ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος Πτυχιακής Εργασίας :

ΑΣΦΑΛΕΙΑ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Σπουδάστρια : Ασλάνογλου Άννα Α.Μ. 6765

Επιβλέπων Καθηγητής : Δρ. Σταύρος Αθανασόπουλος

ΠΑΤΡΑ ΟΚΤΩΒΡΙΟΣ 2011

ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο, όχι πολλά χρόνια πριν, αποτελούσε ένα κατά πολύ μικρότερο «μέρος» συγκριτικά με σήμερα. Οι κόμβοι του ήταν διεσπαρμένοι σε μερικά ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες. Οι χρήστες του περιλάμβαναν φοιτητές, ερευνητές και γενικότερα ανθρώπους που ασχολούνταν κατά τον έναν ή τον άλλο τρόπο με την τεχνολογία και τις επιστήμες. Η υποδομή του, το διάσημο ζεύγος πρωτοκόλλων TCP/IP, είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά, χωρίς να περιλαμβάνει ιδιαίτερους μηχανισμούς ή «δικλίδες».

Όμως κατά την πάροδο των χρόνων υπήρχε τεράστια ανάπτυξη του διαδικτύου που οδηγεί καθημερινά στην μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή-ηλεκτρονική μορφή. Καθώς σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός, ιδρύματα, εταιρείες και ιδιώτες χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο τις περισσότερες φορές για την διαχείριση των δεδομένων τους, η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο συζητιέται. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή.

Η εξάρτηση μας στα συστήματα αυτά, και το γεγονός ότι η λειτουργικότητα και η φιλικότητα των υπολογιστικών συστημάτων έχουν αυξηθεί σημαντικά, οδηγούν σε μια ενισχυμένη πολυπλοκότητα των συστημάτων αυτών. Η πολυπλοκότητα αυτή οδηγεί σε μια πληθώρα αδυναμιών και προβλημάτων στην ασφάλεια των συστημάτων και των δεδομένων, είτε από προγραμματιστικά λάθη, είτε από κακές ρυθμίσεις, είτε από τις σχέσεις εμπιστοσύνης που δημιουργούνται, είτε από άλλους λόγους. Ο πληθυσμός του Internet αν και έχει ακουστά πολλές περιπτώσεις παραβίασης της ασφάλειας συστημάτων και κλοπής δεδομένων, δεν έχει δεχτεί μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια. Οι περισσότεροι χρήστες βρίσκονται σε σύγχυση όσον αφορά την ασφάλεια των δεδομένων τους, μην γνωρίζοντας τους κινδύνους και τις απειλές που αντιμετωπίζουν, ενώ οι εταιρείες παροχής υπηρεσιών –είτε πρόκειται για e-mail, είτε για υποβολή φορολογικών δηλώσεων και web banking- εθίζουν τους χρήστες σε πρακτικές χαμηλής ασφάλειας και παρέχουν μια αίσθηση ότι ασχολούνται

αποτελεσματικά με την ασφάλεια των δεδομένων τους.

Οι χρήστες παραβιασμένων συστημάτων αντιμετωπίζουν πολύ σοβαρούς κινδύνους, χωρίς να το γνωρίζουν τις περισσότερες φορές. Ένας επιτιθέμενος μπορεί να παρακολουθεί ό,τι πληκτρολογείται στον υπολογιστή για να μάθει αριθμούς πιστωτικών καρτών και κωδικούς, να χρησιμοποιήσει το σύστημα για τη διακίνηση πορνογραφικού υλικού, να αποσπάσει ευαίσθητα δεδομένα, ακόμα και να πραγματοποιήσει επιθέσεις σε άλλα συστήματα μέσω αυτού, ώστε να σβήσουν τα ίχνη του. Οι επιθέσεις στο διαδίκτυο αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό, μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων. Καθημερινά ανακοινώνονται καινούργιες αδυναμίες στο λογισμικό και νέοι τρόποι επίθεσης. Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που αυτά περιέχουν και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Όλες αυτές οι απειλές είναι σημαντικοί λόγοι για να αυξηθεί η ασφάλεια στο διαδίκτυο και μεταξύ των χρηστών του. Αυτό περιλαμβάνει τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το διαδίκτυο και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές.

Αν και υπάρχει πολύ πληροφορία στο διαδίκτυο για την ασφάλεια δικτύων και συστημάτων, πολλές φορές δεν μπορεί να κατανοηθεί από χρήστες με λίγες γνώσεις. Άλλες φορές η πληροφορία δεν είναι συγκεκριμένη, δεν προχωράει σε μεγάλα επίπεδα λεπτομέρειας και καταλήγει ελλιπής. Επίσης τα τελευταία χρόνια, σημαντικές είναι και οι αναφορές προβλημάτων γύρω από εμπορικές συναλλαγές που αφορούν ένα νέο είδος εμπορίου. Αυτή η νέα μορφή εμπορίου, το ηλεκτρονικό εμπόριο (electronic commerce) έχει κάνει δυναμική εμφάνιση και διεκδικεί σημαντικό μερίδιο από το παραδοσιακό εμπόριο. Κάθε εμπορική δραστηριότητα που πριν από μερικά χρόνια ήταν δυνατή, μόνο χάρη στη φυσική παρουσία και μεσολάβηση ανθρώπων ή υλικών μέσων (π.χ. εμπορική αλληλογραφία), σήμερα

μπορεί να επιτευχθεί αυτόματα, ηλεκτρονικά και εξ' αποστάσεως. Η ανάπτυξη του ηλεκτρονικού εμπορίου οφείλεται ακριβώς στο γεγονός ότι προσφέρει τη δυνατότητα να πραγματοποιούνται κάθε είδους συναλλαγές, συμπεριλαμβανομένων της πώλησης αγαθών και υπηρεσιών, μέσα από ηλεκτρονικά μέσα με μεγάλη ταχύτητα και μικρό κόστος.

Στις μέρες μας, το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι του παγκοσμίου εμπορίου. Για πολλούς θεωρείται ίσως η δεύτερη μεγαλύτερη τεχνολογική εξέλιξη μετά τη βιομηχανική επανάσταση, καθώς εξοικονομεί χρόνο και χρήμα και μπορεί να μεταμορφώσει μια μικρή εταιρεία ακόμα και σε κολοσσό. Αυτή τη στιγμή περισσότεροι από 40.000.000 άνθρωποι σε όλο τον κόσμο δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και σε πολύ λίγα χρόνια ο αριθμός αυτός αναμένεται να αυξηθεί ραγδαία. Ο όρος ηλεκτρονικό εμπόριο καλύπτει οποιαδήποτε μορφή επιχειρηματικής δραστηριότητας, εμπορικής συναλλαγής ή ανταλλαγής πληροφοριών η οποία διεξάγεται χρησιμοποιώντας κάθε μορφής Τεχνολογία Πληροφορικής ή Επικοινωνιών. Ο ορισμός αυτός ενσωματώνει όχι μόνο συναλλαγές που λαμβάνουν χώρα μέσω του Διαδικτύου, αλλά μια ευρεία γκάμα δυνατοτήτων συναλλαγής, όπως για παράδειγμα μέσω κινητών τηλεφώνων ή πρωτοκόλλων διακίνησης δεδομένων που επιτρέπουν την Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange, EDI).

Αν και ο παραπάνω ορισμός για το ηλεκτρονικό εμπόριο, καλύπτει ένα ευρύ φάσμα συναλλαγών, συνήθως χρησιμοποιείται για τις αγοραπωλησίες που πραγματοποιούνται διαμέσου του Διαδικτύου. Για τις υπόλοιπες δραστηριότητες χρησιμοποιείται, τα τελευταία χρόνια, ο όρος ηλεκτρονικό επιχειρείν (electronic business). Η έννοια του ηλεκτρονικού επιχειρείν καλύπτει και άλλες επιχειρηματικές δραστηριότητες όπως την ενδοεπιχειρησιακή επικοινωνία και τη συνεργασία σε επίπεδο επιχειρήσεων.

Οι επιχειρήσεις, στην προσπάθεια διατήρησης σημαντικής θέσης στην αγορά ή απόκτησης ανταγωνιστικού πλεονεκτήματος μέσω καινοτόμων διαδικασιών μείωσης κόστους και βελτίωσης της εξυπηρέτησης των πελατών, ολοένα και περισσότερο στρέφονται στο ηλεκτρονικό εμπόριο. Ήδη, πλειάδα επιχειρήσεων, τόσο στην Ευρώπη όσο και στην Αμερική, διαθέτουν τα προϊόντα τους μέσω του Διαδικτύου. Κορυφαίο παράδειγμα αυτής της εξέλιξης αποτελεί το Amazon.com, το οποίο είναι αυτή τη στιγμή το μεγαλύτερο ηλεκτρονικό βιβλιοπωλείο στον

κόσμο. Στην Ελλάδα, αν και υπάρχει μια σχετική καθυστέρηση σε αυτό τον τομέα, οι εξελίξεις είναι σημαντικές και υπάρχουν ήδη αρκετές εταιρείες και επιχειρήσεις που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Επιπλέον υπάρχουν ήδη στη χώρα μας και εταιρείες που προσφέρουν λύσεις ηλεκτρονικού εμπορίου σε επιχειρήσεις που έχουν ανοίξει ή θα ήθελαν να ανοίξουν κάποιο ηλεκτρονικό κατάστημα. Σε κάθε περίπτωση, ο κύριος λόγος που μια επιχείρηση δραστηριοποιείται σε ηλεκτρονικό επίπεδο είναι για να προσελκύσει αγοραστικό κοινό πέρα από τα στενά όρια της γεωγραφικής της έδρας, αυξάνοντας έτσι τις πωλήσεις των προϊόντων της.

1ο ΚΕΦΑΛΑΙΟ: ΕΙΣΑΓΩΓΗ

1.1 Η Ιστορία του Internet

Το σημερινό Internet αποτελεί τη σημερινή εξέλιξη του ARPANET, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του ’60 στις ΗΠΑ όπου στα πανεπιστήμια αρχίζουν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο ARPANET γεννιέται το 1969 με πόρους του προγράμματος ARPA (Advanced Research Project Agency) του Υπουργείου Αμύνης με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Στην αρχική του μορφή το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), συμφώνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή. Στόχος ήταν η δημιουργία νέος διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων. Κάθε πακέτο θα είχε την πληροφορία που χρειαζόταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνδεση του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης. Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

Το 1973 ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Πρόγραμμα Διαδικτυακής (Internetting Project) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται ένα νέο πρωτόκολλο το Internet Protocol (IP) (Πρωτόκολλο Διαδικτύωσης), από την οποία θα πάρει αργότερα το όνομα του το Internet. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε τελικά οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με

οποιονδήποτε άλλον. Παράλληλα, σχεδιάζεται ένα νέο πρωτόκολλο για τον έλεγχο της μετάδοσης των δεδομένων, το Transmission Control Protocol (TCP) (Πρωτόκολλο Έλεγχου Μετάδοσης). Ορίζονται προδιαγραφές για την μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (e-mail). Σταδιακά συνδέονται με το ARPANET ιδρύματα από άλλες χώρες, με πρώτα το University College of London και το Royal Radar Establishment στην Νορβηγία.

Το 1983 το πρωτόκολλο TCP/IP (δηλαδή ο συνδυασμός TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος Berkley UNIX το οποίο περιλαμβάνει το TCP/IP συντελεί στη γρήγορη εξάπλωση της Διαδικτύωσης των υπολογιστών. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983 χωρίζεται σε δυο τμήματα: στο MILNET (για στρατιωτικές επικοινωνίες) και στο νέο ARPANET(για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και για συνέχιση της έρευνας στη δικτύωση). Το 1986, το National Science Foundation (NFS) δημιουργεί ένα δικό του γρήγορο δίκτυο, το NSFNET χρησιμοποιώντας το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπέρ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του ’80 όλο και περισσότερες χώρες συνδέονται στο NSFNET (Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμάνια, Ιταλία κ.ά.). Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό ως Internet και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Το 1990 το ARPANET πλέον καταργείται.

Στις αρχές της δεκαετίας του ’90 όλο και περισσότερες χώρες αρχίζουν να συνδέονται στο Internet, μεταξύ των οποίων και η Ελλάδα το 1990. Το 1993 το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (Παγκόσμιος Ιστός, το γνωστό πλέον www) που ανατήχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασης τους σε ηλεκτρονικές σελίδες, στις όποιες μπορεί νε περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρηστή. Παράλληλα εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες

παροχής υπηρεσιών Internet (Internet Service Providers-ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα.
Εν τω μεταξύ, κατά τη διάρκεια της δεκαετίας, το Διαδίκτυο φιλοξενεί επιτυχώς την πλειοψηφία των παλιότερων δημόσιων δικτύων υπολογιστών (αν και ορισμένα δίκτυα παρέμειναν χωριστά). Κατά τη διάρκεια της δεκαετίας του 1990, υπολογίστηκε ότι το Διαδίκτυο αυξήθηκε κατά 100 τοις εκατό ανά έτος, με μια σύντομη περίοδο εκρηκτικής ανάπτυξης το 1996 και το 1997. Αυτή η ανάπτυξη συχνά αποδίδεται στην έλλειψη κεντρικής διοίκησης, η οποία επιτρέπει οργανική ανάπτυξη του διαδίκτυου, καθώς και στο μη ιδιόκτητο ανοικτό χαρακτήρα των πρωτόκολλων του Διαδικτύου, τα οποία ενθαρρύνουν τη διαλειτουργικότητα των πωλητών και αποτρέπουν κάθε μια εταιρεία από την άσκηση υπερβολικού έλεγχου στο δίκτυο. Ο εκτιμώμενος πληθυσμός των χρηστών του Διαδικτύου είναι 1.97 δις από τις 30 Ιουνίου 2010.

1.2 Το Internet Σήμερα

Στις μέρες μας το Internet, σε συνδυασμό με την ολοένα αναπτυσσόμενη ψηφιακή τεχνολογία, έχει δημιουργήσει μία τεράστια αγορά γνώσεων/πληροφοριών. Παραδοσιακές μορφές τέχνης (όπως για παράδειγμα ο κινηματογράφος και η μουσική) μέσω της ψηφιακής τεχνολογίας παίρνουν την ίδια μορφή (αρχείων δεδομένων) με αντικείμενα που εκ πρώτης όψεως είναι εντελώς διαφορετικά (όπως για παράδειγμα η ιατρική επιστήμη ή κάποιο πρόγραμμα λογισμικού). Παρατηρείται λοιπόν μία συγκέντρωση γνώσης ή, αν είναι δυνατό να λεχτεί, πολιτιστικής κληρονομιάς, που σχετίζεται άμεσα με το Internet. Το μεγάλο ερώτημα που προκύπτει πλέον είναι το "ποιος θα διοικήσει, ποιος θα ελέγξει την γνώση αυτή".
Από τη στιγμή που το Διαδίκτυο είναι ένα δίκτυο συνδεδεμένων υπολογιστών, κάθε χρήστης έχει την δυνατότητα να μοιραστεί πληροφορίες με άλλους χρήστες γενόμενος, πολλές φορές, ο ίδιος δημιουργός και πάροχος των πληροφοριών αυτών. Δεν υπάρχει άμεσος έλεγχος των πληροφοριών που "ανεβαίνουν" στο Διαδίκτυο από κάποιον ιεραρχικά ανώτερο χρήστη ή οργανισμό. Το θέμα της μη

ιεραρχημένης πληροφορίας, όμως, τίθεται υπό αμφισβήτηση. Ο όγκος της πληροφορίας στο Διαδίκτυο είναι πράγματι μεγάλος. Παρ' όλα αυτά, υπάρχουν πληροφορίες ευκολότερα και δυσκολότερα προσβάσιμες από τον χρήστη.

Το Internet έκανε δυνατή την συγκέντρωση μεγάλου όγκου πληροφοριών και επηρέασε σημαντικά τον τρόπο διάθεσής τους. Δεν συμβαίνει, όμως, στον ίδιο βαθμό το ίδιο και στον τρόπο παραγωγής αυτών. Για παράδειγμα, ο τρόπος παραγωγής μιας κινηματογραφικής ταινίας δεν έχει επηρεαστεί σημαντικά από την ύπαρξη του Internet, ανεξάρτητα από το αν έχει επηρεαστεί ή όχι από την ψηφιακή τεχνολογία. Παρ' όλα αυτά, το Διαδίκτυο ασκεί μεγάλη επίδραση στην διαδικασία παραγωγής δημοσιογραφικών προϊόντων. Η δημιουργία της είδησης παύει να είναι πλέον μονοπώλιο λίγων, αφού ο κάθε χρήστης μπορεί εάν το επιθυμεί να δημιουργήσει πληροφορία ανά πάσα στιγμή. Το πιο τρανταχτό παράδειγμα της επίδρασης αυτής είναι τα ιστολόγια (blogs), όπου μπορεί κανείς να εκφέρει απόψεις και να σχολιάσει γεγονότα πάσης φύσεως. Ως αποτέλεσμα της επιρροής αυτής του Internet στη παραγωγή ειδήσεων τα όρια μεταξύ ενός απλού χρήστη του διαδικτύου και ενός επαγγελματία δημοσιογράφου γίνονται περισσότερο δυσδιάκριτα. Αυτό με τη σειρά του οδηγεί στην ανάγκη για επαναπροσδιορισμό της έννοιας της δημοσιογραφίας καθώς και της απαραίτητης εκπαίδευσης των δημοσιογράφων. Η ανάγκη για τον επαναπροσδιορισμό της δημοσιογραφίας, όμως, δεν είναι τόσο μεγάλη σύμφωνα με τους υποστηριχτές της "αντι-πλουραλιστικής" προσέγγισης, καθώς θεωρούν πως το Internet δεν μπορεί να ασκήσει ουσιαστική επίδραση στην επικοινωνία γενικότερα και στην δημοσιογραφία ειδικότερα.

Επίσης, λόγω της μεγάλης συγκέντρωσης γνώσης στο Διαδίκτυο, η έννοια της κοινωνικής ισότητας παίρνει και πάλι μεγάλη σημασία. Το χάσμα ανάμεσα σε πληροφοριακά πλούσιους και πληροφοριακά φτωχούς θα διευρύνεται όσο αυξάνεται η συγκέντρωση της γνώσης αυτής. Το παραπάνω αποτελεί ακόμα έναν λόγο που κάνει πιο επιτακτική την ανάγκη για διερεύνηση του αρχικού ερωτήματος "ποιος θα ελέγξει τη γνώση αυτή".

Στην πρώτη δεκαετία του 21ου αιώνα, η πρώτη γενιά μεγαλώνει με ευρεία διαθεσιμότητα της σύνδεσης στο Internet, φέρνοντας συνέπειες και ανησυχίες σε τομείς όπως η ιδιωτική ζωή και η ταυτότητα, και την κατανομή των υλικών με

πνευματικά δικαιώματα. Αυτή η «ψηφιακά αναθρεμμένη» γενιά αντιμετωπίζει ποικίλες προκλήσεις που δεν ίσχυαν κατά την προηγούμενη γενιές.

Το Διαδίκτυο έχει επιτύχει νέο ενδιαφέρον ως πολιτικό εργαλείο, οδηγώντας σε λογοκρισία του Διαδικτύου από ορισμένα κράτη. Η προεδρική εκστρατεία του Howard Dean το 2004 στις Ηνωμένες Πολιτείες ήταν αξιοσημείωτη για την επιτυχία της στο να ζητά τη δωρεά μέσω του Διαδικτύου. Πολλές πολιτικές ομάδες χρησιμοποιούν το Διαδίκτυο για να επιτευχθεί μια νέα μέθοδος οργάνωσης με σκοπό την εκπλήρωση της αποστολής τους, με αποτέλεσμα να έχει ανθίσει ο ακτιβισμός στο Διαδίκτυο. Ορισμένες κυβερνήσεις, όπως αυτές του Ιράν, της Βόρειας Κορέας, της Λαϊκής Δημοκρατίας της Κίνας και της Σαουδικής Αραβίας, περιορίζουν αυτό που οι άνθρωποι στις χώρες τους μπορούν να έχουν πρόσβαση στο Διαδίκτυο, ιδίως πολιτικού και θρησκευτικού περιεχομένου. Αυτό επιτυγχάνεται μέσω λογισμικού που φιλτράρει domain names και περιεχόμενο έτσι ώστε να μην μπορεί να είναι εύκολα προσβάσιμο.

Πολλοί άνθρωποι χρησιμοποιούν το World Wide Web για να αποκτήσουν πρόσβαση σε ειδήσεις, να μάθουν τα νέα για τον καιρό και τα αθλητικά, να σχεδιάσουν και να κλείσουν τις διακοπές τους και για να μάθουν περισσότερα για τα ενδιαφέροντά τους. Επίσης χρησιμοποιούν το chat και τα e-mail για να μένουν σε επαφή με τους φίλους τους σε όλο τον κόσμο, όπως υπήρχαν παλιότερα οι φίλοι δι' αλληλογραφίας.

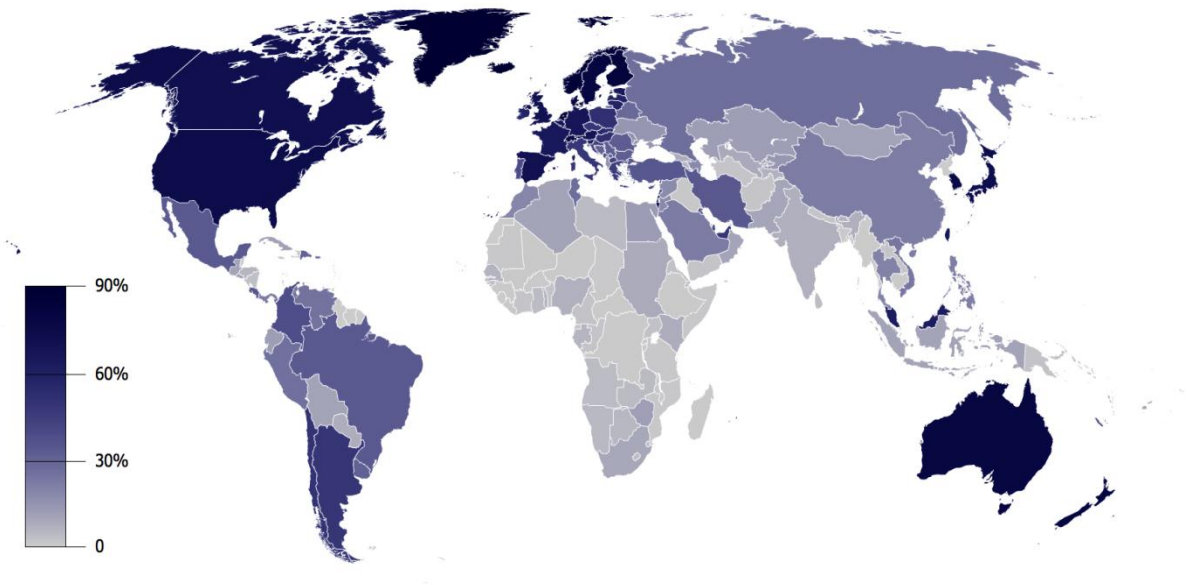
Η γλώσσα που χρησιμοποιείται περισσότερο στη διακίνηση της πληροφορίας στο Διαδίκτυο είναι η Αγγλική. Έχοντας αναπτυχθεί τα τελευταία χρόνια, το Διαδίκτυο περιλαμβάνει πλέον ποιοτικά και ποσοτικά ευρύ περιεχόμενο και στις υπόλοιπες γλώσσες των περισσότερο αναπτυγμένων χωρών. Ωστόσο, υπάρχουν ακόμα δυσλειτουργίες και τεχνικά προβλήματα σχετικά με την κωδικοποίηση, όπως το mojibake το οποίο είναι η αδυναμία ενός λογισμικού να αναπαράγει με ακριβή τρόπο ένα κείμενο, τηρώντας τη σχετική κωδικοποίηση χαρακτήρων.

1.3 Η Πρόσβαση στο Διαδίκτυο

Κοινές μέθοδοι πρόσβασης στο Διαδίκτυο στο σπίτι είναι οι dial-up συνδέσεις, οι ευρυζωνικές (πάνω από ομοαξονικό καλώδιο, οπτικές ίνες ή χαλκόσύρματα), μέσω Wi-Fi, δορυφόρο και κινητά τηλέφωνα 3G τεχνολογίας. Δημόσιοι χώροι για χρήση

του Διαδικτύου περιλαμβάνουν τις βιβλιοθήκες και τα Internet cafes, όπου υπάρχουν διαθέσιμοι Η/Υ με σύνδεση στο Διαδίκτυο. Υπάρχουν, επίσης, σημεία πρόσβασης στο Διαδίκτυο σε δημόσιους χώρους όπως αίθουσες αναμονής αεροδρομίων, μερικές φορές μόνο για σύντομη χρήση ενόσω βρισκόμαστε σε αναμονή. Τέτοια σημεία είναι γνωστά και με διάφορους άλλους όρους, όπως «δημόσια περίπτερα Διαδικτύου», «δημόσια τερματικά Διαδικτύου» και «ιστο - τηλέφωνα».

Η δικτύωση μέσω Wi-Fi παρέχει ασύρματη πρόσβαση στο Διαδίκτυο. Ασύρματα σημεία πρόσβασης (hotspot) που παρέχουν τέτοια πρόσβαση περιλαμβάνουν τα Wifi-cafes, όπου κάποιος αρκεί να φέρει τις δικές του/της ασύρματες συσκευές όπως φορητό Η/Υ,PDA ή κινητό τηλέφωνο. Οι υπηρεσίες αυτές μπορεί να είναι δωρεάν σε όλους, είτε δωρεάν μόνο σε πελάτες, είτε επί πληρωμή. Ένα hotspot δεν χρειάζεται να περιορίζεται σε ένα συγκεκριμένο περιβάλλον. Ολόκληρες πανεπιστημιουπόλεις και πάρκα έχουν αυτή τη δυνατότητα, ακόμα και ολόκληρες περιοχές. Οι εμπορικές υπηρεσίες Wi-Fi που καλύπτουν μεγάλες περιοχές της πόλης έχουν τεθεί σε εφαρμογή σε Λονδίνο, Βιέννη, Τορόντο, Σαν Φρανσίσκο, Φιλαδέλφεια, Σικάγο και Πίτσμπουργκ, ακόμα και σε πολλές πόλεις στην Ελλάδα, όπως Καλαμάτα, Τρίπολη, κ.ά.



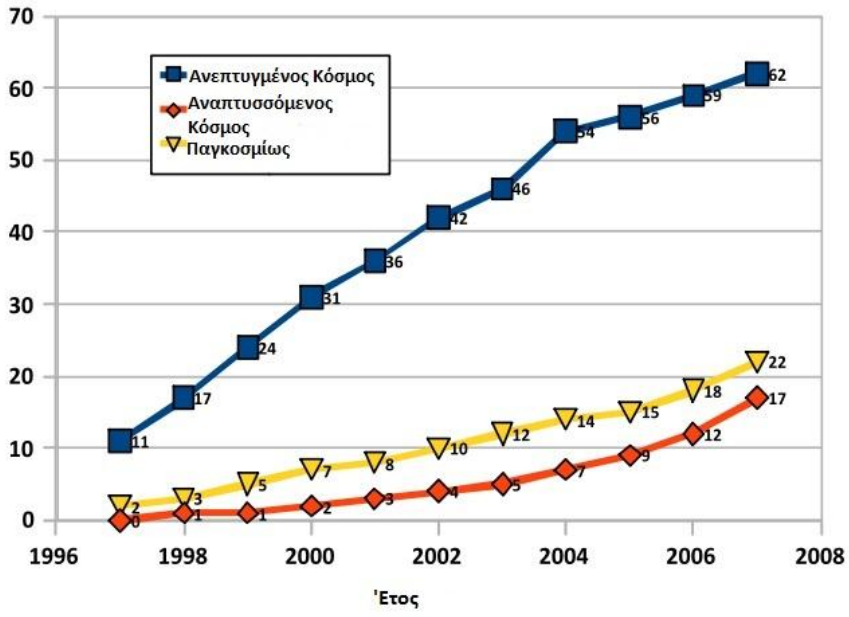
Παγκόσμια Πρόσβαση στο Internet (Ιούνιος 2009)

Τα πλεονεκτήματα της πρόσβασης ενός χρήστη μέσω του δικού του υπολογιστή (αντί μέσω δημόσιου τερματικού) περιλαμβάνουν τη δυνατότητα για κατέβασμα

και ανέβασμα αρχείων χωρίς περιορισμούς, τη χρήση του αγαπημένου του φυλλομετρητή (web browser) και των ρυθμίσεων αυτού (το μενού των ρυθμίσεων μπορεί να απενεργοποιηθεί σε έναν δημόσιο υπολογιστή) και την εκτέλεση δραστηριοτήτων στο Ίντερνετ με τη χρήση δικών του προγραμμάτων και δεδομένων.

Χώρες με πολύ καλή πρόσβαση στο Ίντερνετ περιλαμβάνουν την Νότια Κορέα, όπου το 50% του πληθυσμού έχει ευρυζωνική πρόσβαση, τη Σουηδία και τις ΗΠΑ. Από το 2009 και μετά, το Διαδίκτυο αναμένεται να αυξηθεί σημαντικά στη Βραζιλία, τη Ρωσία, την Ινδία, την Κίνα και την Ινδονησία (BRICI χώρες). Αυτές οι χώρες έχουν μεγάλο πληθυσμό και μέτρια έως υψηλή οικονομική ανάπτυξη, αλλά ακόμα χαμηλά ποσοστά διείσδυσης του Διαδικτύου. Το 2009, οι χώρες BRICI αντιπροσώπευαν περίπου το 45 τοις εκατό του παγκόσμιου πληθυσμού και είχαν περίπου 610 εκατομμύρια χρήστες του Διαδικτύου, αλλά μέχρι το 2015, οι χρήστες του Διαδικτύου στις BRICI χώρες θα διπλασιαστεί στα 1,2 δισ. ευρώ, και θα τριπλασιαστεί στην Ινδονησία.

Χρήστες του Internet ανά 100 κατοίκους 1997-2007



1.4 Η Χρήση του Διαδικτύου στην Ελλάδα

Σχετικά με τη χρήση του Διαδικτύου στην Ελλάδα, παρατηρείται σημαντική αύξηση του αριθμού των χρηστών (από 13% το 2001 σε 31% το 2007) ηλικίας 15 έως 65 ετών που κατέχουν προσωπικό Η/Υ. Αντίστοιχα, παρατηρείται αύξηση των ωρών χρήσης του Διαδικτύου που φτάνουν κατά μέσω όρο τις 8,6 ανά εβδομάδα.

Η υπηρεσία που χρησιμοποιείται περισσότερο είναι το ηλεκτρονικό ταχυδρομείο (e-mail) αλλά και η ενημέρωση (νέα, καιρός, αθλητικά) αποτελεί από τους κυριότερους λόγους χρήσης του Διαδικτύου. Αντίθετα, η αναζήτηση για προϊόντα και υπηρεσίες ακολουθεί πτωτική πορεία από το 2002. Ιδιαίτερα χαμηλή παραμένει η χρήση του Διαδικτύου για αγορά προϊόντων και υπηρεσιών. Περίπου 18% των χρηστών προχώρησε σε κάποια αγορά κατά το 2006 ωστόσο το ποσοστό αυτό ανέρχεται μόλις στο 4,5% του γενικού πληθυσμού. Παρόλα αυτά, οι αγορές πραγματοποιήθηκαν κυρίως από ελληνικούς ιστοχώρους (sites) (41%) έναντι των ξένων (35%). Οι χρήστες που αγοράζουν μέσω του Διαδικτύου συνήθως δεν επισκέπτονται τα αντίστοιχα καταστήματα, ενώ οι κυριότεροι λόγοι αγοράς είναι η προσιτή τιμή και η καλή εξυπηρέτηση. Τέλος, αξιοσημείωτο είναι το γεγονός ότι σε ποσοστό πάνω από 60% οι χρήστες θεωρούν ότι ο κίνδυνος διαρροής προσωπικών δεδομένων κατά τη χρήση πιστωτικής κάρτας στις ηλεκτρονικές αγορές είναι μεγάλος ή πολύ μεγάλος.*(Η έρευνα πραγματοποιήθηκε (για το διάστημα 2001-2006) από την εταιρία VPRC για λογαριασμό του ebusinessforum και του Εθνικού Δικτύου Έρευνας και Τεχνολογίας.)*

2ο ΚΕΦΑΛΑΙΟ: ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

2.1 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Τα τελευταία χρόνια ολοένα και μεγαλύτερος αριθμός εμπορικών συναλλαγών γίνεται μέσω του Διαδικτύου (Internet). Η δραστηριότητα αυτή είναι γνωστή ως ηλεκτρονικό εμπόριο. Το ηλεκτρονικό εμπόριο, ανάμεσα στα άλλα, περιλαμβάνει τραπεζικές εργασίες πραγματικού χρόνου (on-line banking), χρηματιστηριακές συναλλαγές, αγορά και πώληση αγαθών μέσω του Διαδικτύου. Κάθε καταναλωτής, χρησιμοποιώντας τη πιστωτική του κάρτα, μπορεί για παράδειγμα να αγοράσει ένα βιβλίο να κάνει κράτηση αεροπορικών εισιτηρίων, να νοικιάσει αυτοκίνητο, να κλείσει δωμάτια σε ξενοδοχεία ενώ κάθεται απλά στον υπολογιστή του (ή απλά χρησιμοποιώντας το κινητό του τηλέφωνο στο λεγόμενο M–commerce).

