του στο Διαδίκτυο.

2.2 Κίνδυνοι που απειλούν τις ηλεκτρονικές συναλλαγές

Προκειμένου να εστιάσουμε στους κινδύνους που απειλούν τις ηλεκτρονικές συναλλαγές, καλό είναι να ορίσουμε τι είναι κίνδυνος. **Κίνδυνος** λοιπόν είναι κάθε απειλή που σκοπό έχει να βλάψει την ακεραιότητα των ηλεκτρονικών συναλλαγών και να εκμεταλλευτεί οποιαδήποτε πληροφορία που μπορεί να αποκομίσει παραβιάζοντας την ιδιωτικότητά τους. Οι κίνδυνοι λοιπόν είναι:

- **Η υποκλοπή δεδομένων**. Το γεγονός αυτό συμβαίνει όταν ο χρήστης καταφέρνει να υποκλέψει δεδομένα που μεταδίδονται δε μια διαδικτυακή επικοινωνία. Αυτό παραβιάζει την ιδιωτική ζωή των ατόμων και επίσης μπορεί να εκμεταλλευτεί δεδομένα που έχουν υποκλαπεί όπως συνθηματικά ή στοιχεία από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά.
- **Η καταστροφή / μαζική αλλοίωση δεδομένων,** δηλαδή όταν ο χρήστης τροποποιεί ή πλαστογραφεί δεδομένα.

- **Οι απάτες(ψεύτικες συναλλαγές),** η περίπτωση όπου κάποιος έχει μπει στο σύστημα κάποιου ηλεκτρονικού καταστήματος και έχει γράψει στοιχεία για ανύπαρκτες συναλλαγές ή τροποποιεί στοιχεία.
- **Η άρνηση εξυπηρέτησης,** όταν κάποιος ενεργεί με σκοπό να αποτρέψει την διάθεση πόρων και υπηρεσιών προς νόμιμους χρήστες.
- **Η μεταμφίεση,** όταν ένας χρήστης υποκρίνεται ότι είναι κάποιος άλλος προκειμένου να έχει εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες σε άτομα, επιχειρήσεις κτλ.
- **Τα SpyWare,** είναι μικρά προγράμματα που μπαίνουν στον Η/Υ χωρίς να το καταλάβουμε και στέλνουν πληροφορίες στον αποστολέα τους σχετικά με το λειτουργικό μας σύστημα, τις σελίδες που επισκεπτόμαστε κτλ.
- **Το Phising,** με τον όρο phising δεν χαρακτηρίζεται κάποιο πρόγραμμα, αλλά η προσπάθεια ορισμένων να πάρουν κρίσιμα δεδομένα(αριθμοί πιστωτικών καρτών κτλ.) προσποιούμενοι ότι είναι κάποιος φορέας που το υποψήφιο θύμα εμπιστεύεται (τράπεζες,κτλ)
- **Τα αυτόνομα κακόβουλα προγράμματα,** τέτοια είναι οι ιοί, σκουλήκια και οι δούρειοι ίπποι τα οποία μπορεί να είναι πολύ καταστροφικά για έναν υπολογιστή.

2.2.1 Ιοί Ηλεκτρονικών Υπολογιστών

Ένας **ιός υπολογιστών** είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν **μεταμορφικό ιό**. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο, την υπηρεσία συνομιλιών (Internet Relay Chat, IRC). Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι

"καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.

2.2.1.1 Τύποι Ιών

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

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

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

Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:

- Πολυμορφικοί ιοί
- Αόρατοι ιοί (Stealth Viruses)
- Θωρακισμένοι ιοί (Armored Viruses)
- Πολυτμηματικοί ιοί (Multipartite Viruses)
- Ιοί πλήρωσης κενών (Spacefiller Viruses)
- Ιοί παραλλαγής (Camouflage Viruses)

2.2.2 Δούρειος Ίππος (Trojan Horse)

Ο όρος "δούρειος ίππος" χρησιμοποιήθηκε αρχικά από τον Κεν Τόμσον στην ομιλία του το 1983 κατά την τελετή απονομής των βραβείων Turing. Ο Τόμσον παρατήρησε ότι είναι δυνατόν να προστεθεί κακόβουλος κώδικας στην εντολή login του Unix για την υποκλοπή κωδικών πρόσβασης. Αυτήν του την ανακάλυψη την ονόμασε "δούρειο ίππο". Επιπροσθέτως υποστήριξε ότι οποιοσδήποτε μεταγλωττιστής C μπορεί να μετατραπεί κατάλληλα ούτως ώστε να προσθέτει αυτόματα κακόβουλο κώδικα στα προγράμματα που δημιουργεί. Με τον τρόπο αυτό ο εντοπισμός του κακόβουλου κώδικα γίνεται ακόμη πιο δύσκολος. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι η εξής. Συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία. Οι πιο γνωστοί είναι Downloader-EV Dropper-EV, Pest Trap, NetBus, flooder, Tagasaurus, Vundo Trojan, Gromozon Trojan, Sub-7, Cuteqq_Cn.exe

2.2.3 Σκουλήκια (Worms)

Είναι τα προγράμματα που διαδίδουν αυτόματα τον εαυτό τους στα άλλα συστήματα ενός δικτύου. Προχωρούν μέσα στο δίκτυο, εγκαθίστανται σε συνδεδεμένες μηχανές και στην συνέχεια, προσπαθούν από εκεί να βρουν

επόμενους στόχους για να τους προσβάλουν. Το χαρακτηριστικό τους γνώρισμα είναι ότι μπορούν να λειτουργούν αυτόνομα και να έχουν την δυνατότητα να ξεχωρίζουν τους στόχους τους. Τα σκουλήκια και οι ιοί ταχυδρομείων είναι περισσότερο ταχείας καύσεως. Έχουν την δυνατότητα να εξαπλώνονται παντού πριν οι κατασκευαστές των AnriVirus βρουν τον χρόνο να αναλύσουν το πρόβλημα και να διανείμουν μέτρα ανίχνευσης και απολύμανσης. Σε μερικές περιπτώσεις, το κακόβουλο αυτό λογισμικό που αναφέρεται ως σκουλήκι, είναι στην πραγματικότητα εξειδικευμένος ιός, που προσβάλει ένα μόνο αρχείο. Δεν υπάρχουν αποδεκτές κατηγορίες στις οποίες μπορούμε να κατατάξουμε τα σκουλήκια, παρά μόνο σε μια μελέτη του Carrey Nachenberg ο οποίος πρότεινε σχηματοποίηση με βάση τις εξής κατευθύνσεις:

- **Σκουλήκια ηλεκτρονικού ταχυδρομείου**, που προφανώς εξαπλώνονται μέσω αυτού.
- **Αυθαίρετα σκουλήκια**, που εξαπλώνονται με τα πρωτόκολλα και δεν βασίζονται σε ηλεκτρονικό ταχυδρομείο (IRC/DCC, FTP, TCP/IP)

Υπάρχει ακόμα μια κατάταξη σύμφωνα με το μηχανισμό μεταφοράς. Επιπλέον ο Nachenberg πρότεινε ακόμα μια συμφωνία με το μηχανισμό εκδήλωσης όπως:

- **Αυτοπυροδοτούμενα σκουλήκια**, όπως το σκουλήκι του Παγκόσμιου Ιστού (Internet Worm), που δεν απαιτούν την συνεργασία του υπολογιστή για να εξαπλωθούν. Απλά επωφελούνται από τα τρωτά σημεία του περιβάλλοντος που τα φιλοξενεί, χωρίς να προσπαθούν να ξεγελάσουν τον χρήστη ώστε να εκτελέσει τον μολυσμένο κώδικα. Εκμεταλευόμενοι κάποιο σφάλμα του περιβάλλοντος είναι σε θέση να αυτό-εκτελούνται

χωρίς εξωτερική συνδρομή η παρέμβαση. Τέτοιου είδους σκουλήκια είναι το KAK και BybbleBoy.

- **Σκουλήκια που πυροδοτεί ο χρήστης,** αυτά χρειάζονται την αλληλεπίδραση του χρήστη. Απαιτούν τη χρήση ορισμένων τεχνικών μέσων κοινωνικής επιτηδειότητας προκειμένου να πείσουν τον χρήστη να ανοίξει/ κλείσει το συνημμένο αρχείο, ώστε το σκουλήκι να μπορέσει να διεισδύσει στο περιβάλλον αυτό και να αυτό- εκτελεστεί στην επόμενη ομάδα συστημάτων που θα το φιλοξενήσουν.

ΚΕΦΑΛΑΙΟ 3^{Ο} Η ΚΡΥΠΤΟΓΡΑΦΙΑ

3.1 Εισαγωγή στην Κρυπτογραφία

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet. Από την στιγμή που άρχισαν να μεταφέρονται πληροφορίες, ξεκίνησε και η ιδέα της κρυπτογράφησης ή του κώδικα για να ασφαλιστούν τα μηνύματα. Με άλλα λόγια η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Για την καλύτερη κατανόηση αυτών που θα αναλύσουμε είναι σκόπιμο να δώσουμε ορισμούς στους παρακάτω όρους:

Κρυπτογράφηση(encryption): ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (*decryption*)**.

Αρχικό κείμενο (*plaintext*): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

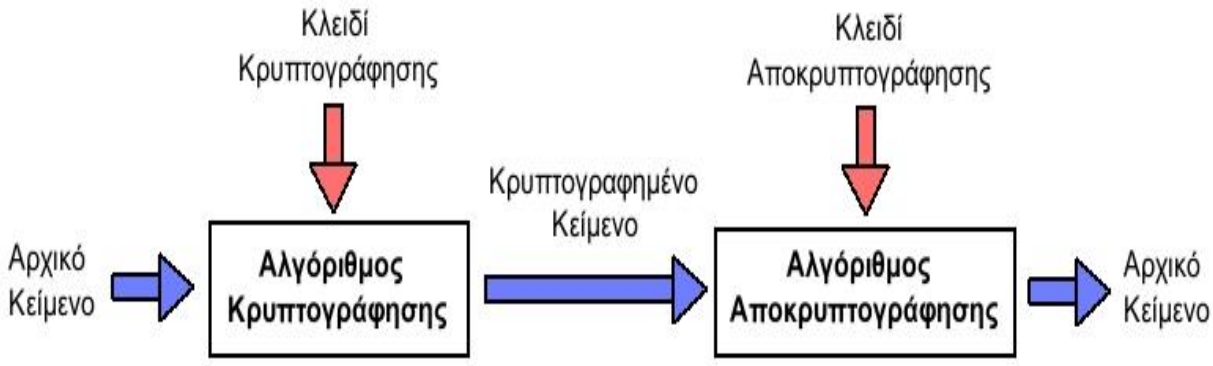
Κρυπτογραφημένο κείμενο (*ciphertext*): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτογραφικός αλγόριθμος (cipher):είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Κλειδί (*key*):είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.

Κρυπτανάλυση (*cryptanalysis*): είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.



Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

3.2 Η Ιστορία της Κρυπτογραφίας

Η κρυπτογραφία ξεκινάει από το 1900 π.Χ έως σήμερα και χωρίζεται σε τρεις(3) μεγάλες περιόδους.

Πρώτη Περίοδος Κρυπτογραφίας (1900 π.χ. – 1900 μΧ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασιζόταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές αλλά στηριζόταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί, ότι, εάν μας είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί. Όπως προκύπτει, από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο με βάση τον Kahn. Επίσης ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα. Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφεύραν τη «σκυτάλη» (σχήμα 3.1), την πρώτη κρυπτογραφική συσκευή, στην οποία, χρησιμοποίησαν για την κρυπτογράφηση, τη μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» Σχήμα (2.1), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο

σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης. Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που ανακάλυψαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, ανακαλύφθηκε από αυτούς γύρω στον 14ο αιώνα.

Σχήμα 3.1

Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950 μ.Χ. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma Σχήμα(3.2)

Ο Marian Rejewski, στην Πολωνία, επιτέθηκε και παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (μια ηλεκτρομηχανική κρυπτογραφική μηχανή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της χιλιετίας. Στην συνέχεια ακολούθησαν και άλλα κρυπτογραφικά συστήματα από το Ιαπωνικό υπουργείο εξωτερικών με την μηχανή Purple, οι ΗΠΑ με την Μηχανή –Μ κα.

Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard)στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας. Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση

πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

3.3 Οι Τρόποι και οι Λειτουργίες Της Κρυπτογράφησης

Τα κρυπτογραφικά συστήματα (Ciphers), σύμφωνα με τον τρόπο που κρυπτογραφούν μπορούν να χωριστούν σε δύο κατηγορίες, τα stream & block ciphers. Τα block chippers κρυπτογραφούν το Plaintext ανά κομμάτια (blocks) συνήθως μεγέθους 64 και 128 bits. Αντίθετα τα stream ciphers κρυπτογραφούν το κάθε bit ξεχωριστά. Σημαντικό να αναφερθούν δύο τρόποι κρυπτογράφησης, ο XOR & η λειτουργία MODULO.

- XOR: είναι ο πιο εύκολος τρόπος κρυπτογράφησης. Βασικά πρόκειται για έναν αλγόριθμο συμμετρικής κρυπτογράφησης, ο οποίος όμως δεν παρέχει ένα υψηλό ασφαλείας επίπεδο από μόνος, ωστόσο η μέθοδος XOR ενσωματώνεται μέσα στην λειτουργία αλγορίθμων οι οποίοι παρέχουν υψηλά επίπεδα ασφαλείας. Για την πιο εύκολη κατανόηση η κατανόηση της λειτουργίας δίνετε το παρακάτω παράδειγμα:π.Χ

  Έστω ότι έχουμε το plaintext: 70 65 81

Αυτό μεταφράζεται σε δυαδική μορφή σε: 011100000110010110000000

Έστω ότι τώρα έχουμε τα παρακάτω κλειδί: 86

Το οποίο σε δυαδική μορφή είναι το: 10000110

Στο σχήμα 3.1 φαίνεται η λειτουργία κρυπτογράφησης της XOR

XOR	Input 1	
	0	1
Input 2 0	0	1
1	1	0

Σχήμα 3.1

- MODULO: Σύμφωνα με αυτήν την λειτουργία, αν θέλουμε να υπολογίσουμε το y mod x (y modulo x) αφαιρούμε από τον Υ όλα τα πολλαπλάσια του x και κρατάμε το υπόλοιπο. Έτσι, για παράδειγμα έχουμε:

15 mod 7= 1

25 mod 5= 0

33 mod 12= 9

203 mod 256= 203 κ.ο.κ

Κατά την διάρκεια της κρυπτογράφησης τα block ciphers χρησιμοποιούν διάφορες τεχνικές γνωστές ως **τρόποι λειτουργίας.** Προκειμένου να είναι χρήσιμο ένα mode πρέπει να είναι τουλάχιστον τόσο αποδοτικό και τόσο ασφαλές όσο το block cipher. Οι κυριότεροι τρόποι λειτουργίας είναι: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), & Output Feedback (OFB).

Electronic Code Book (ECB)

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

Cipher Block Chaining Mode (CBC)

Αυτό το mode χρησιμοποιεί ανατροφοδότηση. Πιο συγκεκριμένα πριν κρυπτογραφεί το κάθε block συνδυάζεται με το ciphertext του προηγούμενου block με την μέθοδο XOR. Έτσι αυτό που επιτυγχάνεται είναι ότι ακόμα και αν υπάρχουν πολλά ίδια blocks στο plaintext μετά την κρυπτογράφηση τα αντίστοιχα ciphertext blocks θα διαφέρουν μεταξύ τους. Όπως και στον τρόπο ECB έτσι και στην περίπτωση του CBC εάν ένα Bit ενός block αλλοιωθεί, τότε αλλοιώνεται όλο το περιεχόμενο του block, μόνο που σε αυτήν την περίπτωση θα αλλοιωθεί μαζί με αυτό το block και το περιεχόμενο των Block που ακολουθούν. Τα λάθη κατά την μετάδοση των δεδομένων είναι αναπόφευκτα,

γι ‘αυτό και εάν λείπει ένα και ένα byte από το ciphertext, το περιεχόμενο του plaintext δεν μπορεί να ανακτηθεί από εκείνο το σημείο και μετά.

CipherFeedbackMode(CFB)

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

Output Feedback Mode (OFB)

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

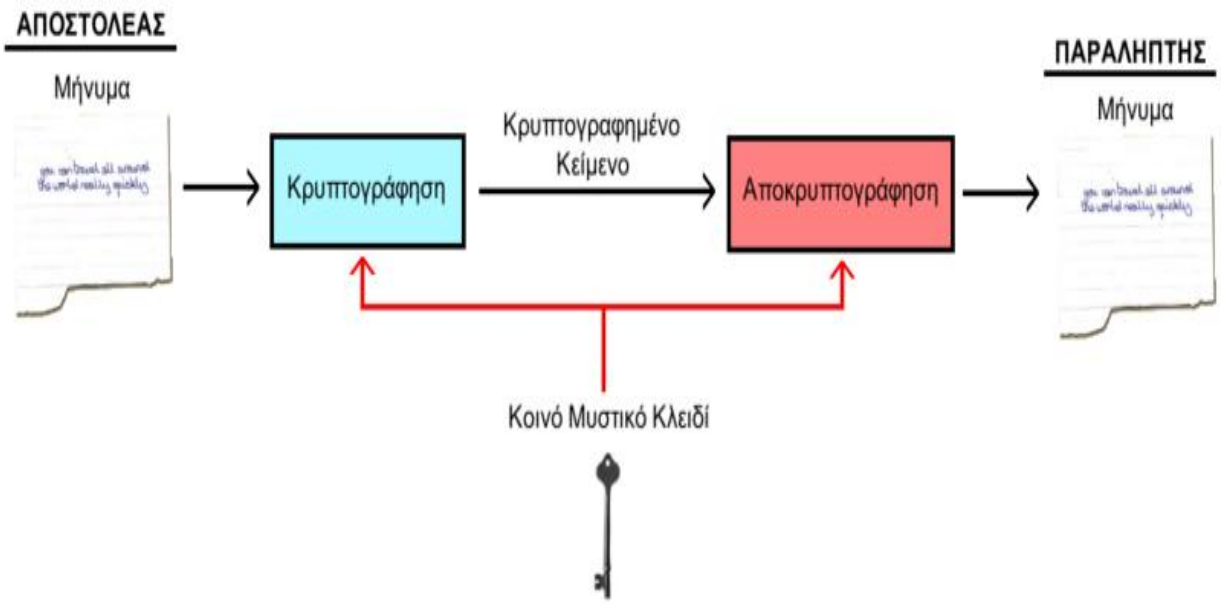
3.4 Μέθοδοι Κρυπτογράφησης

Για την κρυπτογράφηση χρησιμοποιούνται τρεις(3) μέθοδοι, η συμμετρική, ασύμμετρη ή δημοσίου κλειδιού και οι αλγόριθμοι κατακερματισμού. Ο λόγος που χρησιμοποιούνται τρεις διαφορετικοί τρόποι κρυπτογράφησης είναι ότι ο καθένας είναι ιδανικός για διαφορετικές εφαρμογές. Για παράδειγμα οι αλγόριθμοι κατακερματισμού είναι ιδανικοί για ακεραιότητα δεδομένων, γιατί οποιαδήποτε αλλαγή γίνει στα περιεχόμενα του μηνύματος θα οδηγήσει σε ολοκληρωτική του αλλαγή. Η συμμετρική κρυπτογραφία βρίσκει εφαρμογή στην ανταλλαγή μηνυμάτων γιατί είναι πολύ πιο γρήγορη από την ασύμμετρη

κρυπτογραφία. Ενώ η τελευταία 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.

3.4.1 Συμμετρική Κρυπτογράφηση

Σύμφωνα με την συμμετρική κρυπτογραφία ο αποστολέας του μηνύματος χρησιμοποιεί ένα κλειδί, κρυπτογραφεί το μήνυμα και στην συνέχεια ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί και αποκρυπτογραφεί το μήνυμα. Δηλαδή χρησιμοποιείται το ίδιο κλειδί κατά την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος. Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν σ' αυτήν την κατηγορία οι οποίοι είναι:



Σχήμα 3.3

3.4.1.1 **Data Encryption Standard (DES)**

Το DES αναπτύχθηκε κατά την δεκαετία του ’70 και σήμερα χρησιμοποιείται ευρέως. Το μήκος του κλειδιού που χρησιμοποιεί είναι 56 bits και θεωρείται μικρό για την επίτευξη υψηλής προστασίας ανταλλασσόμενων μηνυμάτων από επιθέσεις. Το DES κρυπτογραφεί τα δεδομένα σε διακριτά μπλοκ των 64 Bits και συχνά χρησιμοποιείται σε συνδυασμό με μια άλλη μέθοδο που ονομάζεται cipherblock chaining (CBC). Ο συνδυασμός αυτών των δύο μεθόδων έχει σαν αποτέλεσμα η κρυπτογράφηση καθενός μπλοκ να εξαρτάται από το περιεχόμενο του προηγούμενου αυξάνοντας με αυτόν τον τρόπο την ασφάλεια του των κρυπτογραφημένων μηνυμάτων. Σημαντικό να αναφερθεί ότι ο DES έχει και άλλους τρόπους λειτουργίας όπως η ECB OFB CFB.

3.4.1.2 Triple **DES, DESX, GDES. RDES.**

Οι αλγόριθμοι αυτοί, αποτελούν παραλλαγές του DES και μειώνουν τον κίνδυνο αποκρυπτογράφησης από εισβολείς, χρησιμοποιώντας μεγαλύτερου μήκους κλειδιά. Συγκεκριμένα το Triple Des κρυπτογραφεί τα μηνύματα με τρία(3) μυστικά κλειδιά στη σειρά, φθάνοντας το μήκος του κλειδιού στα 112 bits.

3.4.1.3 **RC2, RC4, RC5**

Οι αλγόριθμοι αυτοί αναπτύχθηκαν από την RSA Security Inc. Και χρησιμοποιούν κλειδιά με διάφορα μήκη που φθάνουν έως τα 2048 bits. Παρουσιάζουν ιδιαίτερο ενδιαφέρον, καθώς χρησιμοποιούνται για την

κρυπτογράφηση / αποκρυπτογράφηση μηνυμάτων που μεταδίδονται στο διαδίκτυο.

3.4.1.4 **International Data Encryption Algorithm (IDEA).**

Ο αλγόριθμος αυτός είναι ιδιαίτερα διαδεδομένος στην Ευρώπη και χρησιμοποιεί μήκος κλειδιού 128 bits. Ο IDEA αποτελεί την καρδιά πολλών λογισμικών κρυπτογράφησης ηλεκτρονικών μηνυμάτων.

3.4.1.5 **Advanced Encryption Standard (AES)**

AES βασίζεται στο αλγόριθμο Rijndael, που εφευρέθηκε από Joan Daemen και Vincent Rijmen. AES διευκρινίζει τρεις βασικούς εγκριθεί μήκη: 128-bit, 192-bits και 256-bit.

3.4.2 Ασύμμετρη ή Δημοσίου Κλειδιού Κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο

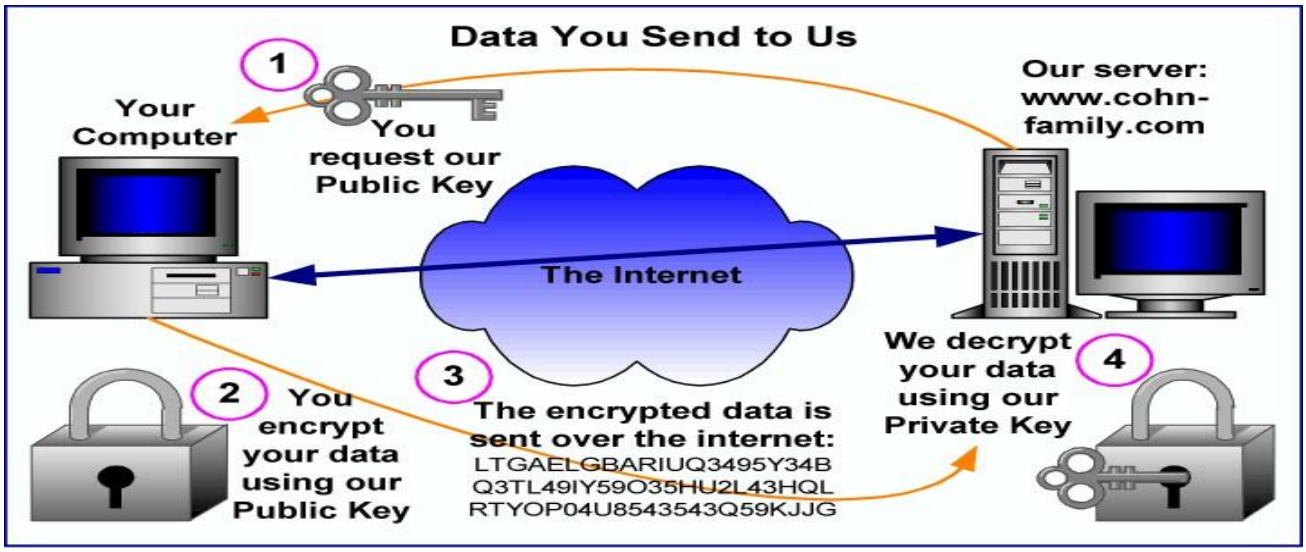
Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας

δημόσιου κλειδιού. Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει 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. Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα. Ο πιο γνωστός αλγόριθμος αυτού του είδους είναι ο RSA.

3.4.2.1 **RSA**

Ο αλγόριθμος RSA σχεδιάστηκε από τους Ron Rivest, Adi Shamir και Len Adleman, από όπου και πήρε το όνομα του το 1977. Πρόκειται για έναν αλγόριθμο ασύμμετρου κλειδιού, ο οποίος παρά την ηλικία του δεν έχει σπαστεί ακόμα και θεωρείται αρκετά ασφαλής, σε συνδυασμό βέβαια με το μήκος του κλειδιού που θα χρησιμοποιηθεί κάθε φορά. Γενικά ένα κλειδί μεγέθους 1024 bits θεωρείται ικανοποιητικά ασφαλές, παρόλα αυτά ορισμένοι υποστηρίζουν ότι στις μέρες μας το κλειδί πρέπει να έχει μήκος τουλάχιστον 2048 bits. Σε αυτό πρέπει να σημειωθεί ότι όσο μεγαλύτερο είναι ένα κλειδί τόσο πιο αργά κρυπτογραφεί. Ο RSA όπως και όλοι οι αλγόριθμοι ασύμμετρου κλειδιού, δεν βρίσκει εφαρμογή στην κρυπτογράφηση μεγάλων plaintext λόγω του ότι οι αλγόριθμοι συμμετρικού κλειδιού κρυπτογραφούν και αποκρυπτογραφούν πολύ

πιο γρήγορα. Η ασφάλεια του RSA πηγάζει από την δυσκολία της πραγματοποίησης μεγάλων αριθμών.



Σχήμα 3.4 (Τρόπος λειτουργίας RSA)

3.4.3 Αλγόριθμοι Κατακερματισμού (hash functions)

Τέλος υπάρχουν και οι αλγόριθμοι κατακερματισμού (hash functions). Σύμφωνα με αυτόν τον τρόπο κρυπτογραφίας, ο αλγόριθμος παίρνοντας σαν είσοδο το Plaintext, το μετατρέπει σε μια καθορισμένου μήκους τιμή κατακερματισμού (hash value), έτσι θα έλεγε κανείς ότι δεν χρησιμοποιείται καθόλου κλειδί. Με την χρήση των αλγορίθμων κατακερματισμού το περιεχόμενο καθώς και το μέγεθος του plaintext είναι αδύνατο να ανακτηθούν από το chiphertext, επίσης είναι σχεδόν αδύνατο ότι δύο διαφορετικά plaintext θα έχουν την ίδια τιμή κατακερματισμού. Οι πιο γνωστοί αλγόριθμοι που ανήκουν σ' αυτήν την κατηγορία είναι ο MD5 & SHA-1.

3.4.3.1 Message-Bush algorithm 5 (**MD5**)

Η συνάρτηση κατακερματισμού (hash value) MD5 σχεδιάστηκε 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 έχουν δείξει εμφανή σημεία αδυναμίας. Η MD5 είναι μια συνάρτηση κατακερματισμού που ανεξαρτήτως του μεγέθους του μηνύματος 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 αξία κατακερματισμού πρέπει να γίνουν 2^{64} υπολογισμοί, ενώ για να αντικατασταθεί ένα αρχείο με ένα άλλο που παράγει την ίδια αξία κατακερματισμού πρέπει να γίνουν 2^{128} υπολογισμοί ή αλλιώς 340.282.366.920.938.463.463.374.607.431.768.211.456 υπολογισμοί!

3.4.3.2 Secure Hash Algorithm (**SHA-1**)

Ο αλγόριθμος SHA περιλαμβάνει πέντε(5) κρυπτογραφικές λειτουργίες οι οποίες είναι 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.

3.5 Υποδομή Δημοσίου Κλειδιού (PKI)

Η υποδομή δημοσίου κλειδιού (Public Key Infastructure – PKI) είναι μια βάση ασφαλείας που βεβαιώνει ότι οι συναλλαγές μέσω του WEB μπορούν να είναι αξιόπιστες. Το PKI είναι το καθολικό όνομα που αναφέρεται στα ατομικά μέτρα ασφαλείας που βεβαιώνουν ότι οι συναλλαγές είναι εμπιστευτικές, που εξαναγκάζουν τους συνεργάτες μια επιχείρησης να αποδεικνύουν την ταυτότητά τους, που εμποδίζουν τροποποιήσεις ή αλλοιώσεις των συναλλαγών και εφαρμόζουν νομικά το αναμφισβήτητο των συναλλαγών. Συμπερασματικά λοιπόν το PKI επανακαθορίζει την εμπιστοσύνη των εταιριών όσον αφορά συναλλαγές που γίνονται στο Διαδίκτυο. Το PKI αποτελείτε από έξι(6) διαφορετικά μέρη που δουλεύουν μαζί για να δημιουργήσουν την βάση ασφαλείας τα οποία είναι:

- Κρυπτογράφηση Δημοσίου Κλειδιού
- Ψηφιακή Υπογραφή
- Συνάρτηση ταξινόμησης του Μηνύματος
- Ψηφιακούς Φάκελους.
- Αρχή Έκδοσης Πιστοποιητικών (Certificate Authority –CA)
- Αρχή Έκδοσης Εγγράφων (Registration Authority- RA)

3.5.1 Κρυπτογράφηση Δημοσίου κλειδιού

Η βάση του PKI είναι μια τεχνολογία που ονομάζεται κρυπτογράφηση δημοσίου κλειδιού (Puplic Key Cryptography), είναι η τεχνολογική λύση στο πρόβλημα που δημιουργείται από τα άτομα που υποκλέπτουν τα εμπιστευτικά μηνύματα που στέλνονται μέσω Διαδικτύου. Είναι ο μαθηματικός μυστικός κώδικας με τον οποίο κάθε γράμμα αλλάζει σε ένα διαφορετικό γράμμα, αριθμό ή σύμβολο, δημιουργώντας μια σελίδα που δεν

έχει έννοια, ώστε το μήνυμα να μην μπορεί να διαβαστεί, ακόμα και αν υποκλαπεί. Η κρυπτογράφηση του δημοσίου κλειδιού διαθέτει δύο κλειδιά. Δημιουργείται από έναν μαθηματικό κώδικα που βασίζεται σε έναν αλγόριθμο και σε μια τιμή, μ' έναν συμπληρωματικό αλγόριθμο και τιμή. Η ευελιξία αυτού του συστήματος είναι ότι αυτός ο αλγόριθμος μπορεί να κρυπτογραφήσει το μήνυμα και ο άλλος να το αποκρυπτογραφήσει.

3.5.2 Ψηφιακές Υπογραφές (**Digital Signatures**)

Οι ψηφιακές υπογραφές εφαρμόζονται χρησιμοποιώντας το δημόσιο κλειδί κρυπτογράφησης. Η καθεμία από αυτές αποτελεί ένα κρυπτογραφικό μηχανισμό, που βεβαιώνει την πηγή προέλευσης και το περιεχόμενο ενός μηνύματος. Τα μηνύματα κρυπτογραφούνται με την βοήθεια του ιδιωτικού κλειδιού του χρήστη και μπορούν να αποκρυπτογραφηθούν μόνο με το δημόσιο κλειδί του. Η λειτουργία των ψηφιακών υπογραφών είναι η εξής: Αρχικά ο χρήστης δημιουργεί μια εντολή αναγνώρισης, δηλαδή ένα απλό κείμενο, κωδικοποιεί το κείμενό του με το ιδιωτικό του κλειδί δημιουργώντας μια κρυπτογραφημένη υπογραφή. Έπειτα τοποθετεί την υπογραφή του στο μήνυμα που θέλει να στείλει και κρυπτογραφεί και τα δύο μαζί με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αποκωδικοποιεί το μήνυμα με το ιδιωτικό του κλειδί και διαχωρίζει το μήνυμα από την ψηφιακή υπογραφή. Τέλος, ο παραλήπτης αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και εφόσον αποκωδικοποιηθεί σωστά, τότε πιστοποιείται η ταυτότητα του αποστολέα.