2.1.1 Ιστορία Ηλεκτρονικού Εμπορίου

1970: Εμφανίζονται τα πρώτα συστήματα ηλεκτρονικής μεταφοράς χρηματικών πόρων (Electronic Funds Transfer EFT) μεταξύ τραπεζών, που χρησιμοποιούν ασφαλή ιδιωτικά δίκτυα. Τα συστήματα αυτά αλλάζουν με την πρωτοπορία τους τη μορφή των αγορών.

1980: Οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονται στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα Electronic Data Interchange EDI 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 παλιότερα απαιτούσαν έντυπα, όπως παραγγελίες αγοράς , συνοδευτικά έγγραφα και επιταγές πληρωμής, μπορούν να γίνουν κατά ένα μέρος ή στο σύνολο τους ηλεκτρονικά , με δομημένο τρόπο χάρη στα συστήματα EDI ή μέσω του ηλεκτρονικού ταχυδρομείου.

Τέλη 1980-Αρχες 1990: Τα ηλεκτρονικά δίκτυα προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας, με δυνατότητες όπως ηλεκτρονικό ταχυδρομείο, ηλεκτρονική διάσκεψη ,και ηλεκτρονική συνομιλία , ομάδες συζήτησης ,

μεταφορά αρχείων κτλ. Η πρόσβαση στο διαδίκτυο γίνεται φθηνότερη λόγω της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών .

Μέσα δεκαετίας 1990: Η εμφάνιση του παγκοσμίου ιστού (www) στο ιντερνέτ και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών 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 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 ευαγώγων- εξαγωγών και των επικοινωνιών, καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών.

2.1.2 Τι είναι το Ηλεκτρονικό Εμπόριο

Με τον όρο "ηλεκτρονικό εμπόριο" εννοούμε κάθε είδος εμπορικής συναλλαγής μεταξύ πρόσωπων (φυσικών και μη) που πραγματοποιείται με ηλεκτρονικά μέσα. Ουσιαστικά, είναι η διάθεση και η αγοραπωλησία προϊόντων ηλεκτρονικά, η διεκπεραίωση εμπορικών λειτουργιών και συναλλαγών χωρίς τη χρήση χαρτιού, συνήθως μέσω δικτύων ηλεκτρονικών υπολογιστών. Πρόκειται δηλαδή για την αγοραπωλησία αγαθών, πληροφοριών και υπηρεσιών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

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 ιντερνέτ ανεξάρτητα από τη γεωγραφική απόσταση.
- Επικοινωνία: Ως δυνατότητα παροχής πληροφοριών, προϊόντων ή υπηρεσιών και πληρωμών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

Στα συστήματα ηλεκτρονικών συναλλαγών εντάσσεται κάθε μέθοδος που χρησιμοποιείται για να εξυπηρετήσει την πραγματοποίηση αγορών μέσω Internet. Ορίζοντας τις ηλεκτρονικές συναλλαγές με αυτόν τον τρόπο, μπορούμε να συμπεριλάβουμε σε αυτές- εκτός από τις αμιγώς ψηφιακές – και κάποιες παραδοσιακές μεθόδους. Έτσι, σύστημα ηλεκτρονικών συναλλαγών θεωρούνται όχι μόνο η χρήση πιστωτικών καρτών, το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές, αλλά και το έμβασμα, η αντικαταβολή, η μεταφορά χρημάτων σε λογαριασμό κ.ά. Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι μπορούν να ενσωματωθούν στη λειτουργία ενός on-line καταστήματος εξυπηρετώντας τις αγοραπωλησίες και το εν γένει ηλεκτρονικό εμπόριο.

Στις μέρες μας το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι του παγκοσμίου εμπορίου. Πολλοί θεωρούν ότι είναι η δεύτερη μεγαλύτερη τεχνολογική εξέλιξη μετά τη βιομηχανική επανάσταση, καθώς εξοικονομεί χρόνο και χρήμα και μπορεί να μεταμορφώσει μια μικρή εταιρία ακόμα και σε κολοσσό. Αυτή τη στιγμή περισσότεροι από 40.000.000 άνθρωποι σε όλο τον κόσμο δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και σε πολύ λίγα χρόνια ο αριθμός αυτός αναμένεται να αυξηθεί ραγδαία. Υπολογίζεται πως το αργότερο σε 10 χρόνια όλες οι συναλλαγές θα γίνονται ηλεκτρονικά. Με άλλα λόγια, το ηλεκτρονικό εμπόριο είναι το εμπόριο του μέλλοντος.

2.1.3 Κατηγορίες Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο μπορεί να διαχωριστεί σε διάφορες κατηγορίες. Ο διαχωρισμός του ηλεκτρονικού εμπορίου γίνεται με κριτήριο τις οντότητες που εμπλέκονται σε μια ηλεκτρονική συναλλαγή. Έτσι μπορούμε να διακρίνουμε τις παρακάτω κατηγορίες ηλεκτρονικού εμπορίου.

1) Business-to-Government

Η κατηγορία Business-to-Government σημαίνει ότι πραγματοποιούνται ηλεκτρονικές συναλλαγές μεταξύ κυβέρνησης και επιχειρήσεων. Αυτός ο τρόπος

εμπορίου συχνά περιγράφει τον τρόπο με τον οποίο οι κυβερνήσεις αγοράζον προϊόντα και υπηρεσίες μέσω του διαδικτύου.

2) Government-to-Citizen

Η κατηγορία αυτή περιλαμβάνει κάθε είδους αλληλεπίδραση μεταξύ ενός πολίτη και της κυβέρνησης. Σε αυτήν την κατηγορία οι οντότητες που εμπλέκονται μεταξύ τους μπορούν να αναπτύξουν τις εξής δραστηριότητες: πληρωμή φόρων, ψηφοφορίες, ανανέωση διπλώματος οδήγησης καθώς και διάφορες άλλες δραστηριότητες.

3) Business-to-consumer

Στην κατηγορία αυτή τα εμπλεκόμενα μέλη που συναλλάσσονται μεταξύ τους είναι ένας καταναλωτής και μια επιχείρηση. Οι επιχειρήσεις προσφέρουν την δυνατότητα στους καταναλωτές να αγοράσουν τα προϊόντα που προωθούν μέσω του διαδικτύκου (ρούχα, αεροπορικά εισιτήρια, διάφορες υπηρεσίες κ.ά.). Πρόκειται για την πιο διαδεδομένη μορφή ηλεκτρονικού εμπορίου. Ο καταναλωτής έχει πρόσβαση σε μια τεράστια ποικιλία προϊόντων σε δικτυακούς κόμβου – καταστήματα, βλέπει, επιλέγει, αν επιθυμεί να αγοράσει είδη ένδυσης μπορεί ενίοτε και να τα δοκιμάζει (μέσω ειδικών προγραμμάτων), ανακαλύπτει προϊόντα τα οποία δε 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.

4) Consumer-to-Consumer

Η κατηγορία αυτή περιλαμβάνει τις περιπτώσεις όπου κάποιο άτομο προβάλει τα προϊόντα του στο διαδίκτυο. Με αυτόν τον τρόπο κάθε πολίτης έχει τη δυνατότητα να πουλά τα προϊόντα του εύκολα και γρήγορα χωρίς να έρχεται σε επαφή με τον αγοραστή. Το πιο διάσημο παράδειγμα σε αυτήν την περίπτωση είναι οι ηλεκτρονικές δημοπρασίες που γίνονται στο www.eBay.com.

5) Business-to-Business

Αυτή η κατηγορία ηλεκτρονικού εμπορίου αφόρα την πώληση αγαθών ή υπηρεσιών από μια επιχείρηση σε μια άλλη. Για παράδειγμα, μια εταιρία μπορεί να αγοράσει πρώτες ύλες από μια άλλη όταν παρουσιαστεί κάποιο έλλειμμα στην αποθήκη της κι έτσι θα σταλθεί αυτόματα στο σύστημα παραγγελιών της άλλης για να την προμηθεύσει. 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 επίπεδου αποθεμάτων. Επιπλέον καθιστά ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και ποιοτικότερη την εξυπηρέτηση των πελατών.

2.2 Ηλεκτρονικές Συναλλαγές

Με τη συνεχώς αυξανόμενη εμπορευματοποίηση του Internet και τη χρήση του Web πολλές επιχειρήσεις έχουν οδηγηθεί στην υλοποίηση συστημάτων και μεθόδων ηλεκτρονικών πληρωμών προκειμένου να υποστηρίξουν πρακτικά την ανάπτυξη του ηλεκτρονικού εμπορίου στο σύγχρονο επιχειρησιακό περιβάλλον. Έτσι όχι μόνο δεν θεωρείται αρκετή η ανάπτυξη ηλεκτρονικών επιχειρήσεων χωρίς την ανάπτυξη και την εξέλιξη τέτοιων συστημάτων πληρωμών μέσα στο διαδίκτυο, αλλά είναι αδύνατο να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων (πληρωμής) μέσω της ψηφιακής υποδομής.

Στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι πληρωμές γίνονταν εκτός του διαδικτύου με καταβολή των ποσών σε κάποια τράπεζα. Ο αναχρονιστικός όμως αυτός τρόπος χρηματικής εκκαθάρισης των διαδικτυακών συναλλαγών δε συμβάδιζε με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές. Για το λόγο αυτό μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκε σταδιακά. Τα συστήματα αυτά είτε αποτελούσαν μια μεταφορά παραδοσιακών πρακτικών του πραγματικού κόσμου στο διαδίκτυο όπως είναι η περίπτωση on-line πληρωμών με πιστωτική κάρτα, είτε οι δημιουργοί τους προχώρησαν σε καινοτομικές λύσεις που εκμεταλλεύονται τα χαρακτηριστικά του διαδικτύου προκειμένου να προτείνουν πρωτοποριακές λύσεις όπως οι πληρωμές με ηλεκτρονικό χρήμα.

Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο τμήμα του ηλεκτρονικού εμπορίου. Στη γενική του μορφή, ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες, ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις, οι οποίες εκτελούνται με τη μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Κάθε ηλεκτρονική πληρωμή γίνεται εξ αποστάσεως χωρίς

τη φυσική παρουσία του πληρωτή και φυσικά δεν περιλαμβάνει μετρητά. Το περιεχόμενο αυτής της πληρωμής έχει τη μορφή κάποιου ψηφιακού οικονομικού μέσου (π.χ. κρυπτογραφημένους αριθμούς πιστωτικών καρτών, ηλεκτρονικές επιταγές, ή ψηφιακό χρήμα) το οποίο μέσο υποστηρίζεται από κάποιον χρηματοπιστωτικό οργανισμό, τράπεζα ή άλλον ενδιάμεσο φορέα.

Οι ηλεκτρονικές πληρωμές μπορούν να ταξινομηθούν σε τρεις κατηγορίες με βάση την τεχνολογία δικτύου που χρησιμοποιούν. Οι συναλλαγές αυτές μπορούν να πραγματοποιηθούν:

μέσω τηλεφώνου: Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μια καινούργια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρώματα. Πολλές επιχειρήσεις, τράπεζες αλλά και δημόσιες υπηρεσίες επιτρέπουν την εξόφληση λογαριασμών μέσω τηλεφώνου.

μέσω διαδικτύου: Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η εύκολη πρόσβαση στο διαδίκτυο από την πλειοψηφία του καταναλωτικού κοινού, καθιστά τα εν λόγω συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα σημαντικά στην ανάπτυξη του ηλεκτρονικού εμπορίου.

μέσω κινητής τηλεφωνίας (m–payments): Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό καθιστά το κινητό ηλεκτρονικό εμπόριο (m-commerce) ιδιαίτερα δημοφιλή.

2.2.1 Συστήματα Ηλεκτρονικών Πληρωμών

Ο διαρκώς αυξανόμενος όγκος συναλλαγών μέσω διαδικτύου έχει καταστήσει απαραίτητη την ανάπτυξη και διάδοση καινοτομικών συστημάτων ηλεκτρονικών πληρωμών. Στόχος των συστημάτων αυτών είναι να μπορούν να υποστηρίξουν τα ιδιαίτερα χαρακτηριστικά των συναλλαγών στο διαδίκτυο όπως ταχύτητα και αμεσότητα χωρίς όμως παράλληλα να θυσιάζουν βασικά πλεονεκτήματα των παραδοσιακών μέσων πληρωμών όπως είναι η ασφάλεια και η ευκολία.

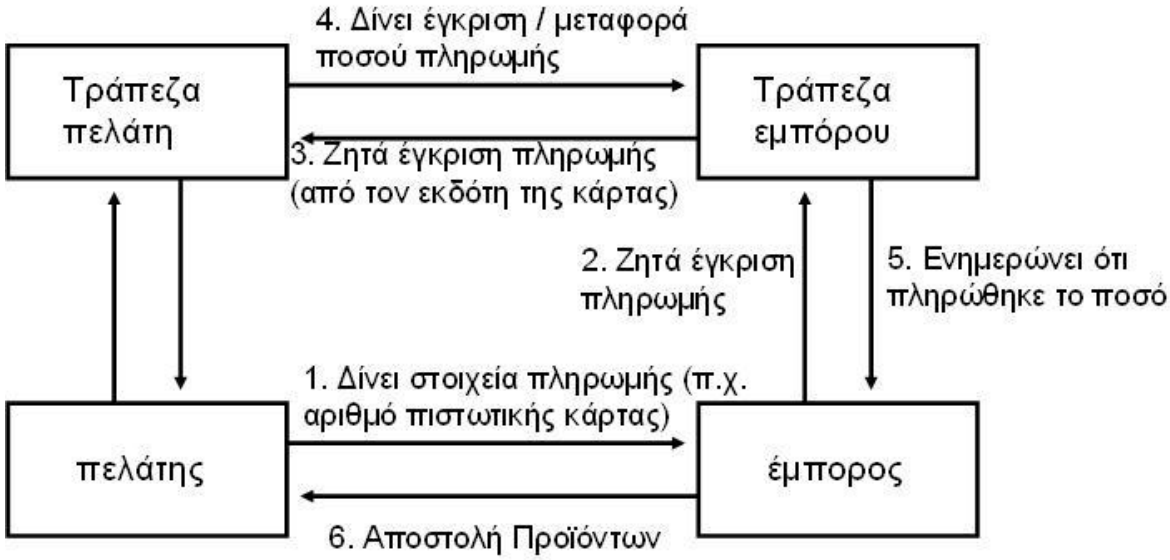
Τα συστήματα ηλεκτρονικών πληρωμών ασχολούνται με οποιοδήποτε είδος υπηρεσίας δικτύου που περιλαμβάνει ανταλλαγή χρημάτων για αγαθά ή υπηρεσίες.

Τα αγαθά μπορεί να είναι φυσικά όπως βιβλία, ή ηλεκτρονικά όπως ηλεκτρονικά έγγραφα, φωτογραφίες, μουσική. Όμοια οι υπηρεσίες μπορεί να είναι φυσικές όπως κράτηση μιας πτήσης, ή ηλεκτρονικές όπως ανάλυση χρηματιστικής αγοράς σε ηλεκτρονική μορφή.

Σε ένα τυπικό σύστημα ηλεκτρονικών πληρωμών μέσω του διαδικτύου, για να γίνει δυνατή μια συναλλαγή πρέπει τόσο ο πελάτης όσο και ο έμπορας να έχουν πρόσβαση στο διαδίκτυο και επίσης πρέπει να έχουν από ένα τραπεζικό λογαριασμό σε κάποια τράπεζα ή χρηματοπιστωτικό οργανισμό. Η τράπεζα (ή χρηματοπιστωτικός οργανισμός) του πελάτη και του έμπορα συνδέονται μεταξύ τους μέσω ενός διατραπεζικού δικτύου και έτσι μπορούν να έρθουν σε επαφή.

Μια τυπική συναλλαγή στο διαδίκτυο (Σχήμα 1) αποτελείται από τα εξής βήματα:

- Ο πελάτης επισκέπτεται το δικτυακό τόπο (site) του εμπόρου και επιλέγει τα προϊόντα που επιθυμεί. Έπειτα στέλνει πληροφορίες στον έμπορο σχετικά με τον τρόπο πληρωμής. Δηλαδή αν ο πελάτης επιθυμεί να πληρώσει με την πιστωτική του κάρτα, στέλνει στον έμπορο τον αριθμό της πιστωτικής του κάρτας και κάποιες άλλες πληροφορίες (π.χ. ημερομηνία έκδοσης της κάρτας κλπ.).
- Ο έμπορος προωθεί τις πληροφορίες που έλαβε από τον πελάτη στην τράπεζα του, προκειμένου να εξακριβώσει την εγκυρότητα του τρόπου πληρωμής (π.χ. της πιστωτικής κάρτας).
- Στη συνέχεια η τράπεζα του έμπορα ζητά έγκριση πληρωμής από την τράπεζα του πελάτη π.χ. από τον οργανισμό έκδοσης της πιστωτικής του κάρτας.
- Η τράπεζα του πελάτη παρέχει έγκριση πληρωμής (αν π.χ. η συγκεκριμένη πιστωτική κάρτα μπορεί να χρεωθεί) και μεταβιβάζει το συμφωνημένο πληρωτέο ποσό από το λογαριασμό του πελάτη στην τράπεζα του έμπορα.
- Η τράπεζα του έμπορα ενημερώνει τον έμπορο πως η συναλλαγή είναι έγκυρη και πως έχει πληρωθεί το συγκεκριμένο χρηματικό ποσό της αξίας των προϊόντων που έχει αγοράσει ο πελάτης.
- Τέλος ο έμπορος αποστέλλει τα προϊόντα ή παρέχει τις συμφωνημένες υπηρεσίες στον πελάτη, σύμφωνα με την παραγγελία.



Σχήμα 1: Τυπική Συναλλαγή Πληρωμής.

Σημειώνεται ότι η όλη διαδικασία της συναλλαγής είναι τελείως διάφανη στους δύο τελικούς χρήστες. Ο πελάτης εμπιστεύεται την τράπεζα του και αγοράζει τα προϊόντα που θέλει, χωρίς να γνωρίζει καμιά από τις υπόλοιπες ενέργειες που μεσολαβούν μέχρι την τελική παράδοση των προϊόντων στο σπίτι του. Από την άλλη πλευρά, ο έμπορος εμπιστεύεται τη δική του τράπεζα η οποία και εγγυάται την πληρωμή των προϊόντων που πωλεί εκείνος, χωρίς να γνωρίζει περισσότερες λεπτομέρειες.

2.3 Σύγχρονες Μέθοδοι Πληρωμής

2.3.1 Πιστωτικές Κάρτες

Αυτή την περίοδο, οι πιστωτικές κάρτες παρέχουν τον πιο διαδεδομένο τρόπο πληρωμής στο διαδίκτυο. Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι των εναλλακτικών μεθόδων πληρωμής. Κατ' αρχήν είναι διεθνώς γνωστές και αποδεκτές από τους εμπόρους, επιτρέποντας έτσι την πραγματοποίηση ακόμη και διεθνών συναλλαγών. Επιπλέον η χρήση τους στις ηλεκτρονικές συναλλαγές δεν διαφέρει και πολύ από την χρήση τους στις φυσικές συναλλαγές. Στις φυσικές συναλλαγές ο πελάτης δίνει την κάρτα του στον έμπορα για χρέωση χέρι με χέρι, ενώ στις

ηλεκτρονικές συναλλαγές ο πελάτης δίνει στον έμπορα τις πληροφορίες της κάρτας του μέσω του διαδικτύου. Αυτό έχει σαν αποτέλεσμα την πραγματοποίηση συναλλαγών χωρίς σημαντικές επενδύσεις από την πλευρά των εμπόρων αλλά και χωρίς αλλαγή στη συμπεριφορά των καταναλωτών.

Κατά την πληρωμή μέσω πιστωτικών καρτών στο διαδίκτυο ο πελάτης κοινοποιεί στον έμπορα τον αριθμό της πιστωτικής του κάρτας, καθώς και άλλες πληροφορίες της κάρτας όπως εκδότη, ημερομηνία λήξεως κλπ. Ο έμπορας ζητά έγκριση από την τράπεζα του η οποία σε συνεργασία με την τράπεζα του πελάτη (οργανισμό έκδοσης της κάρτας) δίνουν ή όχι έγκριση. Σε περίπτωση έγκρισης, ειδοποιείται ο έμπορος ότι η δαπάνη εγκρίθηκε και στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη προωθεί τα χρήματα στο λογαριασμό του έμπορα μέσω του διατραπεζικού συστήματος, και χρεώνει το ποσό στο λογαριασμό της πιστωτικής κάρτας του πελάτη. Σε τακτά χρονικά διαστήματα (συνήθως κάθε μήνα) η τράπεζα του πελάτη τον ειδοποιεί για τις συναλλαγές και τις δαπάνες του. Αυτός ο τρόπος πληρωμής παρέχει άμεση πρόσβαση στους τραπεζικούς λογαριασμούς του αγοραστή και του πωλητή και καταγράφει άμεσες μεταβολές στους λογαριασμούς τους.

Με την εμφάνιση του ηλεκτρονικού εμπορίου έχουν γίνει μεγάλης κλίμακας απάτες, κυρίως με κλεμμένους αριθμούς πιστωτικών καρτών. Η έγκριση που απαιτείται στα συστήματα πληρωμών είναι μια μορφή προστασίας. Είναι σημαντικό οι αριθμοί των πιστωτικών καρτών (και γενικά οι πληροφορίες πληρωμής) να είναι δυσανάγνωστες σε όλους, εκτός από τον πελάτη και την τράπεζα του. Δεν υπάρχει λόγος ο έμπορας να γνωρίζει τον αριθμό της πιστωτικής κάρτας του πελάτη. Για το λόγο αυτό, τα δεδομένα πληρωμής στέλνονται κρυπτογραφημένα υπό μορφή μηνύματος μέσα στο διαδίκτυο καθώς υπάρχει πιθανότητα το μήνυμα να υποκλαπεί.

Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά τη διεξαγωγή των συναλλαγών μεταξύ του πελάτη και του εμπόρου, μια καλή επιλογή είναι η χρησιμοποίηση του πρωτοκόλλου SSL (Secure Sockets Layer). Το πρωτόκολλο αυτό αναλύεται στην παράγραφο 3.6.1. Η χρησιμοποίηση web server και web browser που υποστηρίζουν το πρωτόκολλο SSL, εξασφαλίζει την προστασία των δεδομένων από κάποιο τρίτο. Δεν εγγυάται όμως ότι τα δεδομένα αυτά δε θα χρησιμοποιηθούν σκόπιμα από τον έμπορο (για παράδειγμα, χρήση των στοιχείων

της πιστωτικής κάρτας από τον έμπορο για τη διεξαγωγή μη εξουσιοδοτημένων αγορών). Θα μπορούσε να χρησιμοποιηθεί ένας ανεξάρτητος φορέας διασφάλισης των συναλλαγών, γνωστός ως Έμπιστη Τρίτη Οντότητα (Trusted Third Parties – TTP). Μια TTP μεσολαβεί ανεξάρτητα στην όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή.

2.3.2 Ηλεκτρονικές Επιταγές

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών, που τώρα υπογράφονται και μεταβιβάζονται ηλεκτρονικά, και μπορούν να έχουν όλες τις παραλλαγές των κοινών επιταγών, όπως ταξιδιωτικές επιταγές ή πιστοποιημένες επιταγές.

Μια επιταγή χρησιμοποιείται για να μεταφέρει ένα μήνυμα προς την τράπεζα του αποστολέα για τη μεταφορά ενός συγκεκριμένου χρηματικού ποσού από το λογαριασμό του αποστολέα στο λογαριασμό κάποιου άλλου. Σε αντιστοιχία με την παραδοσιακή διαδικασία η ηλεκτρονική επιταγή αποστέλλεται αρχικά στον αποδέκτη του χρηματικού ποσού, ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό. Στη συνέχεια η εξοφλημένη και επικυρωμένη επιταγή επιστρέφεται στον αποστολέα ο οποίος τη χρησιμοποιεί ως απόδειξη πληρωμής.

Μια ηλεκτρονική επιταγή έχει τα ίδια χαρακτηριστικά με μια έντυπη επιταγή. Είναι ένα ηλεκτρονικό έγγραφο που περιέχει τον αριθμό της επιταγής, το όνομα του πληρωτή, τον αριθμό λογαριασμού του πληρωτή και το όνομα της τράπεζας, το όνομα του δικαιούχου πληρωμής (αποδέκτη), το πληρωτέο ποσό, τη μονάδα χρήματος που χρησιμοποιείται, την ημερομηνία λήξης, την ηλεκτρονική υπογραφή του πληρωτή και την ηλεκτρονική επικύρωση του δικαιούχου πληρωμής.

Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές αναλύονται στο κεφάλαιο 4. Από πλευράς ασφάλειας η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη, αφού ο αποστολέας μπορεί να προστατέψει τον εαυτό του από μια απάτη. Κάτι τέτοιο επιτυγχάνεται με την κρυπτογράφηση του αριθμού λογαριασμού του με το δημόσιο κλειδί της τράπεζας του, με αποτέλεσμα να μην αποκαλύπτεται στον έμπορα ο αριθμός του λογαριασμού.

Σε μια συναλλαγή πληρωμής με ηλεκτρονικές επιταγές ο πελάτης παραγγέλλει κάποια προϊόντα από τον έμπορα και για πληρωμή του στέλνει μια ηλεκτρονική επιταγή ψηφιακά υπογεγραμμένη. Ο έμπορας γνωρίζοντας το δημόσιο κλειδί του πληρωτή, μπορεί να επιβεβαιώσει την ορθότητα της ψηφιακής υπογραφής και έτσι να επικυρώσει τη συγκεκριμένη επιταγή. Μετά την παραλαβή και επικύρωση της επιταγής, ο έμπορας στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη αποσύρει το ποσό πώλησης από το λογαριασμό του πελάτη και μέσω του διατραπεζικού συστήματος το εν λόγω ποσό πιστώνεται στο λογαριασμό του έμπορα.

2.3.3 Ηλεκτρονικό Χρήμα

Το ηλεκτρονικό χρήμα είναι ένα σύγχρονο μέσο πληρωμής στο διαδίκτυο. Οι περισσότεροι αναλυτές συμφωνούν πάνω στο γεγονός, ότι η ανάπτυξη του ηλεκτρονικού εμπορίου οδηγεί αντίστοιχα στην ανάπτυξη του ηλεκτρονικού χρήματος. Η χρήση ηλεκτρονικού χρήματος για την αγορά καταναλωτικών αγαθών μοιάζει να προτιμάται από πολλούς καταναλωτές, καθώς μπορεί να οδηγήσει στην ολοκλήρωση της διαδικασίας πολύ πιο γρήγορα από τη συμπλήρωση όλων των στοιχείων της πιστωτικής κάρτας.

Τα σχήματα ηλεκτρονικού χρήματος στηρίζονται είτε σε κάρτες αποθηκευμένης αξίας είτε σε ειδικό λογισμικό. Στην πρώτη περίπτωση η κάρτα περιέχει ένα χρηματικό ποσό ανάλογο με αυτό που έχει προπληρώσει ο κάτοχος της. Η κάρτα μπορεί να είναι είτε ανώνυμη είτε ονοματική. Ο κάτοχος της μπορεί τη φορτίζει κάθε φορά με το ποσό που επιθυμεί. Για λόγους ασφάλειας, η κάρτα προστατεύεται από ένα κωδικό. Στα σχήματα ηλεκτρονικού χρήματος μέσω λογισμικού πραγματοποιείται έκδοση ηλεκτρονικών νομισμάτων από έναν παροχέα υπηρεσιών πληρωμών (συνήθως τράπεζα). Τα ηλεκτρονικά αυτά νομίσματα είναι αποθηκευμένα σε ένα ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη ο οποίος μπορεί να τα χρησιμοποιήσει για αγορές μέσω διαδικτύου. Το βασικό πλεονέκτημα των σχημάτων ηλεκτρονικών πληρωμών και στις δύο περιπτώσεις είναι ότι μπορεί να διατηρηθεί η ανωνυμία των συναλλαγών που είναι ιδιαίτερα σημαντική για τους πελάτες.

Ως ηλεκτρονικό χρήμα, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει «την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να

χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς τη χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά».

Ωστόσο, γενικά με τον όρο ηλεκτρονικό χρήμα περιγράφεται κάθε μορφή μεταφοράς χρήματος μεταξύ δύο ή περισσότερων μερών που γίνεται με ψηφιακό τρόπο και χωρίς τη μεσολάβηση κάποιου υλικού μέσου. Τα χαρακτηριστικά που πρέπει να έχει το ηλεκτρονικό χρήμα είναι τα εξής:

- Ικανοποιητικό επίπεδο ασφάλειας.
- Ανωνυμία.
- Μεταφερσιμότητα (από μια μορφή σε άλλη π.χ. από ηλεκτρονικά νομίσματα σε μετρητά).
- Διαιρετότητα (να μπορεί να διαιρεθεί σε όσα τμήματα ίσης συνολικής αξίας θέλει ο κάτοχος).
- Ευρεία αποδοχή.
- Ευχρηστία.
- Σταθερή αξία (προστασία από πληθωρισμό, υποτίμηση κλπ.).

Σε μια συναλλαγή πληρωμής με ηλεκτρονικό χρήμα ο πελάτης αρχικά έχει προμηθευτεί ψηφιακά νομίσματα από την τράπεζα του ή κάποιον άλλο οργανισμό έκδοσης ψηφιακών νομισμάτων. Με τα νομίσματα που αγόρασε ο πελάτης μπορεί να κάνει αγορές στο διαδίκτυο. Επειδή συνήθως τα ψηφιακά νομίσματα χρησιμοποιούνται για αγορές αγαθών ή υπηρεσιών χαμηλού κόστους, ο έμπορος πολλές φορές δίνει τα προϊόντα χωρίς να ζητήσει έγκριση πληρωμής. Στη συνέχεια ο έμπορος στέλνει αίτημα εξαγοράς νομισμάτων στην τράπεζα του. Μέσω του διατραπεζικού δικτύου η τράπεζα του έμπορα εξαργυρώνει τα νομίσματα στον οργανισμό που τα έκδωσε και πιστώνει το λογαριασμό του έμπορα με το ισοδύναμο ποσό.

Ο οργανισμός έκδοσης νομισμάτων για να εξασφαλίσει ότι το κάθε νόμισμα χρησιμοποιείται μόνο μια φορά, καταγράφει τον αύξοντα αριθμό του κάθε νομίσματος καθώς αυτό ξοδεύεται. Αν ο αριθμός αυτός είναι ήδη καταγραμμένος

στη βάση δεδομένων ο οργανισμός διαπιστώνει απάτη, ακυρώνει το νόμισμα πριν τη συναλλαγή και ειδοποιεί τον έμπορο.

2.3.4 Ηλεκτρονικό Πορτοφόλι

Το ηλεκτρονικό πορτοφόλι είναι ένα νέο εργαλείο πληρωμών που προσφέρει σημαντικά πλεονεκτήματα τόσο στους καταναλωτές, όσο και στους εμπόρους και χαράζει την πορεία προς την αντικατάσταση των μετρητών, τουλάχιστον όσον αφορά τις καθημερινές μικροσυναλλαγές και γενικότερα συμβάλει στη διευκόλυνση των συναλλαγών μέσω ηλεκτρονικού εμπορίου.