3.5.3 Συνάρτηση Ταξινόμησης Μηνύματος(**One Way Hashes**)

Οι συναρτήσεις ταξινόμησης του μηνύματος παρέχουν ένα πραγματικά αξιόπιστο έλεγχο της ακεραιότητας του μηνύματος. Αυτές επιδίδονται στο να τεμαχίζουν το απλό κείμενο σε μικρά κομμάτια και το μετατρέπουν σε μια μορφή που δείχνει τυχαία. Τα μικρά αυτά κομμάτια του αρχικού μηνύματος, έχουν σταθερό μήκος και ονομάζονται hashes. Εξαιτίας του μικρού μήκους των hashes, η συνολική πληροφορία του μηνύματος χάνεται καθώς δεν υπάρχει τρόπος αποκωδικοποίησης του ενός hash. Η ταξινόμηση του μηνύματος λειτουργεί σαν ψηφιακό δακτυλικό αποτύπωμα για το αρχικό μήνυμα, καθώς μια μικρή αλλαγή του απλού κειμένου συνεπάγεται την πλήρη μεταβολή της ταξινόμησής του. Η λειτουργία των συναρτήσεων ταξινόμησης είναι η εξής: Η εκτέλεση της συνάρτησης ταξινόμησης για ένα μήνυμα θα δημιουργήσει το hash αυτού του μηνύματος, το hash υπογράφεται με το ιδιωτικό κλειδί του αποστολέα και στην συνέχεια το hash και το αρχικό μήνυμα στέλνεται στον παραλήπτη. Τέλος ο παραλήπτης αποκωδικοποιεί το hash χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα και συγκρίνει τα αποτελέσματα με αυτό που προκύπτει από την εκτέλεση της συνάρτησης ταξινόμησης για το παραπάνω μήνυμα, αν τα δύο αποτελέσματα είναι ίδια, τότε ο παραλήπτης επικυρώνει την ταυτότητα του αποστολέα αλλά και την αυθεντικότητα του μηνύματος. Τέτοιες συναρτήσεις είναι Sha & MD5

3.5.4 Ψηφιακοί φάκελοι **(Digital Envelopes)**

Η κρυπτογράφηση δημοσίου κλειδιού είναι ιδανική για την ασφαλή ανταλλαγή μηνυμάτων μέσω Διαδικτύου, όμως τα μειονεκτήματα της μικρής ταχύτητας εκτέλεσης των απαραίτητων αλγορίθμων σε σχέση με αυτή των συμμετρικών αλγόριθμων, καθιστά την ασύμμετρη κρυπτογράφηση ακατάλληλη για την μεταφορά μεγάλων μηνυμάτων. Η λύση στο πρόβλημα

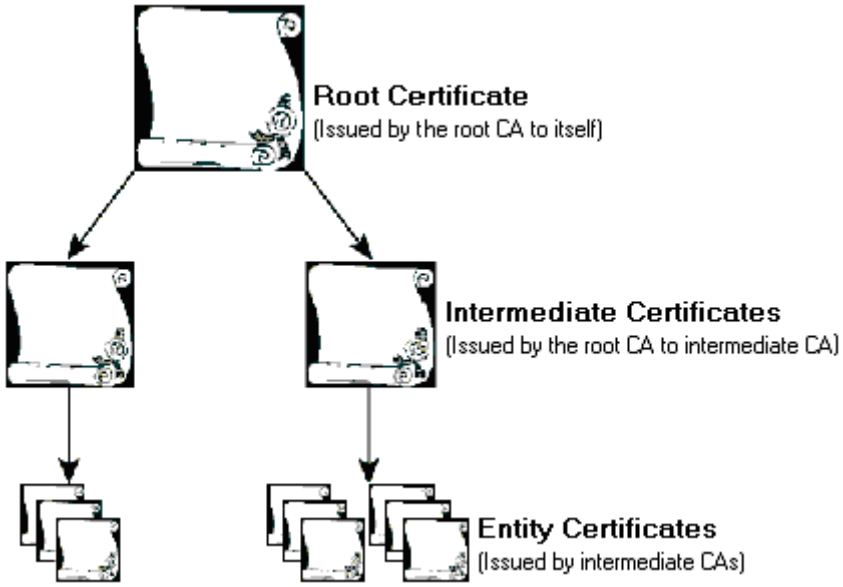
αυτό είναι ο ψηφιακός φάκελος ο οποίος συνδυάζει τα δύο συστήματα κρυπτογράφησης προκειμένου να χρησιμοποιηθούν τα καλύτερα χαρακτηριστικά τους. Το σύστημα φακέλου χρησιμοποιείται για την εγκατάσταση διπλής επικοινωνίας. Ο αποστολέας προκειμένου να εκμεταλλευτεί αυτό το σύστημα, πρέπει αρχικά να παράγει ένα τυχαίο μυστικό κλειδί το οποίο ονομάζεται session key γιατί απορρίπτεται μετά το πέρας της επικοινωνίας του αποστολέα και του παραλήπτη. Στην συνέχεια το μήνυμα κρυπτογραφείται με την βοήθεια του session Key και του συμμετρικού αλγόριθμου. Το Session Key κωδικοποιείται με το δημόσιο κλειδί του παραλήπτη μορφοποιώντας τον ψηφιακό φάκελο. Ο αποστολέας προωθεί στον παραλήπτη το κρυπτογραφημένο μήνυμα και τον ψηφιακό φάκελο. Ο παραλήπτης με την σειρά του χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το ψηφιακό και να αποκτήσει το Session Key, με την βοήθεια του οποίου αποκωδικοποιείται το μήνυμα. Τελικά, τόσο το μήνυμα, όσο και το Session Key είναι ασφαλή, αφού το μήνυμα κρυπτογραφήθηκε με το συμμετρικό Session Key, που το γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης, ενώ το Session Key κρυπτογραφήθηκε με την βοήθεια της μεθόδου κρυπτογράφησης του δημοσίου κλειδιού.

3.5.5 Αρχές Πιστοποίησης **(Certifying Aythorities –CA)**

Η λειτουργία της κρυπτογράφησης του δημοσίου, στηρίζεται στην αρχή ότι ο αποστολέας ενός μηνύματος έχει στην κατοχή του το δημόσιο κλειδί του παραλήπτη. Σύμφωνα με την αρχή αυτή, ο κάθε χρήστης του Διαδικτύου θα έπρεπε να έχει στον σκληρό δίσκο του υπολογιστή του τα δημόσια κλειδιά των χιλιάδων ιστοσελίδων που έχει επισκεφθεί, ώστε να μπορεί να επικοινωνεί μαζί τους με ασφάλεια. Στην πραγματικότητα δεν συμβαίνει αυτό, γιατί όλος αυτός ο μηχανισμός στηρίζεται στις έμπιστες οντότητες, που ονομάζονται αρχές πιστοποίησης. Οι αρχές πιστοποίησης είναι εμπορικοί οργανισμοί που έχουν σαν κύριο μέλημά τους την επικύρωση της

ταυτότητας των χρηστών του Διαδικτύου, αλλά και των ψηφιακών καταστημάτων. Η συμμετοχή τους στο σύστημα είναι σημαντική, καθώς ο χρήστης δεν χρειάζεται να κατέχει τα δημόσια κλειδιά όλων των δικτυακών τόπων, παρά μόνο των λίγων και γνωστών αρχών πιστοποίησης. Επομένως κάθε ψηφιακό κατάστημα ή ιστοσελίδα μπορεί να διαθέτει ένα ψηφιακό πιστοποιητικό, που έχει εκδοθεί από μια αρχή πιστοποίησης και μέσω αυτής επιβεβαιώνουν την αυθεντικότητά τους και διανέμουν το δημόσιο κλειδί τους. Η δημιουργία ενός πιστοποιητικού για ένα ψηφιακό κατάστημα έχει ως εξής: Το ψηφιακό κατάστημα ένα ζευγάρι ιδιωτικού και δημοσίου κλειδιού, στέλνει το δημόσιο κλειδί σε μία αρχή πιστοποίησης μαζί με τις απαραίτητες πληροφορίες και την ταυτότητα του ψηφιακού καταστήματος. Η αρχή πιστοποίησης θα εξακριβώσει τις πληροφορίες και την ταυτότητα του ψηφιακού καταστήματος. Αφού επιβεβαιωθούν οι πληροφορίες, η αρχή πιστοποίησης θα εκδώσει ένα πιστοποιητικό που θα περιέχει το δημόσιο κλειδί μαζί με τις πληροφορίες πιστοποίησης, την ηλεκτρονική διεύθυνση, την διεύθυνση ηλεκτρονικών μηνυμάτων, το λογότυπο του ψηφιακού καταστήματος και την χρονική διάρκεια ισχύος του πιστοποιητικού. Η αρχή πιστοποίησης δημιουργεί ένα μήνυμα που περιέχει το πιστοποιητικό και αφού εκτελέσει την δική της συνάρτηση ταξινόμησης, υπογράφει κάθε hash με το ιδιωτικό της κλειδί και στέλνει το μήνυμα αυτό στο ψηφιακό κατάστημα. Ο κάθε πελάτης που ζητά το πιστοποιητικό του ψηφιακού καταστήματος αποκωδικοποιεί το hash με το γνωστό δημόσιο κλειδί της αρχής πιστοποίησης για να εξακριβώσει την ταυτότητα του ψηφιακού καταστήματος. Οι αρχές πιστοποίησης έχουν δεδομένη ιεραρχία(σχήμα 3.4), όπου στην κορυφή της πυραμίδας βρίσκονται οι root CA’s απ’ όπου παίρνουν τα πιστοποιητικά τους και το δικαίωμα έκδοσής τους οι υπόλοιπες CA’s της πυραμίδας.

Σχήμα 3.4 Ιεραρχική Πυραμίδα



3.5.6 Αρχές Έκδοσης Εγγράφων (Registration Authorities – RA)

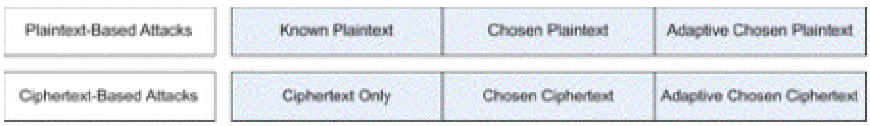
Οι αρχές έκδοσης εγγράφων είναι εταιρίες διαφορετικές από τις CA, που εγγράφουν ή ορίζουν χρήστες στο PKI. Με άλλα λόγια οι RA είναι ένας ενδιάμεσος που λαμβάνει την αίτηση για τα πιστοποιητικά από τον χρήστη, κάνει την νομική δουλειά πιστοποιώντας την ταυτότητα του χρήστη, και μετά έρχεται σε επαφή με την CA. Η RA δεν μπορεί να δώσει ψηφιακές υπογραφές. Υπάρχουν αρκετά καλοί λόγοι για να χρησιμοποιήσει κάποιος την RA. Ένα πλεονέκτημα της RA είναι ότι οι ενέργειες της αίτησης και της πιστοποίησης της ταυτότητας μπορούν να διαχωριστούν τελείως από τις ενέργειες που δίνουν το πιστοποιητικό. Πρόκειται δηλαδή για ένα επιπλέον βήμα ασφάλειας που διαχωρίζει τις ιδιωτικές πληροφορίες από το ιδιωτικό πιστοποιητικό. Τέλος απελευθερώνεται χρόνος από την CA έτσι ώστε να επικεντρωθεί σε άλλα θέματα από όπως την διαχείριση του PKI.

3.6 Πως Μπορεί να Σπάσει η Κρυπτογραφία

Οι κρυπτογραφικές επιθέσεις έχουν ως σκοπό να υπονομεύσουν την ασφάλεια των κρυπτογραφικών αλγορίθμων, και χρησιμοποιούνται για να προσπαθήσουν να αποκρυπτογραφήσουν τα στοιχεία χωρίς προγενέστερη 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.

Κρυπτογραφικές μέθοδοι επίθεσης

Υπάρχουν έξι(6) σχετικές κρυπτογραφικές μέθοδοι επίθεσης, οι τρεις βασίζονται στην μέθοδο του plaintext και οι άλλες τρεις στου Ciphertext



I. Known Plaintext and Ciphertext only Attacks

Μια γνωστή plaintext επίθεση είναι μια επίθεση όπου κάποιος έχει πρόσβαση σε ένα plaintext και στο αντίστοιχο cipherText και επιδιώκει να ανακαλύψει έναν συσχετισμό μεταξύ των δύο.

Μια known Ciphertext Attack είναι μια επίθεση όπου κάποιος έχει πρόσβαση σε ένα CipherText αλλά δεν έχει πρόσβαση στην αντιστοιχία plaintext. Με απλά ciphers, όπως Cipher Caesar, ή η ανάλυση συχνότητας μπορεί να χρησιμοποιηθεί για να σπάσει cipher.

II. Chosen plaintext and Chosen CipherText Attacks

Μια επιλεγμένη Plaintext Attack είναι μια επίθεση όπου ο κρυπταναλυτής κρυπτογραφεί ένα Plaintext της επιλογής του και μελετάει τα αποτελέσματα του CipherText. Είναι η πιο κοινή επίθεση ενάντια στα ασύμμετρα κρυπτογραφικά συστήματα όπου ο κρυπταναλυτής έχει πρόσβαση στο δημόσιο κλειδί.

Μια επιλεγμένη CipherText επίθεση είναι μια επίθεση όπου ο κρυπταναλυτής επιλέγει ένα CipherText και προσπαθεί να βρει το αντίστοιχό του Plaintext. Αυτό μπορεί να γίνει με μια μηχανή αποκρυπτογράφησης η οποία αποκρυπτογραφεί χωρίς έκθεση του κλειδιού. Αυτό συνήθως χρησιμοποιείται σε επιθέσεις δημοσίου κλειδιού.

III. Adaptive Chosen PlainText and Adaptive Chosen CipherText Attacks

Και στις δύο προσαρμοστικές επιθέσεις ένας κρυπταναλυτής επιλέγει τα περαιτέρω PlainText και CipherText (προσαρμόζει την επίθεση) βασισμένα στα προγενέστερα αποτελέσματα.

3.6.1 Επιθέσεις σε Αλγόριθμους Συμμετρικού Κλειδιού

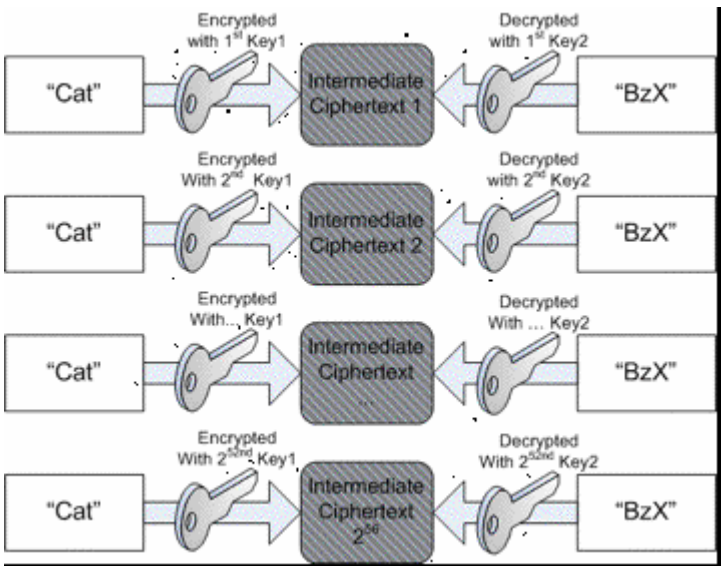
Brute Force Attacks (Επιθέσεις Ωμής Βίας)

Μια επίθεση ωμής βίας χρησιμοποιεί συστηματικά κάθε πιθανό κλειδί. Λαμβάνοντας υπόψη ένα πεπερασμένο βασικό μήκος κλειδιού και ένα αρκετό χρόνο, μία επίθεση ωμής βίας είναι πάντα επιτυχής. Οι αλγόριθμοι κρυπτογράφησης μπορούν να γίνουν ευαίσθητοι στις επιθέσεις ωμής βίας με την πάροδο του χρόνου καθώς οι ταχύτητες CPU αυξάνονται. Αλγόριθμοι όπως ο DES παρά το 56 bit μήκος κλειδιού που χρησιμοποιεί μπορεί να παραβιαστεί εντός ημερών χρησιμοποιώντας ένα ειδικό Hardware όπως αυτό της Electronic Frontier Foundation's το Deep Crack. Ο Triple Des (168 bit) ο οποίος αναπτύχθηκε λόγω της αδυναμίας του DES σε Brute Force Επιθέσεις και στην

συνέχεια ακολούθησε ο AES, αν υποθέσουμε ότι ένα μηχάνημα θα μπορούσε να σπάσει ένα κλειδί του DES το δευτερόλεπτο θα του έπαιρνε 149 τρισεκατομμύρια χρόνια να σπάσει έναν AES 128 bit.

Meet-in-the-Middle Attack

Τέτοιου είδους επιθέσεις χρησιμοποιούνται σε κρυπτογραφικούς αλγόριθμους οι οποίοι χρησιμοποιούν πολλαπλά κλειδιά για κρυπτογράφηση όπως ο διπλός DES (112bit). Αυτού του είδους η επίθεση είναι μια επίθεση Known PlainText, δηλαδή έχουμε πρόσβαση στο PlainText αλλά και στο CipherText. Ας υποθέσουμε ότι έχουμε το PlainText Cat και το CipherText είναι Bxz. Θέλουμε να ανακτήσουμε και τα δύο κλειδιά που χρησιμοποιεί ο διπλός DES (112 bit). Ο Cracker μας αρχικά χρησιμοποιεί μια Brute Force Attack στο κλειδί1 δοκιμάζοντας 2^{56} διαφορετικά κλειδιά DES(56 bit) για να κρυπτογραφήσει το PlainText Cat και σώζει το κάθε κλειδί και το ενδιάμεσο CipherText σε έναν πίνακα. Στην συνέχεια χρησιμοποιείται η ίδια μέθοδος για το κλειδί2 για να αποκρυπτογραφήσει το CipherText.



Όταν η δεύτερη Brute Force Attack αποκρυπτογραφήσει ένα ενδιάμεσο CipherText το οποίο είναι ήδη στον πίνακα τότε η επίθεση έχει ολοκληρωθεί και τα κλειδιά είναι γνωστά. Λόγω της αυτής της επίθεσης ο Double DES δεν χρησιμοποιείται ευρέως.

Το«σπάσιμο»τουDES

Ένας διαγωνισμός που εμφανίζεται τακτικά στο Internet αφορά το σπάσιμο ενός κρυπτογραφημένου μηνύματος σε χρόνο ρεκόρ. Το 1999 μια ομάδα ερευνητών και χρηστών υπολογιστών αποκρυπτογράφησε ένα μήνυμα κωδικοποιημένο σε τον DES σε 22 ώρες χρησιμοποιώντας 100000 υπολογιστές σε όλο τον κόσμο. Η υπολογιστική εργασία που χρειάστηκε για να σπάσει ο κώδικας κατανεμήθηκε σε όλους αυτούς τους υπολογιστές και συντονίστηκε από κάποιους άλλους υπολογιστές. Αυτή η μορφή μαζικής κατανεμημένης επεξεργασίας διαδίδεται όλο και περισσότερο στο Internet. Για παράδειγμα, υπάρχει ένα σύστημα το οποίο χρησιμοποιεί τον αδρανή χρόνο υπολογιστών σε όλο τον κόσμο για να αναλύσει ραδιοκύματα από το διάστημα, ενώ υπάρχει και ένα άλλο σύστημα για τον υπολογισμό του π με ένα πολύ μεγάλο αριθμό δεκαδικών ψηφίων.

3.6.2 Επιθέσεις σε Αλγόριθμους Δημοσίου Κλειδιού

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού. Η πρώτη είναι επίθεση με δεδομένα (**factoring attack)**. Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται. Για παράδειγμα, ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το knapsack. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.