Υπάρχουν δύο είδη ηλεκτρονικού πορτοφολιού:

1) **Προπληρωμένες κάρτες:** Οι κάρτες αυτές έχουν το μέγεθος και τη μορφή πιστωτικών καρτών και χρησιμοποιούνται για συναλλαγές στο διαδίκτυο. Οι εν λόγω κάρτες μπορεί να είναι είτε ονομαστικές είτε ανώνυμες. Σε περίπτωση που είναι ονομαστικές, κάθε πελάτης παίρνει από την τράπεζα του μια κάρτα αποθηκευμένης αξίας, στην οποία μεταφέρει χρήματα από το λογαριασμό του, και τη χρησιμοποιεί για τις αγορές του στο διαδίκτυο και όχι μόνο. Για λόγους ασφάλειας και ευελιξίας υπάρχει μια τάση οι κάρτες αυτές να είναι έξυπνες κάρτες. Στη δεύτερη περίπτωση όπου η κάρτα είναι ανώνυμη, ο κάτοχος της μπορεί να τη χρησιμοποιεί για τις αγορές του στα ηλεκτρονικά καταστήματα εύκολα, ανώνυμα και με ασφάλεια οποιαδήποτε ώρα της ημέρας επιθυμεί. Ένα άλλο πλεονέκτημα της ανώνυμης κάρτας είναι ότι η κάρτα μπορεί να μεταβιβαστεί από ένα άτομο σε ένα άλλο, ενώ η ονομαστική δεν μπορεί να μεταβιβαστεί. Η χρήση προπληρωμένων καρτών δημιουργεί έναν εναλλακτικό τρόπο πληρωμής ώστε να είναι δυνατή η χρήση του διαδικτύου για την πραγματοποίηση αγορών ακόμα και από εκείνους τους καταναλωτές που είναι επιφυλακτικοί στη χρήση της πιστωτικής κάρτας για λόγους ασφάλειας.
2) **Ειδικό λογισμικό**: Χρησιμοποιείται ένας ειδικά διαμορφωμένος τύπος λογισμικού (ιδεατό πορτοφόλι) για την αποθήκευση χρηματικής αξίας με τη μορφή ψηφιακών νομισμάτων. Τα ψηφιακά αυτά νομίσματα που είναι αποθηκευμένα στο ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη, μπορούν να χρησιμοποιηθούν για αγορές στο διαδίκτυο.

Γενικά, ένα Ηλεκτρονικό Πορτοφόλι διαθέτει ένα συγκεκριμένο χρηματικό ποσό και μπορεί να χρησιμοποιηθεί για αγορές στα συνεργαζόμενα με την τράπεζα που το εκδίδει, ηλεκτρονικά καταστήματα. Το ηλεκτρονικό πορτοφόλι παρέχει μέγιστη ασφάλεια, καθώς το ποσό χρέωσης δε μπορεί να υπερβεί το αποθηκευμένο ποσό που υπάρχει στο πορτοφόλι.

2.3.5 Έξυπνες Κάρτες

Μια έξυπνη κάρτα είναι μια πλαστική ίση σε μέγεθος με μια πιστωτική κάρτα, στην οποία έχει ενσωματωθεί ένα ολοκληρωμένο κύκλωμα (chip). Το ολοκληρωμένο κύκλωμα μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Το κύριο πλεονέκτημα των έξυπνων καρτών είναι ότι παρέχουν φυσική προστασία των αποθηκευμένων δεδομένων. Μια από τις πλέον ενδιαφέρουσες ιδιότητες των έξυπνων καρτών είναι ότι είναι εξαιρετικά δύσκολο να αντιγραφούν. Με την αύξηση της διαθέσιμης υπολογιστικής δύναμης και μνήμης μεγαλώνει και ο αριθμός των εφαρμογών με έξυπνες κάρτες. Οι έξυπνες κάρτες χρησιμοποιούνται ήδη στις εφαρμογές ηλεκτρονικού εμπορίου.

Οι έξυπνες κάρτες διευκολύνουν την εφαρμογή των Υποδομών Δημοσίου Κλειδιού, οι οποίες χρησιμοποιούνται ευρέως στο ηλεκτρονικό εμπόριο. Οι υποδομές δημοσίου κλειδιού μπορούν να εξασφαλίσουν υψηλό επίπεδο εμπιστοσύνης στις ηλεκτρονικές συναλλαγές. Επιπλέον παρέχουν ακεραιότητα δεδομένων, ασφάλεια και ιδιωτικότητα. Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν τα ιδιωτικά κλειδιά με ασφάλεια. Σε αντίθετη περίπτωση τα ιδιωτικά κλειδιά αποθηκεύονται στους υπολογιστές των κατόχων τους, όπου είναι τρωτά σε επιθέσεις εισβολέων με σκοπό την απόκτηση τους. Η μεταφορά του ιδιωτικού κλειδιού μέσα στην έξυπνη κάρτα διευκολύνει ιδιαίτερα τις ηλεκτρονικές συναλλαγές.

Όπως είναι γνωστό, για να γίνει μια ηλεκτρονική συναλλαγή απαιτείται η ανταλλαγή ευαίσθητων προσωπικών δεδομένων μεταξύ των συναλλασσόμενων πλευρών. Οι έξυπνες κάρτες αποτελούν ένα άριστο μέσο για τη μεταφορά ευαίσθητων προσωπικών δεδομένων όπως για παράδειγμα αριθμούς πιστωτικών καρτών, κλειδιά κρυπτογράφησης και αποκρυπτογράφησης κλπ. Οι έξυπνες κάρτες μπορούν επιπλέον να αντικαταστήσουν κάρτες όπως οι τηλεκάρτες, οι πιστωτικές κάρτες, οι κάρτες ανάληψης μετρητών και άλλες παρόμοιες κάρτες.

Μπορούν επίσης να χρησιμοποιηθούν ως προπληρωμένες κάρτες για την αποθήκευση ψηφιακών νομισμάτων. Μια τέτοια κάρτα πολλαπλών εφαρμογών που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές είναι η Java Card.

2.4 Υπηρεσίες Ασφάλειας Πληρωμών

Ένα ηλεκτρονικό σύστημα πληρωμών, θα πρέπει να περιλαμβάνει τις εξής υπηρεσίες ασφάλειας:

Ανωνυμία Χρήστη: Προστατεύει από την κοινοποίηση της ταυτότητας του χρήστη σε μια συναλλαγή πληρωμής. Συνήθως ο χρήστης επιθυμεί να πραγματοποιεί τις συναλλαγές του ανώνυμα.

Η ανωνυμία χρήστη θα μπορούσε να πραγματοποιηθεί με τη χρήση ενός ψευδωνύμου αντί της πραγματικής ταυτότητας του χρήστη. Σε περίπτωση όμως που το δίκτυο συναλλαγής παγιδευόταν, τέτοιος τύπος ανωνυμίας δεν είναι ικανοποιητικός. Η υπηρεσία μη ανίχνευσης θέσης μπορεί να προστατεύσει από την κοινοποίηση της θέσης όπου γίνεται η συναλλαγή, χρησιμοποιώντας ανώνυμα hosts, μέσω των οποίων στέλνονται τα μηνύματα κατά τη διάρκεια της συναλλαγής πληρωμής.

Μη Ανίχνευση Θέσης: Προστατεύει από την κοινοποίηση της θέσης όπου γίνεται η συναλλαγή. Χρησιμοποιώντας μόνο ανωνυμία χρήστη, η IP διεύθυνση και το host name του υπολογιστή, από τον οποίο έγινε κάποια συναλλαγή, είναι γνωστά. Και στην περίπτωση που ο υπολογιστής είναι προσωπικός, είναι δεδομένη η IP διεύθυνση του και άρα μπορεί να προσδιοριστεί ο χρήστης. Με την υπηρεσία μη ανίχνευσης θέσης εξασφαλίζεται ότι η IP διεύθυνση και το host name του υπολογιστή δεν θα αποκαλυφθούν.

Μη Ανίχνευση Συναλλαγής Πληρωμής: Προστατεύει από τη σύνδεση δύο διαφορετικών συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πελάτη. Ένας πληρωτής θέλοντας να διατηρήσει την ανωνυμία του, μπορεί να κρύβεται πίσω από ένα ψευδώνυμο. Εάν χρησιμοποιεί την ίδια ταυτότητα σε όλες τις συναλλαγές του, τότε η συμπεριφορά του μπορεί να παρατηρηθεί και η ταυτότητα του να αποκαλυφθεί. Η υπηρεσία μη ανίχνευσης συναλλαγής πληρωμής, κρύβει τη σύνδεση μεταξύ συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πληρωτή.

Εμπιστευτικότητα των Δεδομένων της Συναλλαγής Πληρωμής: Προστατεύει από την κοινοποίηση των δεδομένων της συναλλαγής πληρωμής σε τρίτους. Επιπλέον η υπηρεσία αυτή προστατεύει και κάποια δεδομένα της συναλλαγής πληρωμής από επιλεγμένους εμπλεκόμενους. Για παράδειγμα αποκρύπτει από τον έμπορα τις πληροφορίες για την πιστωτική κάρτα του πελάτη.

Τα δεδομένα μιας συναλλαγής πληρωμής αποτελούνται από δύο μέρη: την οδηγία πληρωμής και τις πληροφορίες της παραγγελίας. Η οδηγία πληρωμής περιέχει λεπτομέρειες για τον τρόπο πληρωμής, δηλαδή περιλαμβάνει τον αριθμό της πιστωτικής κάρτας του πελάτη ή τον αριθμό του λογαριασμού του και κάποιες άλλες σχετικές πληροφορίες. Ο έμπορας, για λόγους ασφάλειας, δε θα έπρεπε να γνωρίζει τον αριθμό της πιστωτικής κάρτας του πελάτη. Σε μερικές περιπτώσεις οι πληροφορίες που περιλαμβάνονται σε μια οδηγία πληρωμής προσδιορίζουν μεμονωμένα τον πληρωτή. Συνεπώς προστασία από αναρμόδιους και ανέντιμους συμβαλλόμενους σημαίνει επίσης και ανωνυμία πληρωτή. Οι πληροφορίες παραγγελίας διευκρινίζουν τον τύπο και τον αριθμό των προϊόντων που παραγγέλθηκαν, καθώς και την τιμή τους. Οι πληροφορίες αυτές θα πρέπει να είναι δυσανάγνωστες στην τράπεζα. Δεν υπάρχει λόγος η τράπεζα να γνωρίζει πληροφορίες για τα προϊόντα και τις υπηρεσίες που αγοράζει ο πελάτης. Προκειμένου να επιτευχθεί η εμπιστευτικότητα των πιο πάνω δεδομένων χρησιμοποιείται κρυπτογραφία δημοσίου κλειδιού.

Μη αποκήρυξη των Μηνυμάτων της Συναλλαγής Πληρωμής: Προστατεύει από ενδεχόμενη άρνηση της προέλευσης των μηνυμάτων που ανταλλάσσονται σε μια συναλλαγή πληρωμής. Μπορεί ένας πελάτης να υποστηρίξει ότι ποτέ δεν έδωσε εντολή πληρωμής, ή ένας έμπορας να υποστηρίξει ότι δεν έλαβε πληρωμή από τον πελάτη. Η υπηρεσία μη αποκήρυξης μηνυμάτων λύνει τέτοιες διαφωνίες χρησιμοποιώντας μηχανισμούς ψηφιακής υπογραφής.

Είναι δεδομένο ότι για να μπορεί να γίνεται αξιόπιστα μια συναλλαγή πληρωμής, πρέπει οι συμβαλλόμενοι να μην μπορούν αργότερα να αποκηρύξουν την προέλευση ή την παραλαβή μηνυμάτων. Η μη αποκήρυξη προέλευσης αποτρέπει την άρνηση αποστολής ενός μηνύματος και η μη αποκήρυξη παραλαβής αποτρέπει την άρνηση παραλαβής ενός μηνύματος. Η μη αποκήρυξη μηνυμάτων εξασφαλίζεται με μηχανισμούς ψηφιακής υπογραφής.

Μη Επανάληψη Μηνυμάτων Συναλλαγής Πληρωμής: Προστατεύει από επαναλαμβανόμενα μηνύματα σε συναλλαγή πληρωμής. Σε περίπτωση που ένας πελάτης στείλει ένα μήνυμα με τις πληροφορίες της πιστωτικής του κάρτας ως πληρωμή, το μήνυμα αυτό, ακόμη και σε κρυπτογραφημένη μορφή, μπορεί να παρθεί από έναν επιτιθέμενο ο οποίος να το επαναχρησιμοποιήσει. Η υπηρεσία μη επανάληψης μηνυμάτων προστατεύει από τέτοιου είδους επιθέσεις.

Αυτή η υπηρεσία προστατεύει από επιθέσεις τύπου επανάληψης. Εμποδίζει τους ωτακουστές ή τους ανέντιμους συμμετέχοντες να επαναχρησιμοποιήσουν τα μηνύματα που ανταλλάχθηκαν σε μια συναλλαγή πληρωμής. Η μη επανάληψη μηνυμάτων εξασφαλίζεται με τη χρησιμοποίηση τυχαίων αριθμών (nonce) και χρονικών σφραγίδων.

Μια λύση είναι η τοποθέτηση μιας χρονικής σφραγίδας σε κάθε μήνυμα. Αν κάποιος λάβει ένα ληγμένο μήνυμα θα πρέπει να το απορρίψει. Το πρόβλημα στην περίπτωση αυτή είναι ότι τα ρολόγια μέσα στο δίκτυο δεν είναι ποτέ συγχρονισμένα. Για το λόγο αυτό υπάρχει δυνατότητα να επιτραπεί κάποια ανοχή για ένα μικρό διάστημα, αλλά αυτό εισάγει πρόσθετη αβεβαιότητα διότι κάποιος πολύ γρήγορα μπορεί να αναπαραγάγει ένα μήνυμα και να το στείλει εκ νέου.

Άλλη λύση είναι η τοποθέτηση ενός τυχαίου αριθμού nonce μιας χρήσης σε κάθε μήνυμα.

Όταν φθάνει τέτοιο μήνυμα σε κάποιο μέρος, πρέπει να συγκρίνεται ο αριθμός του μηνύματος με όλους τους προηγούμενους αριθμούς και να απορρίπτεται κάθε μήνυμα που περιέχει έναν ήδη χρησιμοποιημένο, ως μήνυμα επανάληψης. Το πρόβλημα στην περίπτωση αυτή είναι ότι όσο μεγαλώνει ο αριθμός των nonce που φυλάγονται στη μνήμη, τόσο θα αυξάνεται το πρόβλημα ελεγξιμότητας και μνήμης. Ο συνδυασμός χρονικών σφραγίδων και τυχαίων αριθμών, θα μειώσει το πλήθος των τυχαίων αριθμών που θα αποθηκεύονται στη μνήμη και θα υπάρχει κάποιο διάστημα ανοχής για τις χρονικές σφραγίδες. Αν κάποιο μήνυμα που φτάνει είναι έγκυρο χρονικά και ο τυχαίος του αριθμός είναι διαφορετικός από τους αποθηκευμένους, τότε το μήνυμα θα θεωρείται καινούργιο.

2.5 Κατηγορίες Ψηφιακού Χρήματος.

Γενικά υπάρχουν δύο ξεχωριστοί τύποι ηλεκτρονικού χρήματος (e-money): το ηλεκτρονικό χρήμα που προσδιορίζει την ταυτότητα του ιδιοκτήτη του (identified e-money) και το ανώνυμο ηλεκτρονικό χρήμα (anonymous e-money), γνωστό επίσης και ως ψηφιακά μετρητά (digital cash). Ο πρώτος τύπος περιλαμβάνει πληροφορίες που γνωστοποιούν την ταυτότητα του προσώπου που έκανε την ανάληψη χρημάτων από την τράπεζα (οργανισμό έκδοσης των χρημάτων αυτών) και βοηθάει την τράπεζα να ανιχνεύσει την διακίνηση του μέσα στην οικονομία, λειτουργεί δηλαδή με τον ίδιο τρόπο με τον οποίο λειτουργούν και οι πιστωτικές κάρτες. Τα ψηφιακά νομίσματα, όπως και τα παραδοσιακά χαρτονομίσματα έχουν ένα serial number. Είναι εύκολο να δημιουργηθεί ένα μεγάλο αρχείο στο οποίο θα καταχωρείται ποιος πελάτης έλαβε ποιους serial number ψηφιακών νομισμάτων, αμέσως μόλις ο πελάτης αγοράσει ψηφιακά νομίσματα από την τράπεζα. Ο δεύτερος τύπος ηλεκτρονικού χρήματος μοιάζει με τα χάρτινα μετρητά που κυκλοφορούν. Το ανώνυμο ηλεκτρονικό χρήμα μπορεί να ξοδευτεί ή και να χαθεί ακόμα, χωρίς όμως η τράπεζα να γνωρίζει κάτι για τη διακίνηση του από την ανάληψη του και μετά.

Οι πιο πάνω τύποι ηλεκτρονικού χρήματος συναντιόνται σε δύο κατηγορίες: on-line και offline. Η πρώτη κατηγορία προϋποθέτει αλληλεπίδραση του πελάτη με την τράπεζα (διαμέσου δικτύου) για να διεξαχθεί η εμπορική πράξη μέσω του έμπορα. Με τη δεύτερη κατηγορία ηλεκτρονικού χρήματος δεν απαιτείται η απευθείας εμπλοκή της τράπεζας για να διεκπεραιωθεί η οικονομική συναλλαγή. Η συναλλαγή με offline ανώνυμο ηλεκτρονικό χρήμα είναι και η περισσότερο περίπλοκη συναλλαγή ηλεκτρονικού χρήματος, αφού η μυστικότητα η οποία προσφέρει δημιουργεί και την ευκαιρία διπλού ξοδέματος του από τον κάτοχο του.

2.5.1 Επαναχρησιμοποίηση ή Διπλό Ξόδεμα του ψηφιακού χρήματος.

Από τη στιγμή που το ηλεκτρονικό χρήμα είναι μια σειρά από δυαδικά ψηφία, ένα κομμάτι του πολύ εύκολα μπορεί να αντιγραφεί. Αυτό το αντίγραφο, αφού δε διαφέρει σε τίποτα από το αρχικό τμήμα που αντιγράφηκε, το ίδιο εύκολα μπορεί να επαναχρησιμοποιηθεί. Ένα επιπόλαιο σύστημα ηλεκτρονικού χρήματος μπορεί κάτι τέτοιο να το επέτρεπε, ωστόσο όμως ένα πραγματικό σύστημα ηλεκτρονικού

χρήματος μπορεί να ανιχνεύσει και να εμποδίσει τη διπλή επαναχρησιμοποίηση του ηλεκτρονικού χρήματος.

Τα συστήματα του on-line ηλεκτρονικού χρήματος(ανώνυμο ή μη) εμποδίζουν το διπλό ξόδεμα με το να απαιτούν από τους εμπόρους να επικοινωνούν με την τράπεζα για κάθε συναλλαγή. Το σύστημα της τράπεζας διατηρεί μια βάση δεδομένων που περιέχει τα serial number όλων των ψηφιακών νομισμάτων που έχουν ξοδευτεί και έτσι εύκολα και γρήγορα υποδεικνύεται στον έμπορα αν τα ψηφιακά νομίσματα που έλαβε έχουν ήδη ξοδευτεί νόμιμα. Αν μετά από συνεννόηση με την τράπεζα αποδειχθεί ότι το συγκεκριμένο ποσό του ηλεκτρονικού χρήματος έχει ήδη ξοδευτεί μέσω κάποιας άλλης συναλλαγής ο έμπορος απορρίπτει την πώληση.

Τα συστήματα του offline ηλεκτρονικού χρήματος ανιχνεύουν το διπλό ξόδεμα του ηλεκτρονικού χρήματος με δύο διαφορετικούς τρόπους. Ο πρώτος αναφέρεται στη χρήση έξυπνων καρτών (smart cards) στις οποίες περιέχεται ενσωματωμένο ένα chip που στα περισσότερα συστήματα ονομάζεται Observer. Σε αυτό το chip αποθηκεύεται μια μικρή βάση δεδομένων που περιέχει το ποσό του ηλεκτρονικού χρήματος που έχει ξοδευτεί μέσω της έξυπνης κάρτας. Σε περίπτωση που ο κάτοχος της έξυπνης κάρτας προσπαθήσει να ξοδέψει διπλά ηλεκτρονικό χρήμα, το chip που βρίσκεται μέσα στην κάρτα και καταγράφει κάθε πληρωμή θα ανιχνεύσει την προσπάθεια και θα καταστήσει αδύνατη τη συναλλαγή. Η βάση δεδομένων που περιέχεται στο Observer chip δεν μπορεί να καταστραφεί ούτε να διαγραφεί, εκτός και αν καταστραφεί ολοκληρωτικά η έξυπνη κάρτα.

Ο δεύτερος τρόπος των συστημάτων του offline ηλεκτρονικού χρήματος για τη διαχείριση διπλού ξοδέματος αναφέρεται στο ηλεκτρονικό χρήμα που προσδιορίζει την ταυτότητα του ιδιοκτήτη του, και βασίζεται στη δομή του ηλεκτρονικού χρήματος και στα πρωτόκολλα κρυπτογράφησης, ώστε από τη στιγμή που φτάνει πίσω στην τράπεζα το ηλεκτρονικό χρήμα που ξοδεύτηκε διπλά να ανιχνευθεί και η ταυτότητα εκείνου που το είχε στη διάθεση του και το ξόδεψε διπλά. Έτσι αν οι χρήστες γνωρίζουν ότι μετά το διπλό ξόδεμα του ηλεκτρονικού χρήματος θα αποκαλυφθούν θεωρητικά το φαινόμενο αυτό θα μειωθεί.

2.6 Διαθέσιμα Συστήματα Ηλεκτρονικών Πληρωμών

2.6.1 CyberCash

Το CyberCash είναι ένα προϊόν της CyberCash Corporation το οποίο χρησιμοποιεί εξειδικευμένο λογισμικό από την πλευρά του πελάτη και του πωλητή για να εξασφαλίσει ασφαλείς ηλεκτρονικές συναλλαγές μέσω διαδικτύου. Το CyberCash υποστηρίζει πληρωμές τόσο με πιστωτικές κάρτες όσο και με ηλεκτρονικές επιταγές.

Το σύστημα CyberCash βρίσκεται σε χρήση από ένα μεγάλο αριθμό επιχειρήσεων κάθε μεγέθους, που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Ο κίνδυνος για τους αγοραστές που χρησιμοποιούν το σύστημα CyberCash είναι ελάχιστος, και συχνά καλύπτεται από την πολιτική των οργανισμών πιστωτικών καρτών. Το πλεονέκτημα του συστήματος CyberCash είναι ότι χρησιμοποιεί ισχυρή κρυπτογράφηση, ενώ το κύριο μειονέκτημα του είναι ότι δεν παρέχει ανωνυμία στον πελάτη, όπως συμβαίνει με όλα τα συστήματα που χρησιμοποιούν πιστωτικές κάρτες.

2.6.2 DigiCash

Το σύστημα DigiCash είναι ένα ψηφιακό σύστημα πληρωμής, όπου οι χρήστες χρησιμοποιούν ειδικά χαρτονομίσματα που ονομάζονται «CyberBucks». Πριν τη χρησιμοποίηση των CyberBucks, ο χρήστης θα πρέπει να εγγραφεί ψηφιακά σε μια τράπεζα που υποστηρίζει το σύστημα αυτό. Στη συνέχεια, ο χρήστης μπορεί να χρησιμοποιήσει τα CyberBucks όπως ακριβώς και τα πραγματικά χρήματα. Όταν ο πελάτης αποφασίσει να αγοράσει κάποιο προϊόν από ένα on-line κατάστημα, μεταφέρει ηλεκτρονικά έναν αριθμό από CyberBucks στον υπολογιστή του εμπόρου. Έπειτα, ο έμπορος μπορεί να εξαργυρώσει τα CyberBucks με πραγματικά χρήματα. Οι συναλλαγές του συστήματος είναι ανώνυμες και επειδή τα CyberBucks είναι ψηφιακά υπογεγραμμένα, δε μπορούν να πλαστογραφηθούν.

Το σύστημα DigiCash απαιτεί την εγκατάσταση ειδικού λογισμικού, τόσο στον υπολογιστή του πελάτη, όσο και στον υπολογιστή του εμπόρου. Το λογισμικό αυτό είναι διαθέσιμο για διάφορες υπολογιστικές πλατφόρμες (Windows, Unix).

2.6.3 SET (Secure Electronic Transactions)

Οι δύο μεγαλύτεροι οργανισμοί πιστωτικών καρτών Visa και Mastercard, σε συνεργασία με τη Netscape και τη Microsoft, έχουν αναπτύξει το πρωτόκολλο SET για την ασφαλή πραγματοποίηση συναλλαγών μέσω πιστωτικών καρτών και επιταγών ανάμεσα στους πελάτες και στους εμπόρους. Το SET παρέχει τα ακόλουθα χαρακτηριστικά ασφαλείας: α) αυθεντικοποίηση, όλα τα μέρη που συμμετέχουν σε μια συναλλαγή αυθεντικοποιούνται, β) ακεραιότητα μηνύματος, κανένας δε μπορεί να επέμβει στη συναλλαγή με σκοπό να μεταβάλει κάποιο μήνυμα, γ) ασφάλεια των δεδομένων από τρίτους και δ) δυνατότητα απόδειξης της συναλλαγής. Επιπλέον παρέχει τη δυνατότητα κρυπτογράφησης των δεδομένων που διακινούνται μέσω του διαδικτύου αλλά και φύλαξης ευαίσθητων πληροφοριών που περιέχονται πάνω στην πιστωτική κάρτα από τρίτα μέρη όπως ο έμπορος.

Βασικά το πρωτόκολλο SET περιλαμβάνει τις ίδιες διαδικασίες που υπάρχουν ήδη για την πληρωμή με πιστωτικές κάρτες: ο έμπορος επικοινωνεί με τον οργανισμό έκδοσης της πιστωτικής κάρτας, δίνει τον αριθμό της πιστωτικής κάρτας του πελάτη και την αξία της πώλησης και ζητά έγκριση. Στη συνέχεια ο έμπορος εισπράττει την πληρωμή του από τον οργανισμό που έκδωσε την πιστωτική κάρτα. Το πρωτόκολλο SET ουσιαστικά επιτρέπει την επικοινωνία για την έγκριση της συναλλαγής μέσα από το ψηφιακό δίκτυο.

Το πρωτόκολλο SET είναι ένα πολύπλοκο και συμπαγές σύστημα που χρησιμοποιεί ισχυρή μέθοδο κρυπτογράφησης και ψηφιακά πιστοποιητικά για την προστασία κάθε συναλλαγής.

2.6.4 Millicent

Το σύστημα Millicent παρουσιάστηκε από τη DEC (Digital Equipment Corporation) και χρησιμοποιείται για την εξυπηρέτηση μικρών ηλεκτρονικών αγορών. Η καινοτομία του είναι η χρήση των «brokers» (χρηματομεσίτες) και των «scrips» (χαρτονομίσματα). Ένα scrip έχει μια μικρή ονομαστική αξία και μπορεί να εξαργυρωθεί μόνο σε ένα συγκεκριμένο εμπορικό κατάστημα. Εάν η τιμή του scrip είναι μεγαλύτερη από την αξία του προϊόντος, ο έμπορος επιστρέφει τη διαφορά στον πελάτη με τη μορφή ενός νέου scrip.

Το scrip αριθμείται σειριακά και υπογράφεται ψηφιακά, έτσι ώστε ο έμπορος να μπορεί να επαληθεύσει γρήγορα ότι είναι έγκυρο και ότι δεν έχει ήδη χρησιμοποιηθεί. Τα scrips αγοράζονται σε μεγάλους αριθμούς σε χοντρική τιμή από τους brokers (χρηματομεσίτες) οι οποίοι στη συνέχεια τα μεταπωλούν σε διάφορους πελάτες. Επειδή τα scrips δημιουργούνται και υπογράφονται από τους εμπόρους, δεν απαιτείται η ύπαρξη κεντρικών εξυπηρετητών που θα ελέγχουν την εγκυρότητα τους και ότι δεν έχουν ήδη χρησιμοποιηθεί. Αυτό έχει σαν αποτέλεσμα την ταχύτητα και το χαμηλό κόστος του συστήματος. Επειδή το σύστημα Millicent διαχειρίζεται μικρά ποσά, δε χρειάζεται ούτε πολύ ισχυρή κρυπτογραφία ούτε και μια υποδομή δημόσιου κλειδιού για πιστοποίηση αυθεντικότητας. Το μειονέκτημα του συστήματος αυτού είναι τα scrips ισχύουν μόνο για ένα έμπορο, με τον οποίο ο πελάτης πρέπει να έχει συχνές συναλλαγές. Αν ένας πελάτης χρειάζεται διαφορετικά scrips για πολλούς διαφορετικούς εμπόρους, η χρήση του συστήματος γίνεται ασύμφορη και μπορεί να επιβαρύνει τον ηλεκτρονικό υπολογιστή του.

2.6.5 Mondex

Είναι ένα σύστημα ηλεκτρονικών μετρητών που βασίζεται σε ειδικές ηλεκτρονικές κάρτες, στις έξυπνες κάρτες, και απαιτεί προεργασία για τη χρήση του. Η ανεξαρτησία των καρτών αυτών είναι το μεγαλύτερο πλεονέκτημα τους. Το chip της κάρτας περιέχει ένα «πορτοφόλι» μέσα στο οποίο η αξία του Mondex κρατάτε ηλεκτρονικά. Το πορτοφόλι διαιρείται σε πέντε διαφορετικά τμήματα, επιτρέποντας πέντε διαφορετικά συναλλάγματα να διατηρούνται στην κάρτα οποιαδήποτε στιγμή. Οι συναλλαγές γίνονται χωρίς να απαιτείται η έγκριση της τράπεζας, παρέχοντας ταυτόχρονα ασφάλεια στις on-line αγορές χωρίς να δίνει προσωπικές λεπτομέρειες.

2.6.6 CAFE

Είναι ένα σύστημα ψηφιακών μετρητών που χρησιμοποιεί έξυπνες κάρτες με μικροεπεξεργαστή, και παρέχει ισχυρές εγγυήσεις για την ανωνυμία των χρηστών.

3ο ΚΕΦΑΛΑΙΟ: ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

3.1 Γενικά για την Ασφάλεια

Το διαδίκτυο προσφέρει στις επιχειρήσεις αλλά και στους καταναλωτές μια μοναδική ευκαιρία επικοινωνίας τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση, είναι μόνο μερικοί από τους παράγοντες που βοήθησαν στην ανάπτυξη του ηλεκτρονικού εμπορίου. Ωστόσο, από πολύ νωρίς φάνηκαν και τα προβλήματα τα όποια συνδέονται με το ηλεκτρονικό εμπόριο και τα οποία έπρεπε να αντιμετωπιστούν αποτελεσματικά για την περαιτέρω εξέλιξή του. Ο πιο σημαντικός φραγμός για την υιοθέτηση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών. Για παράδειγμα, ο χρήστης που κάνει μια on-line αγορά πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής του κάρτας δε θα υποκλαπεί. Κάθε φορά που συνδιαλέγεται δικτυακά με την τράπεζά του (e-banking) θέλει να γνωρίζει ότι όντως έρχεται σε επαφή με την ίδια την τράπεζα και όχι με κάποιον που επιχειρεί να τον εξαπατήσει. Όταν αποστέλλει στο διαδίκτυο ευαίσθητα δεδομένα θέλει να ξέρει ότι δεν θα έχει πρόσβαση σε αυτά κανένας άλλος εκτός από τον πραγματικό παραλήπτη τους.

Μέσα σε αυτό το κλίμα αυξάνονται δυστυχώς και οι ευκαιρίες για ηλεκτρονικές άπατες. Θύματα επιθέσεων, ενοχλητικών έως και επικινδύνων "crackers" πέφτουν συχνά ακόμα και μεγάλοι δικτυακοί τόποι όπως το Yahoo,το Amazon και το eBay. Η ασφάλεια των web εφαρμογών γενικότερα και η ασφάλεια στο ηλεκτρονικό εμπόριο ειδικότερα είναι ένας σημαντικός και πολύπλοκος στόχος.

Πολλοί ακούγοντας τον όρο ασφάλεια web εφαρμογών έχουν την τάση να σκέφτονται αμέσως επιτιθέμενους που παραμορφώνουν ιστοσελίδες, κλέβουν αριθμούς πιστωτικών καρτών και βομβαρδίζουν με μηνύματα ιστοσελίδες προκαλώντας επιθέσεις τύπου άρνηση υπηρεσίας (denial of service attack). Επίσης σκέφτονται τα προβλήματα που προκαλούν οι ιοί (viruses), οι δούρειοι ίπποι (Trojan horses) και τα σκουλήκια (worms). Αυτοί είναι οι τύποι προβλημάτων που

απασχολούν περισσότερο το κοινό, λόγω του ότι αντιπροσωπεύουν μερικές από τις σημαντικότερες απειλές που αντιμετωπίζουν σήμερα οι web εφαρμογές.

Τα παραπάνω, είναι μόνο μερικά από τα προβλήματα που παρουσιάζονται. Κάποια άλλα σημαντικά προβλήματα συχνά αγνοούνται. Οι εσωτερικές απειλές από απατεώνες διοικητές, από δυσαρεστημένους ή απρόσεκτους υπαλλήλους και από περιστασιακούς χρήστες αποτελούν επίσης σημαντικό κίνδυνο.