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

ΚΕΦΑΛΑΙΟ 4^{Ο} ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ

4.1 Mime-S/Mime

Το e-mail αρχικά ήταν σχεδιασμένο έτσι ώστε να στέλνονται με αυτό μόνο μηνύματα κειμένου. Με λίγα λόγια ήταν αδύνατη η μεταφορά ενός αρχείου Π.χ σε δυαδική μορφή μέσω e-mail. Αρχικά είχαν επινοηθεί διάφορες μέθοδοι ώστε να μπορούν αποστέλλονται διάφορα είδη αρχείων. Οι μέθοδοι αυτοί κωδικοποιούσαν τα δεδομένα σε μορφή κειμένου και έτσι μπορούσαν να σταλούν μέσω του ηλεκτρονικού ταχυδρομείου. Το 1992 όμως η Internet Engineering Task Force (IEFT) επινόησε το Multipurpose Internet Extensions (mime) το οποίο είχε σαν σκοπό την ενοποίηση και τον συντονισμό όλων των προηγούμενων μεθόδων. Το mime δεν υπαγορεύει ένα και μοναδικό πρότυπο για την κωδικοποίηση των δεδομένων αλλά επιτρέπει στους χρήστες του να χρησιμοποιήσουν την κωδικοποίηση που επιθυμούν αυτοί. Το mime όμως δεν παρέχει κάποιο είδος ασφαλείας, έτσι έχει επινοηθεί το s/mime (secure mime), το οποίο, θα μπορούσαμε να πούμε ότι καλύπτει το κενό αυτό της ασφάλειας. Το s/mime χρησιμοποιεί ασύμμετρη κρυπτογραφία κατά την μεταφορά των αρχείων. Έτσι κάποιος που θέλει να στείλει ένα μήνυμα χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει τα δεδομένα και τα αποστέλλει στον κατάλληλο εξυπηρετητή. Για να ανακτηθεί το plaintext τα δεδομένα αποκρυπτογραφούνται στον e-mail server ή στον e-mail client.

- Αποκρυπτογράφηση στον **e-mail client**. Την δεδομένη στιγμή δεν υπάρχουν πολλοί e-mail clients που να υποστηρίζουν αποκρυπτογράφηση με το σύστημα s/mime, αλλά στην περίπτωση που αυτή είναι εφικτή μπορούν να προκύψουν διάφορα προβλήματα. Για παράδειγμα μπορεί να χρειαστεί ένας e-mail client να αλλάξεις το μέλλον το ζεύγος των

κλειδιών του. Το πρόβλημα που προκύπτει σε αυτήν την περίπτωση είναι ότι 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.

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

4.2 Pretty Good Privacy (**PGP**)

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Είναι πολύ σημαντικό να γίνεται σωστή επιλογή του προϊόντος που θα χρησιμοποιηθεί. Υπάρχουν προγράμματα που είτε δεν χρησιμοποιούν αρκετά ασφαλείς αλγόριθμους είτε δημιουργούν σφάλματα (bugs) στην υλοποίηση της κρυπτογράφησης. Επίσης, θα πρέπει η τεχνική κρυπτογράφησης να ελέγχεται από ειδικούς, ενώ οι μέθοδοι πρέπει να είναι γνωστές και το λογισμικό που τις υλοποιεί υψηλής ποιότητας. Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors). Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό αξιόπιστο.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της. Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (λογισμικό ανοιχτού/ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnupgp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του. Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντάς το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

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

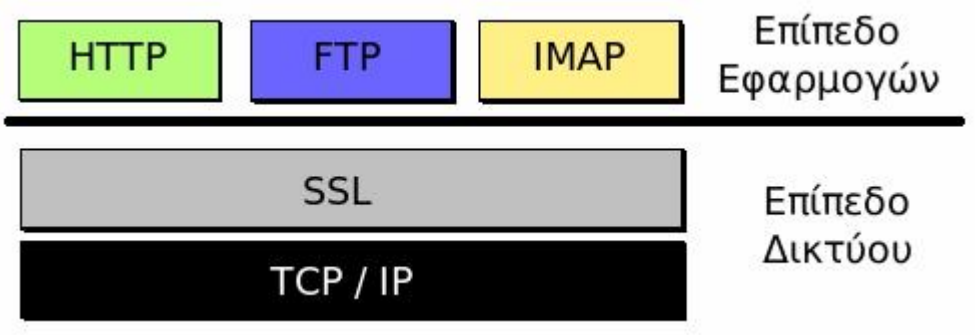
- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)

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

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

4.3 Secure Sockets Layer (**SSL**)

Το **πρωτόκολλο SSL (Secure Sockets Layer ή ασφαλές στρώμα υποδοχών)** αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. 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. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ. Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.



Σχήμα 4.1 Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: 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.

Τρόπος λειτουργίας

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει

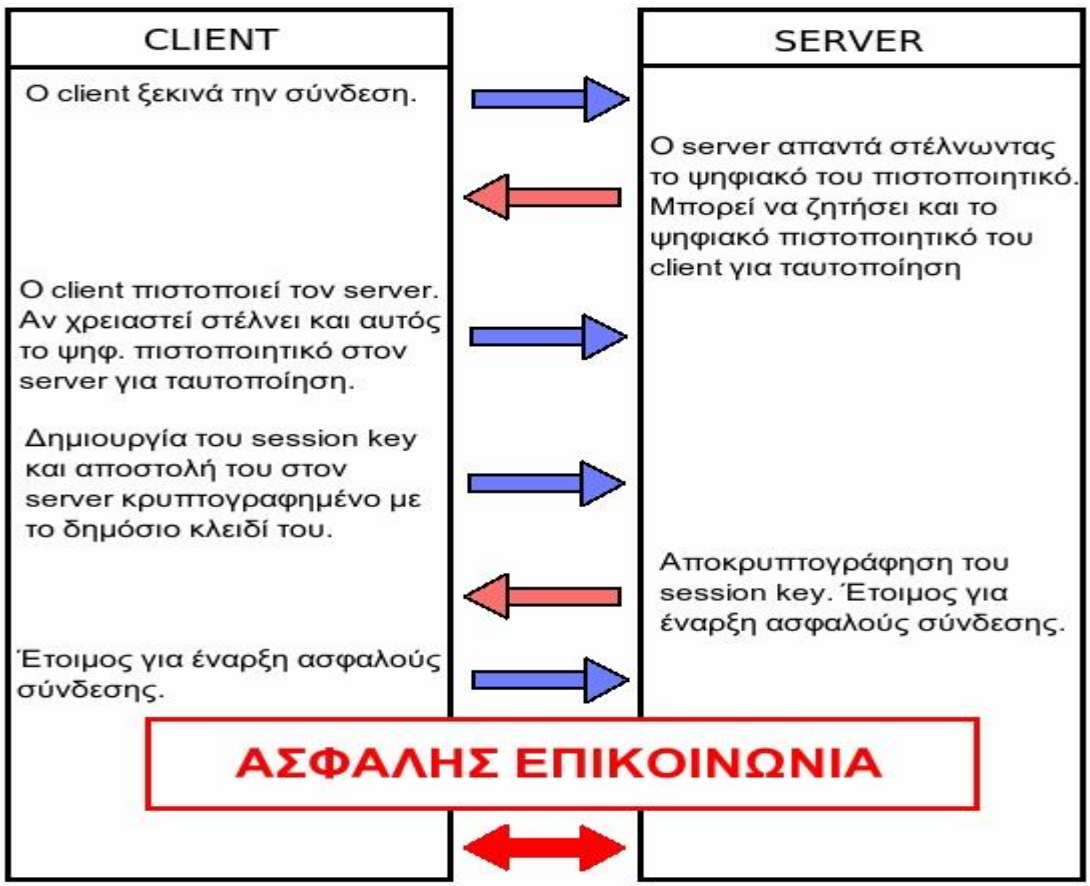
στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

I. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
II. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
III. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
IV. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που

αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.

V. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
VI. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
VII. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

Η διαδικασία της χειραψίας φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί. Σχήμα 4.2



Επιβάρυνση από το SSL

Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

- Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.
- Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

4.4 Transport Layer Security **(TLS)**

Η ασφάλεια στρώματος μεταφορών (TLS) και ο προκάτοχός της, SSL, είναι κρυπτογραφικά πρωτόκολλα που παρέχουν τις ασφαλείς ανακοινώσεις σχετικά με το διαδίκτυο για τέτοια πράγματα όπως το ξεφύλλισμα Ιστού, το ηλεκτρονικό ταχυδρομείο, την 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 μέσω ένα δίκτυο με σκοπό με τέτοιο τρόπο

ώστε να αποτρέψει να κρυφακούσει κάποιος, να πειράξει, και να παραποιήσει μηνύματα. Το TLS παρέχει την επικύρωση σημείου τέλους και την ιδιωτικότητα επικοινωνιών μέσω του Διαδικτύου χρησιμοποιώντας την κρυπτογραφία. Χαρακτηριστικά, μόνο ο κεντρικός υπολογιστής επικυρώνεται (δηλ., η ταυτότητά της εξασφαλίζεται) ενώ ο πελάτης όχι, αυτό σημαίνει ότι ο τελικός χρήστης (είτε ένα άτομο είτε μια εφαρμογή, όπως μια μηχανή αναζήτησης Ιστού) μπορεί να είναι βέβαιος με ποιους επικοινωνεί. Το επόμενο επίπεδο ασφάλειας στο οποίο και οι δύο άκρες της «συνομιλίας» είναι σίγουρες με ποιους επικοινωνούν είναι γνωστό ως αμοιβαία επικύρωση. Η αμοιβαία επικύρωση απαιτεί κρυπτογράφηση δημοσίου κλειδιού (PKI) στους πελάτες εκτός αν 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.

TLS περιλαμβάνει τρεις βασικές φάσεις:

1. Διαπραγμάτευση χρηστών για την υποστήριξη αλγορίθμου
2. Ανταλλαγή κλειδιών και επικύρωση
3. Συμμετρικές cipher κρυπτογράφησης και επικύρωση μηνυμάτων

Κατά τη διάρκεια της πρώτης φάσης, ο πελάτης και ο κεντρικός υπολογιστής 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.

Οι αλγόριθμοι που χρησιμοποιούνται είναι:

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

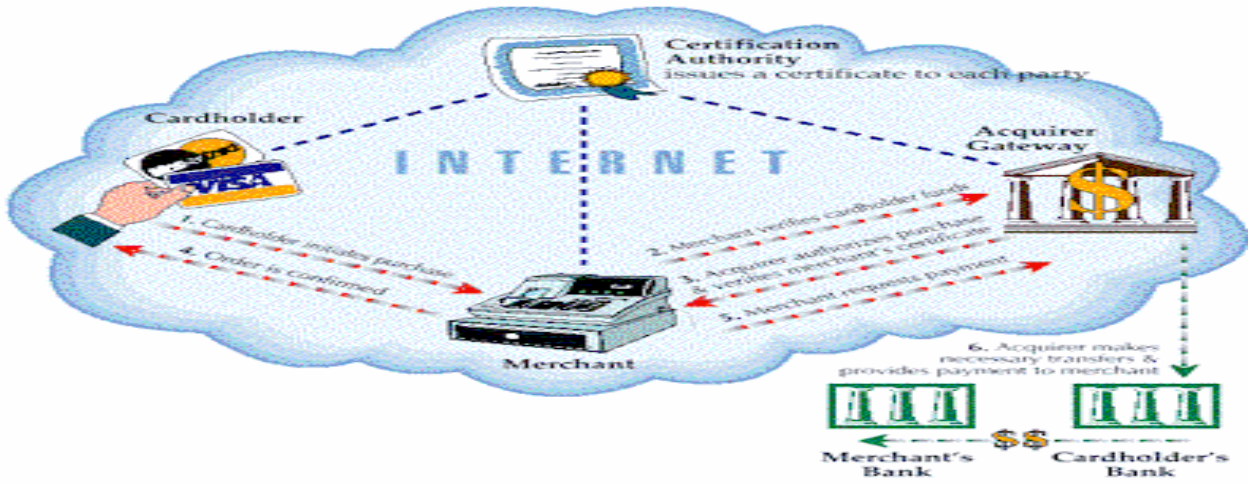
4.5 Secure Electronic Transactions (**SET**)

Το SET (Secure Electronic Transactions ή ασφαλείς ηλεκτρονικές συναλλαγές) είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών σε ανοικτά δίκτυα, το οποίο 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 το οποίο είναι ένα σύστημα κρυπτογραφίας γενικού σκοπού, το SET χρησιμοποιείται για την διενέργεια μόνο χρεωστικών και πιστωτικών συναλλαγών καρτών μεταξύ εμπόρων και πελατών. Το SET παρέχει Πιστοποίηση, Μη άρνηση αποδοχής, Εμπιστευτικότητα και Ακεραιότητα.

Τρόπος λειτουργίας

Το SET χρησιμοποιεί τον ασφαλή αλγόριθμο κατακερματισμού (SHA) ο οποίος 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 επίσης κρυπτογραφεί τις πληροφορίες που αφορούν την παραγγελία με την χρήση ενός τυχαίου συμμετρικού κλειδιού συνόδου και τις «πακετάρει» σε ένα ψηφιακό φάκελο χρησιμοποιώντας το δημόσιο κλειδί του εμπόρου. Οι πληροφορίες που αφορούν την πληρωμή της παραγγελίας (αριθμός πιστωτικής κάρτας του πελάτη και πληροφορίες της τράπεζας) κρυπτογραφούνται παρόμοια αλλά σε 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, ενώ ταυτόχρονα 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.



Σχήμα 4.3 Τρόπος λειτουργίας SET

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.

4.6 Private Communication Technology (**PCT**)

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

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

4.7 Secure Hyper-Text Transfer Protocol (HTTPS)

Το **HTTPS** *(Secure HTTP)* χρησιμοποιείται στην επιστήμη των υπολογιστών για να δηλώσει μία ασφαλή http σύνδεση. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα (443 αντί 80) και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες (πχ αριθμοί πιστωτικών καρτών, passwords κοκ)

Τρόπος λειτουργίας

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αναφέρεται στον συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle. Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Σε servers που χρησιμοποιούν το

λειτουργικό σύστημα UNIX αυτό μπορεί να γίνει μέσω του προγράμματος OpenSSL. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.

Εφαρμογές

Όπως αναφέρθηκε προηγουμένως, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας που περιγράφηκε στην προηγούμενη ενότητα και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται. Πολλοί χρήστες πιστωτικών καρτών θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση. Αυτό όμως δεν ισχύει: Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον server. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον server χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι χάκερ να έχουν επιτεθεί στον server και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

4.8 Domain Name System Security (DNSSEC)

Το DNS αναπτύχθηκε πολύ πριν φανταστεί κανείς τα προβλήματα ασφαλείας του Διαδικτύου που θα προέκυπταν. Λόγω του γεγονότος ότι το DNS είναι μια υπηρεσία η οποία βασίζεται στο πρωτόκολλο UDP προκύπτουν πολλά προβλήματα ασφαλείας. Σε αντίθεση με το TCP το UDP δεν διαθέτει κάποιο μηχανισμό ώστε να πιστοποιούνται οι αποστολείς των πακέτων που

λαμβάνονται. Έτσι το UDP και κατά συνέπεια το DNS μπορεί να επιτρέψει την εξαπάτηση ως προς τον 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 DNSSEC προσπαθεί με την χρήση ενός διανομέα δημοσίων κλειδιών να αποτρέψει την εξαπάτηση, ως προς τον αποστολέα, των πακέτων (source spoofing) και να εξασφαλίσει ακεραιότητα των δεδομένων. Παρόλα αυτά το DNSSEC θα μπορούσαμε να πούμε ότι δεν καλύπτει μερικά κενά ασφαλείας αφού δεν παρέχει εμπιστευτικότητα και δεν κρυπτογραφεί τα δεδομένα που μεταφέρονται μέσω του διαδικτύου.

4.9 Internet Protocol Security (IPsec)

Η ασφάλεια πρωτοκόλλου Διαδικτύου (IPsec) είναι μια ακολουθία των πρωτοκόλλων για την εξασφάλιση των επικοινωνιών πρωτοκόλλου Διαδικτύου (IP) με την επικύρωση ή/και την κρυπτογράφηση κάθε πακέτου IP σε ένα ρεύμα στοιχείων. Το IPsec περιλαμβάνει επίσης τα πρωτόκολλα για την κρυπτογραφική βασική καθιέρωση. Η υπάρχουσα έκδοση του IP πρωτοκόλλου είναι η IPv4, η οποία σχεδιάστηκε την δεκαετία του ’70. Όμως, παρά την λειτουργικότητά του στις μέρες μας προκύπτει ένα πλήθος προβλημάτων από την χρησιμοποίησή του. Έτσι το Internet Engineering Task Force (IEFT) ίδρυσε το IP Security Protocol Working Group το οποίο με την σειρά του ανέπτυξε το IPsec. Το IPsec δεν είναι από μόνο του ένα πρωτόκολλο αλλά ένα σύνολο πρωτοκόλλων με σκοπό την παροχή ασφάλειας κατά την χρησιμοποίηση του πρωτοκόλλου IP. Αν και αρχικά το IPsec προοριζόταν για το IPv6 μπορεί να χρησιμοποιηθεί και πάνω από το πρωτόκολλο IPv4.

Λειτουργία

Τα πρωτόκολλα **IPsec** λειτουργούν στο στρώμα δικτύων, στρώμα 3 του προτύπου της OSI. (Open Systems Interconnection Basic Reference Model**)** Άλλα πρωτόκολλα ασφάλειας Διαδικτύου σε διαδεδομένη χρήση, όπως η SSL, TLS και SSH, λειτουργούν από το στρώμα μεταφορών επάνω (στρώματα της OSI 4 - 7). Αυτό καθιστά IPsec πιο εύκαμπτο, δεδομένου ότι μπορεί να χρησιμοποιηθεί για την προστασία του στρώματος 4 πρωτόκολλα, και συμπεριλαμβανομένου του TCP και UDP, τα ο 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.

4.9.1 IPv4

Η έκδοση 4 πρωτοκόλλου Διαδικτύου (IPv4) είναι η τέταρτη επανάληψη του πρωτοκόλλου Διαδικτύου (IP) και είναι η πρώτη έκδοση του πρωτοκόλλου που επεκτείνεται ευρέως. Το IPv4 είναι το κυρίαρχο πρωτόκολλο στρώματος δικτύων σχετικά με το διαδίκτυο και εκτός από IPv6 είναι το μόνο τυποποιημένο πρωτόκολλο internetwork-στρώματος που χρησιμοποιείται στο διαδίκτυο. Το IPv4 είναι ένα στοιχείο-προσανατολισμένο πρωτόκολλο που χρησιμοποιείται σε ένα πακέτο - μεταστρεφόμενο internetwork (π.χ., Ethernet). Είναι ένα καλύτερο πρωτόκολλο προσπάθειας δεδομένου ότι δεν εγγυάται την παράδοση. Δεν κάνει οποιεσδήποτε εγγυήσεις στην ακρίβεια των στοιχείων αυτό μπορεί να οδηγήσει στα αναπαραχθέντα πακέτα ή τα πακέτα που παραδίδονται από τη διαταγή. Αυτές οι πτυχές εξετάζονται από ένα ανώτερο πρωτόκολλο στρώματος (π.χ. TCP, και εν μέρει από UDP). IPv4 χρησιμοποιεί 32bit διευθύνσεις το οποίο περιορίζει το διάστημα διευθύνσεων σε 4.294.967.296 (232) πιθανές μοναδικές διευθύνσεις.

4.9.2 IPv6

Σύμφωνα με υπολογισμούς το IPv4 σε μερικά χρόνια δεν θα μπορεί να καλύψει τον συνεχώς αυξανόμενο αριθμό των υπολογιστών που το χρησιμοποιούν, οπότε πρέπει να βρεθεί μια άλλη λύση ή μάλλον να επινοηθεί ένα άλλο πρωτόκολλο για την διευθυνσιοδότηση. Έτσι το (IEFT) ανέπτυξε το IPv6 το οποίο λύνει αυτό το πρόβλημα αφού χρησιμοποιεί 128 bits για την διευθυνσιοδότηση. Για να γίνει πιο κατανοητό το παραπάνω πρέπει να επισημανθεί ότι ενώ το IPv4 αδυνατεί να δώσει σε κάθε άνθρωπο στον πλανήτη μια διεύθυνση IP το IPv6 επαρκεί για να δώσει περίπου $6,7 \times 10^{17}$ IP διευθύνσεις ανά mm^2 ανά επιφάνεια της γης. Ένα άλλο σημαντικό πρόβλημα που προσπαθεί να λύσει είναι αυτό της ασφάλειας. Το IPv6 διαθέτει προαιρετική κρυπτογραφία και έλεγχο ακεραιότητας των δεδομένων, μια

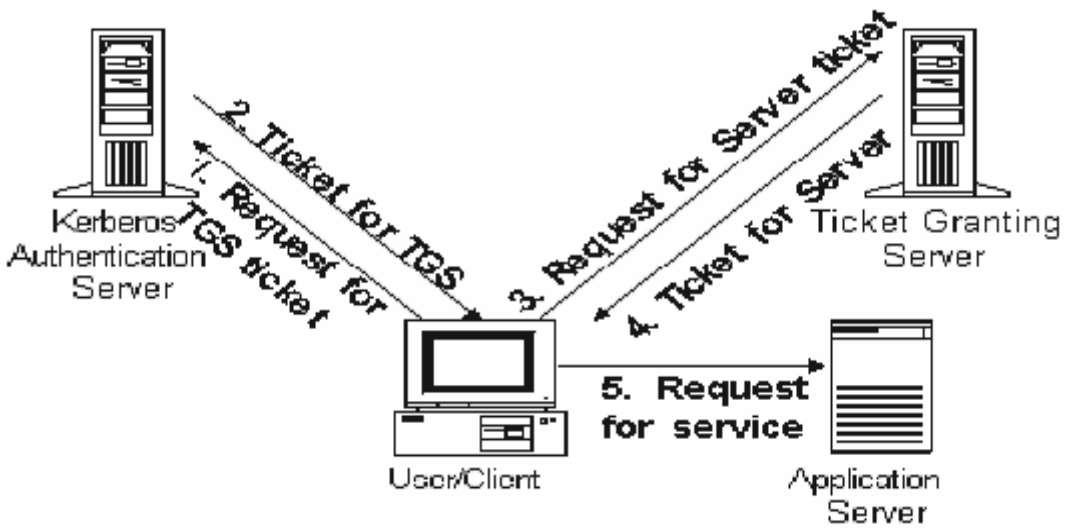
ευκολία γνωστή σαν IPsec. Οποιοσδήποτε υπολογιστής μπορεί να πιστοποιήσει τον εαυτό του και να κρυπτογραφήσει τις επικοινωνίες του. Το μοναδικό ίσως μειονέκτημα είναι ότι χρησιμοποιεί για κρυπτογράφηση ένα DES πλήθους 56 δυαδικών ψηφίων, κάτι που πολλοί θεωρούν ότι είναι ανεπαρκές για εφαρμογές υψηλής ασφάλειας.

4.10 Kerberos Authentication System

Το Kerberos σύστημα αναπτύχθηκε από το Massachusetts Institute of Technology (MIT) για να προστατέψει τις δικτυακές υπηρεσίες που παρέχονταν από το Project Athena και βασίζεται στο μοντέλο διανομής κλειδιών (key distribution model) των Needham και Schoeder. Οι εκδόσεις 1 έως 3 χρησιμοποιήθηκαν εσωτερικά από το MIT. Παρ' όλο που σχεδιάσθηκε αρχικά για χρήση με το Project Athena, η $4^{η}$ έκδοση πέτυχε παγκόσμια υιοθέτηση. Λόγω, όμως, του γεγονότος ότι πολλά περιβάλλοντα είχαν απαιτήσεις που δεν μπορούσε να καλύψει η $4^{η}$ έκδοση, νέα χαρακτηριστικά εισηγήθηκαν με την ανάπτυξη του Kerberos version 5.0 που απευθυνόταν σε περισσότερες περιπτώσεις. Η τρέχουσα έκδοση είναι η 5.0. Το Kerberos είναι ένα σύστημα πιστοποίησης ταυτότητας το οποίο αναπτύχθηκε με την ελπίδα αντικατάστασης του συστήματος που καλείται πιστοποίηση βάσει ισχυρισμού (authentication by assertion). Η πιστοποίηση βάσει ισχυρισμού στηρίζεται στην εξής αρχή: όταν ο χρήστης τρέχει ένα πρόγραμμα που απαιτεί πρόσβαση σε μία δικτυακή υπηρεσία, το πρόγραμμα ανακοινώνει στον server ότι λειτουργεί εκ μέρους του συγκεκριμένου χρήστη. Ο server πιστεύει τα στοιχεία που του παρέχει ο client (δηλαδή το πρόγραμμα) και εξυπηρετεί τον χρήστη χωρίς να ζητά άλλες αποδείξεις. Όπως καταλαβαίνουμε, η παρεχόμενη ασφάλεια είναι πολύ χαμηλού επιπέδου έως και ανύπαρκτη.

Λειτουργία

Το κέρβερος βασίζεται σε ένα εξυπηρετητή διανομής κλειδιών η αλλιώς KDS (Key Distribution Server). Ο KDS αποθηκεύει πληροφορίες σχετικά με την πιστοποίηση και τις χρησιμοποιεί για να εξασφαλίσει ασφαλή πιστοποίηση στους χρήστες (εφαρμογές) του πρωτοκόλλου Κέρβερος. Ένας χρήστης ή μια εφαρμογή (Principal) για να χρησιμοποιήσει το Κέρβερος πρέπει να επικοινωνήσει με το KDS έτσι ώστε να του δοθεί εισιτήριο. Η χρησιμότητα των εισιτηρίων είναι η παροχή πιστοποίησης μεταξύ των Principals. Όλα τα εισιτήρια ισχύουν για περιορισμένο χρονικό διάστημα και γι' αυτό πρέπει να υπάρχει ένας ασφαλής τρόπος επικοινωνίας μεταξύ του KDS και των Principals ώστε να ανανεώνονται. Η πρακτική πλευρά του Κέρβερος είναι η ενσωμάτωσή του με διάφορες εφαρμογές όπως το Ftp, Pop κτλ. Επίσης χρησιμοποιεί τους εξής αλγόριθμους: DES in CBC mode σε συνδυασμό με τους CRC-32, MD4, MD5.



Αδυναμίες

Το Kerberos δεν έχει την δυνατότητα να προστατέψει ένα δίκτυο από κάθε είδους απειλή. Λειτουργεί βάσει συγκεκριμένων υποθέσεων όσον αναφορά την υποκείμενη δικτυακή δομή.

1. Επιθέσεις του τύπου άρνησης εξυπηρέτησης (denial of service attack) δεν μπορούν να αντιμετωπιστούν με το Kerberos. Ένας εισβολέας μπορεί εκμεταλλευόμενος τις αδυναμίες του συστήματος να αποτρέψει έναν server από το να συμμετέχει στα κανονικά βήματα πιστοποίησης. Η ανίχνευση και η επιδιόρθωση τέτοιων καταστάσεων αφήνεται στα χέρια των διαχειριστών και των χρηστών.
2. Οι χρήστες πρέπει να κρατούν τους κωδικούς τους μυστικούς. Το Kerberos δεν είναι σε θέση να προστατέψει το δίκτυο από ασυνείδητους χρήστες που μοιράζουν τους κωδικούς τους ή που δεν είναι αρκετά προσεκτικοί για να τον κρατήσουν κρυφό.
3. Επιθέσεις που βασίζονται στην πρόβλεψη εύκολων κωδικών (password guessing attack) δεν αντιμετωπίζονται από τον Kerberos. Ένας εισβολέας με χρήση ενός λεξικού, μπορεί εύκολα να "σπάσει" μικρούς και εύκολους κωδικούς που αποτελούνται από λέξεις που μπορούν να βρεθούν σε λεξικό.
4. Κάθε μηχανή του δικτύου πρέπει να έχει ένα καλά ρυθμισμένο ρολόι. Μηχανές με ρυθμίσεις ώρας που διαφέρουν σημαντικά (πάνω από 5 λεπτά)μπορεί να δημιουργήσουν πρόβλημα στην πιστοποίηση των timestamps που εμπεριέχονται στα μηνύματα. Έτσι, ένας εισβολέας εκμεταλλευόμενος αυτή την αδυναμία μπορεί να πραγματοποιήσει επίθεση επανάληψης (replay attack). Ή ακόμα βρίσκοντας τον απαραίτητο χρόνο, να σπάσει αδύναμους κωδικούς χρηστών.

ΚΕΦΑΛΑΙΟ 5^{Ο} ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Στο πρόσφατο παρελθόν οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα ο πωλήσεις των εμπόρων γίνονταν με καθαρά συμβατικά μέσα. Οι καταναλωτές προκειμένου να αγοράσουν αυτό που επιθυμούσαν ή να δεχτούν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά. Ένας από τους νέους και τάχιστους τρόπους εξυπηρέτησης των καταναλωτών είναι το Ηλεκτρονικό Εμπόριο το οποίο αναπτύσσεται ραγδαία στο εξωτερικό αλλά και στην Ελλάδα με πιο αργούς όμως ρυθμούς. Ενδεικτικό της καθυστερημένης ανάπτυξης του ηλεκτρονικού εμπορίου στην Ελλάδα είναι οι δύο υπουργικές αποφάσεις 3035/Β2-48.2001 και 7681/Β2-255.2001 που προωθούν τη διενέργεια δοκιμαστικής έρευνας για το ηλεκτρονικό εμπόριο. Οι αποφάσεις αυτές είναι του 2001, χρονιά που σε άλλες ευρωπαϊκές χώρες ανθούσε το ηλεκτρονικό εμπόριο. Αλλά και οι υπουργικές αποφάσεις 4708/2003, 36/2003 και 10220/Γ3-571/2004 που καταδεικνύουν το ίδιο πράγμα.

5.1Ορισμός Ηλεκτρονικού Εμπορίου

Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. Το ηλεκτρονικό εμπόριο αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως (ΠΔ 39.2001). Ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών. Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και φαξ. Το ηλεκτρονικό εμπόριο διακρίνεται σε έμμεσο και άμεσο. Ο πρώτος όρος

χρησιμοποιείται όταν πρόκειται για την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο. Μέσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών.

5.2 Ιστορία Ηλεκτρονικού Εμπορίου

Δεκαετία του 1970

Εμφανίζονται τα συστήματα ηλεκτρονικής μεταφοράς χρηματικών πόρων (EFT-Emotional Freedom Techniques) μεταξύ τραπεζών, που χρησιμοποιούν ασφαλή ιδιωτικά δίκτυα. Τα συστήματα EFT αλλάζουν τη μορφή των αγορών.

Δεκαετία του 1980

Οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονται στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα EDI-Electronic Data Interchange και ηλεκτρονικό ταχυδρομείο) αποκτούν σημαντική διάδοση. Πολλές δραστηριότητες, που παραδοσιακά διεκπεραιώνονταν με βασικό μέσο το χαρτί, μπορούν πλέον να γίνουν ταχύτερα και με μικρότερο κόστος. Οι συναλλαγές, που παλαιότερα απαιτούσαν έντυπα, όπως παραγγελίες αγοράς, συνοδευτικά έγγραφα και επιταγές πληρωμής, μπορούν να γίνουν κατά ένα μέρος ή στο σύνολό τους ηλεκτρονικά - με δομημένο τρόπο χάρη στα συστήματα EDI ή μέσω του ηλεκτρονικού ταχυδρομείου.

Τέλη της δεκαετίας του 1980 - αρχές της δεκαετίας του 1990

Τα ηλεκτρονικά δίκτυα προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας, με δυνατότητες όπως ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονική διάσκεψη (conferencing) και ηλεκτρονική συνομιλία (IRC), ομάδες συζήτησης (newsgroups, forums), μεταφορά αρχείων (FTP) κτλ. Η πρόσβαση στο δίκτυο γίνεται φθηνότερη λόγω της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών.

Μέσα της δεκαετίας του 1990

Η εμφάνιση του Παγκόσμιου Ιστού (WWW) στο Internet και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) που χρησιμοποιούν λειτουργικά συστήματα τύπου Windows, προσφέρουν μεγάλη ευκολία χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο Διαδίκτυο. Το ηλεκτρονικό εμπόριο γίνεται ένας πολύ φθηνότερος τρόπος για την πραγματοποίηση μεγάλου όγκου συναλλαγών, ενώ συγχρόνως διευκολύνει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων, επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις.

Τέλη της δεκαετίας του 1990

Η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η σχετική προσαρμογή της νομοθεσίας στους τομείς των εισαγωγών-εξαγωγών και των επικοινωνιών, καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών.

5.3 Νομοθεσία Ηλεκτρονικού Εμπορίου

1. Σύμβαση από απόσταση, με την έννοια αυτού του άρθρου, είναι σύμβαση που αφορά αγαθό ή υπηρεσία και συνάπτεται ύστερα από πρόταση του προμηθευτή χωρίς ταυτόχρονη φυσική παρουσία του προμηθευτή και του καταναλωτή, με τη χρησιμοποίηση τεχνικής επικοινωνίας από απόσταση για τη διαβίβαση της πρότασης για σύναψη σύμβασης και της αποδοχής.

2. Σύμβαση από απόσταση είναι άκυρη υπέρ του καταναλωτή, αν κατά την πρόταση σύναψης σύμβασης ο καταναλωτής δεν ενημερώθηκε με τα μέσα της χρησιμοποιούμενης τεχνικής επικοινωνίας κατά τρόπο σαφή για τα ακόλουθα ιδίως στοιχεία:

α) την ταυτότητα του προμηθευτή,

β) τα ουσιώδη χαρακτηριστικά του αγαθού ή της υπηρεσίας,
γ) την τιμή, την ποσότητα και τις δαπάνες μεταφοράς, καθώς και το φόρο προστιθέμενης αξίας, εφόσον δεν περιλαμβάνεται στην τιμή,
δ) τον τρόπο πληρωμής, παράδοσης και εκτέλεσης,
ε) τη διάρκεια ισχύος της πρότασης για σύναψη σύμβασης και
στ) το δικαίωμα υπαναχώρησης.

3. Ο καταναλωτής δεν επιβαρύνεται για τις δαπάνες της επικοινωνίας από απόσταση για τη διαβίβαση της αποδοχής ή για την εκτέλεση της υπηρεσίας, εκτός αν αυτό αναφέρεται σαφώς στην πρόταση για σύναψη σύμβασης.

4. Απαγορεύεται να αποστέλλονται στον καταναλωτή αγαθά ή να παρέχονται υπηρεσίες χωρίς προηγούμενη παραγγελία εκ μέρους του όταν αυτός καλείται να τα αποκτήσει έναντι πληρωμής ή να τα επιστρέψει, έστω και χωρίς να καταβάλλει τις δαπάνες αποστολής. Αν η αποστολή αυτή πραγματοποιηθεί, ο καταναλωτής έχει το δικαίωμα να διαθέσει το αγαθό ή την υπηρεσία, κατά την κρίση του, χωρίς να οφείλει οποιοδήποτε τίμημα, εκτός αν η αποστολή οφείλεται σε προφανές λάθος, οπότε το θέτει, για εύλογο χρόνο και εφόσον η φύση του αγαθού ή της υπηρεσίας το επιτρέπει, στη διάθεση του προμηθευτή. Η παράληψη απάντησης δεν ισοδυναμεί σε καμία περίπτωση με συναίνεση.