Όλες οι επιθέσεις σε επίπεδο εφαρμογών έχουν σαν στόχο να επωφεληθούν από τις υπάρχουσες αδυναμίες ασφάλειας με αποτέλεσμα να πλήξουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των επιχειρηματικών δεδομένων που επεξεργάζονται μέσω της εκάστοτε εφαρμογής.

Οι συνέπειες από την παραβίαση της ασφάλειας είναι τεράστιες: απώλεια εισοδημάτων, ζημιά στην αξιοπιστία της επιχείρησης, νομική ευθύνη, και το χειρότερο για έναν οργανισμό ηλεκτρονικού εμπορίου είναι η απώλεια της εμπιστοσύνης του πελάτη.

Ο όρος ασφάλεια περιλαμβάνει την προστασία αγαθών των επιχειρήσεων. Τα αγαθά μπορεί να είναι απτά στοιχεία όπως μια ιστοσελίδα ή η βάση δεδομένων των πελατών της επιχείρησης, ή μπορεί να είναι λιγότερο απτά όπως η φήμη μιας επιχείρησης.

Οι κίνδυνοι στα συστήματα ηλεκτρονικών πληρωμών είναι:

- Τα ψηφιακά έγγραφα μπορούν αυθαίρετα να αντιγραφούν.
- Οι ψηφιακές υπογραφές μπορούν να παραχθούν από οποιοδήποτε γνωρίζει το ιδιωτικό κλειδί.
- Η ταυτότητα του πληρωτή μπορεί να συνδεθεί με κάθε συναλλαγή πληρωμής, με αποτέλεσμα να γίνονται γνωστές οι καταναλωτικές και όχι μόνο συνήθειες του πληρωτή.

Προφανώς χωρίς πρόσθετα μέτρα ασφάλειας, το διαδεδομένο ηλεκτρονικό εμπόριο δεν θα ήταν βιώσιμο. Γενικά τα ηλεκτρονικά συστήματα πληρωμών αντιμετωπίζουν τους εξής επιτιθέμενους:

- Αυτούς που κρυφακούν στη γραμμή επικοινωνίας και συλλέγουν πληροφορίες (π.χ. αριθμούς πιστωτικών καρτών) τις οποίες χρησιμοποιούν για απάτες με σκοπό το δικό τους οικονομικό όφελος.

- Αυτούς που επεμβαίνουν και τροποποιούν τα μηνύματα που ανταλλάσσονται σε μια συναλλαγή πληρωμής, προκειμένου να κλέψουν αγαθά ή χρήματα.
- Τους ανέντιμους συμμετέχοντες στη συναλλαγή πληρωμής (π.χ. έμπορος), οι οποίοι χρησιμοποιούν για απάτες τις πληροφορίες πληρωμής (π.χ. αριθμούς πιστωτικών καρτών) που τους δίνει ο πελάτης.

3.1.1 Βασικές Απαιτήσεις για την Ασφάλεια των Web Εφαρμογών

1) **Αυθεντικοποίηση** (Authentication): Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας την οποία ισχυρίζεται ότι έχει ένας πελάτης της εφαρμογής. Ο πελάτης μπορεί να είναι κάποιος τελικός χρήστης, κάποια υπηρεσία, διαδικασία ή υπολογιστής. Στο ηλεκτρονικό εμπόριο η πιστοποίηση της ταυτότητας των μερών που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη ώστε κάθε συναλλασσόμενο μέρος να είναι σίγουρο για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται συνήθως μέσω των ψηφιακών υπογράφων.
2) **Εμπιστευτικότητα** (Confidentiality): Είναι έννοια στενά συνδεδεμένη με την ιδιωτικότητα και τη μυστικότητα. Αφορά στη μη αποκάλυψη των ευαίσθητων πληροφοριών σε άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση. Για το ηλεκτρονικό εμπόριο η εμπιστευτικότητα αποτελεί ύψιστης σημασίας συστατικό στην προστασία οικονομικών δεδομένων του οργανισμού καθώς και στην προστασία των προσωπικών δεδομένων των πελατών. Τεχνικές κρυπτογράφησης χρησιμοποιούνται για να εξασφαλίσουν την εμπιστευτικότητα.
3) **Εξουσιοδότηση** (Authorization): Η εξουσιοδότηση περιλαμβάνει τον έλεγχο της πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτημένα μέλη μπορούν να πραγματοποιήσουν, όπως για παράδειγμα εκτέλεση συναλλαγών, μεταφορά χρημάτων από τον έναν λογαριασμό σε άλλο ή αύξηση του πιστωτικού ορίου κάποιου πελάτη.
4) **Ακεραιότητα** (Integrity): Η ακεραιότητα είναι η εγγύηση ότι τα δεδομένα προστατεύονται από τυχαία ή σκόπιμη τροποποίηση. Διασφαλίζει την

εγκυρότητα την ορθότητα και την πληρότητα των δεδομένων κατά τη φάση της εισαγωγής τους, της αποθήκευσης και της μεταφοράς τους. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς σταλθήκαν.

5) **Μη αποποίηση ευθύνης** (non-repudation): Μη αποποίηση ευθύνης σημαίνει ότι ένας χρήστης δεν μπορεί να αρνηθεί την εκτέλεση μιας λειτουργίας και κανένα από τα συναλλασσόμενα μέρη δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σ ε μια συναλλαγή. Οι υπηρεσίες μη αποποίηση ευθύνης πρέπει σε περίπτωση που χρειαστεί να μπορούν να αποδείξουν την προέλευση, τη μεταφορά και την παραλαβή των δεδομένων.
6) **Διαθεσιμότητα** (Availability): Αφορά την άμεση πρόσβαση στις υπηρεσίες του συστήματος για τους νόμιμους χρήστες τους. Πολλοί επιτιθέμενοι χρησιμοποιώντας επιθέσεις τύπου άρνησης υπηρεσίας έχουν σαν στόχο να καταστρέψουν την εφαρμογή ώστε οι υπόλοιποι χρήστες να μην μπορούν να έχουν πρόσβαση σε αυτή.

3.1.2 Επίδραση Έλλειψης Ασφάλειας στο Επιχειρησιακό Περιβάλλον

Οι κίνδυνοι ασφάλειας εφαρμογών αφορούν στην απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών. Η σημαντικότητα των κινδύνων αυτών προσδιορίζεται από την επίδρασή τους στο επιχειρησιακό περιβάλλον και από την πιθανότητα εκδήλωσής τους.

Η επίδραση από την απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών είναι:

- Απώλεια ανταγωνιστικού πλεονεκτήματος.
- Αδυναμία διεκπεραίωσης βασικών επιχειρηματικών δραστηριοτήτων.
- Προσβολή της εμπιστοσύνης των πελατών προς την εταιρεία.
- Προσβολή της εικόνας και της φήμης της εταιρείας.
- Αδυναμία επαναλειτουργίας λόγω πολλών ανεκτέλεστων διαδικασιών οι οποίες δεν μπορούν να εκτελεστούν είτε λόγω χρονικού περιορισμού, είτε επειδή έχουν χαθεί.
- Πιθανότητα απάτης.

- Αδυναμία λειτουργίας λόγω απώλειας διαθεσιμότητας των πληροφοριακών πόρων.

3.2 Προβλήματα Ασφάλειας στο Διαδίκτυο

Τα μέτρα για την ασφαλή πλοήγηση έχουν αφετηρία υπηρεσίες του παροχέα (provider) πρόσβασης στο διαδίκτυο. Ένας καλός παροχέας μπορεί να προσφέρει φιλτράρισμα των ιστοσελίδων που επισκέπτεται όπως επίσης και φιλτράρισμα των επισυναπτόμενων αρχείων στα e-mails που δέχεται ο χρήστης-πελάτης. Είναι ωστόσο συχνές οι περιπτώσεις κατά τις οποίες σελίδες που περιέχουν ακατάλληλο υλικό δεν περιέχουν τις λέξεις που φιλτράρουν τα προγράμματα αυτά ή δεν έχουν καταχωρηθεί στην μαύρη λίστα. Αντιθέτως, ιστοσελίδες που δεν περιέχουν ακατάλληλο υλικό μπορεί να απαγορεύονται επειδή περιέχουν λέξεις που φιλτράρει το πρόγραμμα. Σε αυτές τις περιπτώσεις είναι καλό ο χρήστης να ενημερώνει τον διαχειριστή του προγράμματος (Cachemaster). Ωστόσο ακόμα και οι καλύτερες υπηρεσίες ενός παροχέα σύνδεσης δεν εξασφαλίζουν τον χρήστη από τους κινδύνους που ελλοχεύουν κατά την πλοήγηση αν ο ίδιος δεν λάβει τα κατάλληλα μέτρα προστασίας και δεν υιοθετήσει μια πολύ προσεκτική συμπεριφορά. Ο βασικότερος κανόνας είναι η προσεκτική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στην οθόνη του υπολογιστή. Παρακάτω αναλύονται τα προβλήματα που υπάρχουν στο διαδίκτυο, με ποιον τρόπο μπορεί κάποιος να εξαπατηθεί κ τι πρέπει να προσέχει.

3.2.1 Phishing

Όπως το ίδιο το όνομά του υπονοεί -παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα. Phishing αποκαλείται στην ορολογία του Internet η διαδικασία κατά την οποία κάποιος προσπαθεί να αποκτήσει ευαίσθητες προσωπικές πληροφορίες, όπως όνομα χρηστή, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών, με δόλια και παράνομα μέσα και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα

οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο Internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας. Συνήθως είναι απομιμήσεις δημοφιλών κοινωνικών site, site δημοπρασιών και site online πληρωμών (τράπεζες, ηλεκτρονικά καταστήματα, υπηρεσίες ηλεκτρονικών πληρωμών κλπ.). Το Phishing διενεργείται συνήθως μέσω e-mail ή άμεσων μηνυμάτων μέσω των οποίων οι χρήστες οδηγούνται σε ένα site το οποίο φαίνεται σαν το νόμιμο και τους ζητείται να δώσουν τα προσωπικά τους στοιχειά. Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια μοναδική ευκαιρία και ζητά από τον ανυποψίαστο χρήστη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας. Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου –σύντομου- χρονικού διαστήματος ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος. Στη συνέχεια, τα στοιχεία που απέσπασαν από τον χρήστη θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών.

Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω Phishing. Τα e-mail που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά τους. Το Phishing είναι ένα παράδειγμα των τεχνικών του social engineering που χρησιμοποιούνται για να ξεγελάσουν τους χρήστες και να εκμεταλλευτούν την κακή χρήση των σημερινών τεχνολογιών ασφάλειας στο διαδίκτυο.

3.2.2 Κλοπές Λογαριασμών

Οι κλοπές λογαριασμών αναφέρονται σε κλοπές λογαριασμών e-mail, ηλεκτρονικών τραπεζών, κοινωνικών site κ. ά. Έτσι εάν κάποιος κλέψει το λογαριασμό που έχει κάποιος χρηστής σε μια ηλεκτρονική τράπεζα μπορεί να κάνει τις συναλλαγές που αυτός επιθυμεί και να χρεώνεται η πιστωτική κάρτα του ανυποψίαστου χρηστή. Ακόμα, η κλοπή ενός e-mail είναι και αυτή επικίνδυνη καθώς μπορεί να υπάρχουν καταχωρημένα εκεί προσωπικά του στοιχεία όπως passwords και αριθμοί πιστωτικών καρτών. Οι τρόποι που κάποιος μπορεί να κλέψει τον λογαριασμό ενός χρηστή είναι :

- **Μη ασφαλή passwords**

Συνήθως οι περισσότεροι χρηστές που δε γνωρίζουν τους κινδύνους που υπάρχουν στο Internet χρησιμοποιούν για password τα γενέθλια τους, κάποια επέτειο, ή ακόμα και το ίδιο το όνομα τους, με αποτέλεσμα εάν κάποιος έχει το username του χρήστη ή το e-mail του να κάνει κάποιες δόκιμες και να το βρει μέσα σε λίγη ώρα και έτσι να μπορέσει να χρησιμοποιήσει τα δεδομένα αυτά εις βάρος του χρήστη.

- **Social Engineering**

Το Social engineering είναι ένας τρόπος όπου κάποιος εκμεταλλεύεται κάποιον άλλον με μοναδικό του στόχο του να αποκτήσει παράνομα και ευαίσθητα δεδομένα (όπως passwords, στοιχεία πιστωτικής κάρτας κ.ά.). Οι Social Engineers παρατηρούν το προσωπικό περιβάλλον των θυμάτων τους και χρησιμοποιούν πλαστές ταυτότητες έτσι ώστε να "κερδίσουν" απόρρητες πληροφορίες ή ακόμα και δωρεάν υπηρεσίες. Στις περισσότερες περιπτώσεις το Social Engineering χρησιμοποιείται για να διεισδύσει σε κάποιον τρίτο υπολογιστή και να κατασκοπεύσουν τα προσωπικά του δεδομένα, σε αυτήν την περίπτωση λέγεται και Social Hacking.

Ένα από τα πρώτα κρούσματα του Social Engineering σημειώθηκε στις αρχές της δεκαετίας του 1980 και ονομάστηκε Phreaking. Οι Phreakers τηλεφώνησαν σε τηλεφωνικές εταιρίες ισχυριζόμενοι ότι είναι διαχειριστές του συστήματος και ζήτησαν passwords τα οποία χρησιμοποίησαν για να συνδεθούν στο Internet παράνομα και χωρίς χρέωση.

3.2.3 Ιοί

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.

Ιός μέσω ηλεκτρονικού ταχυδρομείου

Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο. Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail. Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα. Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Trojan

Στην επιστήμη των υπολογιστών, ο δούρειος ίππος (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Το όνομά του προκύπτει από την Ιλιάδα του Ομήρου, όπου αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στην κοιλιά του οποίου κρύβονταν Αχαιοί πολεμιστές. Με τον τρόπο αυτό ξεγέλασε τους κάτοικους της Τροίας, εισήγαγε τον στρατό των Αχαιών μέσα στην πόλη και την κυρίευσε. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, οπότε πήραν και αυτήν την ονομασία. 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.

Υπάρχουν δύο είδη δούρειων ίππων:

- Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι χάκερς μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer –to- peer), προγράμματα ανακοίνωσης καιρικών συνθηκών κοκ.
- Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κοκ), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Τέλος, στην επιστήμη της αρχιτεκτονικής υπολογιστών, η λέξη "δούρειος ίππος" μπορεί επίσης να αναφέρεται και σε κενά ασφαλείας που επιτρέπουν σε διάφορα προγράμματα να διαβάσουν αρχεία χωρίς εξουσιοδότηση.

Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, το ανοιγόκλεισμα του οδηγού CD-ROM, η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες, απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή, απενεργοποίηση προγραμμάτων firewall ή αντιϊκών και πολλά άλλα.

3.2.4 Spoofed e-mails

E-mail spoofing είναι ένας όρος που χρησιμοποιείται για να περιγράψει δόλια e-mail δραστηριότητα κατά την οποία η διεύθυνση του αποστολέα καθώς και άλλα μέρη της κεφαλίδας (header) του e-mail έχουν αλλοιωθεί έτσι ώστε να φαίνεται ότι προέρχεται το e-mail από διαφορετική πηγή. E-mail spoofing είναι μια τεχνική

που χρησιμοποιείται συχνά σαν spam e-mail και ως τεχνική Phishing για να αποκρύψει την πραγματική προέλευση ενός μηνύματος e-mail. Με την αλλαγή ορισμένων ιδιοτήτων του e-mail, όπως τα πεδία «*Από»,* και «*Απάντηση-Προς»* (τα οποία μπορούν να βρεθούν στην κεφαλίδα του μηνύματος), οι κακοπροαίρετοι χρήστες μπορούν να κάνουν το μήνυμα του ηλεκτρονικού ταχυδρομείου να φαίνεται ότι είναι από κάποιον άλλο από το πραγματικό αποστολέα. Το αποτέλεσμα είναι ότι, αν και το e-mail φαίνεται να προέρχεται από τη διεύθυνση που αναφέρεται στο πεδίο «*Από*» στην πραγματικότητα προέρχεται από άλλη πηγή.

Όπως πολλοί spammers χρησιμοποιούν ειδικό λογισμικό για να δημιουργήσουν τυχαίες διευθύνσεις αποστολέα, ακόμα και αν ο χρήστης διαπιστώσει την προέλευση του ηλεκτρονικού ταχυδρομείου είναι μάλλον απίθανο ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου θα είναι ενεργή.

- Διαφημίσεις.
- Προειδοποιητικά μηνύματα που καλούν τον χρήστη να προβεί σε ενέργειες (αποδεχόμενος συγκεκριμένες προσφορές) με άγνωστες ή επικίνδυνες για αυτόν συνέπειες.
- Κάλεσμα για παιχνίδια είτε κανονικά είτε τυχερά.
- Δωρεές.
- Δεσμοί σε σελίδες πορνογραφικού περιεχομένου και γενικά ποικιλία δελεαστικών προτάσεων.

Η ενδεδειγμένη ενέργεια είναι να κλείνουν άμεσα αυτά τα παράθυρα. Η εμφάνιση τέτοιων παραθύρων μπορεί να αποφευχθεί χρησιμοποιώντας κατάλληλα προγράμματα (pop up blockers/killers), τα οποία προσφέρονται στο διαδίκτυο. Επισημαίνεται ότι η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την πρόσβαση σε κάποιες, χρήσιμες κατά τα άλλα, ιστοσελίδες. Μία τέτοια περίπτωση είναι αυτή κατά την οποία έγκυρες εταιρείες προσφέρουν μέσω pop up παραθύρων προγράμματα εφαρμογών απαραίτητα για τη σωστή εμφάνιση ενός πλήθους ιστοσελίδων Σε αυτή την περίπτωση οι χρήστες μπορούν προσωρινά να απενεργοποιήσουν τον blocker.

3.2.5 Ενοχλητική αλληλογραφία (spam mail).

Από τα πρώτα δυσάρεστα εμπόδια που κλήθηκαν (και καλούνται) να αντιμετωπίσουν οι χρήστες του Internet ήταν και είναι το spam mail. Τα τελευταία χρόνια, μάλιστα, έχει αποκτήσει και παρέα: τα διαδοχικά pop-up windows με διαφημιστικά banners που αφαιρούν από το web την βασική του γοητεία: την πλοήγηση. Είναι το λεγόμενο spam ή junk mail, δηλαδή μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters). Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Διαδικτύου και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Διαδικτύου και κινδυνεύει η ασφάλεια των δικτύων. Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα. Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος. Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη. Τα περισσότερα από αυτά τα προγράμματα διακρίνονται από εξαιρετική δυνατότητα ανίχνευσης και παρεμπόδισης του spam mail, κάτι που οφείλεται στα προηγμένα τεχνολογικά "έξυπνα" φίλτρα που χρησιμοποιούν τα οποία με την σειρά τους βασίζονται σε συνδυασμούς κριτηρίων που αφορούν στον έλεγχο του περιεχομένου του μηνύματος, τη διεύθυνση του αποστολέα, το θέμα του μηνύματος, αλλά ακόμα και την προέλευσή του (χώρα προέλευσης, κόμβος-στοιχεία που προκύπτουν μέσα από την ανάλυση των headers του μηνύματος.

3.2.6 Μηνύματα απατηλού περιεχομένου (hoaxes).

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

1. «Προειδοποιητικά»: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα
2. «Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται
3. «Εκφοβισμού»: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος. Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

3.2.7 Άλλοι Κίνδυνοι

Ο όρος ασφάλεια περιλαμβάνει την προστασία αγαθών των επιχειρήσεων. Τα αγαθά μπορεί να είναι απτά στοιχεία όπως μια ιστοσελίδα ή η βάση δεδομένων των πελατών της επιχείρησης, ή μπορεί να είναι λιγότερο απτά όπως η φήμη μιας επιχείρησης.

Οι κίνδυνοι στα συστήματα ηλεκτρονικών πληρωμών είναι:

- Τα ψηφιακά έγγραφα μπορούν αυθαίρετα να αντιγραφούν.
- Οι ψηφιακές υπογραφές μπορούν να παραχθούν από οποιοδήποτε γνωρίζει το ιδιωτικό κλειδί.
- Η ταυτότητα του πληρωτή μπορεί να συνδεθεί με κάθε συναλλαγή πληρωμής, με αποτέλεσμα να γίνονται γνωστές οι καταναλωτικές και όχι μόνο συνήθειες του πληρωτή.

Προφανώς χωρίς πρόσθετα μέτρα ασφάλειας, το διαδεδομένο ηλεκτρονικό εμπόριο δεν θα ήταν βιώσιμο. Γενικά τα ηλεκτρονικά συστήματα πληρωμών αντιμετωπίζουν τους εξής επιτιθέμενους:

- Αυτούς που κρυφακούν στη γραμμή επικοινωνίας και συλλέγουν πληροφορίες (π.χ. αριθμούς πιστωτικών καρτών) τις οποίες χρησιμοποιούν για απάτες με σκοπό το δικό τους οικονομικό όφελος.
- Αυτούς που επεμβαίνουν και τροποποιούν τα μηνύματα που ανταλλάσσονται σε μια συναλλαγή πληρωμής, προκειμένου να κλέψουν αγαθά ή χρήματα.
- Τους ανέντιμους συμμετέχοντες στη συναλλαγή πληρωμής (π.χ. έμπορος), οι οποίοι χρησιμοποιούν για απάτες τις πληροφορίες πληρωμής (π.χ. αριθμούς πιστωτικών καρτών) που τους δίνει ο πελάτης.

Οι συνέπειες της έλλειψης ασφάλειας μπορεί να είναι αρκετές:

1. Παραποίηση πληροφορίας
2. Άρνηση παροχής υπηρεσιών
3. Λανθασμένη και ανεπιθύμητη αποστολή πληροφοριών
4. Υποκλοπή πληροφοριών

Τέλος πρέπει να σημειωθεί ότι το internet γίνεται πολύ περισσότερο ευπρόσβλητο σε επιθέσεις με το περάς του χρόνου λόγω της τεράστιας ανάπτυξης του. Υπάρχουν τρεις παράγοντες που οδηγούν σε αυτό το συμπέρασμα. Πρώτον, στις μέρες μας είναι πολύ πιο εύκολο να δημιουργήσει κάποιος ένα κακόβουλο

πρόγραμμα και αυτό γιατί δεν χρειάζεται να έχει κάποιος ιδιαίτερες γνώσεις προγραμματισμού καθώς και το ότι υπάρχει ένας τεράστιος όγκος έτοιμων πληροφοριών διαθέσιμα στο Web όπως προγράμματα δημιουργίας ιων. Δεύτερον, η εκρηκτική ανάπτυξη του αριθμού των χρηστών και των διασυνδεδεμένων υπολογιστών σήμερα σημαίνει πως ο μέσος χρήστης κάθε άλλο παρά ειδικός είναι με αποτέλεσμα να είναι πολύ λιγότερο ικανός να προστατεύσει το σύστημα του , να διαπιστώσει τυχόν περίεργα σημάδια ή πολύ περισσότερο να διορθώσει κάποιο πρόβλημα. Τρίτον, η μεγάλη διάδοση των Windows σημαίνει, σε συνδυασμό με την απειρία των χρηστών, πως οι υπολογιστές σήμερα αποτελούν για το μεγάλο μερίδιο αυτών που τους χρησιμοποιούν, μαύρα κουτιά, το εσωτερικό της λειτουργίας των οποίων παραμένει αόρατο και εκτός της δυνατότητας παρέμβασης του μέσου ή σε πολλές άλλες περιπτώσεις ακόμα και του έμπειρου χρήστη.

3.3 Ασφάλεια Περιμέτρου

Πολλοί οργανισμοί ηλεκτρονικού εμπορίου έχουν συνδέσει τα εσωτερικά τους δίκτυα με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών, αλλά και για τη λήψη χρήσιμων πληροφοριών από τον παγκόσμιο ιστό. Η σύνδεση όμως ενός συστήματος στο διαδίκτυο (δημόσιο δίκτυο) δίνει τη δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Δηλαδή οι χρήστες του ιδιόκτητου δικτύου μπορούν να έχουν πρόσβαση στο διαδίκτυο. Ταυτόχρονα και οι χρήστες του διαδικτύου μπορούν να επικοινωνήσουν με το ιδιόκτητο δίκτυο, κάτι το οποίο δεν είναι πάντα επιθυμητό αφού εμπιστευτικές πληροφορίες που βρίσκονται στα συστήματα ενός οργανισμού μπορούν να διαρρεύσουν.

Ειδικά για το ηλεκτρονικό εμπόριο, όπου στα δίκτυα των οργανισμών φυλάσσονται έμπιστα δεδομένα, απαιτείται ένα υψηλό επίπεδο ασφάλειας δικτύου. Πρέπει δηλαδή να εμποδίζονται οι εξωτερικοί χρήστες από το να προσεγγίσουν τις ιδιωτικές πληροφορίες του οργανισμού έτσι ώστε τα προσωπικά δεδομένα των πελατών του οργανισμού ηλεκτρονικού εμπορίου να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Συνεπώς είναι απαραίτητη η ασφάλεια περιμέτρου του ιδιόκτητου δικτύου.

Ως Περίμετρος Δικτύου ορίζονται, σύμφωνα με την ΑΔΑΕ, «όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (π.χ. διαδίκτυο)». Σύμφωνα πάντα με την ΑΔΑΕ, κάθε οργανισμός που συνδέει το εσωτερικό του δίκτυο με κάποιο δημόσιο δίκτυο, π.χ. το διαδίκτυο, θα πρέπει να εφαρμόζει μια πολιτική ασφάλειας περιμέτρου. Ο πρωταρχικός σκοπός της πολιτικής αυτής είναι να προστατεύσει τους διάφορους πόρους του οργανισμού από εισβολείς, δηλαδή να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του οργανισμού. Η ΑΔΑΕ υποχρεώνει κάθε πάροχο διαδικτύου, οπότε έμμεσα και κάθε οργανισμό ηλεκτρονικού εμπορίου, να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το διαδίκτυο και επιπλέον τον υποχρεώνει να χρησιμοποιεί συστήματα ανίχνευσης εισβολών για την ενίσχυση της προστασίας του δικτύου του.

Ένα σύστημα firewall καλείται να λειτουργήσει ως ένας μηχανισμός «περιμετρικής άμυνας», ο οποίος δρα συμπληρωματικά με τους υπόλοιπους μηχανισμούς ασφάλειας. Σκοπός του είναι ο έλεγχος και η καταγραφή όλων των προσπαθειών προσπέλασης οι οποίες κατευθύνονται προς το προστατευόμενο σύστημα, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του.

Τα συστήματα ανίχνευσης εισβολών (IDS) προσπαθούν να ανιχνεύσουν οποιαδήποτε παράνομη δραστηριότητα στοχεύει σε δικτυακούς και υπολογιστικούς πόρους. Τα συστήματα αυτά συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων και στη συνέχεια αναλύουν τις πληροφορίες για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης.

Τα firewalls και τα IDS αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο. Στη συνέχεια του κεφαλαίου αυτού γίνεται μια αναλυτική περιγραφή των δυνατοτήτων και των περιορισμών των δύο αυτών σημαντικών τεχνολογιών για την ασφάλεια περιμέτρου, των firewalls και των IDS.

3.3.1 Firewalls

Τα δίκτυα των οργανισμών ηλεκτρονικού εμπορίου συνδέονται με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών. Όπως αναφέρθηκε παραπάνω, αυτό εγκυμονεί κινδύνους, αφού οι χρήστες του διαδικτύου μπορούν να προσεγγίσουν τις ιδιωτικές πληροφορίες του οργανισμού.

Για έναν οργανισμό ηλεκτρονικού εμπορίου είναι πολύ σημαντικό να μπορεί να διαφυλάξει τα προσωπικά δεδομένα των πελατών του από μη εξουσιοδοτημένη πρόσβαση. Είναι επιθυμητό να υπάρχει ένα είδος διαχωρισμού ανάμεσα στο δίκτυο του οργανισμού και το διαδίκτυο. Η παρεμβολή ενός ενδιάμεσου συστήματος ανάμεσα στα δύο δίκτυα θα μπορούσε να τα διαχωρίσει. Ένα τέτοιο ενδιάμεσο σύστημα θα προστατεύει το ιδιόκτητο δίκτυο από επιθέσεις που προέρχονται από τον έξω κόσμο και θα παρέχει ένα μοναδικό σημείο ελέγχου, όπου θα ελέγχεται η κίνηση από και προς το δίκτυο. Επιπλέον το ενδιάμεσο αυτό σύστημα θα μπορούσε να χρησιμοποιηθεί και για συλλογή πληροφοριών διαχείρισης για χρήση του δικτύου, αφού μπορεί να καταγράφει οτιδήποτε διακινείται από ή προς το δίκτυο. Αυτά τα ενδιάμεσα συστήματα ονομάζονται φράγματα ασφαλείας (firewalls).

Firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση δεδομένων από και προς το εξωτερικό δίκτυο. Στην πύλη εξετάζεται και αποφασίζεται αν θα επιτραπεί ή όχι η διέλευση των δεδομένων, σύμφωνα με την πολιτική ασφάλειας που εφαρμόζει ο οργανισμός του συστήματος. Το firewall δεν είναι απλώς ένα σύνολο συνιστωσών λογισμικού ή υλικού, αλλά η τεχνική έκφραση μιας συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού.

Ένα firewall είναι ουσιαστικά ένα «τείχος» ασφάλειας μεταξύ του μη ασφαλούς δημόσιου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποία πακέτα επιτρέπεται και ποια όχι να περάσουν στο «απέναντι» δίκτυο.

Ένα firewall δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως του πως έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφάλειας. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας

που βρίσκεται κάθε φορά σε ισχύ και πρέπει να είναι συγκεκριμένη και σαφής. Το firewall αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ τη μοναδική.

Η χρήση ενός φράγματος ασφάλειας δεν αποτελεί πανάκεια για την ασφάλεια του δικτύου. Όπως όλα τα συστήματα ασφάλειας μπορεί να παραβιαστεί από κάποιον ικανό εισβολέα. Επιπλέον το firewall αλληλεπιδρά με το διαδίκτυο και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και την σωστή διαμόρφωσή του.

Η Αναγκαιότητα Χρήσης των Firewalls

Σε ένα περιβάλλον χωρίς firewalls η δικτυακή ασφάλεια αποτελεί αποκλειστικά μέριμνα του κάθε σταθμού ξεχωριστά και όλοι οι σταθμοί πρέπει να συνεργάζονται ώστε να παρέχουν ένα ομοιόμορφα υψηλό επίπεδο ασφάλειας. Όσο πιο μεγάλο είναι το δίκτυο, τόσο πιο δύσκολα επιτυγχάνεται η διατήρηση όλων των σταθμών σε υψηλά επίπεδα ασφάλειας. Εξαιτίας της πολυπλοκότητας του δικτύου, τα λάθη και οι παραλήψεις στην ασφάλεια είναι συχνό φαινόμενο, με αποτέλεσμα να δημιουργούνται «οπές» ασφάλειας τις οποίες μπορούν να ανακαλύψουν και να εκμεταλλευτούν οι εισβολείς. Τα firewalls έχουν σχεδιαστεί έτσι ώστε να παρέχουν προηγμένες λειτουργίες παρακολούθησης και καταγραφής και η διαχείριση τους να είναι σχετικά εύκολή.

Δυνατότητες των Firewalls

Η λειτουργικότητα των firewalls εκτείνεται στα ακόλουθα:

- Το firewall αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφάλειας: Το firewall απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο, το οποίο συνδέει τον οργανισμό με τον εξωτερικό κόσμο, και όχι στον κάθε υπολογιστή χωριστά μέσα σε ολόκληρο το δίκτυο.
- Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο, υλοποιώντας την πολιτική ασφάλειας του οργανισμού: Με βάση την καθορισμένη πολιτική ασφάλειας η οποία περιγράφει σε ποια πακέτα και σε ποιες συνόδους επιτρέπεται η είσοδος ή έξοδος, το firewall αποφασίζει εάν θα επιτρέψει ή θα αρνηθεί τη διέλευση ενός πακέτου ή την έναρξη μιας συνόδου, αφού προηγουμένως πιστοποιήσει την ταυτότητα τόσο των πακέτων, όσο και των συνόδων.

- Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο: Εφόσον όλη η κίνηση διέρχεται από το firewall, μπορεί αυτό να καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων, το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου.
- Το firewall προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού: Μερικές φορές το firewall μπορεί να χρησιμοποιηθεί για να διαχωρίσει ένα τμήμα του δικτύου από κάποιο άλλο. Με τον τρόπο αυτό μπορούμε να αποτρέψουμε την εξάπλωση σε ολόκληρο το δίκτυο ενδεχόμενων προβλημάτων που επηρεάζουν ένα συγκεκριμένο τμήμα.
- Το firewall έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης: Τα τελευταία χρόνια το Internet αντιμετωπίζει πρόβλημα διαθέσιμων IP διευθύνσεων. Οι οργανισμοί που επιθυμούν να συνδεθούν με το Internet μπορεί να μην έχουν διαθέσιμες πραγματικές IP διευθύνσεις. Το firewall ενσωματώνει το NAT (Network Address Translator), το οποίο μεταφράζει τις εσωτερικές διευθύνσεις σε πραγματικές, λύνοντας έτσι το πρόβλημα της έλλειψης διευθύνσεων.

Αδυναμίες των Firewalls

Ένα firewall προσφέρει εξαιρετική προστασία απέναντι σε απειλές κατά του δικτύου, αλλά δεν αποτελεί ολοκληρωμένη λύση ασφάλειας. Υπάρχουν συγκεκριμένες απειλές, οι οποίες βρίσκονται πέρα από τις δυνατότητες ελέγχου του firewall.

Οι αδυναμίες των firewalls είναι οι ακόλουθες:

- Το firewall δεν μπορεί να προστατεύσει από προγράμματα-ιούς: Τα firewalls δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Απλά εξετάζουν τις διευθύνσεις και τις θύρες προέλευσης και προορισμού, για να καθορίσουν εάν επιτρέπεται η είσοδος στο εσωτερικό δίκτυο.
- Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού: Οι εσωτερικοί χρήστες είναι σε θέση να υποκλέψουν δεδομένα, να καταστρέψουν υλικό και λογισμικό, να τροποποιήσουν προγράμματα και γενικότερα να παραβιάσουν την πολιτική ασφάλειας του οργανισμού χωρίς καν να έρθουν

σε επαφή με το firewall. Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή υπολογιστή (host security).

- Το firewall δε μπορεί να προστατέψει τον οργανισμό απέναντι σε επιθέσεις συσχετιζόμενες με δεδομένα: Τέτοιου είδους επιθέσεις συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρετητές του οργανισμού, είτε διαμέσου του ηλεκτρονικού ταχυδρομείου, είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος.
- Το firewall δεν μπορεί να προστατέψει τον οργανισμό από απειλές άγνωστου τύπου: Το firewall μπορεί να προστατέψει το δίκτυο μόνο από γνωστές απειλές που έχουν αντιμετωπιστεί στο παρελθόν, εφόσον διαθέτει την απαιτούμενη τεχνολογία.
- Το firewall δεν μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό: Αν για παράδειγμα επιτρέπεται σε κάποιους έμπιστους χρήστες να έχουν πρόσβαση στο διαδίκτυο παρακάμπτοντας τους μηχανισμούς ασφάλειας του firewall, τότε το firewall δεν μπορεί να προστατέψει τις συνδέσεις αυτές. Ένα firewall μπορεί να ελέγξει αποτελεσματικά την κίνηση που διέρχεται μέσα από αυτό.
- Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του firewall: Είναι δυνατό ένα firewall να ρυθμιστεί με πολύ αυστηρό τρόπο, με κίνδυνο να εμποδίσει τη διαδικτύωση ή να προκαλεί δυσαρέσκεια στους χρήστες, εξαιτίας των πολλών ελέγχων και της ελαττωμένης φιλικότητας και ευχρηστίας που εισάγει.

3.3.2 Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems, IDS)

Τα τελευταία χρόνια, η ανάπτυξη του διαδικτύου και του ηλεκτρονικού εμπορίου έχει οδηγήσει στην αύξηση των παράνομων δραστηριοτήτων, όχι μόνο από εξωτερικούς εισβολείς, αλλά και από υπαλλήλους των οργανισμών ηλεκτρονικού εμπορίου που καταχρώνται τα δικαιώματα που τους δίνονται για προσωπικό όφελος.

Ειδικά για τους οργανισμούς ηλεκτρονικού εμπορίου, όπου στα δίκτυα τους φυλάσσονται έμπιστα δεδομένα, όπως είναι τα προσωπικά στοιχεία των πελατών

τους, η ανίχνευση εισβολών σε δίκτυα έχει ιδιαίτερη σημασία. Οι οργανισμοί αυτοί πρέπει να παρέχουν ένα υψηλό επίπεδο ασφάλειας δικτύου και για το λόγο αυτό θα πρέπει να χρησιμοποιούν συστήματα ανίχνευσης εισβολών (IDS), τα οποία ενισχύουν την προστασία του δικτύου τους. Τα συστήματα ανίχνευσης εισβολών (IDS) αποτελούν ένα ισχυρό εργαλείο για την ασφάλεια δικτύων, το οποίο συμπληρώνει τη λειτουργία των συστημάτων firewalls.

Με την αύξηση των παράνομων δραστηριοτήτων και εισβολών στα δικτυωμένα συστήματα υπήρξε παράλληλη ανάπτυξη και στα συστήματα ανίχνευσης εισβολών (IDS), τόσο στον εμπορικό όσο και στον ερευνητικό τομέα. Αυτά τα συστήματα προσπαθούν να ανιχνεύσουν οποιαδήποτε παράνομη δραστηριότητα στοχεύει σε δικτυακούς και υπολογιστικούς πόρους. Τα συστήματα αυτά συνήθως μπορούν να ανιχνεύσουν μόνο περιορισμένο εύρος εισβολών.

Τα συστήματα ανίχνευσης εισβολών είναι προϊόντα με μορφή λογισμικού ή και υλικού, τα οποία αυτοματοποιούν τη διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε παράνομες δραστηριότητες. Τα συστήματα αυτά συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων και στη συνέχεια αναλύουν τις πληροφορίες για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης.

Όταν το σύστημα ανίχνευσης εισβολών συλλέγει πληροφορίες για το δίκτυο συνεχώς και προσπαθεί να αποφανθεί για το αν το δίκτυο είναι υπό επίθεση ή όχι, τότε έχουμε «δικτυακό σύστημα ανίχνευσης εισβολής» (Network Based IDS – NIDS). Ενώ όταν συλλέγονται και επεξεργάζονται πληροφορίες στον υπολογιστή του δικτύου για να αποφασίσει το σύστημα αν βρίσκεται υπό επίθεση, τότε έχουμε «σύστημα ανίχνευσης εισβολής εγκατεστημένο σε υπολογιστή» (Host Based IDS - HIDS).

Βασικά Ζητήματα Ανίχνευσης Εισβολών

Τα υπολογιστικά συστήματα, στην κανονική τους λειτουργία, πληρούν τα ακόλουθα χαρακτηριστικά:

Οι ενέργειες των χρηστών και των διεργασιών ακολουθούν, σε γενικές γραμμές, ένα στατιστικά προβλέψιμο πρότυπο. Για παράδειγμα ένας χρήστης που χρησιμοποιεί προγράμματα αυτοματισμού γραφείου θεωρείται απίθανο να προσπαθήσει να εκτελέσει λειτουργίες συντήρησης συστήματος.

Οι ενέργειες των χρηστών και των διεργασιών δεν περιλαμβάνουν ακολουθίες εντολών που να υπονομεύουν την πολιτική ασφάλειας του συστήματος. Θεωρητικά, τέτοιες ακολουθίες εντολών πρέπει να μη γίνονται δεκτές. Στην πραγματικότητα, όμως, μπορούν να ανιχνευθούν μόνο γνωστές ακολουθίες υπονόμευσης του συστήματος.

Οι ενέργειες των διεργασιών συμμορφώνονται με ένα σύνολο προδιαγραφών που περιγράφουν επιτρεπτές ενέργειες.

Όταν όλα λειτουργούν κανονικά σε ένα υπολογιστικό σύστημα, τα πιο πάνω χαρακτηριστικά πληρούνται. Σε περίπτωση όμως επίθεσης στο δίκτυο, τουλάχιστον ένα από τα πιο πάνω χαρακτηριστικά δεν ισχύει. Τα συστήματα ανίχνευσης εισβολών έχουν ως γενικό πλαίσιο για την ανίχνευση εισβολής αυτά τα χαρακτηριστικά. Δηλαδή αν ανιχνεύσουν παραβίαση κάποιου χαρακτηριστικού, τότε σημάνουν συναγερμό για πιθανή εισβολή.

Εσωτερική Λειτουργία των Συστημάτων Ανίχνευσης Εισβολών

Ένα απλοποιημένο μοντέλο ενός συστήματος ανίχνευσης εισβολών μπορεί να καθοριστεί σαν μια ομάδα από διάφορα αλληλοεξαρτώμενα μέρη. Αυτά είναι:

- Συλλογή πρωτογενών δεδομένων από κατάλληλους αισθητήρες.
- Ανίχνευση και ενημέρωση του κατάλληλου προσωπικού για τα γεγονότα.
- Ανάλυση των δεδομένων.
- Αποθήκευση των δεδομένων σε μια αντίστοιχη βάση.
- Αντίδραση στα γεγονότα.
- Γραφικό περιβάλλον εργασίας για τη διεπαφή με το διαχειριστή.

Οι παραπάνω λειτουργίες μπορούν να υλοποιηθούν σε ξεχωριστά συστήματα, παρουσιάζοντας όμως το τελικό αποτέλεσμα σε ένα κεντρικό σταθμό διαχείρισης.

Ο σκοπός λειτουργίας των αισθητήρων είναι η συλλογή πληροφοριών σχετικά με συγκεκριμένα γεγονότα, καθώς και η προώθηση αυτών των πληροφοριών στα υπόλοιπα μέρη, αφού πρώτα φιλτράρουν τις πληροφορίες μειώνοντας έτσι τον όγκο τους.

Η λειτουργία της μηχανής ανάλυσης έχει να κάνει με την πιο διεξοδική ανάλυση των στοιχείων που παρέχονται από την προηγούμενη λειτουργία της συλλογής (χωρίς περιττά στοιχεία), καθώς και την εξαγωγή συμπερασμάτων για την απόπειρα ή πραγματοποίηση μιας επίθεσης.

Η λειτουργία της αποθήκευσης δεδομένων του συστήματος ανίχνευσης εισβολών καθορίζει το μέσο στο οποίο αποθηκεύονται οι πληροφορίες που αφορούν την ασφάλεια ενός συστήματος, ώστε να μπορούν αργότερα να χρησιμοποιηθούν από το προσωπικό για περαιτέρω ανάλυση.

Τέλος η λειτουργία αντίδρασης στα γεγονότα αναλαμβάνει να προειδοποιήσει το κατάλληλο προσωπικό για ένα περιστατικό ασφάλειας αλλά και να δράσει δυναμικά (π.χ. διακοπή μιας σύνδεσης), έτσι ώστε να προστατευτεί το δίκτυο από περαιτέρω επιθέσεις.

Χαρακτηριστικά των Συστημάτων Ανίχνευσης Εισβολών

Ένα ιδανικό Σύστημα Ανίχνευσης Εισβολών πρέπει να έχει τα παρακάτω χαρακτηριστικά:

- Πρέπει να ανιχνεύει μεγάλο εύρος εισβολών: Τα συστήματα ανίχνευσης εισβολών πρέπει να μπορούν να εντοπίσουν γνωστές και άγνωστες επιθέσεις. Η δυνατότητα αυτή έχει ως προϋπόθεση την ύπαρξη ενός μηχανισμού εκμάθησης ή προσαρμογής στους νέους τύπους επίθεσης και στις αλλαγές της συνήθους δραστηριότητας των χρηστών.
- Πρέπει να ανιχνεύει έγκαιρα τις εισβολές: Απαιτείται η ανακάλυψη μιας εισβολής σε εύλογο χρονικό διάστημα. Σε περίπτωση που πραγματοποιηθεί μια εισβολή, πρέπει σε σύντομο χρονικό διάστημα αυτή να προσδιοριστεί, διότι αλλιώς δεν έχει ιδιαίτερη χρησιμότητα ο προσδιορισμός της εισβολής.
- Πρέπει να λειτουργεί με ακρίβεια: Δεν πρέπει να δίνει ψευδές θετικό σήμα (false positive), δηλαδή να αναφέρει μια επίθεση ενώ στην πραγματικότητα δεν υπάρχει σχετική επίθεση σε εξέλιξη. Τα ψευδώς θετικά σήματα μειώνουν την αξιοπιστία του συστήματος και αυξάνουν χωρίς λόγο την απαιτούμενη εργασία. Από την άλλη πλευρά, ένα σύστημα ανίχνευσης εισβολών δεν πρέπει να δίνει ψευδώς αρνητικά σήματα (false negative), δηλαδή να μην αναφέρει μια πραγματική επίθεση που βρίσκεται σε εξέλιξη. Αυτό είναι ακόμη χειρότερο, αφού σκοπός των συστημάτων ανίχνευσης εισβολών είναι ακριβώς να αναφέρουν τις πραγματικές επιθέσεις.
- Πρέπει να μπορεί να αντιμετωπίσει τυχόν σφάλματα: Το σύστημα πρέπει να μπορεί να επανέλθει μετά από αποτυχίες του συστήματος, και επιπλέον

μετά από αποτυχία πρέπει να μπορεί να επανέλθει ακριβώς στην προηγούμενη του κατάσταση, σαν να μην είχε συμβεί τίποτα.

- Πρέπει να τρέχει συνεχώς με ελάχιστη ανθρώπινη παρακολούθηση.
- Πρέπει να μπορεί να διαμορφώνεται εύκολα, ώστε να προσαρμόζεται με ακρίβεια στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
- Πρέπει να μην μπορεί να καταστραφεί: Πρέπει να είναι αδύνατο να τροποποιήσει ή να αχρηστεύσει κάποιος το σύστημα ανίχνευσης εισβολών.
- Σε περίπτωση που δεν υπάρχουν υπολογιστές αποκλειστικά για το σύστημα ανίχνευσης εισβολών, και το σύστημα αυτό τρέχει στους υπολογιστές του δικτύου, θα πρέπει αυτό να επηρεάζει ελάχιστα την απόδοση των υπολογιστών, ώστε να μην παρεμποδίζει την κανονική τους λειτουργία.
- Πρέπει να είναι ανεξάρτητο λειτουργικού συστήματος, δηλαδή πρέπει να μπορεί να λειτουργεί για ανίχνευση εισβολών σε οποιοδήποτε λειτουργικό σύστημα.

Τεχνολογίες των Συστημάτων Ανίχνευσης Εισβολών

Ένα σύστημα ανίχνευσης εισβολών εξετάζει τη δραστηριότητα σε ένα σύστημα ή δίκτυο με στόχο να βρει πιθανές εισβολές ή επιθέσεις. Τα συστήματα ανίχνευσης εισβολών βασίζονται σε δύο τεχνολογίες, στις Network-Based και στις Host-Based.

Τα Network-Based συστήματα είναι τα πιο διαδεδομένα και εξετάζουν τη διερχόμενη δικτυακή κίνηση για ίχνη εισβολής. Τα κομβικά (Host-Based) συστήματα ανίχνευσης εισβολών παρακολουθούν τη δραστηριότητα χρηστών και εφαρμογών στο τοπικό μηχάνημα για ίχνη εισβολής.

Ένα σύστημα ανίχνευσης εισβολών χρησιμοποιεί κάποιους μηχανισμούς ανάλυσης για να μπορέσει να προσδιορίσει αν κάτι είναι ύποπτο ή όχι. Γενικά υπάρχουν τρία είδη μηχανισμών ανάλυσης:

Ανάλυση με βάση γεγονότα ή υπογραφές: Τα συστήματα που βασίζονται σε γεγονότα ή υπογραφές λειτουργούν παρόμοια με τα antivirus προγράμματα. Ο κατασκευαστής παράγει μια λίστα με «υπογραφές» δηλαδή χαρακτηριστικά τμήματα που θεωρεί ότι είναι ύποπτα ή ενδεικτικά μιας επίθεσης. Το σύστημα ανίχνευσης εισβολών ερευνά και αναλύει το περιβάλλον ελέγχοντας για γνωστές υπογραφές. Σε περίπτωση που βρει γνωστές υπογραφές το σύστημα ανίχνευσης

εισβολών μπορεί να αντιδράσει εκτελώντας μια προκαθορισμένη ενέργεια. Τα περισσότερα συστήματα ανίχνευσης εισβολών λειτουργούν με αυτό τον τρόπο.

Στατιστική ανάλυση: Τα συστήματα που βασίζονται στη στατιστική ανάλυση κατασκευάζουν στατιστικά πρότυπα του περιβάλλοντος, όπως τη μέση διάρκεια μιας συνόδου telnet και στη συνέχεια κοιτάζουν για αποκλίσεις από τα πρότυπα αυτά.

Προσαρμόσιμα συστήματα: Τα προσαρμόσιμα συστήματα ξεκινούν με γενικούς κανόνες για το περιβάλλον και στη συνέχεια προσαρμόζονται σε τοπικές καταστάσεις που διαφορετικά θα τις θεωρούσαν ασυνήθιστες. Το σύστημα φτάνει στο σημείο να καταλαβαίνει την αλληλεπίδραση ανθρώπων-περιβάλλοντος και προειδοποιεί τους υπεύθυνους για ασυνήθιστες δραστηριότητες.

Οποιοδήποτε σύστημα ανίχνευσης εισβολών θα έχει ενδείξεις κινδύνου όταν όλα είναι φυσιολογικά και δε θα ανιχνεύσει επίθεση όταν υπάρχει ύποπτη δραστηριότητα. Για αυτό δε θα πρέπει να υποτιμάται ο ανθρώπινος παράγοντας, η ύπαρξη του οποίου θα βελτιώσει περισσότερο την αλληλεπίδραση του σύστημα ανίχνευσης εισβολών με το περιβάλλον.

3.4 Ασφάλεια Web Εξυπηρετητών

Η ασφάλεια του εμπορίου στο διαδίκτυο είναι ίσως η μεγαλύτερη πρόκληση που έχουν να αντιμετωπίσουν οι “ειδικοί” στο χώρο του διαδικτύου. Η προστασία των ηλεκτρονικών συναλλαγών αποτελεί τη μια πτυχή του προβλήματος. Για να υπάρχει όμως ασφάλεια στις συναλλαγές απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου (web server). Ο web εξυπηρετητής πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης (web browser) του πελάτη στον εξυπηρετητή του καταστήματος. Οι web εξυπηρετητές διαχειρίζονται και διανέμουν τις πληροφορίες στο διαδίκτυο. Σήμερα οι web εξυπηρετητές αποτελούν τον αγαπημένο στόχο των hackers. Επιπλέον πολλές εφαρμογές διαδικτύου απαιτούν την αλληλεπίδραση του εξυπηρετητή διαδικτύου με βάσεις δεδομένων των εταιρειών, δημιουργώντας έτσι ένα σύνδεσμο με τα εσωτερικά τοπικά δίκτυα.

Οι web εξυπηρετητές είναι πολύπλοκα και εξειδικευμένα προγράμματα, τα οποία δίνουν τη δυνατότητα στις σελίδες HTML (Hypertext Markup Language) να

καταστούν προσπελάσιμες από τα προγράμματα πλοήγησης, εφόσον υπάρχει σύνδεση του υπολογιστή με το διαδίκτυο. Είναι δηλαδή σχεδιασμένοι να δέχονται ανώνυμες αιτήσεις από άγνωστους υπολογιστές σε όλο το διαδίκτυο και να παραδίδουν τις ζητούμενες πληροφορίες γρήγορα και αποτελεσματικά. Δυστυχώς, όμως, δεν υπάρχει λογισμικό που η χρήση του να μην περικλείει κινδύνους και οι web εξυπηρετητές δεν αποτελούν εξαίρεση.

Πολλοί οργανισμοί χρησιμοποιούν web εξυπηρετητές, ο πηγαίος κώδικας των οποίων είναι ελεύθερα διαθέσιμος στο διαδίκτυο. Μονολότι αυτό επιτρέπει τη δοκιμή και τον έλεγχο του προγράμματος, δίνει τη δυνατότητα σε κάποιον, που έχει τις απαραίτητες γνώσεις, να ανακαλύψει ατέλειες που κάνουν τον web εξυπηρετητή ευάλωτο σε επιθέσεις.

Ένας web εξυπηρετητής μπορεί να ενσωματώνει προγράμματα στις ηλεκτρονικές σελίδες του. Τα προγράμματα αυτά δημιουργούνται με το πρωτόκολλο Common Gateway Interface (CGI) και ονομάζονται CGI scripts. Τα CGI scripts, που εκτελούνται στην πλευρά του εξυπηρετητή κάθε φορά που κάποιος θέλει να συνδεθεί με αυτόν, μπορεί να είναι εξαιρετικά απλά, όπως για παράδειγμα ένας μετρητής που αυξάνει κάθε φορά που κάποιος επισκέπτεται τη σελίδα ή αρκετά πολύπλοκα, όπως για παράδειγμα αυτά που παρέχουν τη δυνατότητα για αγορά προϊόντων ή άλλες οικονομικές συναλλαγές μέσα από το διαδίκτυο.

Στον web εξυπηρετητή περιέχονται το root directory (κατάλογος ρίζας) και το document root (ρίζα εγγράφων). Στο document root φυλάσσονται οι αιτούμενες ιστοσελίδες του εξυπηρετητή. Τοποθετούνται εκεί, ώστε να υπάρχει πρόσβαση σε αυτές από το διαδίκτυο. Στο root directory βρίσκονται τα αρχεία που ρυθμίζουν τις λειτουργίες του εξυπηρετητή και τα αρχεία CGI.

3.4.1 Λειτουργίες των Web Εξυπηρετητών

Οι web εξυπηρετητές εκτελούν τις παρακάτω λειτουργίες:

- Εξυπηρετούν αιτήσεις HTTP.
- Παρέχουν έλεγχο προσπέλασης, καθορίζοντας ποιος μπορεί να προσπελάσει συγκεκριμένους καταλόγους ή αρχεία στον εξυπηρετητή διαδικτύου.

- Εκτελούν scripts ή προγράμματα, είτε για να προσθέσουν λειτουργικότητα στις ιστοσελίδες, είτε για να παράσχουν πρόσβαση πραγματικού χρόνου (real - time access) σε βάσεις δεδομένων και σε άλλα δυναμικά δεδομένα.
- Καταγράφουν τις συναλλαγές ηλεκτρονικού εμπορίου που πραγματοποιούν οι χρήστες.

Οι εξυπηρετητές μπορούν να διακριθούν από τα εξής:

Πλατφόρμες: μερικοί είναι σχεδιασμένοι για συγκεκριμένη πλατφόρμα (π.χ. Windows), ενώ άλλοι για μια ποικιλία αυτών.

Απόδοση: αριθμός ταυτόχρονων αιτήσεων που μπορούν να χειριστούν, ταχύτητα επεξεργασίας, κλπ.

Ασφάλεια: δυνατότητα πρόσθετων υπηρεσιών ασφάλειας όπως υποστήριξη ανταλλαγής κρυπτογραφημένων δεδομένων.

Εμπόριο: δυνατότητα προχωρημένων υπηρεσιών υποστήριξης ηλεκτρονικών συναλλαγών.

3.4.1 Σφάλματα στην Ασφάλεια του Web Εξυπηρετητή

Τη διαμόρφωση του web εξυπηρετητή την αναλαμβάνει συνήθως κάποιος χρήστης/ διαχειριστής. Πρέπει να επισημανθεί ότι ένας εξυπηρετητής με κακή διαμόρφωση (configuration) μπορεί να δημιουργήσει προβλήματα ασφάλειας ακόμη και σε ένα πολύ καλά σχεδιασμένο σύστημα ασφάλειας. Για το λόγο αυτό, πρέπει να αναλαμβάνει τη διαχείριση του web εξυπηρετητή ένα έμπειρο και αξιόπιστο άτομο.

Ο εξυπηρετητής πρέπει να είναι και φυσικά ασφαλής. Αν ο web εξυπηρετητής βρίσκεται σε ένα εργαστήριο υπολογιστών, σε μια κοινή αίθουσα ή σε άλλες κοινές περιοχές, δεν είναι ασφαλής. Αν έχει το ρόλο ενός σταθμού εργασίας γενικού σκοπού, πιθανώς ούτε εκεί είναι ασφαλής. Ακόμη και αν το μηχάνημα απαιτεί ένα όνομα χρήστη και ένα κωδικό πρόσβασης, είναι απλό για κάποιον επιτιθέμενο να κλέψει ή να τροποποιήσει δεδομένα.

Η ικανότητα των web εξυπηρετητών να ενσωματώνουν CGI scripts περιπλέκει σημαντικά την εφαρμογή ενός συστήματος ασφάλειας. Τα CGI scripts προσθέτουν νέα χαρακτηριστικά και δυνατότητες σε έναν web εξυπηρετητή. Ταυτόχρονα όμως καθιστούν τον εξυπηρετητή πιο ευαίσθητο σε θέματα ασφάλειας. Για παράδειγμα, ένας web εξυπηρετητής μπορεί να έχει ρυθμιστεί έτσι ώστε να έχει πρόσβαση σε

αρχεία ενός συγκεκριμένου καταλόγου, αλλά ένας χρήστης να εγκαταστήσει, ηθελημένα ή όχι, ένα CGI script που να επιτρέπει την ανάγνωση κάθε αρχείου στον υπολογιστή.

Η σύνταξη των CGI scripts πρέπει να γίνεται με ιδιαίτερη προσοχή. Οι περισσότεροι χρήστες δεν έχουν εμπειρία στη σύνταξη ασφαλών CGI scripts και συνεπώς υπάρχει υψηλή πιθανότητα να περιέχουν αδυναμίες, επιτρέποντας έτσι σε εισβολείς να εκτελέσουν οποιαδήποτε εντολή στο σύστημα του web εξυπηρετητή.

Τα κενά στην ασφάλεια του web εξυπηρετητή, που δημιουργούνται από τα λάθη ή την άγνοια των χρηστών, μπορεί να έχουν δυσάρεστες συνέπειες τόσο για τον ίδιο τον εξυπηρετητή όσο και για την ακεραιότητα των αρχείων που φυλάσσονται σε αυτόν. Κάποια ενδεικτικά προβλήματα που είναι πιθανό να παρουσιαστούν είναι τα εξής:

- Ένας εισβολέας μπορεί να εκμεταλλευτεί ατέλειες του web εξυπηρετητή ή των CGI scripts για να αποκτήσει μη εγκεκριμένη πρόσβαση σε αρχεία του εξυπηρετητή, να επέμβει στον εξυπηρετητή τροποποιώντας το σύστημα και να θέσει τον εξυπηρετητή σε προσωρινή αχρηστία.
- Εμπιστευτικές πληροφορίες που βρίσκονται αποθηκευμένες στον web εξυπηρετητή μπορεί να διανεμηθούν σε μη εξουσιοδοτημένα άτομα.
- Εμπιστευτικές πληροφορίες που ανταλλάσσονται μεταξύ του εξυπηρετητή διαδικτύου και του προγράμματος πλοήγησης μπορεί να υποκλαπούν ή να υπάρξει παρεμπόδιση στην αποστολή των δεδομένων, σε οποιοδήποτε σημείο της διαδρομής μεταξύ του εξυπηρετητή και του προγράμματος πλοήγησης.
- Η εμπιστευτικότητα των ηλεκτρονικών συναλλαγών πληρωμής είναι ένα από τα σημαντικότερα ζητήματα ασφάλειας στο ηλεκτρονικό εμπόριο και, σύμφωνα με τα παραπάνω, απαιτείται ένα υψηλό επίπεδο ασφάλειας στον web εξυπηρετητή.

3.4.2 Πολιτική Ασφάλειας Web Εξυπηρετητή

Για την ασφάλεια του web εξυπηρετητή και κατ' επέκταση για την ασφάλεια όλου του δικτύου, πρέπει να υπάρχει ένα ολοκληρωμένο σύστημα προστασίας. Η υλοποίηση του ανατίθεται στο διαχειριστή του εξυπηρετητή. Για την κατασκευή

ενός ασφαλούς web εξυπηρετητή σε οποιαδήποτε πλατφόρμα, πρέπει να ληφθούν υπόψη τα εξής:

- Οι χρήστες του δικτύου δεν πρέπει σε καμιά περίπτωση να μπορούν να εκτελούν προγράμματα ή εντολές κελύφους στον υπολογιστή όπου στεγάζεται ο εξυπηρετητής.
- Τα CGI scripts που τρέχουν στον εξυπηρετητή πρέπει να είναι ελεγμένα διεξοδικά ώστε να επιτελούν τη λειτουργία για την οποία προορίζονται.
- Στην περίπτωση που ο εξυπηρετητής δεχθεί επίθεση, ο επιτιθέμενος δε θα πρέπει να είναι σε θέση να τον χρησιμοποιήσει για να εξαπολύσει επιθέσεις εναντίον των υπόλοιπων υπολογιστών του δικτύου.

Για να ελαχιστοποιηθεί ο κίνδυνος της παρακολούθησης της επικοινωνίας πολλοί οργανισμοί ηλεκτρονικού εμπορίου αγοράζουν ασφαλείς web εξυπηρετητές, που βασίζονται σε κρυπτογραφικά πρωτόκολλα. Αλλά αυτοί οι εξυπηρετητές απαιτούν ψηφιακά υπογεγραμμένα πιστοποιητικά για να λειτουργήσουν και τα πιστοποιητικά αυτά πρέπει να ανανεώνονται τακτικά γεγονός που καθιστά τους εξυπηρετητές ευάλωτους στις επιθέσεις "άρνησης υπηρεσίας".

Ένας οργανισμός ηλεκτρονικού εμπορίου για την υλοποίηση του συστήματος προστασίας θα πρέπει να εφαρμόσει μια πολιτική ασφάλειας σύμφωνα με τους κανονισμούς της ΑΔΑΕ. Η εν λόγω πολιτική ασφάλειας είναι καλό να συμπεριλάβει και παράγοντες όπως:

- Ποιοι επιτρέπεται να χρησιμοποιούν το δίκτυο.
- Πότε επιτρέπεται να το χρησιμοποιούν.
- Τι επιτρέπεται να κάνουν.

Είναι πιθανό διαφορετικές ομάδες χρηστών να έχουν διαφορετικά δικαιώματα εισόδου στα διάφορα μέρη του web εξυπηρετητή. Επίσης οι διαδικασίες παροχής εισόδου στο σύστημα και οι διαδικασίες ανάκλησης της εισόδου, όταν για παράδειγμα ένας χρήστης φεύγει από το σύστημα, αποτελούν ένα σημαντικό κομμάτι του συστήματος προστασίας.

Ένα ακόμη σημείο το οποίο πρέπει να ληφθεί υπόψη είναι το πώς ορίζεται η αποδεκτή χρήση του συστήματος. Ακόμη, στο σύστημα προστασίας, πρέπει να συμπεριληφθούν οι μέθοδοι εισόδου (login) σε αυτό, τόσο για τους εσωτερικούς όσο και για τους εξωτερικούς χρήστες. Τέλος ιδιαίτερο βάρος πρέπει να δοθεί στα

πρωτόκολλα που αφορούν τις αντιδράσεις του συστήματος σε τυχόν κενά ασφάλειας.

3.4.3 Ασφάλεια Συστήματος και Λογισμικού των Web Εξυπηρετητών

Στο εμπόριο και το διαδίκτυο υπάρχουν πολλά λειτουργικά συστήματα. Μερικά από αυτά είναι πιο ασφαλή και μπορούν να χρησιμοποιηθούν ως πλατφόρμες για web εξυπηρετητές. Όσο πιο ευέλικτο και δυναμικό είναι ένα σύστημα τόσο πιο ευάλωτο είναι στις επιθέσεις κατά του εξυπηρετητή. Επίσης, όσα περισσότερα χαρακτηριστικά χρήσης και ευκολίας προσφέρει ο εξυπηρετητής τόσο πιο πιθανό είναι να περιέχει κενά στην ασφάλεια του.

Οι εισβολείς υπολογιστών συνεχώς αναζητούν λάθη σε λογισμικό εξυπηρετητή γιατί κάθε λάθος αναπαριστά μια πιθανή πόρτα εισόδου. Κατασκευάζοντας με προσοχή τα δεδομένα εισόδου που δίνονται στον εξυπηρετητή, ο πονηρός εισβολέας μπορεί να ξεγελάσει το λογισμικό ώστε να πραγματοποιήσει μια μη εγκεκριμένη ενέργεια.

Το πιο ασφαλές σύστημα για web εξυπηρετητή είναι ένας υπολογιστής που τρέχει αποκλειστικά τον εξυπηρετητή και καμιά άλλη εφαρμογή. Παρόλο που ο βασικός εξυπηρετητής του διαδικτύου μπορεί να είναι αρκετά μικρός, αφού χρειάζεται μόνο να ακούει τις εισερχόμενες αιτήσεις για URL, να ανακτά τα αντίστοιχα αρχεία από το δίσκο και να τα στέλνει στο δίκτυο, οι μοντέρνοι web εξυπηρετητές είναι οτιδήποτε παρά απλοί. Οι απλοί εξυπηρετητές που περιέχουν μόνο τα στατικά αρχεία αιτήσεων και καμιά άλλη εφαρμογή θεωρούνται ασφαλέστεροι από τους πολύπλοκους εξυπηρετητές που εκτελούν CGI scripts, αλληλεπιδρούν με μια ποικιλία βάσεων δεδομένων, υποστηρίζουν τις απομακρυσμένες συνδέσεις και προσφέρουν χαρακτηριστικά όπως η λίστα των directories ή τα περιεχόμενα του εξυπηρετητή.