5. Οι διατάξεις της προηγούμενης παραγράφου δεν εφαρμόζονται όταν ο προμηθευτής αδυνατεί να παραδώσει το αγαθό ή να παράσχει την υπηρεσία που του παραγγέλθηκε, προμηθεύει όμως ισοδύναμο αγαθό ή παρέχει ισοδύναμη υπηρεσία της ίδιας ποιότητας και στην ίδια τιμή γνωστοποιώντας εγγράφως στον καταναλωτή, ότι μπορεί να επιστρέψει το προϊόν ή την υπηρεσία υποκατάστασης, εάν δεν μείνει ικανοποιημένος. Δεν εμπίπτει στις διατάξεις της προηγούμενης παραγράφου και η αποστολή δειγμάτων ή διαφημιστικών δώρων.

6. Η χρησιμοποίηση των τεχνικών επικοινωνίας πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή. Απαγορεύεται χωρίς τη συναίνεση του καταναλωτή η χρησιμοποίηση τεχνικών επικοινωνίας για την πρόταση σύναψης σύμβασης όπως τηλεφώνου, αυτόματης κλήσης, φαξ, ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου επικοινωνίας.

7. Απαγορεύεται η είσπραξη όλου ή μέρους του τιμήματος, ακόμη και με τη μορφή αρραβώνα, εγγύησης, έκδοσης ή αποδοχής αξιόγραφων ή άλλη μορφή, πριν από την παράδοση του προϊόντος ή την παροχή της υπηρεσίας.

8. Όταν δεν αναφέρεται προθεσμία εκτέλεσης στην πρόταση για σύναψη σύμβασης, η παροχή οφείλεται το αργότερο 30 ημέρες μετά τη λήψη της παραγγελίας από τον προμηθευτή.

9. Η σύμβαση από απόσταση είναι άκυρη υπέρ του καταναλωτή, αν αυτός δεν λάβει γραπτά και στη γλώσσα που χρησιμοποιήθηκε στην πρόταση σύναψης σύμβασης τις ακόλουθες τουλάχιστον πληροφορίες:

α) τις πληροφορίες που προβλέπονται στην παράγραφο 2 αυτού του άρθρου,

β) την επωνυμία και τη διεύθυνση του πιο προσιτού για τον καταναλωτή καταστήματος του προμηθευτή,

γ) τον τρόπο καταβολής του τιμήματος, περιλαμβανομένων των όρων πίστωσης ή πληρωμής με δόσεις, καθώς και τους όρους εξασφάλισης και

δ) το δικαίωμα υπαναχώρησης και, σε ξεχωριστό έντυπο, υπόδειγμα δήλωσης υπαναχώρησης του καταναλωτή από τη σύμβαση κατά την επόμενη παράγραφο.

10. Σε κάθε σύμβαση από απόσταση ο καταναλωτής έχει το δικαίωμα να υπαναχωρήσει αναιτιολογήτως μέσα σε 10 εργάσιμες ημέρες από την ημερομηνία παραλαβής του αγαθού ή της υπηρεσίας, αν δεν συμφωνήθηκε

μακριότερη προθεσμία, επιστρέφοντας το αγαθό στην αρχική του κατάσταση. Αποκλείεται η επιβάρυνσή του με δαπάνη άλλη από τα έξοδα επιστροφής. Για την άσκηση του δικαιώματος αυτού η προθεσμία των 10 ημερών αρχίζει, για τα αγαθά, από την παραλαβή τους και, για τις υπηρεσίες, από την παραλαβή των εγγράφων που ενημερώνουν τον καταναλωτή ότι έχει συναφθεί η σύμβαση. Παραίτηση από το δικαίωμα αυτό είναι άκυρη.

11. Οι διατάξεις του παρόντος άρθρου δεν εφαρμόζονται:
α)στους αυτόματους διανομείς,
β) στους εμπορικούς χώρους αυτόματης πώλησης,
γ) στις συμβάσεις προμήθειας τροφίμων, ποτών ή άλλων αγαθών που προορίζονται για την τρέχουσα οικιακή κατανάλωση και τα οποία παραδίδουν κατ' οίκον διανομείς σε τακτά χρονικά διαστήματα και
δ) στις συμβάσεις παροχής υπηρεσιών με κράτηση που έχουν ως αντικείμενο μεταφορές, κατάλυμα, σίτιση και ψυχαγωγία.

12. α. Κάθε προμηθευτής ο οποίος προτίθεται να συνάπτει συμβάσεις της παραγράφου 1 του παρόντος, υποχρεούται πριν από την έναρξη της δραστηριότητάς του αυτής να ζητήσει καταχώρησή του στο ειδικό μητρώο που τηρείται στο Υπουργείο Ανάπτυξης. Κανένας προμηθευτής δεν μπορεί να προτείνει τη σύναψη των ανωτέρω συμβάσεων, εάν εντός τριών μηνών από τη δημοσίευση του παρόντος δεν εγγραφεί στο μητρώο αυτό.
β. Η ανωτέρω καταχώρηση αποτελεί απαραίτητη προϋπόθεση για τη θεώρηση των αναγκαίων φορολογικών βιβλίων και στοιχείων από την αρμόδια οικονομική υπηρεσία και αποδεικνύεται με βεβαίωση που χορηγείται από την αρμόδια υπηρεσία του Υπουργείου Ανάπτυξης.
γ. Ο Υπουργός Ανάπτυξης μπορεί, με αιτιολογημένη απόφασή του να αρνείται για σοβαρούς λόγους την εγγραφή ή να προβαίνει σε, εκτός των κυρώσεων των

προβλεπομένων στη παράγραφο 3 του άρθρου 14 του παρόντος, προσωρινή ή οριστική διαγραφή από το εν λόγω μητρώο, αν διαπιστωθεί παραβίαση από τον εν λόγω προμηθευτή των κείμενων διατάξεων. Η διαγραφή αυτή συνεπάγεται την αυτοδίκαιη κατάργηση της σύμβασης, η δε απόφαση κοινοποιείται στην Ένωση Τραπεζών και στην αρμόδια δημόσια οικονομική υπηρεσία.

δ. Με αποφάσεις του Υπουργού Ανάπτυξης, που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως, καθορίζονται οι όροι και οι προϋποθέσεις τήρησης του προαναφερθέντος μητρώου.

5.4 Διακρίσεις Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο μπορεί να οριστεί από τέσσερις διαφορετικές οπτικές γωνίες:

- **Επιχειρήσεις:** Ως εφαρμογή νέων τεχνολογιών προς την κατεύθυνση του αυτοματισμού των συναλλαγών και της ροής εργασιών.
- **Υπηρεσίες:** Ως μηχανισμός που έχει στόχο να ικανοποιήσει την κοινή επιθυμία προμηθευτών και πελατών για καλύτερη ποιότητα υπηρεσιών, μεγαλύτερη ταχύτητα εκτέλεσης συναλλαγών και μικρότερο κόστος.
- **Απόσταση:** Ως δυνατότητα αγοραπωλησίας προϊόντων και υπηρεσιών μέσω του Internet ανεξάρτητα από τη γεωγραφική απόσταση.
- **Επικοινωνία:** Ως δυνατότητα παροχής πληροφοριών, προϊόντων ή υπηρεσιών, και πληρωμών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

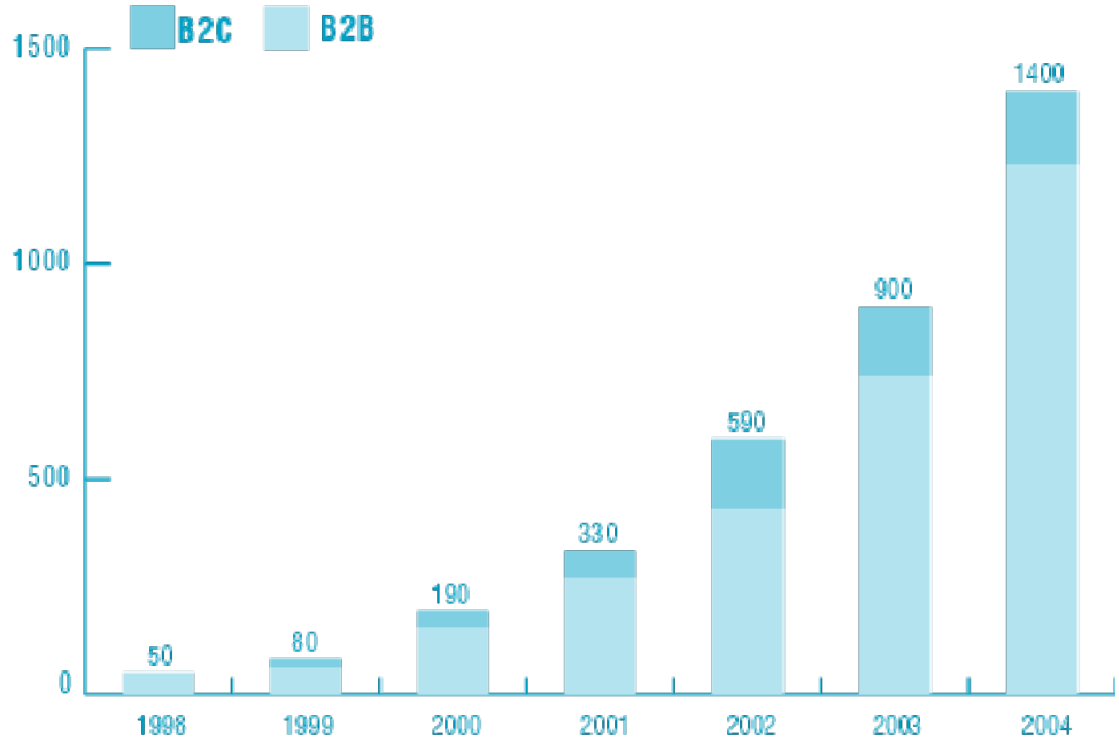
Το ηλεκτρονικό εμπόριο σε πρακτικό επίπεδο, μπορεί να διακριθεί σε:

- **Συναλλαγές μεταξύ επιχειρήσεων (Business-to-Business - B2B):** Το ηλεκτρονικό εμπόριο επιτρέπει σε επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες και το κόστος των προμηθειών, την ταχύτερη αποστολή των προμηθειών και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επιπλέον καθιστά

ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και ποιοτικότερη την εξυπηρέτηση πελατών. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς καθώς και η πραγματοποίηση ηλεκτρονικών πληρωμών βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές περιορίζουν το ανθρώπινο σφάλμα, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών. Το ηλεκτρονικό εμπόριο προσφέρει τη δυνατότητα αυξημένης πληροφόρησης σχετικά με τα προσφερόμενα προϊόντα - είτε από τους προμηθευτές είτε από ενδιάμεσους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου.

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

Στο παρακάτω σχήμα βλέπουμε τα συνολικά έσοδα από το ηλεκτρονικό εμπόριο παγκοσμίως αλλά και το ποσοστό χρησιμοποίησης του B2B με το B2C ηλεκτρονικό εμπόριο.



Συνολικά Έσοδα από το e-Commerce, Παγκοσμίως (δις $)

Πηγή: Keenan Vision

5.5 Εργαλεία Ηλεκτρονικού Εμπορίου

Τα εργαλεία που θα παρουσιαστούν διαφοροποιούνται ως προς το εύρος των δυνατοτήτων που παρέχουν, από εργαλεία για την κατασκευή ολοκληρωμένης δικτυακής παρουσίας μέχρι σουίτες για την παροχή ολοκληρωμένων λύσεων για το ηλεκτρονικό εμπόριο. Επίσης κάποια από αυτά είναι εμπορικά, ενώ κάποια άλλα είναι διαθέσιμα με τη μορφή Ανοικτού Κώδικα (OpenSource) 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:

CommerceServer 2002 (http://www.microsoft.com/commerceserver)

Αποτελεί την πρόταση της Microsoft για εργαλεία ανάπτυξης ολοκληρωμένων λύσεων ηλεκτρονικού εμπορίου. Είναι μια δημοφιλής πλατφόρμα που συνεργάζεται με την υπάρχουσα τεχνολογία της Microsoft και με τα προϊόντα ExchangeServer, BizTalkServerκαι SQLServer και παρέχει

- **Ευέλικτο σύστημα δημιουργίας προφίλ** το οποίο δίνει τη δυνατότητα διατήρησης καταλόγων, τιμολόγησης και επεξεργασία επιχειρηματικών δεδομένων (businessprocessing) προσαρμοσμένων στους χρήστες, καθώς και εστιασμένο merchandising.
- **Ευέλικτο σύστημα καταλόγων προϊόντων,** το οποίο παρέχει Καθολικούς Καταλόγους (GlobalCatalogs), με δυνατότητα παροχής προϊόντων/τιμών για πολλαπλές χώρες νομίσματα, Εικονικούς καταλόγους (VirtualCatalogs)οι οποίοι παρέχουν 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.

Ως προς την ασφάλεια των δεδομένων, αυτή εξασφαλίζεται με μονόπλευρο κατακερματισμό (one-wayhashing) και ασύμμετρη κρυπτογράφηση. Φυσικά η παράμετρος της αποθήκευσης εναποτίθεται στον MicrosoftSQLServer, την εφαρμογή βάσεων δεδομένων της Microsoft.

BizTalkServer

Ο BizTalkServer είναι η εφαρμογή της Microsoft που διευκολύνει την αυτοματοποίηση της επικοινωνίας στην 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. Η ασφαλής μεταφορά δεδομένων εξασφαλίζεται από το πρότυπο SecureMIME (S/MIME). Η χρησιμότητά του ως εργαλείο, ισχυροποιείται από το γεγονός ότι υποστηρίζει δυνατότητα συνεργασίας με την πλατφόρμα CommerceServer.

MicrosoftExchange

ToMicrosoftExchange έχει σχεδιαστεί για να υποβοηθήσει την ανταλλαγή μηνυμάτων στις τάξεις της εταιρείας. Συγκεκριμένα παρέχει μια πλατφόρμα για την ανταλλαγή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου και την συνεργασία μέσω του ενδοδικτύου (Intranet) της εταιρείας. Το Exchange συνεργάζεται με την γνωστή εφαρμογή MicrosoftOutlook για την ανταλλαγή μηνυμάτων, ενώ έχει ενδιαφέρον να τονιστεί ότι στην έκδοση 2003 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 αντιμετωπίζονται και εδώ με τη χρήση SecureMIME

Παραδείγματα:

http://www.dell.com

http://www.h2oplus.com

OpenSourceCommerce (www.oscommerce.com)

είναι μία πλατφόρμα ηλεκτρονικού εμπορίου ελευθέρου λογισμικού που παρόλο του ότι βρίσκεται υπό ανάπτυξη είναι αρκετά δημοφιλής. Αυτό οφείλεται τόσο στο γεγονός ότι παρέχεται δωρεάν και στηρίζεται σε τεχνολογίες ελευθέρου λογισμικού (Apache,MySql) όσο και στο ότι η πλατφόρμα μπορεί να παραμετροποιηθεί πλήρως κατά περίπτωση αλλάζοντας τον κώδικα.

Λειτουργίες

- Λογαριασμοί πελατών
- Κατάλογος διευθύνσεων πελατών
- Ιστορικό παραγγελιών
- Temporary (not logged on) and permanent (logged on) shopping carts
- Κατάλογος προϊόντων (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 προϊόντων και πελατών
- Δυναμική επεξεργασία χαρακτηριστικών προϊόντων
- Διατήρηση κατηγοριών φορολόγησης (Tax zones, classes, and rates)

Yahoo Store (www.store.yahoo.gr)

Η υπηρεσία αυτή είναι ένα on-line σύστημα που κάποιος μπορεί να σχεδιάσει και να διαχειρισθεί πλήρως ένα ηλεκτρονικό κατάστημα. Κύριο πλεονέκτημα της εφαρμογής αυτής είναι ότι το κατάστημα μπορεί να φιλοξενηθεί σε εξυπηρετητή του Yahoo γεγονός που κάνει το ανέβασμα του καταστήματος στο δίκτυο πιο γρήγορο.

Λειτουργίες

- Σχεδιασμός εμφάνισης του καταστήματος : εμφάνιση, λογότυπο, χρώματα γραμματοσειρές κλπ
- Διαχείριση από απόσταση (μέσω web)
- Λήψη των παραγγελιών είτε μέσω του web είτε μέσω email , fax
- Ασφαλείς Επικοινωνία μέσω SSL
- Εισαγωγή/ Προσθήκη/ Επεξεργασία/ Διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών και αξιολογήσεων
- Ιστορικό παραγγελιών
- Κατάλογος προϊόντων (Αναζήτηση με βάση το είδος ή τον κατασκευαστή
- Ενημερώσεις μέσω E-mail
- Καλάθι αγορών και πλήρης επεξεργασία του
- Αριθμός διαθέσιμων Προϊόντων (stock)
- Παρουσίαση Εναλλακτικών Αγορών και αγορών που έγιναν με ένα συγκεκριμένο προϊόν
- Στατιστικά προϊόντων

Παραδείγματα

www.alight.com

http://store.yahoo.com/eurekaservice

PHPAuction (www.phpauction.net)

Είναι από η πιο πλήρης στην κατηγορία των ηλεκτρονικών δημοπρασιών. Έχει χαμηλό κόστος αφού έχει μικρή τιμή απόκτησης και στηρίζεται σε ελεύθερες αρχιτεκτονικές (Apache/MySql).

Λειτουργίες

- Εγγραφή μέλους
- Κατάλογος δημοπρατούμενων προϊόντων- Ευρετήριο
- Αναζήτηση
- Εκτεταμένη αναζήτηση
- Πληροφορίες δημοπρασίας
- Επιβεβαίωση
- Ασφάλεια - χρήση προσωπικών κωδικών
- Πιστοποίηση
- Προφίλ πελάτη
- Προτάσεις – προτεινόμενες δημοφιλείς δημοπρασίες
- Προφίλ εταιρίας
- Πληροφορίες επικοινωνίας
- Φόρμα επικοινωνίας
- Νέα και γεγονότα
- Newsletter
- Βοήθεια
- FAQ (συχνές ερωτήσεις)
- Μηνύματα λάθους
- Χώροι συζήτησης

- Χάρτης
- Χρήσιμες συνδέσεις
- Ξένη γλώσσα – υποστήριξη πολλών γλωσσών
- Νομικό πλαίσιο - ξεκάθαρη δήλωση όρων και προϋποθέσεων συναλλαγών
- Δημοπρασίες χρήστη
- Σωστή κατηγοριοποίηση auctions
- Inverse δημοπρασίες
- Αυτόματη προσφορά – μπορεί ένας πελάτης να θέσει ένα άνω όριο χρημάτων και όταν κάποιος άλλος, τότε αυτόματα υποβάλει μία νέα πρόσφορα εφόσον η τελική τιμή δεν ξεπερνά το άνω όριο.

Παραδείγματα

www.jetcityauction.com

www.auction.fish-forum.com

www.laundromatic.net/newauction

www.rarelots.com

phpShop (www.phpshop.com)

Είναι μία άλλη πρόταση ελευθέρου λογισμικού, η οποία συνεχώς αυξάνεται και βελτιώνεται από την OpenSourceκοινότητα. Είναι αρκετά δημοφιλής εξαιτίας τόσο του μηδενικού της κόστους όσο και της πληρότητας αλλά και της μεγάλης δυνατότητας παραμετροποίησης που εμφανίζει.

Λειτουργίες

- Κατάλογος προϊόντων (Αναζήτηση με βάση το είδος ή τον κατασκευαστή
- Διαχείριση καταλόγου: Εισαγωγή/ Προσθήκη/ Επεξεργασία/ Διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών
- Λογαριασμοί 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 (stock)
- Παρουσίαση Δημοφιλών Προϊόντων
- Παρουσίαση Εναλλακτικών Αγορών και αγορών που έγιναν με ένα συγκεκριμένο προϊόν
- Στατιστικά προϊόντων και πελατών
- Διαχείριση των τρόπων πληρωμής και παράδοσης

Παραδείγματα

www.cynthiavictoria.com/store/

www.viet-dragon.com

WebSphere (http://www-3.ibm.com/software/info1/websphere)

Το WebSphere είναι η πρόταση της IBM στον τομέα των ολοκληρωμένων λύσεων για ηλεκτρονικό επιχειρείν. Η λογική του προϊόντος και σ' αυτή την περίπτωση ξεφεύγει από το στενά όρια της δημιουργίας και υποστήριξης λειτουργιών ηλεκτρονικού καταστήματος καθώς στοχεύει στην υποστήριξη όσο το δυνατόν πιο ευρείας γκάμας επιχειρηματικών μοντέλων. Η πλατφόρμα του WebSphere αποτελείται από τα εξής επί μέρους κομμάτια:

- **Application Developer**: Είναι το εργαλείο ανάπτυξης εφαρμογών της για ηλεκτρονικό εμπόριο που συνοδεύει το WebSphere. Οι δυνατότητες ανάπτυξης εφαρμογών περιλαμβάνουν δυνατότητες ανάπτυξης σε J2EE 1.2, Java, ανάπτυξης εφαρμογών WebServices με UDDI, SOAP, WSIL, περιβάλλον ανάπτυξης για XML, Βάσεις Δεδομένων (DB2) και Ιστοσελίδες.
- **Studio:** για ολοκληρωμένη ανάπτυξη και διαχείριση διαδικτυακών τόπων
- **Portal:** Περιβάλλον για ανάπτυξη και διαχείριση δικτυακών πυλών (portals), 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 (EnterpriseRequirementsPlanning), CRM(Customer Relationship Management) και Διαχείρισης Αλυσίδας Προμηθειών (SupplyChainManagement).
- **Commerce:** Αποτελεί την κεντρική εφαρμογή της σουίτας, η οποία προσφέρει λύσεις για τις πωλήσεις, τις αγορές και την διαχείριση

καναλιών (όπως on-line πωλήσεις, η-προμήθειες μέχρι ολοκληρωμένες multi-tier αλυσίδες απαιτήσεων). Χωρίζεται στα **CommerceExpress**, για την παροχή του βασικού πακέτου λύσεων σε επιχειρήσεις που χρειάζονται άμεση δικτυακή εμπλοκή, το **CommerceBusinessEdition** για δημιουργία λύσεων με μεγάλο όγκο συναλλαγών σε επίπεδο B2B ή προχωρημένο B2C και το **CommerceProfessional**για λύσεις σε επίπεδο λιανικής πώλησης B2B και B2C.

Λειτουργίες

- Έλεγχος πρόσβασης και προηγμένα χαρακτηριστικά διαχείρισης χρηστών και δημιουργίας προφίλ.
- Διαχειριστή καταλόγων
- Συνεργασία σε Συνεργατικούς Χώρους Εργασίας (CollaborativeWorkspaces) για την έκδοση Business και υποστήριξη χρηστών.
- Παροχή on-line συνεργασίας με το Lotus-SameTime
- 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 (accesslogging)
- XML πάνω από HTTP

Ενώ επιπλέον παρέχονται:

- Ενσωμάτωση υποστήριξης μέσω e-mail
- 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 κ.α.
- Ανάλυση της κίνησης στο δικτυακό κατάστημα με τη χρήση του TivoliWebSiteAnalyzer
- Υποστήριξη συστήματος πληρωμών με τεχνολογία paymentcassettes και σε συνεργασία με το πρωτόκολλο SSH.
- Αυτόματος Εντοπισμός Προβλημάτων και παρακολούθηση της απόδοσης.
- WebServices.

Η σουίτα της IBM είναι επίσης διαθέσιμη για ένα αρκετά μεγάλο εύρος λειτουργικών συστημάτων όπως Windows, Solaris, AIX.Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι η IBM έχει αναπτύξει το πακέτο που ονομάζεται **WebSphereVoice**, το οποίο παρέχει δυνατότητες ανάπτυξης εφαρμογών ηλεκτρονικού εμπορίου, οι οποίες θα είναι προσπελάσιμες από τους χρήστες μέσω φωνής. Για το σκοπό αυτό παρέχονται τόσο λογισμικό αναγνώρισης φωνής (VoiceServer) αλλά και εργαλεία ανάπτυξης όπως το VoiceServerSDK και το VoiceToolkit, το οποίο υποστηρίζει την ανάπτυξη εφαρμογών σε περιβάλλον VoiceXML.

Παραδείγματα

- www.manchesterairport.co.uk
- www.raja.fr
- www.orica-chemicals.com
- http://whirlpoolcorp.com/

iBuilder (www.ibuilder.com)

Είναι σχετικά νέα και όχι τόσο διαδεδομένη. Η πλατφόρμα που προσφέρει αποτελείται από διάφορα ανεξάρτητα κομμάτια : SiteBuilder, StoreBuilder, TrafficBuilder.

SiteBuilder

Εργαλείο για τον σχεδιασμό του ηλεκτρονικού καταστήματος : της εμφάνισης , της πλοήγησης, των γραφικών των γραμματοσειρών κλπ.

StoreBuilder

- Κατάλογος προϊόντων (Αναζήτηση με βάση το είδος ή τον κατασκευαστή
- Διαχείριση καταλόγου: Εισαγωγή/ Προσθήκη/ Επεξεργασία/ Διαγραφή κατηγοριών, προϊόντων, κατασκευαστών, πελατών
- Κατάλογος διευθύνσεων πελατών
- Αξιολόγηση προϊόντων από πελάτες
- Καλάθι αγορών και πλήρης επεξεργασία του ανά πάσα στιγμή
- Ασφαλής Επικοινωνία μέσω SSL
- Παρουσίαση Δημοφιλών Προϊόντων
- Στατιστικά προϊόντων και πελατών
- Διαχείριση των τρόπων πληρωμής και παράδοσης

TrafficBuilder

- Καταχωρήσεις σε μηχανές αναζήτησης
- Διαφήμιση μέσω banner και email

Παραδείγματα

http://sundancemall.com/sales.htm

5.6 Οφέλη Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο αλλάζει ριζικά την παραδοσιακή θεώρηση της δοσοληψίας και γι' αυτό το λόγο, παρουσιάζει σημαντικά οφέλη σε ότι αφορά τόσο τους καταναλωτές όσο και τις επιχειρήσεις που το υιοθετούν.

Ας δούμε κάποια από αυτά που αφορούν την μεριά των **χρηστών**:

- Υπάρχει απεριόριστη δυνατότητα επιλογών προϊόντων.
- Οι καταναλωτές έχουν τη δυνατότητα να κάνουν άμεση σύγκριση τιμών στα προϊόντα που αγοράζουν, απλώς με μερικά κλικ του ποντικιού
- Παρέχεται η δυνατότητα χρήσης του καταστήματος και πραγματοποίησης συναλλαγών σε οποιαδήποτε ώρα, οποιασδήποτε μέρας.
- Εξοικονομείται ο χρόνος που πιθανόν να σπαταλούταν σε πολύωρη αναμονή για εξυπηρέτηση και στην εμπλοκή με γραφειοκρατικές διαδικασίες.
- Αίρονται οι γεωγραφικοί φραγμοί στις αγορές.
- Εξατομίκευση των πληροφοριών και των περιεχομένων του καταστήματος με βάση τις προτιμήσεις και τις ιδιαιτερότητες του πελάτη
- Συχνά η τιμή που πώλησης ενός προϊόντος από το ηλεκτρονικό κατάστημα είναι μικρότερη, ενώ πολλές φορές υπάρχουν προσφορές.

Σε ότι αφορά τις **επιχειρήσεις** κι εδώ τα οφέλη είναι πολύ μεγάλα:

- Οι Μικρομεσαίες Επιχειρήσεις (ΜΜΕ), δεν μπορούν παρά να ωφελούνται από την παγκόσμια φύση του Διαδικτύου για να προωθήσουν την παρουσία τους. Το Διαδίκτυο, τους παρέχει μιας

πρώτης τάξης ευκαιρία να μπορέσουν να διευρύνουν τον κύκλο εργασιών τους σε νέες αγορές και σε καινούριο αγοραστικό κοινό

- Οι εταιρείες μπορούν να προσβλέπουν σε αύξηση των εσόδων τους γιατί το ηλεκτρονικό κατάστημα, προσφέρει μια νέα οδό προώθησης προϊόντων
- Μείωση κόστους μιας σειράς διαδικασιών που λαμβάνουν χώρα σε μια επιχείρηση, όπως: Λειτουργικό κόστος από την ακριβέστερη πληροφόρηση για τις πωλήσεις, κόστους προώθησης/διαφήμισης, λειτουργικού κόστους ενδοπληροφόρησης, αυτοματοποίση της διαχείρισης παραγγελιών, JIT διαχείριση της αποθήκης
- Βελτίωση της εικόνας της επιχείρησης μέσω της ταχύτερης διεκπεραίωσης, τόσο των συναλλαγών με τους αγοραστές όσο και της επικοινωνίας με άλλες επιχειρήσεις.
- Αυξημένη αξιοπιστία στις συναλλαγές και στις παραγγελίες, εφόσον ελαχιστοποιείται η πιθανότητα ανθρωπίνων λαθών.
- Δυνατότητα αλλαγής των προϊόντων, των τιμών τους και των χαρακτηριστικών τους με εύκολο και άμεσο τρόπο.

5.7 Φραγμοί Ηλεκτρονικού Εμπορίου

Ως εμπορικό μέσο το δίκτυο εισάγει επίσης 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.

- **Αλλαγή του επιχειρησιακού περιβάλλοντος και των τεχνολογικών δομών**

Το παραδοσιακό επιχειρηματικό περιβάλλον μεταλλάσσεται με μεγάλα άλματα καθώς οι πελάτες και οι επιχειρήσεις επιθυμούν να έχουν την ελαστικότητα και την δυνατότητα να αλλάξουν εμπορικούς εταίρους, πλατφόρμες και δίκτυα κατά βούληση. Αν και δεν είναι δυνατό να υπολογίσουμε το κόστος, καθώς εξαρτάται από την ήδη υπάρχουσα εγκατεστημένη τεχνολογία της επιχείρησης και το βαθμό που αυτή επιθυμεί να συσχετισθεί με το Ηλεκτρονικό Εμπόριο, εντούτοις μπορούμε να πούμε πως στην πιο απλή περίπτωση η επιχείρηση θα χρειασθεί έναν προσωπικό υπολογιστή, ένα μόντεμ και μια συνδρομή σε ένα Δίκτυο Προστιθέμενης Αξίας (VAN). Μια επιχείρηση με πιο εκτεταμένη ανάμειξη με το Ηλεκτρονικό Εμπόριο θα πρέπει να ενσωματώσει τις εμπορικές συναλλαγές με την αγοραστική δύναμη, με εμπορικά και λογιστικά συστήματα. Επίσης χρειάζεται και συνεχής εκπαίδευση του έμψυχου δυναμικού μιας και οι νέες τεχνολογίες εισάγονται με ραγδαίους ρυθμούς.

- **Δυσπιστία σε θέματα Ασφάλειας**

Ένα σημαντικό μειονέκτημα προκύπτει από την χρήση του Web ως εμπορικού καναλιού. Ένα καθόλου ευκαταφρόνητο ποσοστό των χρηστών δεν εμπιστεύεται το Δίκτυο ως μέσο πληρωμής. Η αγοραπωλησίες μέσω του Web πραγματοποιούνται με τη χρήση πιστωτικής κάρτας και ακόμα δεν είναι ασφαλές να εισάγουμε τον αριθμό μας στο δίκτυο εξασφαλίζοντας πως κανένας δεν θα τον μάθει. Οποιοσδήποτε μεταφέρει δεδομένα της πιστωτικής του κάρτας στο Δίκτυο δεν μπορεί να είναι σίγουρος για την ταυτότητα του Ηλεκτρονικού πωλητή, ενώ από την άλλη πλευρά ούτε ο πωλητής μπορεί να γνωρίζει την ταυτότητα του καταναλωτή. Κανείς δεν μπορεί να εγγυηθεί σε εκείνον που πληρώνει ότι ο αριθμός της κάρτας του δεν θα καταλήξει κάπου

στο internet για να χρησιμοποιηθεί στη συνέχεια για μοχθηρούς σκοπούς, όπως κανείς δεν μπορεί να εγγυηθεί και στον πωλητή πως ο ιδιοκτήτης της πιστωτικής κάρτας θα αποδεχθεί την αγοραπωλησία.

- **Τα νομικά ζητήματα σε Εθνικό και Διεθνές επίπεδο**

Το θέμα αυτό είναι ένα από τα σημαντικότερα θέματα που αφορούν το Ηλεκτρονικό Εμπόριο. Υπάρχει ένας αριθμός από ζητήματα που αφορούν τις συναλλαγές μέσω του Δικτύου: εγκυρότητα των ηλεκτρονικών υπογραφών, νομιμότητα ενός ηλεκτρονικού συμβολαίου, κίνδυνοι, παραβιάσεις trademark και δικαιωμάτων. Πολλές χώρες, όπως και η Ελλάδα, δεν έχει προλάβει να θέσει νομοθετικό πλαίσιο που να καλύπτει τις συναλλαγές μέσα από το διαδίκτυο. Επίσης σε κάθε χώρα υπάρχει διαφορετική νομοθεσία που διέπει τις εμπορικές συναλλαγές με αποτέλεσμα να είναι αναγκαίες διακρατικές συμφωνίες για την διενέργεια διεθνών αγοροπωλησιών μέσω του internet μιας και αυτό ξεπερνάει τα φυσικά σύνορα.

ΚΕΦΑΛΑΙΟ 6^{Ο} E-BANKING

Το e-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές. "Μεταφέρει" την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών.

6.1 Εισαγωγή στο E-Banking

Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για

τις ΜΜΕ το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές.

Οι βασικότερες υπηρεσίες που παρέχουν μέσω Internet οι ελληνικές τράπεζες είναι οι εξής:

- Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς.
- Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος.
- Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών.
- Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων λογαριασμών.
- Παραγγελία μπλοκ επιταγών.
- Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών.
- Εντολές αγοραπωλησίας μετοχών.
- Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων.
- Δυνατότητα υποβολής αιτήσεων εμβασμάτων.
- Αλλαγή του απορρήτου κωδικού PIN.
- Προσωπικά μηνύματα.

Σε πολλές ευρωπαϊκές χώρες, όπου τα συστήματα πληρωμών είναι περισσότερο ανεπτυγμένα και τυποποιημένα, ο προσανατολισμός των τραπεζών στρέφεται σταδιακά στην παροχή πρόσθετων υπηρεσιών προς τις επιχειρήσεις (corporate sites), πεδίο στο οποίο η γκάμα των επιλογών είναι ιδιαίτερα διευρυμένη.

6.2 Η Διάδοση του E-Banking στην Ελλάδα

Στις τραπεζικές συναλλαγές, μέσω Internet, στρέφονται πλέον ολοένα και περισσότεροι Ελληνες, επιχειρώντας έτσι να αποφύγουν τόσο την ταλαιπωρία από τις ουρές όσο και τις υψηλές προμήθειες - χρεώσεις στο γκισέ. Σύμφωνα με την «Εξπρές» τραπεζικά στελέχη με εξειδίκευση στην ηλεκτρονική τραπεζική, κάνουν λόγο για «κοσμογονία» στον τομέα των τραπεζικών συναλλαγών μέσω του Internet, τηρουμένων βεβαίως των αναλογιών, καθώς τα χρηματοπιστωτικά ιδρύματα δέχονται καθημερινά περί τις 1.200 αιτήσεις για άνοιγμα νέων κωδικών e-banking.