Το λειτουργικό σύστημα UNIX θεωρείται ως μη βέλτιστη επιλογή για web εξυπηρετητή λόγω:

- Της πληθώρας των γλωσσών προγραμματισμού.
- Των εσωτερικά σε αυτό εγκαταστημένων εξυπηρετητών.
- Της πλούσιας ποικιλίας εργαλείων.
- Της ικανότητας σύνδεσης πολλών χρηστών την ίδια στιγμή από οποιοδήποτε απομακρυσμένο σημείο του διαδικτύου.

Επειδή υπάρχουν πολλοί τρόποι εισόδου στο σύστημα, είναι εύκολο για τους εισβολείς να εισβάλουν σε αυτό.

Με το σκεπτικό αυτό, λιγότερο ικανά συστήματα, με περιορισμένα εργαλεία και ευκολίες, όπως τα MS-WINDOWS και τα MACINTOSH, είναι δυσκολότερο να δεχθούν επίθεση και επομένως πιο κατάλληλα για web εξυπηρετητές. Ο βασικός λόγος που τα MACINTOSH είναι ασφαλές είναι λόγω του ότι δεν έχουν ερμηνευτή εντολών, στην πλειοψηφία τους δεν εκτελούν οποιαδήποτε υπηρεσία δικτύου και γενικά οι προκαθορισμένες δυνατότητες τους είναι περιορισμένες. Βέβαια το σύστημα UNIX είναι πιο γρήγορο λειτουργικό από το MacOS και είναι διαθέσιμο για πλατφόρμες που είναι πιο γρήγορες από αυτές που χρησιμοποιούν MS-WINDOWS.

Όσοι επιλέγουν να τρέξουν έναν εξυπηρετητή Window NT ή UNIX έχουν τα πλεονεκτήματα που προσφέρει ένα σύστημα πολυπρογραμματισμού (multitasking). Στο σύνολο τους τα Window NT είναι τρωτά. Αυτό συμβαίνει γιατί το σύστημα αρχείων NT και το σύστημα λογαριασμών των χρηστών είναι αρκετά περίπλοκο και δύσκολο να ρυθμιστεί.

Μερικές από τις προφυλάξεις που πρέπει να λαμβάνονται όταν οι web εξυπηρετητές τρέχουν σε περιβάλλον UNIX ή NT είναι: περιορισμός των λογαριασμών εισόδου (login) που είναι διαθέσιμοι στο σύστημα, διαγραφή των μη ενεργών χρηστών, κλείσιμο των μη απαραίτητων ή μη χρησιμοποιούμενων υπηρεσιών του συστήματος και συχνός έλεγχος των αρχείων πρόσβασης (log files) του εξυπηρετητή και του συστήματος για ύποπτες ενέργειες.

Σε γενικές γραμμές η εμπειρία των ανθρώπων που διαχειρίζονται τον κεντρικό υπολογιστή του εξυπηρετητή και το λογισμικό είναι η πιο σημαντική παράμετρος στην ασφάλεια του συστήματος. Ένα σύστημα UNIX το οποίο διαχειρίζεται ένας έμπειρος χρήστης είναι πιο ασφαλές από ένα MS-WINDOWS σύστημα που διαχειρίζεται κάποιος αρχάριος.

3.4.4 Ταυτότητα Χρήστη (User Identifier, UID) του Εξυπηρετητή

Οι περισσότεροι web εξυπηρετητές είναι σχεδιασμένοι για να ξεκινούν από τον υπερχρήστη (root). Αυτό είναι αναγκαίο για να μπορεί ο εξυπηρετητής να χρησιμοποιεί τη θύρα (port) 80 για τις εισερχόμενες αιτήσεις εξυπηρέτησης, που είναι η τυποποιημένη θύρα HTTP για να μπορεί να γράφει στα αρχεία πρόσβασης

(log files). Μετά την έναρξη της λειτουργίας του, ο εξυπηρετητής περιμένει να δεχθεί εισερχόμενες αιτήσεις. Μόλις παραλάβει μια, δημιουργεί μια θυγατρική διεργασία, που θα αναλάβει την εξυπηρέτηση της αίτησης, ενώ η γονική διεργασία επιστρέφει στην παρακολούθηση της θύρας 80, περιμένοντας την επόμενη αίτηση.

Η θυγατρική διεργασία αλλάζει το UID της (το ενεργό ID της) στο όνομα του χρήστη και συνέχεια επεξεργάζεται την αίτηση. Όλες οι ενέργειες που εκτελούνται προς απάντηση της αίτησης, όπως η εκτέλεση CGI scripts ή η ανάλυση των περιεχομένων του εξυπηρετητή, πραγματοποιούνται κάτω από τη δικαιοδοσία του απλού χρήστη, που ορίζεται στο αρχείο ρύθμισης του εξυπηρετητή (configuration file). Αυτό σημαίνει ότι η θυγατρική διεργασία αποκτά τα δικαιώματα που έχει στον εξυπηρετητή ο εν λόγω χρήστης.

Το όνομα χρήστη κάτω από το οποίο τρέχουν οι θυγατρικές διεργασίες δεν πρέπει να είναι αυτό του root, γιατί έτσι δημιουργείται ένα μεγάλο κενό ασφάλειας. Για παράδειγμα, κάθε CGI script που εκτελείται από τη θυγατρική διεργασία με root UID έχει απεριόριστη πρόσβαση στο σύστημα αρχείων του εξυπηρετητή. Αντίθετα θα πρέπει να χρησιμοποιείται όνομα χρήστη που δεν έχει ιδιαίτερες δυνατότητες σε ότι αφορά τη διαχείριση του εξυπηρετητή.

3.4.5 Ρυθμίσεις του Web Εξυπηρετητή που Πρέπει να Αποφεύγονται

Σε πολλούς web εξυπηρετητές συναντάται μια ομάδα προαιρετικών χαρακτηριστικών που σκοπό έχουν να διευκολύνουν τη χρήση του. Η χρήση των χαρακτηριστικών αυτών, όταν γίνεται χωρίς προσοχή μπορεί να δημιουργήσει ρήγματα στην ασφάλεια του εξυπηρετητή. Μερικά από τα χαρακτηριστικά αυτά είναι η αυτόματη λίστα των directories, η φόρμα των περιεχομένων του εξυπηρετητή και οι κατάλογοι (directories) που συντηρούνται από το χρήστη. Στη συνέχεια περιγράφονται τα προβλήματα που μπορεί να δημιουργηθούν κατά τη χρήση των χαρακτηριστικών αυτών.

Αυτόματη λίστα των καταλόγων (Automatic Directory Listing)

Οι περισσότεροι web εξυπηρετητές παρουσιάζουν σε λίστα τα περιεχόμενα ενός καταλόγου. Όμως όσα πιο πολλά έχει τη δυνατότητα να μάθει ο εισβολέας για το σύστημα τόσο πιο πιθανό είναι να ανακαλύψει κάποιες τρύπες ασφάλειας. Η αυτόματη λίστα των διευθύνσεων που προσφέρουν κάποιοι εξυπηρετητές είναι

λειτουργική. Παράλληλα όμως αυξάνει την πιθανότητα ο εισβολέας να βρει τρόπο πρόσβασης σε σημαντικές πληροφορίες.

Τα περιεχόμενα του εξυπηρετητή (Server- side Includes)

Οι εντολές ενσωμάτωσης (Server-side Includes, SSI), είναι εντολές που ενσωματώνονται σε ένα έγγραφο HTML και υφίστανται επεξεργασία από τον εξυπηρετητή πριν το έγγραφο αποσταλεί στον πελάτη που το ζήτησε. Χρησιμοποιούνται για να συμπεριλάβουν ένα άλλο έγγραφο στο αρχικό έγγραφο ή για την εκτέλεση ενός προγράμματος και παρουσίαση του αποτελέσματος. Τελικά η φόρμα "exec" των περιεχομένων του εξυπηρετητή δημιουργεί ένα μεγάλο κενό στην ασφάλεια του. Η φόρμα πρέπει να αφαιρεθεί τελείως ή η χρήση της να περιοριστεί μόνο στους έμπιστους χρήστες. Στους περισσότερους εξυπηρετητές διαδικτύου είναι κανονικά απενεργοποιημένες, ενώ σε μερικούς επιτρέπεται η μερική ενεργοποίηση τους.

Η διαχείριση καταλόγων από τους χρήστες (User-maintained Directories)

Το να επιτρέπεται κάθε χρήστης του κεντρικού συστήματος να προσθέσει κείμενα σε ένα δικτυακό τόπο είναι κάτι δημοκρατικό. Με αυτό τον τρόπο δίνεται η δυνατότητα σε κάθε χρήστη να διατηρεί τον δικό του κατάλογο με τις ηλεκτρονικές σελίδες. Δυστυχώς όμως δεν μπορεί να ελεγχθεί ο χρήστης για τα αρχεία που δημοσιοποιεί και για τα CGI scripts που συντάσσει. Είναι επομένως δυνατό ο χρήστης να δημιουργήσει, άθελα του, προβλήματα ασφάλειας. Αν το χαρακτηριστικό αυτό δεν κρίνεται απαραίτητο, καλό είναι να μην υπάρχει.

3.4.6 Ασφαλή CGI Scripts

Τα περισσότερα κενά ασφάλειας ενός συστήματος δε δημιουργούνται σκόπιμα. Συνήθως οφείλονται σε άτομα που δεν έχουν την απαιτούμενη εμπειρία να γράψουν ασφαλή CGI scripts. Όσο περισσότεροι είναι οι χρήστες που αναλαμβάνουν να γράψουν scripts, τόσο μεγαλύτερη είναι η πιθανότητα ένα από αυτά τα scripts να περιέχει ένα σημαντικό λάθος. Τα scripts είναι προκλητικά εύκολο να γραφούν, αλλά όχι τόσο εύκολο να γραφούν καλά. Ένα μικρό λάθος στο script θα εκθέσει τον web εξυπηρετητή και τον κεντρικό υπολογιστή του σε επιθέσεις. Για αυτό το λόγο κανένα script δεν πρέπει να εγκαθίσταται στον εξυπηρετητή εάν προηγουμένως δεν το έχει ελέγξει κάποιος ειδικός.

Τα CGI scripts μπορούν να κάνουν ότι θέλουν. Είναι πρώτης τάξεως προγράμματα που εκτελούνται στον κεντρικό υπολογιστή του εξυπηρετητή διαδικτύου και έχουν τόση πρόσβαση στο σύστημα αρχείων, το δίκτυο και στις συσκευές υλικού όση οποιοδήποτε άλλο πρόγραμμα. Αυτό επιτρέπει στα scripts να ανοίγουν συνδέσεις βάσεων δεδομένων, να γράφουν τις παραγγελίες των πελατών στο δίσκο, να στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου, να αποτυπώνουν εικόνες από ψηφιακές κάμερες κλπ.

Όταν ένας απομακρυσμένος χρήστης ζητήσει ένα URL που δείχνει σε ένα CGI script, ο εξυπηρετητής εκτελεί το script περνώντας του διάφορα κομμάτια πληροφοριών για την παρούσα σύνοδο. Το CGI script επεξεργάζεται την πληροφορία και δίνει ως δεδομένο εξόδου ένα έγγραφο, που είναι συχνά μια HTML σελίδα. Αυτή η σελίδα επιστρέφεται τότε στον φυλλομετρητή του χρήστη που τη ζήτησε.

Λάθη των CGI scripts

Υπάρχουν τρεις κατηγορίες κινδύνων από λανθασμένα CGI scripts:

- Μπορεί να διαρρεύσουν πληροφορίες χωρίς πρόθεση, που θα βοηθήσουν τους εισβολείς να μπουν ή να αποκτήσουν πρόσβαση σε απόρρητα έγγραφα.
- Μπορεί να ξεγελαστούν στο να κάνουν μη εξουσιοδοτημένες μετατροπές σε αρχεία στο χώρο του ιστού ή στη μηχανή του κεντρικού υπολογιστή του εξυπηρετητή.
- Μπορεί να ξεγελαστούν στο να εκτελέσουν εντολές στη μηχανή του κεντρικού υπολογιστή του εξυπηρετητή.

Τα προσεκτικά σχεδιασμένα προνόμια χρηστών είναι η πρώτη γραμμή άμυνας απέναντι σε αυτά τα λάθη. Οτιδήποτε περιορισμοί ισχύουν στον web εξυπηρετητή, ισχύουν και για τα CGI scripts. Για παράδειγμα αν ο εξυπηρετητής εκτελείται σε ένα UNIX σύστημα, που έχει υλοποιήσει το σχήμα του αρχείου κρυμμένων κωδικών προσπέλασης, ο χρήστης του web εξυπηρετητή δε θα μπορεί να διαβάσει το αρχείο των κωδικών προσπέλασης. Ένα λανθασμένο CGI script δε μπορεί να ξεγελαστεί στο να διαρρεύσει κωδικούς προσπέλασης του συστήματος. Συνεπώς ο εξυπηρετητής δεν πρέπει να ποτέ να εκτελεστεί με περισσότερα προνόμια από ότι χρειάζεται.

Χρήσιμες Συμβουλές

Πολλές γλώσσες προγραμματισμού, συμπεριλαμβανομένων των C, ksh, sh, csh Perl παρέχουν τα μέσα για τη δημιουργία διεργασιών. Αυτές οι δυνατότητες πρέπει να αποφεύγονται κατά τη σύνταξη CGI scripts. Εάν είναι αναγκαίο να δημιουργηθεί μια διεργασία, πρέπει να αποφευχθεί να περαστούν στη διεργασία ακολουθίες χαρακτήρων που παρήχθησαν από το χρήστη. Εάν πάλι είναι αναγκαίο να περαστούν στη διεργασία δεδομένα του χρήστη, πρέπει να δοθεί προσοχή να μην περιέχονται χαρακτήρες όπως οι: $ | ; > *< &.

Ακολουθούν κάποιες βασικές συμβουλές, χρήσιμες σε θέματα ασφάλειας:

- Η πρόσβαση στον κατάλογο με τα CGI scripts πρέπει να είναι περιορισμένη. Δεν πρέπει να επιτρέπεται στους τοπικούς χρήστες να εγκαθιστούν ή να αφαιρούν script ή να τροποποιούν τα υπάρχοντα χωρίς την επίβλεψη του διαχειριστή. Επιπλέον, καλό είναι, να αφαιρείται το δικαίωμα ανάγνωσης του, ώστε οι χρήστες του διαδικτύου να μην έχουν τη δυνατότητα να ανιχνεύσουν τυχόν ατέλειες.
- Πρόσβαση στα ευαίσθητα CGI scripts πρέπει να δίνεται μόνο όταν είναι απαραίτητο και σε χρήστες που έχουν αυθεντικοποιηθεί στον εξυπηρετητή διαδικτύου.
- Συνίσταται η χρήση του προγράμματος Tripwire (ή οποιουδήποτε παρόμοιου) για επίβλεψη των αλλαγών που γίνονται στα scripts.
- Τα αρχεία ασφαλείας (backup files) που παράγουν αυτόματα κάποιοι διορθωτές κειμένου, πρέπει να σβήνονται. Ξεχασμένα τέτοια αρχεία μπορούν να εκτελεστούν από ένα εισβολέα με ανεπιθύμητα αποτελέσματα.

Διάγνωση Εισβολής

Για τα συστήματα UNIX υπάρχει το πρόγραμμα Tripwire που ελέγχει περιοδικά το σύστημα και ανιχνεύει εάν έχουν τροποποιηθεί αρχεία ή προγράμματα του συστήματος. Επίσης τα αρχεία λάθους (error log files) και τα αρχεία πρόσβασης (access log files) του εξυπηρετητή πρέπει να ελέγχονται σε τακτά χρονικά διαστήματα για ύποπτες ενέργειες. Η παρουσία εντολών, όπως οι “rm”, “login”, “/bin/sh” και “perl” στα αρχεία πρόσβασης, καθώς και η παρουσία πολύ μεγάλων γραμμών URL, πρέπει να θεωρούνται επικίνδυνες. Επίσης, πρέπει να γίνεται έλεγχος για τυχόν επανειλημμένες ανεπιτυχείς προσπάθειες πρόσβασης σε ένα προστατευμένο έγγραφο.

Χρήση του Μηχανήματος μόνο από τον Web Εξυπηρετητή

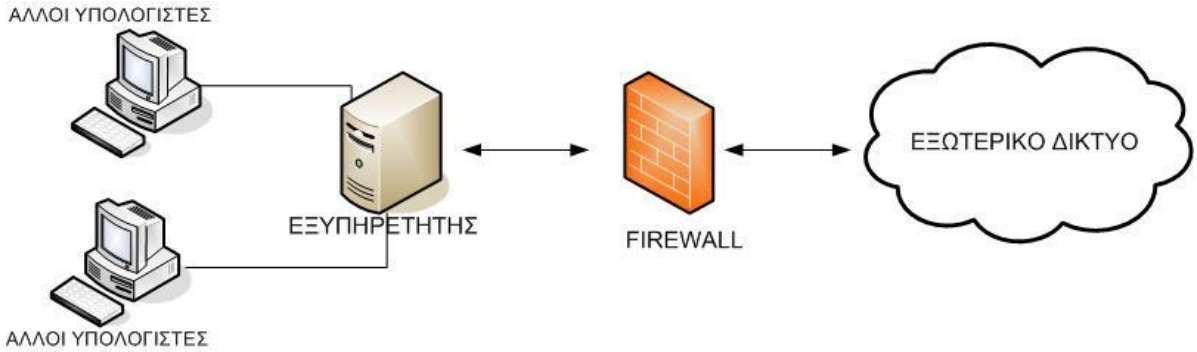
Όταν ένας υπολογιστής χρησιμοποιείται αποκλειστικά ως web εξυπηρετητής, η ασφάλεια του δικτύου αυξάνεται. Κάτι τέτοιο κάνει πιο δύσκολη την έναρξη επιτυχημένης επίθεσης κατά του μηχανήματος. Αλλά ακόμη και αν ο επιτιθέμενος εισβάλει στο μηχάνημα, δε θα μπορεί να κάνει επιπλέον ζημιά στο δίκτυο. Στην περίπτωση ενός υπολογιστή που λειτουργεί μόνο ως web εξυπηρετητής, συνίσταται η υιοθέτηση των παρακάτω κανόνων:

- Διαγραφή όλων των άχρηστων λογαριασμών.
- Διαγραφή όλων των προγραμμάτων που δε χρησιμοποιούνται από τον web εξυπηρετητή ή από το λογισμικό του μηχανήματος κατά την εκκίνηση του.
- Παροχή των απαιτούμενων υπηρεσιών και μόνο αυτών.
- Μη υποστήριξη υπηρεσιών εξυπηρετητή ηλεκτρονικού ταχυδρομείου (email server).
- Διαγραφή όλων των μεταφραστών γλωσσών (compilers).

3.4.7 Χρήση Συστημάτων Firewalls για την Ασφάλεια του Web Εξυπηρετητή

Πολλά δίκτυα για να αυξήσουν την ασφάλεια των ιστοσελίδων τους χρησιμοποιούν firewalls. Τα firewalls είναι ισχυρά εργαλεία τα οποία όμως δεν υποκαθιστούν σε καμιά περίπτωση άλλα μέτρα ασφαλείας και για το λόγο αυτό χρησιμοποιούνται ως συμπληρωματικά αυτών. Συνήθως τοποθετούνται ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο ενός οργανισμού και παρέχουν έναν απλό τρόπο για να ελέγχουν την ποσότητα και το είδος των δεδομένων που διακινούνται μεταξύ των δύο δικτύων.

Αν το ζητούμενο αποτέλεσμα είναι η δημιουργία ενός εσωτερικού δικτυακού τόπου στο οποίο θα έχουν πρόσβαση μόνο οι χρήστες του τοπικού δικτύου, τότε ο εξυπηρετητής τοποθετείται μέσα στο firewall όπως φαίνεται στο Σχήμα 1.

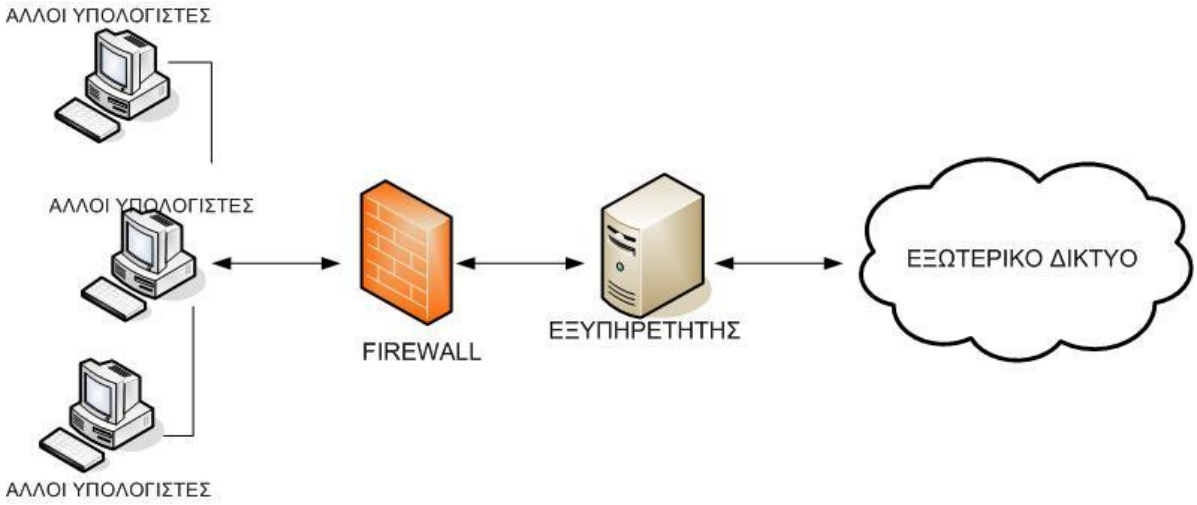


Σχήμα 1: Εξυπηρετητής τοποθετημένος μέσα από το firewall.

Αν πάλι το ζητούμενο αποτέλεσμα είναι να είναι ο εξυπηρετητής διαθέσιμος στον έξω κόσμο, τότε θα πρέπει να τοποθετηθεί κάπου έξω από το firewall. Για την ασφάλεια και του τοπικού δικτύου θα πρέπει να τοποθετηθεί έξω και από την περιοχή του τοπικού δικτύου όπως φαίνεται στο Σχήμα 2.

Η τεχνική αυτή ονομάζεται "διαμόρφωση εξιλαστήριου θύματος" (sacrificial lamb configuration) διότι ο εξυπηρετητής πάντα κινδυνεύει να καταρρεύσει από επιθέσεις, αλλά με αυτόν τον τρόπο δε θα κινδυνεύει το εσωτερικό δίκτυο ακόμα και αν ο εξυπηρετητής καταρρεύσει. Βέβαια υπάρχουν αρχιτεκτονικές όπου χρησιμοποιούνται ζεύγη εξυπηρετητών (εσωτερικοί και εξωτερικοί) ώστε και στον έξω κόσμο να παρέχουν πληροφορίες και να επιτρέπουν μόνο στους εσωτερικούς χρήστες την πρόσβαση σε ιδιωτικά έγγραφα.

Εάν ο εξυπηρετητής βρίσκεται πίσω από το firewall, υπάρχει τρόπος ώστε να εξασφαλιστεί πρόσβαση στον έξω κόσμο. Με τον τρόπο αυτό, όμως, δημιουργούνται οπές στο φράγμα ασφάλειας. Είναι πολύ καλύτερα να χρησιμοποιηθεί ο εξυπηρετητής ως εξιλαστήριο θύμα. Υπάρχουν βέβαια και αρκετές αρχιτεκτονικές firewalls που δεν επιτρέπουν την τοποθέτηση εξυπηρετητών έξω από αυτούς. Σε αυτή την περίπτωση θα πρέπει αναγκαστικά ο εξυπηρετητής να βρίσκεται πίσω από το φράγμα ασφάλειας με δεδομένο πάντα το μειονέκτημα της πιθανής δημιουργίας οπών ασφάλειας.

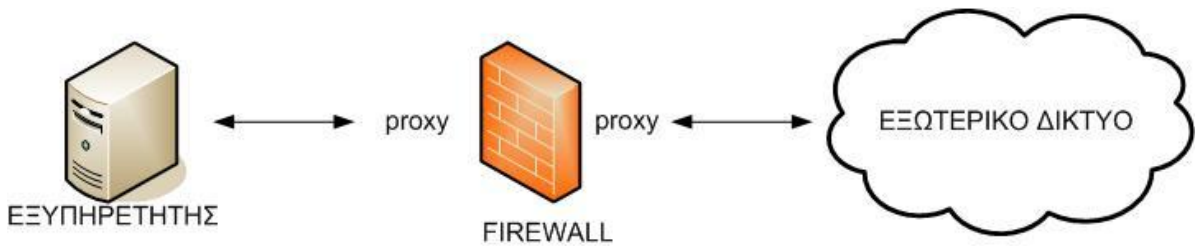


Σχήμα 2: Εξυπηρετητής τοποθετημένος έξω από το firewall

Υπάρχουν δύο τρόποι για να επιτευχθεί η πρόσβαση του εξυπηρετητή, που βρίσκεται πίσω από το φράγμα ασφάλειας, με τον έξω κόσμο:

- Στην περίπτωση που χρησιμοποιείται ο τύπος firewall υπολογιστή διαλογής (screened host), μπορεί να επιτραπεί η είσοδος για αιτήσεις (requests) από τη θύρα 80 (http service) η οποία επικοινωνεί με τον web εξυπηρετητή. Έτσι δημιουργείται μια μικρή οπή ασφάλειας απ' όπου ο έξω κόσμος επικοινωνεί με τον εξυπηρετητή.
- Στην περίπτωση που χρησιμοποιείται ο τύπος διπλοσυνδεδεμένο firewall (dual homed gateway), χρειάζεται η εγκατάσταση proxy στο firewall. Ο proxy μπορεί να δει και από τις δύο πλευρές του φράγματος ασφάλειας, όπως φαίνεται στο Σχήμα 3. Έτσι, οι αιτήσεις για πληροφορίες σταματούν πάνω στον proxy ο οποίος τις προωθεί στον εξυπηρετητή και οι απαντήσεις από τον εξυπηρετητή σταματούν στον proxy ο οποίος τις προωθεί στον αιτούντα.

Τα firewalls παρουσιάζονται αναλυτικά στην παράγραφο 3.3.1



Σχήμα 3: Πρόσβαση του εξυπηρετητή με τον έξω κόσμο.

3.4.8 Προστασία Εμπιστευτικών Αρχείων

Πολλοί οργανισμοί ηλεκτρονικού εμπορίου επιθυμούν να περιορίσουν τις πληροφορίες που θα διανείμουν οι εξυπηρετητές τους, αφού κάποιοι web εξυπηρετητές χρησιμοποιούνται για τη διανομή δεδομένων εμπιστευτικής φύσεως. Τέτοια δεδομένα είναι πληροφορίες για τις ηλεκτρονικές συναλλαγές, όπως τα προσωπικά στοιχεία του πελάτη, τα στοιχεία της συναλλαγής ή πληροφορίες για τους εργαζόμενους του οργανισμού. Για την ικανοποίηση αυτής της απαίτησης, πολλοί web εξυπηρετητές παρέχουν τρόπους προστασίας των εμπιστευτικών εγγράφων. Υπάρχουν τρεις τρόποι περιορισμού της πρόσβασης:

- **Περιορισμός πρόσβασης σύμφωνα με τις IP διευθύνσεις, υποδίκτυα** (subnets), ή τα ονόματα πεδίων (domain names): Έγγραφα και κατάλογοι προστατεύονται με τέτοιο τρόπο ώστε μόνο τα προγράμματα πλοήγησης που συνδέονται από συγκεκριμένες IP διευθύνσεις, IP υποδίκτυα, ή πεδία (domains) να έχουν πρόσβαση σε αυτά.
- **Περιορισμός πρόσβασης σύμφωνα με ονόματα χρηστών και κωδικών:** Έγγραφα και κατάλογοι προστατεύονται με τέτοιο τρόπο ώστε ο απομακρυσμένος χρήστης για να αποκτήσει πρόσβαση σε αυτά να πρέπει να χρησιμοποιήσει κατάλληλο όνομα και κωδικό.
- **Κρυπτογράφηση με χρήση ασύμμετρης κρυπτογραφίας**: Η αίτηση για το έγγραφο και το ίδιο το έγγραφο μεταδίδονται κρυπτογραφημένα, ώστε μόνο ο πραγματικός παραλήπτης να μπορεί να τα διαβάσει. Χρησιμοποιούνται δημόσια κλειδιά και πιστοποιητικά. Αυτό το είδος περιορισμού παρέχεται μόνο από τους εξυπηρετητές που είναι εξοπλισμένοι με το απαραίτητο λογισμικό.

Κάθε μια από τις παραπάνω τεχνικές έχει πλεονεκτήματα και μειονεκτήματα. Ο περιορισμός μέσω των IP διευθύνσεων έχει αποτέλεσμα σε περιπτώσεις απλών χρηστών, αλλά όχι απέναντι σε αποφασισμένους εισβολείς. Με κατάλληλο εξοπλισμό και λογισμικό, ένας εισβολέας μπορεί να αλλάξει την IP διεύθυνση του (IP spoofing) και να εμφανίζεται ως συνδεδεμένος από κάπου αλλού. Επίσης, ο απομακρυσμένος υπολογιστής μπορεί να έχει καταληφθεί και να χρησιμοποιείται ως βιτρίνα. Ο περιορισμός μέσω των IP διευθύνσεων μπορεί να γίνει ασφαλέστερος αν ο εξυπηρετητής προστατεύεται από ένα firewall που είναι ικανό

να εντοπίζει και να απορρίπτει τις προσπάθειες για αλλαγή των IP διευθύνσεων. Οι περιορισμοί μέσω υπολογιστή φιλοξενίας (host) ή ονόματος πεδίου (domain) εμφανίζουν τα ίδια προβλήματα με τους περιορισμούς μέσω IP διευθύνσεων. Για μέγιστη ασφάλεια, η τεχνική αυτή πρέπει να συνδυάζεται με τον έλεγχο της ταυτότητας του χρήστη.

Ο περιορισμός μέσω μυστικών κωδικών έχει και αυτός κάποια προβλήματα. Οι κωδικοί που επιλέγουν οι χρήστες δεν είναι πάντοτε ασφαλείς. Πολύ συχνά χρησιμοποιούν φανερούς κωδικούς όπως ονόματα, ημερομηνίες γέννησης, τηλέφωνα. Τέτοιοι κωδικοί είναι προβλέψιμοι και οι web εξυπηρετητές δεν απαγορεύουν τις επανειλημμένες αποτυχημένες προσπάθειες εισαγωγής του σωστού κωδικού. Ένας εισβολέας μπορεί να εφαρμόσει ένα πρόγραμμα υπόθεσης κωδικών (password guessing program) και να υποθέσει το σωστό κωδικό. Ένα άλλο πρόβλημα με τους κωδικούς είναι ότι είναι ευάλωτοι σε υποκλοπή καθώς μεταδίδονται στο δίκτυο. Επειδή δεν είναι ισχυρά κρυπτογραφημένοι, ένας εισβολέας μπορεί με κατάλληλο υλικό και λογισμικό να τους καταγράψει και να τους χρησιμοποιήσει μελλοντικά. Επιπλέον το πρόγραμμα πλοήγησης στέλνει τον κωδικό στον εξυπηρετητή κάθε φορά που ζητά κάποιο εμπιστευτικό έγγραφο, διευκολύνοντας έτσι τον εισβολέα να υποκλέψει τον κωδικό αυτό.

Ο συνδυασμός όλων των παραπάνω τεχνικών αποτελεί την καλύτερη δυνατή λύση. Με τον περιορισμό των IP διευθύνσεων και των ονομάτων πεδίων περιορίζεται ο αριθμός των υπολογιστών που μπορεί να έχουν πρόσβαση στον εξυπηρετητή, ενώ με τον περιορισμό μέσω κωδικών πρόσβασης περιορίζονται οι χρήστες που έχουν το δικαίωμα να αποκτήσουν πρόσβαση στα εμπιστευτικά αρχεία. Τέλος, με την κρυπτογράφηση, διασφαλίζεται η εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται.