Την ίδια στιγμή οι ίδιες πηγές επισημαίνουν ότι μέχρι το τέλος του χρόνου οι Ελληνες που θα πραγματοποιούν τις τραπεζικές τους συναλλαγές μέσω τους Διαδικτύου θα προσεγγίσουν περίπου το 1,5 εκατ. έναντι 996.500 που ήταν ο αριθμός των χρηστών e – banking στο τέλος του 2007, 800.000 περίπου το 2006 και 500.000 περίπου το 2004.

Ενδεικτικό του περιθωρίου που έχουν οι τράπεζες για περαιτέρω διείσδυση στο e-banking, είναι το γεγονός ότι μόλις το 15% των χρηστών Internet στην Ελλάδα κάνει χρήση και e-banking, ήτοι ποσοστό επί του συνολικού πληθυσμού κάτω από 5%, όταν στη Γερμανία για παράδειγμα ήδη το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες ηλεκτρονικής τραπεζικής.

Σημειώνεται ότι σε σχέση με το παρελθόν, όταν η ηλεκτρονική τραπεζική ήταν «προνόμιο» μόνο των μικρότερων ηλικιών, σταδιακά χρήστες του e-banking γίνονται και αρκετοί πελάτες μεγαλύτερων ηλικιών, ενώ από την

πλευρά τους, οι τράπεζες επενδύουν το τελευταίο διάστημα σημαντικά ποσά στα «εναλλακτικά δίκτυα» προκειμένου να αναβαθμίσουν τις υπηρεσίες τους – κυρίως στο κομμάτι της ασφάλειας των συναλλαγών.

6.3 Το e-Banking των Ελληνικών Τραπεζών

Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SSL(secure socket Layer) καθώς επίσης και το SET (Secure Electronic Transaction), που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape. Υπάρχουν αρκετές εταιρίες που μπορεί να χρησιμοποιήσει ένας οργανισμός για να πετύχει ασφαλή πρόσβαση. Μία από αυτές είναι η VeriSign, το λογισμικό της οποίας χρησιμοποιείται στις τραπεζικές όσο και σε άλλου τύπου διαδικτυακές συναλλαγές.

- Εθνική Τράπεζα (http://www.nbg.gr)

Η αίτηση εισαγωγής στο σύστημα e-banking της Εθνικής γίνεται στα υποκαταστήματα της τράπεζας. Απαραίτητη προϋπόθεση είναι να υπάρχει ένας τουλάχιστον λογαριασμός καταθέσεων ταμιευτηρίου, τρεχούμενου ή όψεως σε ευρώ στην τράπεζα.

Η Εθνική Τράπεζα χρησιμοποιεί κρυπτογράφηση των διακινούμενων στοιχείων 128 bit, μέσω του πρωτοκόλλου SSL 128. Πέραν της κρυπτογράφησης, το σύστημα αυτό ελέγχει συνεχώς την αυθεντικότητα της επικοινωνίας μεταξύ του χρήστη και του κεντρικού συστήματος. Η Εθνική διαθέτει πιστοποιητικό αυθεντικότητας από τη VeriSign. Το πιστοποιητικό εμφανίζεται στο χρήστη κάθε φορά που επισκέπτεται την ιστοσελίδα εισόδου του συστήματος.

Ø EFG Eurobank (http://www.eurobank.gr)

Η Eurobank EFG χρησιμοποιεί τον φορέα πιστοποίησης Verisign. Ανάλογα με το ημερήσιο όριο συναλλαγών που έχει επιλέξει η Εταιρία για κάθε χρήστη κατά την εγγραφή της στην υπηρεσία, το πιστοποιητικό δύναται να εγκατασταθεί είτε στον υπολογιστή ή στην ειδική συσκευή eToken. Το eToken είναι μια ειδική συσκευή στο μέγεθος ενός κλειδιού, η οποία περιέχει έναν κρυπτογραφικό μηχανισμό που δίνει τη δυνατότητα στον κάτοχό του να δημιουργήσει και να αποθηκεύσει το απαραίτητο λογισμικό ώστε να λειτουργεί σαν την ηλεκτρονική του υπογραφή. Όταν συνδεθεί με οποιονδήποτε υπολογιστή μέσω της USB θύρας, το eToken δίνει στον χρήστη τη δυνατότητα να υπογράφει ψηφιακά όλες τις προσωπικές του συναλλαγές. Έτσι, μέσω της προσωπικής ταυτοποίησης επιτυγχάνεται η μέγιστη δυνατή παροχή ασφάλειας. Η χρήση του είναι απαραίτητη σε οποιαδήποτε χρηματική συναλλαγή επιχειρήσετε μέσα από το e-Banking, από μεταφορά χρημάτων μεταξύ λογαριασμών μέχρι εκτέλεση διάφορων πληρωμών. Τέλος Η Eurobank χρησιμοποιεί το πρωτόκολλο επικοινωνίας SSL (Secure Sockets Layer) μαζί με την κρυπτογράφηση στα 128bit, το οποίο εξασφαλίζει την ασφάλεια των συναλλαγών μέσω διαδικτύου. Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από τον Internet Explorer στον server της τράπεζας. Μπορείτε να αναγνωρίσετε εάν η σελίδα η οποία βρίσκετε είναι ασφαλής, καθώς το πρωτόκολλο που εμφανίζεται με την διεύθυνση της τράπεζας μετατρέπεται από «http» σε «https» και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας.

Ø Τράπεζα Κύπρου (http://www.bankofcyprus.gr)

Η Υπηρεσία Internet Banking της Τράπεζας Κύπρου έχει πιστοποιηθεί από το διεθνούς κύρους οργανισμό Verisign. Η μεταφορά των δεδομένων μέσω του Internet Banking της Τράπεζας Κύπρου εξασφαλίζεται από το πλέον εξελιγμένο πρωτόκολλο επικοινωνίας SSL (Secure Sockets Layers) και κρυπτογράφηση 128bit. Επίσης παρέχει μια πρόσθετη ασφάλεια με το S.T.I.C.K (**(Secure Transaction Internet Code Key)** Το S.T.I.C.K. είναι μια συσκευή παραγωγής κωδικών συναλλαγών μιας χρήσης (OTPs: one-time passwords) και αποτελεί την πρόταση της Τράπεζας Κύπρου για την **ενίσχυση** της ασφάλειας των συναλλαγών σας μέσω του **Internet Banking**.

Ø Τράπεζα Πειραιώς (http://www.piraeusbank.gr)

Από την έναρξη έως τη λήξη της σύνδεσής σας (on-line session) με την υπηρεσία winbank internet, όλες οι πληροφορίες και τα προσωπικά σας στοιχεία κρυπτογραφούνται με βάση το πρωτόκολλο κρυπτογράφησης SSL 128-bit. Επίσης το πρωτόκολλο που εμφανίζεται με την διεύθυνση της τράπεζας μετατρέπεται από «http» σε «https» και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας.

Ø Εμπορική Τράπεζα (http://www.emporiki.gr/)

Η τράπεζα εγγυάται την ασφάλεια των συναλλαγών χρησιμοποιώντας την πιστοποίηση της VeriSign και όπως και οι παραπάνω χρησιμοποιεί τα πρωτόκολλα SSL και HTTPS για τις ασφαλείς συναλλαγές τις.

Ø Τράπεζα Εγνατίας (http://www.egnatiabank.gr/)

Οι υπηρεσίες web της Εγνατίας Τράπεζας χρησιμοποιούν Πιστοποιητικό Αυθεντικότητας της VeriSign. Η υπηρεσία παρέχει κρυπτογράφηση των μεταφερόμενων δεδομένων από και προς τον Server της Εγνατίας Τράπεζας με πρωτόκολλο SSL 128bit. Επιπλέον λειτουργεί κάτω από την "ομπρέλα" ενιαίας ασφάλειας των διαδικτυακών εφαρμογών της τράπεζας, που παρέχεται μέσω των κωδικών PIN-TAN του egnatiaTeller. Ταυτόχρονα στα συστήματα της Εγνατίας Τράπεζας εφαρμόζονται επιπλέον μέτρα ασφαλείας όπως Ο αλγόριθμος IDEA 128 bits που χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων που αφορούν τραπεζικές συναλλαγές όταν "ταξιδεύουν" στο Internet.

6.4 Κίνδυνοι του e-Banking

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, η συχνότητά τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on-line υπηρεσίες. Η αύξηση αυτή δεν είναι τεράστια, εντούτοις όμως αποτελεί ένα ανησυχητικό φαινόμενο μια και πολλοί θεωρούν τις οικονομικές πληροφορίες που τους αφορούν άκρως απόρρητες και διατηρούν μια επιφυλακτική στάση απέναντι σε διαδικασίες που τις καθιστούν ευάλωτες στο ευρύ κοινό, όπως είναι το e-banking. Στοιχεία για το ηλεκτρονικό έγκλημα δεν κοινοποιούνται δημοσίως, αλλά υπολογίζεται ότι στις Η.Π.Α. χάνονται ετησίως περίπου 11 δισεκατομμύρια δολάρια από εταιρείες και καταναλωτές λόγω αυτής της μορφής εγκλήματος. Το μεγαλύτερο μέρος προέρχεται από οικονομικά ιδρύματα. Μάλιστα το μεγαλύτερο μέρος των ζημιών δεν προκύπτει από τις κλοπές χρημάτων, αλλά από έξοδα που κάνουν οι εταιρείες μετά από τέτοιου είδους επιθέσεις, προκειμένου να διασφαλίσουν τα συστήματά τους ώστε να μην ξανασυμβούν. Ειδικοί σε θέματα ασφάλειας έχουν υπολογίσει ότι μια τράπεζα μπορεί να ξοδέψει μέχρι και 1 εκατομμύριο δολάρια σε εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» στο σύστημά της.

Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές που θα δοθούν στη δημοσιότητα, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς τους. Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για online banking, οι μεγαλύτεροι κίνδυνοι προέρχονται από τον ανθρώπινο παράγοντα. Έρευνες που έχουν γίνει από ειδικούς σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είχαν την εκούσια ή ακούσια βοήθεια και κάποιου που εργαζόταν στην τράπεζα.

Και χωρίς τη βοήθεια εκ των έσω, πάντως, οι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι άνθρωποι αυτοί αποτελούν τους πιο προκλητικούς στόχους, μια και δεν έχουν συνείδηση του μεγέθους της ζημιάς που μπορούν να κάνουν ανοίγοντας απλά μια επισύναψη στο ηλεκτρονικό τους ταχυδρομείο ή ακολουθώντας ένα link. Οι απλοί χρήστες πέφτουν πολύ εύκολα θύματα προγραμμάτων που υποτίθεται ότι κάνουν κάτι χρήσιμο για αυτούς, αλλά στην πραγματικότητα ανοίγουν «τρύπες» ασφάλειας στο σύστημα επιτρέποντας σε χάκερς, να έχουν πρόσβαση σε αυτό.

Οι κλεμμένες πληροφορίες αποτελούν την πρώτη φάση μιας αρκετά επίπονης διαδικασίας η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες, έτσι ώστε ο χάκερ να υποδυθεί κάποιον άλλο στο διαδίκτυο. Η οποία όμως διευκολύνεται συνεχώς με καινούρια προγράμματα που κυκλοφορούν στην αγορά. Η εποχή που πολλές επιθέσεις θα γίνονται με αυτοματοποιημένο τρόπο δεν απέχει πολύ, σύμφωνα με αρκετούς ειδικούς.

Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως, αλλά σε μια από τις εταιρείες που συνεργάζονται με αυτήν προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της. Σε πολλές περιπτώσεις οι τράπεζες επιτρέπουν στις εταιρείες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρείες επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία κάνουν την κίνησή τους.
Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν

τον ανταγωνισμό με τις μεγαλύτερες τράπεζες. Δυστυχώς όμως λόγω αυτής της βιασύνης, οι τράπεζες αφήνουν πολλές «τρύπες» στα συστήματά τους, κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα.

Οι ειδικοί μας πληροφορούν ότι κλοπές ποσών από 5 μέχρι 10 χιλιάδες δολαρίων μπορούν να πραγματοποιηθούν σε χρονικό διάστημα μερικών εβδομάδων. Για ποσά μέχρι και 1 εκατομμυρίου δολαρίων χρειάζονται 4 μέχρι και 6 μήνες. (πηγή: http://www.go-online.gr)

6.5 Περιπτώσεις Ηλεκτρονικών Επιθέσεων

- **Περιστατικό**: το 1994 Ο Ρώσος χάκερ Βλαντιμίρ Λέβιν απέσπασε πόσο από λογαριασμούς της Citibank που υπολογίστηκε ότι ανερχόταν στα 10 εκατομμύρια δολάρια. Απέκτησε πρόσβαση στα δίκτυα της τράπεζας από την Αγία Πετρούπολη στη Ρωσία. Όταν συνελήφθη από την Σκότλαντ Γιαρντ και το FBI, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς και passwords από πελάτες της τράπεζας και μετέφερε ποσά στο λογαριασμό του. Το 1998, ένα δικαστήριο στις Η.Π.Α. τον καταδίκασε σε 3 χρόνια κάθειρξη. Η τράπεζα ανέκτησε όλο το ποσό εκτός από 400.000 δολάρια.
- **Περιστατικό:** αφορά μια Ολλανδική πολυεθνική τράπεζα, την ABN AMRO. Τον Σεπτέμβριο του 2000 ένα ολλανδικό τηλεοπτικό πρόγραμμα αποκάλυψε πως χάκερς, έκλεβαν σημαντικές πληροφορίες των πελατών της τράπεζας. Οι χάκερς έστελναν στους πελάτες της τράπεζας μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχονταν από την τράπεζα. Τα mails αυτά εγκαθιστούσαν στους υπολογιστές των πελατών προγράμματα τα οποία επέτρεπαν στους χάκερς να έχουν πρόσβαση σε κρίσιμες πληροφορίες των λογαριασμών τους και με αυτόν τον τρόπο να μεταφέρουν χρήματα από αυτούς. Η τράπεζα διένειμε καινούριες εκδόσεις του λογισμικού της.

- **Περιστατικό**: Αφορά την **Charles Schwab η οποία είναι** η μεγαλύτερη online χρηματιστηριακή εταιρεία στις Η.Π.Α. και έγινε τον Δεκέμβριο του 2000. Ο δικτυακός τόπος της εταιρείας έδινε τη δυνατότητα σε χάκερς να έχουν πρόσβαση σε όλους τους λογαριασμούς των πελατών της. Μάλιστα, όσο ο πελάτης ήταν συνδεδεμένος στο σύστημα, ο χάκερ μπορούσε να αγοράσει και να πουλήσει μετοχές από το λογαριασμό του.
- **Περιστατικό:** Έγινε τον Απρίλιο του 2001. Αμερικανοί εισαγγελείς κατηγόρησαν δύο Ρώσους για ηλεκτρονικά εγκλήματα που σχετίζονταν με μια σειρά επιθέσεων σε δίκτυα τραπεζών και άλλων εταιρειών. Οι δύο χάκερς, εισέβαλαν στα συστήματα των εταιρειών, έκλεψαν πολύτιμες πληροφορίες και κατόπιν εμφανίζονταν στις εταιρείες ως σύμβουλοι ασφάλειας και προσέφεραν τις υπηρεσίες τους για διορθωθούν τα σφάλματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Έντυπη

I. Γκλαβά Μ. (2001) «e-Επιχειρήν, Πλήρης Οδηγός Ανάλυσης Τεχνικών και Εμπορικών Θεμάτων» Μ. Γκιούρδας, Αθήνα.

II. Γεωργόπουλος Ν.Β, Πανταζή Μ.Α, Νικολαράκος Χ.Θ & Βαγγελάτος Ι.Χ, (2001) « Ηλεκτρονικό Επιχειρείν, Προγραμματισμός και σχεδίαση» Α' Έκδοση, εκδόσεις Ε. Μπένου Αθήνα

III. Σακλαμπανάκης Γ. «Εισαγωγή στο Internet» εκδόσεις Anubis Αθήνα

IV. Κομνηνός Θ. , Σπυράκης Π. «Ασφάλεια Δικτύων υπολογιστικών συστημάτων, αναχαιτίστε τους εισβολείς. Εκδόσεις Ελληνικά Γράμματα 2002

V. Bennett Falk "The Internet Roadmap" Εκδόσεις Κλειδάριθμος Αθήνα 1996

VI. Νάστου Π., Σπυράκης Π, Σταματίου Γ «Σύγχρονη Κρυπτογραφία» Εκδόσεις Ελληνικά γράμματα 2003.

Ηλεκτρονική

I. http://www.el.wikipedia.org

II. http://www.geocities.com/notesgym/c/Networks/1-networks.htm

III. http://users.forthnet.gr/ath/skonstan/site_1/articles/history_files/Web.html

IV. http://www.tech-faq.com/lang/el/p2p-peer-to-peer-file-sharing.shtml

V. http://www.noc.teikav.edu.gr/gr/1024x768/help/www.htm

VI. http://www.cknow.com/vtutor/TypesofViruses.html

VII. http://www.tech-faq.com/lang/el/aes-advanced-encryption-standard-rijndael.shtml

VIII. http://www.tech-faq.com/lang/el/dh-diffie-hellman.shtml

IX. http://www.go-online.gr/ebusiness/specials/article.html?article_id=713

X. http://www.eett.gr/gr_pages/telec/eSign/IntroEsign.htm

XI. http://www.eeei.gr/interbiz/articles/cryptogr.htm

XII. http://www.go-online.gr/ebusiness/specials/article.html?article_id=715

XIII. http://www.islab.demokritos.gr

XIV. http://www.dnssec.net/

XV. http://www.giac.org/resources/whitepaper/cryptography/57.php

XVI. http://csrc.nist.gov/archive/aes/index.html

XVII. http://www.nemis.cti.gr/ebusiness/distance_course.htm

XVIII. http://www.e-erevna.gr/story.aspx?ID=38449.0000

All the Internet sites valid on 19 September 2008