3.4.9 Web Εξυπηρετητές και Εμπόριο

Στο ηλεκτρονικό εμπόριο κυριαρχούν τρεις web εξυπηρετητές, των οποίων τα κύρια χαρακτηριστικά παρουσιάζονται παρακάτω:

Apache server

- Η απλή του έκδοση είναι δωρεάν, αλλά όχι αυτή με ασφάλεια SSL.
- Εκτελείται καλύτερα σε περιβάλλον UNIX.
- Απαιτείται εμπειρία στοUNIX για να εγκατασταθεί-διαχειριστεί.

- Υποστηρίζεται από εργαλεία τρίτων κατασκευαστών.

Microsoft Internet Information Server (IIS)

- Περιλαμβάνεται στα Windows NT/2000.
- Εύκολη διαχείριση.
- Προσφέρει περιβάλλον ανάπτυξης εφαρμογών.
- Πολύ καλές επιδόσεις.

Netscape Enterprise Server

- Ευκολία εγκατάστασης και διαχείρισης.
- Δυνατότητες εξυπηρέτησης μέχρι 100 εκατομμύρια αιτήσεων την ημέρα.
- Υποστηρίζεται από UNIX και Windows.

3.5 Ασφάλεια Web Εφαρμογών

Ο όρος ασφάλεια περιλαμβάνει την προστασία των αγαθών των επιχειρήσεων. Τα αγαθά μπορεί να είναι απτά στοιχεία, όπως μια ιστοσελίδα ή η βάση δεδομένων των πελατών της επιχείρησης, ή μπορεί να είναι λιγότερο απτά, όπως η φήμη της εταιρείας.

3.5.1 Απαιτήσεις Ασφάλειας Web Εφαρμογών

Οι βασικές απαιτήσεις για την ασφάλεια των web εφαρμογών είναι οι εξής:

Αυθεντικοποίηση (Authentication): Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας, την οποία ισχυρίζεται ότι έχει ένας πελάτης της εφαρμογής. Ο πελάτης μπορεί να είναι κάποιος τελικός χρήστης, κάποια υπηρεσία, διαδικασία ή υπολογιστής. Στο ηλεκτρονικό εμπόριο η πιστοποίηση της ταυτότητας των μερών που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να είναι σίγουρο για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται συνήθως μέσω ψηφιακών υπογραφών.

Εμπιστευτικότητα (Confidentiality): Είναι έννοια στενά συνδεδεμένη με την ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Αφορά τη μη αποκάλυψη των ευαίσθητων πληροφοριών σε άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση. Για το ηλεκτρονικό εμπόριο η εμπιστευτικότητα αποτελεί υψίστης

σημασίας συστατικό στην προστασία των οικονομικών δεδομένων του οργανισμού, καθώς και στην προστασία των προσωπικών δεδομένων των πελατών. Τεχνικές κρυπτογράφησης χρησιμοποιούνται για να εξασφαλίσουν την εμπιστευτικότητα.

Εξουσιοδότηση (Authorization): Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτούμενα μέλη μπορούν να πραγματοποιήσουν, όπως για παράδειγμα εκτέλεση συναλλαγών, μεταφορά χρημάτων από ένα λογαριασμό σε άλλο ή αύξηση του πιστωτικού ορίου κάποιου πελάτη.

Ακεραιότητα (Integrity): Η ακεραιότητα είναι η εγγύηση ότι τα δεδομένα προστατεύονται από τυχαία ή σκόπιμη (κακόβουλη) τροποποίηση. Διασφαλίζει την εγκυρότητα, την ορθότητα και την πληρότητα των δεδομένων κατά τη φάση της εισαγωγής τους, της αποθήκευσης και της μεταφοράς τους. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς στάλθηκαν.

Μη αποποίηση ευθύνης (Non- repudiation): Μη αποποίηση ευθύνης σημαίνει ότι ένας χρήστης δεν μπορεί να αρνηθεί την εκτέλεση μιας λειτουργίας, και κανένα από τα συναλλασσόμενα μέρη δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, σε περίπτωση που χρειαστεί, να μπορούν να αποδείξουν την προέλευση, μεταφορά και παραλαβή των δεδομένων.

Διαθεσιμότητα (Availability): Αφορά την άμεση πρόσβαση στις υπηρεσίες του συστήματος για τους νόμιμους χρήστες του. Πολλοί επιτιθέμενοι, χρησιμοποιώντας επιθέσεις τύπου άρνησης υπηρεσίας (denial of service), έχουν σαν στόχο να συντρίψουν την εφαρμογή, ώστε οι υπόλοιποι χρήστες να μην μπορούν να έχουν πρόσβαση στην συγκεκριμένη εφαρμογή.

3.5.2 Εχθροί, Απειλές και Επιθέσεις Web Εφαρμογών

Απειλή είναι οποιοδήποτε πιθανό περιστατικό, κακόβουλο ή όχι, που μπορεί να βλάψει κάποιο αγαθό. Με άλλα λόγια, απειλή είναι οτιδήποτε κακό μπορεί να συμβεί στα αγαθά.

Ευπάθεια είναι μια αδυναμία που κάνει δυνατή την απειλή. Αυτό μπορεί να γίνει λόγω αδυναμιών στη σχεδίαση, λάθη στη διαμόρφωση ή λόγω ακατάλληλων και επισφαλών τεχνικών κωδικοποίησης.

Επίθεση είναι μια ενέργεια που εκμεταλλεύεται τις ευπάθειες και υλοποιεί μια απειλή. Συνοψίζοντας, απειλή είναι ένα πιθανό γεγονός που μπορεί να έχει επιπτώσεις σε ένα αγαθό, ενώ μια επιτυχής επίθεση εκμεταλλεύεται τις ευπάθειες του συστήματος.

Προκειμένου να σχεδιαστεί και να αναπτυχθεί μια ασφαλής web εφαρμογή, απαιτείται η γνώση τόσο των απειλών όσο και των εχθρών του συστήματος. Είναι σημαντικό να αναλυθεί η αρχιτεκτονική της εφαρμογής και να καθοριστούν οι πιθανές ευπαθείς περιοχές που μπορούν να επιτρέψουν σε ένα χρήστη ή σε έναν επιτιθέμενο με κακόβουλες προθέσεις, να παραβιάσει την ασφάλεια του συστήματος.

- **Εχθροί**

Είναι σημαντικό στην προσπάθεια παροχής ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου, να αναγνωρίζονται αρχικά «εχθροί». Οποιοσδήποτε εμπλέκεται με ζητήματα ασφάλειας ηλεκτρονικού εμπορίου θα πρέπει να τον απασχολούν οι εχθροί του συστήματος, οι προθέσεις τους καθώς και τα μέσα που διαθέτουν. Οι «εχθροί» κατηγοριοποιούνται ως εξής:

Crackers: Οι crackers αρέσκονται στο δημιουργούν προβλήματα για πλάκα, για βανδαλισμούς ή για επίδειξη. Χρησιμοποιούν συνήθως υπάρχοντα προϊόντα επίθεσης από το διαδίκτυο. Οι προθέσεις τους συχνά δεν είναι εχθρικές, αλλά ωστόσο προκαλούν ουσιαστικές ζημιές, είτε προκαλώντας βανδαλισμούς, είτε διακόπτοντας λειτουργίες.

Ερευνητές (Researchers): Ένας ερευνητής μπορεί να εργαστεί πολύ σκληρά στην προσπάθεια του να ανακαλύψει αδυναμίες σε πρωτόκολλα ασφάλειας και στη συνέχεια εκδίδει τα αποτελέσματα του στο διαδίκτυο.

Εγκληματίες (Criminals): Το διαδίκτυο έχει γίνει πολύ ελκυστικό μέρος για εγκλήματα, λόγω της μεγάλης διάδοσης και ανωνυμίας που παρέχει. Το δικτυακά εγκλήματα εκτείνονται από απλές απάτες με κλοπή αριθμών πιστωτικών καρτών έως προσεκτικές επιθέσεις για πρόσβαση σε χρήμα ή πληροφορίες. Πρόθεση τους είναι το οικονομικό όφελος.

Ανταγωνιστές (Competitors): Ένας ανταγωνιστής δεν κλέβει χρήματα, ούτε καταστρέφει αρχεία, αλλά έχει ως στόχο την πρόσβαση στα διάφορα επιχειρηματικά σχέδια, που είναι πολύτιμα για αυτόν.

Εσωτερικοί εχθροί: Δυσαρεστημένοι ή άπληστοι υπάλληλοι μπορούν να αποτελέσουν την πιο σοβαρή απειλή για την ασφάλεια των συστημάτων του οργανισμού. Οι «εσωτερικοί εχθροί» εξ ορισμού έχουν πρόσβαση σε ευαίσθητα συστήματα και πληροφορίες.

- **Απειλές**

Οι θεμελιώδεις απειλές που αντιμετωπίζουν οι web εφαρμογές είναι:

- Διαρροή πληροφοριών (information leakage).
- Παραβίαση της ακεραιότητας των πληροφοριών (integrity violation).
- Διακοπή υπηρεσιών.
- Άρνηση εξυπηρέτησης (denial of services).
- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.
- Κλοπή δεδομένων.
- Παράνομη χρήση διάφορων υπολογιστικών πόρων.
- Καταστροφή πληροφοριών και δικτυακών πόρων.

- **Επιθέσεις**

Η πραγματοποίηση οποιασδήποτε από τις παραπάνω θεμελιώδεις απειλές, μπορεί να γίνει με μια από τις παρακάτω τεχνικές επίθεσης:

Denial of service attacks: Μια από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι με στόχο τη διακοπή παροχής υπηρεσιών από ένα δικτυακό κόμβο ή πληροφοριακό σύστημα είναι οι επιθέσεις τύπου Denial of service. Τα προγράμματα που συνήθως χρησιμοποιούν οι επιτιθέμενοι ακολουθούν την τακτική μαζικής αποστολής μηνυμάτων-αιτημάτων στο στόχο ώστε να προκαλέσουν την αποτυχία ανταπόκρισης του και την κατάρρευση του συστήματος.

Επιθέσεις μεταμφίεσης (Spoofing): Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» σε κάποιο νόμιμο χρήστη, ώστε να αποκτήσει πρόσβαση σε μια εφαρμογή. Δηλαδή ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι

αποτέλεσμα των εξής: α) οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, β) οι κωδικοί πρόσβασης είτε διακινούνται μέσω του δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση, και γ) οι χρήστες χρησιμοποιούν εύκολους κωδικούς.

E-mail Spoofing: Το e-mail spoofing αποτελεί πρακτική παραποίησης ή απόκρυψης της πραγματικής πηγής από την οποία προήρθε το μήνυμα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται συνήθως για να παραπλανήσει το χρήστη ώστε να συλλεχθούν από αυτόν χρήσιμα δεδομένα. Ενδεικτικά αποστέλλονται μηνύματα με υποτιθέμενο αποστολέα τον διαχειριστή του συστήματος, ζητώντας από το χρήστη να επιβεβαιώσει το password που χρησιμοποιεί.

Επιθέσεις παρακολούθησης (Sniffing): Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά συστημάτων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «προγράμματα sniffing». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Οι συσκευές με δυνατότητες sniffing μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών IDS (Intrusion Detection System). Συνεπώς τέτοιου είδους συσκευές είναι χρήσιμες και απαραίτητες. Ωστόσο, είναι προφανές ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις υπηρεσίες που προσφέρουν τα προγράμματα sniffing για την υλοποίηση των παράνομων δραστηριοτήτων τους. Υπάρχουν ειδικά προγράμματα sniffing, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση: α) password, β) στοιχείων οικονομικών συναλλαγών (π.χ. κωδικοί πιστωτικών καρτών), γ) εμπιστευτικών δεδομένων (π.χ. προσωπικά στοιχεία χρηστών, e-mail).

Ιοί (viruses) - σκουλήκια (worms): Οι ιοί είναι προγράμματα ή εντολές που προσαρτώνται σε προγράμματα ή δεδομένα και εκτελούνται παράλληλα με αυτά. Μπορούν να προκαλέσουν την αλλοίωση ή καταστροφή δεδομένων. Τα σκουλήκια αντίστοιχα, είναι προγράμματα που κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Και οι δύο κατηγορίες προγραμμάτων έχουν ως στόχο να πλήξουν το σύστημα στο οποίο εκτελούνται, προκαλώντας ζημιές όπως διαγραφή δεδομένων.

Buffer overflow attacks (υπερχείλιση καταχωρητή): Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο να πλήξουν τις εφαρμογές που αποθηκεύουν δεδομένα σε προσωρινό χώρο μνήμης (buffer) μέχρι να έρθει η ώρα τους για επεξεργασία. Οι επιτιθέμενοι βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της εφαρμογής με τις δικές τους εντολές. Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών, οι επιτιθέμενοι αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.

Cookie Poisoning: Τα Cookies είναι αρχεία υπολογιστών που αποθηκεύονται στον σκληρό δίσκο του υπολογιστή του πελάτη ή στην μνήμη cache, κατά την πρόσβαση του σε μια εφαρμογή διαδικτύου μέσω ενός browser. Αυτά τα αρχεία περιέχουν πληροφορίες όπως όνομα χρήστη, κωδικός πρόσβασης και στοιχεία συνόδου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες με σκοπό τη χρήση του υπολογιστή του πελάτη για κακόβουλες πράξεις. Τα Cookies χωρίζονται σε δύο κατηγορίες: αυτά που μένουν στον υπολογιστή του χρήστη μόνο κατά τη διάρκεια της επίσκεψης του χρήστη στην εφαρμογή διαδικτύου, και αυτά που έχουν ημερομηνία λήξης και παραμένουν στον σκληρό δίσκο του πελάτη μέχρι την ημερομηνία λήξης τους οπότε και διαγράφονται.

3.5.3 Μέσα Προστασίας Web Εφαρμογών

Ασφάλεια Δικτύου, Host και Εφαρμογής

Ο σχεδιασμός και η ανάπτυξη ασφαλών web εφαρμογών προϋποθέτει ότι πρέπει να εφαρμοστεί ασφάλεια και στα τρία στρώματα: Δικτύου (Network), Host και Εφαρμογής (Application).

Ασφάλεια Δικτύου (Network)

Η ασφάλεια μιας web εφαρμογής στηρίζεται πάνω στην ασφαλή υποδομή του δικτύου. Η υποδομή του δικτύου αποτελείται από δρομολογητές (rooters), firewalls και διακόπτες (switches). Ο ρόλος της ασφάλειας δικτύου δεν είναι μόνο για την προστασία του από επιθέσεις βασισμένες στο πρωτόκολλο TCP/IP, αλλά και για την εφαρμογή αντίμετρων όπως ασφαλείς διεπαφές και ισχυροί κωδικοί πρόσβασης. Το ασφαλές δίκτυο είναι επίσης υπεύθυνο για τη διασφάλιση της ακεραιότητας των δεδομένων που διακινούνται μέσα από αυτό.

Τα firewalls μπλοκάρουν τα πρωτόκολλα και τις θύρες που δεν χρησιμοποιεί η εφαρμογή. Επιπλέον εξετάζουν τις επικοινωνίες και παρέχουν υψηλή ασφάλεια στο δίκτυο. Συγκεκριμένα με την εφαρμογή φιλτραρίσματος εμποδίζουν τις κακόβουλες επικοινωνίες. Τα firewalls αποτελούν αναπόσπαστο τμήμα της ασφάλειας, αλλά δεν αποτελούν πλήρη λύση από μόνα τους. Τα firewalls περιγράφονται αναλυτικά στην παράγραφο 3.3.1.

Ασφάλεια Host

Η ασφάλεια web εφαρμογών προϋποθέτει πρώτα από όλα την ασφάλεια του εξυπηρετητή (server), είτε αυτός είναι εξυπηρετητής διαδικτύου (web server), εξυπηρετητής εφαρμογής (application server) ή εξυπηρετητής βάσεων δεδομένων (database server).

Ακολούθως παρατίθενται τα μέτρα προστασίας που πρέπει να λαμβάνονται για την προστασία του εξυπηρετητή, και κατ' επέκταση των web εφαρμογών:

- Patches and Updates: Πολλοί κίνδυνοι ασφάλειας υπάρχουν λόγω του ότι οι ευπάθειες είναι ευρέως γνωστές και διαδεδομένες. Όταν ανακαλύπτονται νέες ευπάθειες, συχνά ο εκμεταλλευόμενος κώδικας δημοσιεύεται στους πίνακες δελτίων του διαδικτύου μέσα σε λίγες ώρες από την πρώτη επιτυχημένη επίθεση. Η συχνή επιδιόρθωση (patching) και ενημέρωση (updating) του λογισμικού του εξυπηρετητή είναι το πρώτο βήμα για την εξασφάλιση της ασφάλειας στον εξυπηρετητή. Η χρήση των patches και updates στον εξυπηρετητή μειώνει τις ευκαιρίες για επίθεση τόσο των επιτιθέμενων όσο και του κακόβουλου κώδικα (malicious code).
- Υπηρεσίες: Η απενεργοποίηση των περιττών και αχρησιμοποίητων υπηρεσιών μειώνει εύκολα και γρήγορα τη διαθέσιμη περιοχή για επιθέσεις (attach surface area).
- Πρωτόκολλα: Η απενεργοποίηση των περιττών και αχρησιμοποίητων πρωτοκόλλων μειώνει επίσης τη διαθέσιμη περιοχή για επιθέσεις και τους ανοικτούς «δρόμους» που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να εισβάλουν στο σύστημα.
- Accounts (Λογαριασμοί): Ο αριθμός των λογαριασμών που έχουν πρόσβαση στον εξυπηρετητή πρέπει να περιοριστεί στον ελάχιστο δυνατό. Επιπλέον θα πρέπει να επιβάλλονται κατάλληλες πολιτικές ασφάλειας των

λογαριασμών όπως είναι η εξουσιοδότηση με ισχυρούς κωδικούς πρόσβασης.

- Ports (Θύρες): Οι υπηρεσίες που τρέχουν σε έναν εξυπηρετητή ακούνε συγκεκριμένες θύρες προκειμένου να εξυπηρετήσουν τις εισερχόμενες αιτήσεις. Οι ανοικτές θύρες σε έναν εξυπηρετητή πρέπει να είναι γνωστές και να ελέγχονται συχνά ώστε καμιά επισφαλής υπηρεσία να μην ακούει.
- Auditing and Logging (Έλεγχος και Καταγραφή): Ο έλεγχος είναι ζωτικής σημασίας στον προσδιορισμό εισβολέων ή επιθέσεων που βρίσκονται σε εξέλιξη. Η καταγραφή αποδεικνύεται ιδιαίτερα χρήσιμη, καθώς αποθηκεύονται πληροφορίες για τον τρόπο που εκτελέστηκε μια επίθεση οι οποίες μπορούν να χρησιμοποιηθούν για ενίσχυση των μέτρων προστασίας ενάντια σε παρόμοιου είδους επιθέσεις.

Ασφάλεια Εφαρμογής

Προκειμένου να εξασφαλιστεί η ασφάλεια των web εφαρμογών ακολουθούνται κάποιες βασικές διαδικασίες οι οποίες είναι οι εξής:

- Επικύρωση δεδομένων εισόδου (Input Validation): Η επικύρωση δεδομένων εισόδου ασχολείται με το πως τα φίλτρα της εφαρμογής δέχονται κάποια δεδομένα εισόδου ως έγκυρα και ασφαλή και κάποια άλλα τα απορρίπτουν ως μη ασφαλή.
- Αυθεντικοποίηση: Αυθεντικοποίηση είναι η διαδικασία κατά την οποία κάποια οντότητα αποδεικνύει την ταυτότητα κάποιας άλλης οντότητας, συνήθως με τη χρήση πιστοποιητικών.
- Εξουσιοδότηση: Η εξουσιοδότηση αναφέρεται στον τρόπο με τον οποίο η εφαρμογή παρέχει έλεγχο πρόσβασης στις διαδικασίες.
- Διαχείριση Διαμόρφωσης: Η διαχείριση διαμόρφωσης ασχολείται με το πως η εφαρμογή χειρίζεται κάποια λειτουργικά ζητήματα όπως είναι ποιες βάσεις δεδομένων ενώνονται με την εφαρμογή, ή με ποιο τρόπο η εφαρμογή διοικείται.
- Ευαίσθητα Δεδομένα: Τα ευαίσθητα δεδομένα αναφέρονται στο πως η εφαρμογή χειρίζεται τα δεδομένα που πρέπει να προστατευτούν.
- Διαχείριση Συνόδου: Μια σύνοδος αναφέρεται σε μια σειρά σχετικών αλληλεπιδράσεων μεταξύ του χρήστη και της web εφαρμογής. Η

διαχείριση συνόδου ασχολείται με το πως η εφαρμογή χειρίζεται και προστατεύει αυτές τις αλληλεπιδράσεις.

- Κρυπτογράφηση: Η κρυπτογράφηση αναφέρεται στο πως η εφαρμογή παρέχει εμπιστευτικότητα και ακεραιότητα.
- Διαχείριση εξαιρέσεων: Η διαχείριση εξαιρέσεων ασχολείται με το τι κάνει η εφαρμογή σε περίπτωση που αποτύχει μια κλήση, δηλαδή αν επιστρέφει φιλικά μηνύματα προς τον χρήστη κλπ.
- Έλεγχος και Καταγραφή: Ο έλεγχος και η καταγραφή αναφέρονται στο πως η εφαρμογή καταγράφει τα σχετικά με την ασφάλεια γεγονότα.

3.5.4 Αρχές Ασφάλειας Web Εφαρμογών

Οι βασικές αρχές ασφάλειας πρέπει να εφαρμόζονται σε κάθε είδους εφαρμογές, ανεξάρτητα από την τεχνολογία της κάθε εφαρμογής. Οποιοσδήποτε ασχολείται με την ασφάλεια των web εφαρμογών πρέπει να τηρεί τις παρακάτω βασικές αρχές ασφάλειας:

- Ελάχιστα δυνατά προνόμια: Θα πρέπει να παραχωρούνται στους χρήστες ελάχιστα προνόμια και δικαιώματα πρόσβασης, ούτως ώστε οι επιτιθέμενοι να έχουν περιορισμένες ικανότητες σε περίπτωση που καταφέρουν να παραβιάσουν την ασφάλεια της εφαρμογής.
- Έλεγχος εγκυρότητας εισαγόμενων δεδομένων: Τα δεδομένα τα οποία εισάγονται στην εφαρμογή από τους χρήστες αποτελούν δίοδο εχθρικού λογισμικού προς την εφαρμογή. Τα δεδομένα αυτά αποτελούν το αρχικό όπλο του επιτιθέμενου στην προσπάθεια του να εισβάλει στην εφαρμογή. Τα εισερχόμενα προς την εφαρμογή δεδομένα θα πρέπει να ελέγχονται. Η πιο ασφαλής τακτική ελέγχου είναι να θεωρούνται όλα τα δεδομένα εισαγωγής κακόβουλα μέχρι να αποδειχθεί το αντίθετο και να γίνεται έλεγχος επικύρωσης όλων των δεδομένων, ώστε η εφαρμογή να αποδέχεται μόνο ασφαλή δεδομένα και να απορρίπτει τα υπόλοιπα.
- Έλεγχος στην πύλη: Όλοι οι επισκέπτες θα πρέπει να αυθεντικοποιούνται κατά την είσοδο τους στο σύστημα.
- Αποτυχία με ασφάλεια: Σε περίπτωση που αποτύχει η εφαρμογή τα ευαίσθητα δεδομένα δεν θα πρέπει να παραμένουν προσιτά σε τρίτους. Θα

πρέπει να επιστρέφονται φιλικά μηνύματα σφάλματος στους χρήστες τα οποία να μην εκθέτουν τις εσωτερικές λεπτομέρειες του συστήματος και γενικά να μην περιλαμβάνουν λεπτομέρειες που θα μπορούσαν να βοηθήσουν τους επιτιθέμενους να εκμεταλλευτούν τις ευπάθειες τις εφαρμογής.

- Δημιουργία ασφαλών προεπιλογών: Οι λογαριασμοί προεπιλογής (default account) θα πρέπει εξ ορισμού να είναι εκτός λειτουργίας και σε περίπτωση ανάγκης να επιτρέπεται ρητά η χρήση τους. Όταν εμφανίζεται ένα λάθος θα πρέπει τα ευαίσθητα δεδομένα να μην διαρρέουν πίσω στον χρήστη ο οποίος ενδεχομένως θα μπορεί να τα χρησιμοποιήσει ενάντια στο σύστημα.
- Μείωση περιοχής επιθέσεων: Θα πρέπει να μειώνεται η διαθέσιμη περιοχή για επιθέσεις. Αυτό μπορεί να γίνει θέτοντας εκτός λειτουργίας ή αφαιρώντας αχρησιμοποίητες συσκευές και πρωτόκολλα.

3.5.5 Πλάνο Ασφάλειας Web Εφαρμογών

Οι υπεύθυνοι για την ασφάλεια web εφαρμογών θα πρέπει να συντάσσουν ένα αναλυτικό πλάνο ασφάλειας το οποίο να ικανοποιεί όλες τις απαιτήσεις ασφάλειας. Κάθε οργανισμός ηλεκτρονικού εμπορίου θα πρέπει να ακολουθεί ένα πλάνο ασφάλειας για την ορθή και ασφαλή λειτουργία του. Σύμφωνα με τους κανονισμούς της ΑΔΑΕ, οι υπεύθυνοι για την δημιουργία ενός πλάνου ασφάλειας θα πρέπει να λαμβάνουν υπόψη τα εξής**:**

Αναγνώριση και έλεγχος αυθεντικότητας

- Αναγνωριστικά χρηστών: Με τη βοήθεια των αναγνωριστικών εξασφαλίζεται η ταυτοποίηση κάθε χρήστη.
- Επιλογή κωδικών πρόσβασης: Οι κωδικοί πρόσβασης (passwords) που υιοθετούν οι χρήστες πρέπει να έχουν αρκετό μήκος και να επιλέγονται με τέτοιο τρόπο, ώστε να είναι δύσκολο για κάποιον εισβολέα να τους μαντέψει.
- Αποθήκευση κωδικών πρόσβασης: Οι κωδικοί πρόσβασης των χρηστών θα πρέπει να αποθηκεύονται σε κατάλληλη μορφή, ώστε κανείς, ακόμα και ο διαχειριστής του συστήματος να μην μπορεί να τους διαβάσει.
- Συχνότητα αλλαγής κωδικών πρόσβασης: Οι κωδικοί πρόσβασης πρέπει να αλλάζουν αρκετά συχνά, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.

Έλεγχος πρόσβασης

- Δικαιώματα πρόσβασης: Για κάθε νέο λογαριασμό χρήστη θα πρέπει να καθορίζονται τα δικαιώματα πρόσβασης στους πόρους του συστήματος.
- Αδρανής σταθμός εργασίας: Οι σταθμοί εργασίας θα πρέπει να κλειδώνονται όταν μένουν αδρανείς για κάποιο χρονικό διάστημα, ώστε να περιοριστεί η πιθανότητα ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση.
- Διαχείριση δικαιωμάτων: Κατάλληλος μηχανισμός επιτρέπει την πρόσβαση σε ιδιαίτερες λειτουργίες του συστήματος μόνο σε χρήστες που πρέπει να έχουν πρόσβαση σε αυτές.
- Ασφάλεια του λογισμικού εφαρμογών: Η πρόσβαση στα αρχεία του λογισμικού εφαρμογών θα πρέπει να ελέγχεται με τη βοήθεια κατάλληλων προγραμμάτων.

Απόδοση ευθυνών

- Καταγραφή γεγονότων: Πρόκειται για την καταγραφή όλων των περιστατικών που λαμβάνουν χώρα στο σύστημα κάθε χρονική στιγμή, ώστε κάθε επεισόδιο να μπορεί να διερευνηθεί και να αποδοθούν ευθύνες.
- Διατήρηση των αρχείων καταγραφής γεγονότων: Θα πρέπει να διατηρείται κατάλληλο αρχείο καταγραφής γεγονότων για αρκετό χρονικό διάστημα.
- Διερεύνηση επεισοδίων: Όταν κάποια επεισόδια ανιχνεύονται ή υπάρχουν υποψίες για αυτά, πρέπει να διερευνούνται σε βάθος.

Προστασία από ιούς

- Πρόληψη και αποτροπή: Θα πρέπει να ελαχιστοποιηθεί η πιθανότητα να προσβληθεί το σύστημα από ιούς οποιασδήποτε μορφής.
- Ανίχνευση: Το σύστημα θα πρέπει να περιλαμβάνει μηχανισμούς περιοδικού ελέγχου για ιούς.
- Αντιμετώπιση: Θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί απομόνωσης και καταστροφής ιών.

Διαχείριση ασφάλειας δικτύου

- Παρακολούθηση του δικτύου: Η κατάσταση του δικτύου θα πρέπει να παρακολουθείται, ώστε να διευκολύνεται η έγκαιρη ανίχνευση των προβλημάτων.

- Εμπιστευτικότητα δεδομένων στο δίκτυο: Η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω διαδικτύου πρέπει να προστατεύεται.

Έλεγχος πρόσβασης μέσω δικτύου

- Απομακρυσμένη πρόσβαση σε μη ενεργές θύρες: Μόνο οι θύρες (ports) που χρησιμοποιούνται θα πρέπει να είναι ενεργές και οι υπόλοιπες πρέπει να είναι κλειδωμένες.
- Firewalls: Τα δίκτυα πρέπει να προστατεύονται μέσω των φραγμάτων ασφαλείας.

Διαχείριση συστήματος

- Διαδικασίες: Δημιουργία εγγράφου στο οποίο θα καθορίζονται αναλυτικά οι διαδικασίες εκτέλεσης των σημαντικότερων εργασιών.
- Έλεγχος πρόσβασης στο λογαριασμό του διαχειριστή του συστήματος: Ο λογαριασμός του διαχειριστή συστήματος είναι ο πιο προνομιούχος λογαριασμός στο σύστημα και για αυτό η χρήση του θα πρέπει να ελέγχεται.

Σχέδιο συνέχειας

- Αποκατάσταση λειτουργίας: Ο υπεύθυνος ασφάλειας θα πρέπει να καταρτίσει σχέδιο συνέχειας για περιπτώσεις αντιμετώπισης έκτακτων περιστατικών και διαδικασιών ανάνηψης. Οι υπολογιστές του συστήματος και οι υπηρεσίες δικτύου θα πρέπει να είναι διαθέσιμες όταν χρειάζονται.
- Εφεδρικά αντίγραφα: Η ύπαρξη εφεδρικών αντιγράφων εξασφαλίζει τη συνεχή διαθεσιμότητα των δεδομένων.

3.6 Ασφάλεια Εφαρμογών Ηλεκτρονικού Εμπορίου

Οι εφαρμογές ηλεκτρονικού εμπορίου αποτελούν αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων και της πλαστοπροσωπίας. Τα προβλήματα αυτά αντιμετωπίζονται με τη χρήση κρυπτογραφίας, η οποία επιτρέπει τη μετάδοση εμπιστευτικών πληροφοριών μέσα από ένα δίκτυο χωρίς να υπάρχει κίνδυνος υποκλοπής ή ανεπιθύμητων παρεμβάσεων. Παράλληλα επιτρέπει

στις δύο πλευρές που επικοινωνούν, δηλαδή στον έμπορα και στον πελάτη, να προβαίνουν σε αμοιβαία πιστοποίηση ταυτότητας.

Στην πράξη, οι κρυπτογραφικές αρχές πρέπει να ενσωματωθούν σε εργάσιμα πρωτόκολλα επικοινωνίας και λογισμικό. Υπάρχει μια ποικιλία κρυπτογραφικών πρωτοκόλλων στο διαδίκτυο, καθένα από τα οποία είναι ειδικευμένο για διαφορετική λειτουργία. Το πρωτόκολλο SSL (Secure Sockets Layer), το οποίο παρέχει κρυπτογραφημένη επικοινωνία μεταξύ ενός προγράμματος πλοήγησης (web browser) και ενός εξυπηρετητή web (web server), αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Το πρωτόκολλο SSL παρέχει απόρρητη επικοινωνία μεταξύ πελατών και εμπόρων, υποστηρίζοντας πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών, προσφέροντας έτσι ένα ικανοποιητικό επίπεδο ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου.

3.6.1 Πρωτόκολλο Ασφάλειας SSL

Το SSL (Secure Socket Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου Ιστού, το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server). Δηλαδή το πρωτόκολλο αυτό μπορεί να παρέχει απόρρητη επικοινωνία μεταξύ εμπόρου και πελάτη σε μια συναλλαγή πληρωμής και για το λόγο αυτό το SSL αποτελεί το κύριο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Συγκεκριμένα, το πρωτόκολλο SSL παρέχει κρυπτογράφηση της μεταδιδόμενης πληροφορίας (data encryption), υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή (server authentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (client authentication) μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Επιπλέον εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity), εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει

την πληροφορία χωρίς να γίνει αντιληπτός. Για κάθε κρυπτογραφημένη συναλλαγή δημιουργείται ένα κλειδί συνόδου (session key) το μήκος του οποίου μπορεί να είναι 40 bits ή 128 bits. Είναι γνωστό ότι όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογραφημένη επικοινωνία.

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Έχουν υπάρξει τρεις εκδόσεις του SSL. Η ιστορία της εξέλιξης του SSL έχει ως εξής:

Ιούλιος 1994: Κυκλοφόρησε η πρώτη έκδοση v.1.0 του πρωτοκόλλου SSL από τη Netscape, η οποία χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της εταιρείας.

Δεκέμβριος 1994: Κυκλοφόρησε η δεύτερη έκδοση v.2.0 του πρωτοκόλλου, η οποία ενσωματώθηκε στο web browser της Netscape, τον Netscape Navigator.

Ιούλιος 1995: Εκδόθηκε ο αντίστοιχος web browser της Microsoft, ο Internet Explorer, ο οποίος υποστηρίζει και αυτός την έκδοση v.2.0 του SSL, με κάποιες όμως επεκτάσεις της Microsoft.

Το SSL πρωτόκολλο, στην έκδοση v.2.0, καθιερώθηκε ως de facto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων. Το HTTP (Hyper Text Transfer Protocol) είναι ένα πρωτόκολλο που φροντίζει τη μεταφορά και τον τρόπο μετάδοσης δεδομένων στο διαδίκτυο. Ωστόσο το SSL v.2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του. Για το λόγο αυτό υπήρχε η ανάγκη για βελτίωση της έκδοσης v.2.0. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία.

Νοέμβριος 1995: Κυκλοφόρησε επισήμως η έκδοση v.3.0 του SSL, ενώ λίγους μήνες πιο πριν εφαρμοζόταν σε προϊόντα της εταιρείας, όπως τον Netscape Navigator.

Μάιος 1996: Το SSL περνά στη δικαιοδοσία του Internet Engineering Task Force -IETF, ο οποίος δημιουργεί την ειδική ομάδα εργασίας TLS group και μετονομάζει την νέα έκδοση του SSL, σε TLS (Transport Layer Security).

Η ομάδα εργασίας TLS group καθιερώθηκε το 1996 για να τυποποιήσει το πρωτόκολλο Transport Layer Security. Η TLS group εργάστηκε πάνω SSL v.3.0 πρωτόκολλο. Η ομάδα αυτή έχει ολοκληρώσει μια σειρά από προδιαγραφές που

περιγράφουν τις εκδόσεις 1.0 και 1.1 του TLS πρωτοκόλλου, και ετοιμάζει την έκδοση 1.2.

Ιανουάριος 1999: Εκδίδεται η πρώτη έκδοση του πρωτοκόλλου TLS, η οποία μπορεί να θεωρείται και ως η έκδοση v.3.1 του SSL.

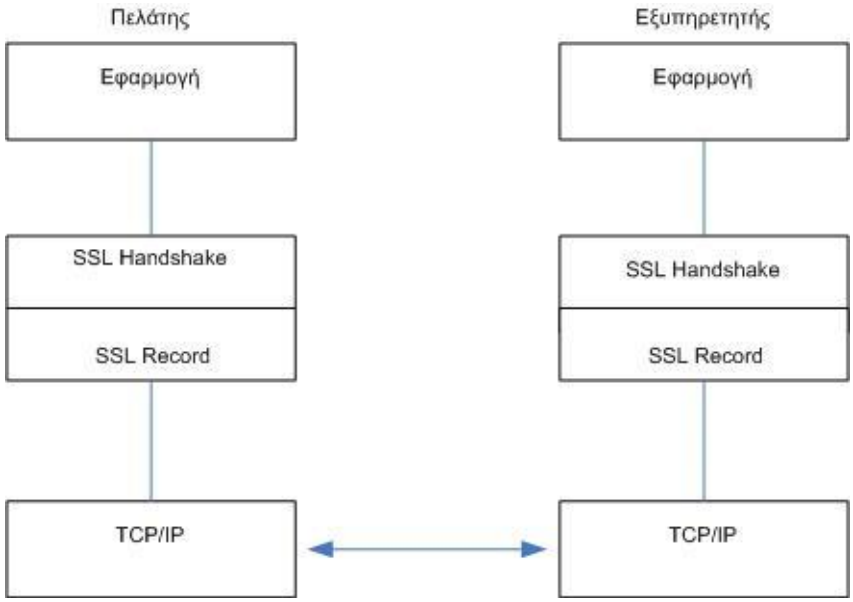
Δεκέμβριος 2005: Δημοσιεύεται η έκδοση 1.1 του TLS πρωτοκόλλου από την TLS group.

Η τρίτη έκδοση του πρωτοκόλλου SSL κάλυψε πολλές αδυναμίες της δεύτερης έκδοσης. Οι σημαντικότερες αλλαγές αφορούν: α) στη μείωση των απαραίτητων μηνυμάτων κατά το στάδιο εγκαθίδρυσης της σύνδεσης («χειραψία», «handshake»), β) στην επιλογή των αλγορίθμων συμπίεσης και κρυπτογράφησης από τον εξυπηρετητή και γ) στην εκ νέου διαπραγμάτευση του κυρίως κλειδιού (master-key) και του «αναγνωριστικού» συνόδου (session-id). Ακόμη αυξάνονται οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης και προστίθενται νέες τεχνικές για τη διαχείριση των κλειδιών. Γενικά, η τρίτη έκδοση του SSL (v.3.0) είναι πιο ολοκληρωμένη σχεδιαστικά από τη δεύτερη, με μεγαλύτερο εύρος υποστήριξης και λιγότερες ατέλειες.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου SSL, γεγονός που ερχόταν σε σύγκρουση με την τότε νομοθεσία των Η.Π.Α περί εξαγωγής κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει τη χρήση αλγορίθμων κρυπτογράφησης με κλειδί των 40 bits στις προς εξαγωγή εφαρμογές SSL, τη στιγμή που η κανονική έκδοση χρησιμοποιεί κλειδί των 128 bits. Γενικές πληροφορίες για την κρυπτογραφία και τους αλγόριθμους κρυπτογράφησης υπάρχουν στο Κεφάλαιο 4.

Αρχιτεκτονική του SSL

Η αρχιτεκτονική τοποθέτηση του SSL απεικονίζεται στο Σχήμα 4**.**



Σχήμα 4: Αρχιτεκτονική Τοποθέτηση του SSL

Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Το TCP/IP (Transmission Control Protocol/Internet Protocol) είναι το πρωτόκολλο επικοινωνίας (communication protocol) για την επικοινωνία ανάμεσα σε υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο. Τα αρχικά TCP/IP αναφέρονται σε δύο από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, δηλ. στο TCP και στο IP. Το FTP (File Transfer Protocol) είναι ένα πρωτόκολλο μεταφοράς αρχείων, το οποίο φροντίζει για τη διακίνηση αρχείων μέσα στο διαδίκτυο, και το TELNET είναι ουσιαστικά μια υπηρεσία του διαδικτύου με την οποία οι χρήστες αποκτούν απευθείας πρόσβαση σε άλλους υπολογιστές στο διαδίκτυο.

Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο διασύνδεσης ανοικτών συστημάτων (Open System Interconnection, OSI), έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επιπλέον η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το

SSL. Το S/HTTP (Secure HTTP) πρωτόκολλο φροντίζει για την ασφαλή μεταφορά δεδομένων στο διαδίκτυο.

Ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείτε στην κορυφή του.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
- Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

Για τη γενική λειτουργία του πρωτοκόλλου SSL υπάρχουν δύο βασικές οντότητες: σύνοδος SSL και σύνδεση SSL.

1) Η σύνοδος SSL αποτελεί τη δημιουργία μιας σχέσης μεταξύ ενός πελάτη και ενός εξυπηρετητή. Οι σύνοδοι δημιουργούνται από το SSL Handshake protocol και είναι ομάδες παραμέτρων ασφάλειας, οι οποίες μπορούν να διαμοιραστούν ταυτόχρονα σε πολλές συνδέσεις. Ο κύριος λόγος για αυτό είναι η αποφυγή χρονοβόρων διαπραγματεύσεων νέων παραμέτρων ασφάλειας για κάθε νέα σύνδεση.

Οι παράμετροι που περιέχονται και μοιράζονται σε μια σύνοδο είναι οι ακόλουθοι:

- Αναγνωριστικό συνόδου: επιλέγεται από τον εξυπηρετητή για αναγνώριση μιας ενεργούς ή επαναληπτικής κατάστασης συνόδου.
- Ψηφιακό πιστοποιητικό (μεταξύ ομότιμων οντοτήτων).
- Μέθοδος συμπίεσης των δεδομένων: Αλγόριθμος που χρησιμοποιείται για συμπίεση δεδομένων πριν την κρυπτογράφηση.
- Αλγόριθμος κρυπτογράφησης των δεδομένων.

- Κύριο μυστικό (master secret): Μοναδικός αριθμός μήκους 48-byte, κοινό μυστικό μεταξύ εξυπηρετητή και πελάτη.
- Δυνατότητα επανεκκίνησης της συνόδου.

2) Σύνδεση SSL είναι η μεταφορά των πληροφοριών μεταξύ δύο οντοτήτων. Στο SSL οι συνδέσεις αυτές είναι σχέσεις μεταξύ ομότιμων οντοτήτων και είναι παροδικές.

Οι παράμετροι που περιέχονται σε μια σύνδεση είναι οι ακόλουθοι:

- Τυχαίοι αριθμοί μεταξύ πελάτη και εξυπηρετητή, οι οποίοι είναι διαφορετικοί για κάθε σύνδεση.
- Μυστικό MAC εξυπηρετητή: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον εξυπηρετητή.
- Μυστικό MAC πελάτη: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον πελάτη.
- Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον εξυπηρετητή και αποκρυπτογράφηση από τον πελάτη.
- Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον πελάτη και αποκρυπτογράφηση από τον εξυπηρετητή.
- Διανύσματα αρχικοποίησης της σύνδεσης
- Αριθμοί ακολουθίας: Κάθε μέλος (εξυπηρετητής, πελάτης) διατηρεί ξεχωριστούς αριθμούς ακολουθίας για αποστολή και λήψη μηνυμάτων σε κάθε σύνδεση.

Όπως απεικονίζεται στο σχήμα 4, το πρωτόκολλο SSL αποτελείται από δύο επιμέρους πρωτόκολλα, το SSL record protocol και το SSL handshake protocol. Το SSL record protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Συγκεκριμένα το πρωτόκολλο αυτό τοποθετεί τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει. Επίσης εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το SSL handshake protocol είναι ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το οποίο επίσης διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας. Συγκεκριμένα το πρωτόκολλο αυτό διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την

πιστοποίηση της ταυτότητας του εξυπηρετητή και του πελάτη αν αυτό ζητηθεί. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας. Τα SSL record protocol και SSL handshake protocol περιγράφονται αναλυτικά παρακάτω.

SSL Record Protocol

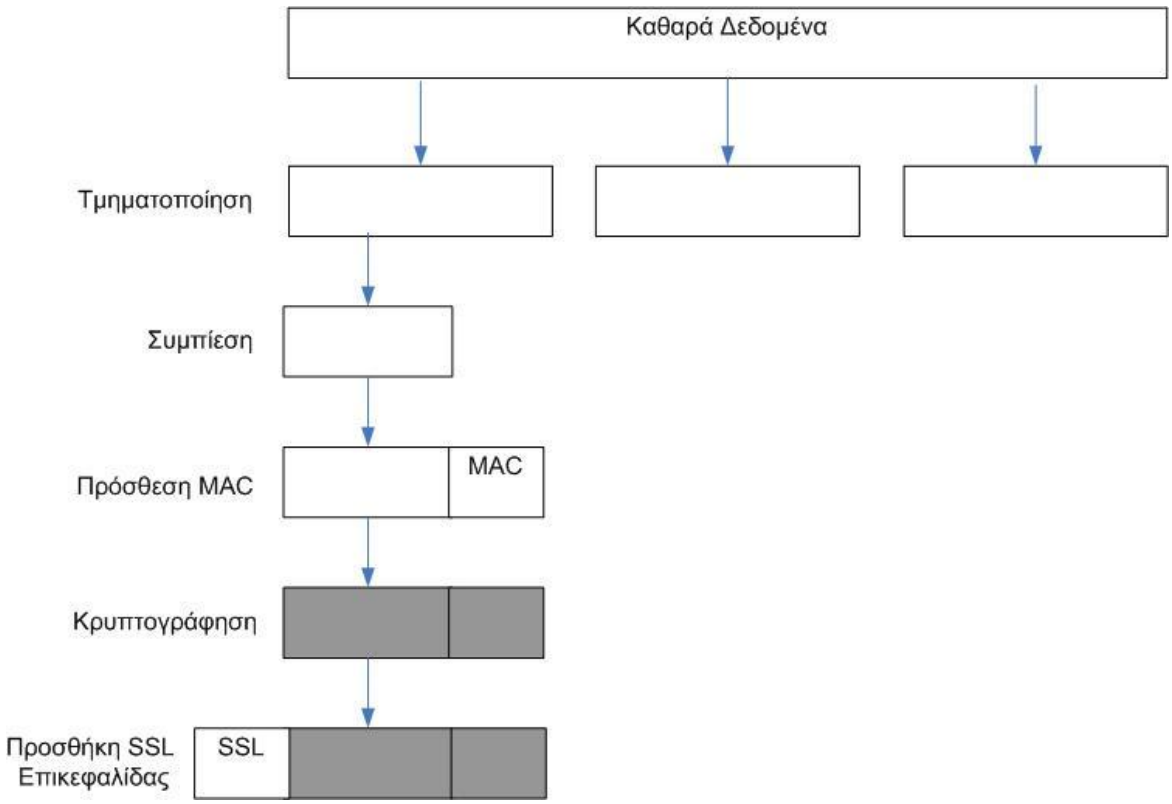
Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις:

Εμπιστευτικότητα: Το Handshake Protocol ορίζει ένα κοινό μυστικό κλειδί, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων του SSL.

Ακεραιότητα: Το Handshake Protocol επίσης ορίζει ένα κοινό μυστικό κλειδί που χρησιμοποιείται για τη δημιουργία MAC όλων των μηνυμάτων που ανταλλάσσονται.

Το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό (fragmentation), τη συμπίεση, την αυθεντικοποίηση και την κρυπτογράφηση δεδομένων. Ουσιαστικά το πρωτόκολλο αυτό μετατρέπει τα προς μετάδοση δεδομένα σε SSL πακέτα.

Το Σχήμα 5 φανερώνει τη λειτουργία του SSL Record Protocol. Συγκεκριμένα το Record Protocol παίρνει το μήνυμα της εφαρμογής που θα μεταδοθεί, τμηματοποιεί τα δεδομένα σε εύχρηστα blocks, προαιρετικά συμπιέζει τα δεδομένα με κατάλληλους μηχανισμούς που επιλέγονται κατά τη «χειραψία» και μετά εφαρμόζει ένα MAC πάνω από τα συμπιεσμένα δεδομένα. Στη συνέχεια κρυπτογραφεί το αποτέλεσμα χρησιμοποιώντας συμμετρική κρυπτογράφηση, προσθέτει μια επικεφαλίδα SSL και στο τέλος μεταδίδει το πακέτο. Η μέθοδος συμπίεσης και ο αλγόριθμος κρυπτογράφησης καθορίζονται κατά τη διάρκεια εκτέλεσης του SSL Handshake Protocol.



Σχήμα 5: Λειτουργία του SSL Record Protocol

Το SSL Record Protocol εκτελεί και την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Συγκεκριμένα τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων.
Διάφορα πρωτόκολλα SSL μπορούν να στρωματοποιούνται στην κορυφή του SSL Record Protocol. Οι προδιαγραφές του SSL 3.0 καθορίζουν τα ακόλουθα τρία πρωτόκολλα SSL:

- Πρωτόκολλο προειδοποίησης (SSL Alert Protocol)
- Πρωτόκολλο χειραψίας (SSL Handshake Protocol)
- Πρωτόκολλο Αλλαγής Προδιαγραφών Κρυπτογραφίας (SSL Change Cipher Spec Protocol)

Το SSL Alert Protocol χρησιμοποιείται για να μεταφέρει προειδοποιήσεις (alerts) μέσω του SSL Record Protocol. Οι προειδοποιήσεις είναι συνήθως μηνύματα προβλημάτων και λαθών (π.χ. "λάθος MAC", "μη αναμενόμενο μήνυμα" κλπ.) που αφορούν τόσο τη σύνδεση όσο και τη μετάδοση των μηνυμάτων μεταξύ δύο

ομότιμων οντοτήτων. Με τον τρόπο αυτό ειδοποιεί το SSL να διακόψει τη σύνδεση ή να προβεί σε όποιες άλλες ενέργειες έχουν καθοριστεί.

Το SSL Handshake Protocol είναι το κύριο πρωτόκολλο SSL και περιγράφεται στην επόμενη ενότητα.

Το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας είναι το απλούστερο από τα πιο πάνω πρωτόκολλα. Χρησιμοποιείται για την αλλαγή μιας προδιαγραφής κρυπτογραφίας με μια άλλη. Κανονικά μια προδιαγραφή κρυπτογραφίας αλλάζει στο τέλος μιας SSL χειραψίας. Μπορεί όμως να τροποποιηθεί και σε οποιαδήποτε άλλη στιγμή.

SSL Handshake Protocol

Το SSL Handshake Protocol είναι το περισσότερο περίπλοκο πρωτόκολλο από τα χρησιμοποιούμενα στο SSL. Αυτό το πρωτόκολλο επιτρέπει προαιρετικά στον πελάτη και τον εξυπηρετητή να εξακριβώσουν ο ένας την ταυτότητα του άλλου, να διαπραγματευτούν τον αλγόριθμο κρυπτογράφησης και τη μέθοδο συμπίεσης, και να δημιουργήσουν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο προκύπτουν τα διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων. Μετά την εκτέλεση του SSL Handshake Protocol αρχίζει η μεταφορά των δεδομένων από το SSL Record Protocol.

Στο SSL Handshake Protocol , για τη δημιουργία μιας SSL συνόδου, ο πελάτης και ο εξυπηρετητής ανταλλάσσουν μεταξύ τους τα ακόλουθα μηνύματα:

C → S : Client_Hello

S → C : Server_Hello

Certificate

Server_Key_Exchange

Certificate_Request

Server_Hello_Done

C → S : Certificate

Client_Key_Exchange

Certificate_Verify

Change_Cipher_Spec

Finished

S → C : Change_Cipher_Spec

Finished

Μια εκτέλεση SSL Handshake Protocol συνήθως αρχίζει με τον πελάτη και τον εξυπηρετητή να αποστέλλουν μηνύματα χαιρετισμού (hello) ο ένας στον άλλο. Τα μηνύματα χαιρετισμού χρησιμοποιούνται για την ανταλλαγή πρόσθετων δυνατοτήτων ασφάλειας.

Στο βήμα 1, όταν ένας πελάτης επιθυμεί να συνδεθεί με ένα συγκεκριμένο εξυπηρετητή, αποστέλλει ένα αντίστοιχο μήνυμα *Client_Hello.* Το μήνυμα αυτό περιλαμβάνει:

- Τον αριθμό της υψηλότερης έκδοσης SSL που μπορεί να υποστηρίξει ο πελάτης (τυπικά v.3.0).
- Μια τυχαία δομή που παράγεται από τον πελάτη, η οποία αποτελείται από μια χρονοσφραγίδα των 32 bits και μια τιμή των 28 byte που παράγεται από μια γεννήτρια τυχαίων αριθμών. Η χρονοσφραγίδα προστατεύει από επιθέσεις τύπου επανάληψης μηνυμάτων.
- Μια ταυτότητα αναγνώρισης συνόδου (session identity ID) που ο πελάτης επιθυμεί να χρησιμοποιήσει για αυτή τη σύνδεση.
- Ένα κατάλογο από περιβάλλοντα κρυπτογραφίας (cipher suites) που υποστηρίζει ο πελάτης.
- Ένα κατάλογο από μεθόδους συμπίεσης (compression methods) που υποστηρίζει ο πελάτης.

Η τιμή ταυτότητας αναγνώρισης συνόδου δηλώνει μια σύνοδο μεταξύ του ίδιου πελάτη και εξυπηρετητή, της οποίας τις παραμέτρους ασφάλειας επιθυμεί να επαναχρησιμοποιήσει ο πελάτης. Η ταυτότητα αναγνώρισης συνόδου μπορεί να προέρχεται από μια προηγούμενη σύνδεση ή κάποια τρέχουσα ενεργή σύνδεση. Το πεδίο ταυτότητας αναγνώρισης συνόδου είναι κενό σε περίπτωση που δεν υπάρχει διαθέσιμη σύνοδος ή ο πελάτης επιθυμεί να δημιουργήσει νέες παραμέτρους ασφάλειας. Ο πελάτης μέσω του μηνύματος *Client_Hello* αποστέλλει στον εξυπηρετητή ένα σύνολο από περιβάλλοντα κρυπτογραφίας που υποστηρίζει. Κάθε περιβάλλον κρυπτογραφίας καθορίζει ένα αλγόριθμο ανταλλαγής κλειδιών και μια προδιαγραφή κρυπτογραφίας. Ο εξυπηρετητής θα επιλέξει ένα περιβάλλον κρυπτογραφίας ή αν δεν υπάρχουν αποδεκτές επιλογές θα επιστρέψει ένα μήνυμα σφάλματος και θα τερματίσει τη σύνδεση. Αφού έχει στείλει το μήνυμα *Client_Hello,* ο πελάτης περιμένει για ένα μήνυμα *Server_Hello.*

Στο βήμα 2, ο εξυπηρετητής επεξεργάζεται το μήνυμα *Client_Hello* και απαντά είτε με ένα μήνυμα σφάλματος είτε με ένα μήνυμα *Server_Hello*. Συγκεκριμένα το μήνυμα *Server_Hello* περιλαμβάνει:

- Έναν αριθμό έκδοσης εξυπηρετητή (συνήθως αυτόν που προτείνεται από τον πελάτη στο μήνυμα *Client_Hello*).
- Μια τυχαία δομή που παράγεται από τον εξυπηρετητή, η οποία επίσης αποτελείται από μια χρονοσφραγίδα των 32 bits και μια τιμή των 28 byte που παράγεται από μια γεννήτρια τυχαίων αριθμών.
- Μια ταυτότητα αναγνώρισης συνόδου (session ID) που αντιστοιχεί στη συγκεκριμένη σύνδεση.
- Ένα περιβάλλον κρυπτογραφίας, το οποίο επιλέχθηκε από τον εξυπηρετητή από τον κατάλογο περιβαλλόντων κρυπτογραφίας που υποστηρίζονται από τον πελάτη.
- Μια μέθοδο συμπίεσης, η οποία επιλέχθηκε από τον εξυπηρετητή από τον κατάλογο μεθόδων συμπίεσης που υποστηρίζονται από τον πελάτη.

Αν η ταυτότητα αναγνώρισης συνόδου στο μήνυμα *Client_Hello* δεν είναι κενή, ο εξυπηρετητής αναζητά την ταυτότητα αυτή στη δική του μνήμη συνόδου. Σε περίπτωση που βρεθεί αυτή η ταυτότητα και ο εξυπηρετητής είναι πρόθυμος να καθιερώσει τη νέα σύνδεση χρησιμοποιώντας την αντίστοιχη κατάσταση συνόδου, απαντά με την ίδια τιμή με αυτή που προμηθεύτηκε από τον πελάτη. Αλλιώς το πεδίο αυτό περιέχει μια διαφορετική τιμή, η οποία προσδιορίζει τη νέα σύνοδο.

Αν ο εξυπηρετητής πρόκειται να αυθεντικοποιηθεί αποστέλλει μετά το μήνυμα *Server_Hello* ένα πιστοποιητικό μέσα σε ένα αντίστοιχο μήνυμα *Certificate*. Ο τύπος του πιστοποιητικού πρέπει να είναι κατάλληλος για τον αλγόριθμο ανταλλαγής κλειδιών του περιβάλλοντος κρυπτογραφίας που επιλέχθηκε και συνήθως είναι ένα X.509 πιστοποιητικό. Πληροφορίες για τα πιστοποιητικά βρίσκονται στο κεφάλαιο 4. Ο ίδιος τύπος μηνύματος θα χρησιμοποιηθεί αργότερα για την απάντηση του πελάτη στο μήνυμα *Certificate_Request* του εξυπηρετητή.

Στη συνέχεια ο εξυπηρετητής στέλνει στον πελάτη το μήνυμα *Server_Key_Exchange.* Το μήνυμα αυτό περιέχει το δημόσιο κλειδί του εξυπηρετητή, ανάλογα με τον αλγόριθμο ανταλλαγής κλειδιών που χρησιμοποιείται. Ο εξυπηρετητής μπορεί προαιρετικά να ζητά ένα πιστοποιητικό που αυθεντικοποιεί τον πελάτη. Στην περίπτωση αυτή αποστέλλει στον πελάτη ένα

μήνυμα *Certificate_Request.* Το μήνυμα περιλαμβάνει ένα κατάλογο από τους τύπους των πιστοποιητικών που ζητούνται, ταξινομημένους κατά τη σειρά προτίμησης του εξυπηρετητή, καθώς επίσης και ένα κατάλογο για αποδεκτά CAs (Certificate Authorities). Στο τέλος του βήματος 2 ο εξυπηρετητής αποστέλλει ένα μήνυμα *Server_Hello_Done* στον πελάτη, το οποίο υποδεικνύει το τέλος του μηνύματος *Server_Hello* και των συσχετιζόμενων μηνυμάτων. Κατά τη λήψη του μηνύματος *Server_Hello* και των συσχετιζόμενων μηνυμάτων ο πελάτης επιβεβαιώνει, αν απαιτείται, ότι ο εξυπηρετητής παρείχε ένα έγκυρο πιστοποιητικό και ελέγχει αν οι παράμετροι ασφάλειας που περιέχονται στο *Server_Hello* μήνυμα είναι αποδεκτές.

Αν ο εξυπηρετητής έχει ζητήσει αυθεντικοποίηση του πελάτη, ο πελάτης στο βήμα 3 του στέλλει ένα μήνυμα *Certificate* το οποίο περιλαμβάνει ένα πιστοποιητικό για το δημόσιο κλειδί του. Στη συνέχεια ο πελάτης αποστέλλει ένα μήνυμα *Client_Key_Exchange,* του οποίου η μορφή εξαρτάται από τον αλγόριθμο ανταλλαγής κλειδιών που επιλέγεται από τον εξυπηρετητή.

Αν χρησιμοποιείται ο αλγόριθμος RSA για αυθεντικοποίηση εξυπηρετητή και ανταλλαγή κλειδιών, ο πελάτης παράγει ένα προ-κύριο μυστικό (pre-master secret) των 48 byte χρησιμοποιώντας μια γεννήτρια τυχαίων αριθμών, το κρυπτογραφεί με το προσωρινό RSA δημόσιο κλειδί του εξυπηρετητή από το μήνυμα *Server_Key_Exchange* και αποστέλλει το αποτέλεσμα πίσω στον εξυπηρετητή μέσω του μηνύματος *Client_Key_Exchange.* Ο εξυπηρετητής χρησιμοποιεί το δικό του ιδιωτικό κλειδί για να αποκρυπτογραφήσει το προ-κύριο μυστικό. Αυτό το προ-κύριο μυστικό χρησιμοποιείται τόσο από την πλευρά του πελάτη, όσο και από την πλευρά του εξυπηρετητή για να παράγουν το κύριο μυστικό.

Το κύριο μυστικό δε χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγαριών κλειδιών. Τα ένα ζευγάρι ανήκει στον πελάτη και αποτελείται από το client-write-key που χρησιμοποιεί ο πελάτης για να κρυπτογραφήσει τα μηνύματα προς τον εξυπηρετητή και το client-read-key για να αποκρυπτογραφήσει ότι λαμβάνει από τον εξυπηρετητή. Το δεύτερο ζευγάρι ανήκει στον εξυπηρετητή και αποτελείται από το server-write-key για κρυπτογράφηση μηνυμάτων προς τον πελάτη και το server-read-key για αποκρυπτογράφηση των λαμβανομένων. Αξίζει να σημειωθεί ότι το client-write-

key είναι το ίδιο με το server-read-key και το client-read-key είναι το ίδιο με το server-write-key.

Στη συνέχεια ο πελάτης μπορεί να στείλει στον εξυπηρετητή ένα μήνυμα *Certificate_Verify*. Αυτό το μήνυμα χρησιμοποιείται για να παρέχει επιβεβαίωση του πιστοποιητικού του πελάτη. Τελικά ο πελάτης ολοκληρώνει το βήμα 3 αποστέλλοντας ένα μήνυμα *Change_Cipher_Spec* και ένα αντίστοιχο μήνυμα *Finished* στον εξυπηρετητή. Το μήνυμα *Change_Cipher_Spec* δηλώνει ότι ο πελάτης είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία. Το μήνυμα *Finished* αποστέλλεται πάντοτε αμέσως μετά το μήνυμα *Change_Cipher_Spec* για να επιβεβαιώσει ότι η ανταλλαγή κλειδιών και οι διαδικασίες πιστοποίησης αυθεντικότητας ήταν πράγματι επιτυχείς.

Η εκτέλεση του SSL Handshake Protocol ολοκληρώνεται έχοντας τον εξυπηρετητή να αποστέλλει ένα *Change_Cipher_Spec* μήνυμα και ένα αντίστοιχο μήνυμα *Finished* στον πελάτη, στο βήμα 4.

Μετά την ολοκλήρωση του SSL Handshake Protocol, καθιερώνεται μια ασφαλής σύνδεση μεταξύ του πελάτη και του εξυπηρετητή. Αυτή η σύνδεση μπορεί τώρα να χρησιμοποιηθεί για την αποστολή δεδομένων εφαρμογών μέσω του SSL Record Protocol.

Αντοχή του SSL σε Γνωστές Επιθέσεις

1) **Επίθεση Λεξικού (Dictionary Attack)**

Κατά την επίθεση αυτή, ένα τμήμα του μη κρυπτογραφημένου κειμένου βρίσκεται στην κατοχή κακόβουλων προσώπων. Το τμήμα αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί ένα κομμάτι που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του κειμένου έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα (128 bits). Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bits κλειδιά και παρ' όλο που τα 88 bits αυτών μεταδίδονται χωρίς κρυπτογράφηση, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών καθιστά την επίθεση εξαιρετικά δύσκολη.

2) **Βίαιη Επίθεση (Brute Force Attack)**

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι ατελέσφορη.

3) Επίθεση Επανάληψης (Replay Attack)

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ πελάτη - εξυπηρετητή και προσπαθεί να χρησιμοποιήσει ξανά τα μηνύματα του πελάτη για να αποκτήσει πρόσβαση στον εξυπηρετητή, έχουμε επίθεση τύπου replay attack. Όμως το SSL κάνει χρήση του αναγνωριστικού συνόδου (connection-ID), το οποίο παράγεται από τον εξυπηρετητή με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια αναγνωριστικά σύνδεσης.

4) Επίθεση Παρεμβολής (Man-In-The-Middle-Attack)

Η επίθεση Man-In-The-Middle-Attack συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του εξυπηρετητή και του πελάτη. Αφού επεξεργαστεί τα μηνύματα του πελάτη και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον εξυπηρετητή. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον εξυπηρετητή. Δηλαδή, προσποιείται στον πελάτη ότι είναι ο εξυπηρετητής και αντίστροφα.

Το SSL υποχρεώνει τον εξυπηρετητή να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη.

Το SSL στο Ηλεκτρονικό Εμπόριο

Το πρωτόκολλο SSL μπορεί να χρησιμοποιείται για την εγκαθίδρυση ασφαλών συνδέσεων μεταξύ εξυπηρετουμένων (πελάτης) και εξυπηρετητών (έμπορας). Συγκεκριμένα μπορεί να χρησιμοποιείται για να αυθεντικοποιεί έναν εξυπηρετητή και προαιρετικά τον εξυπηρετούμενο, να εκτελεί ανταλλαγή κλειδιών και να παρέχει αυθεντικοποίηση και ακεραιότητα μηνυμάτων σε εφαρμογές ηλεκτρονικού εμπορίου και γενικά σε εφαρμογές διαδικτύου. Για τους λόγους αυτούς το πρωτόκολλο SSL αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο.

Η μη διασφάλιση αυθεντικοποίησης εξυπηρετούμενου βοήθησε το πρωτόκολλο SSL να διαδοθεί σε περιβάλλοντα ηλεκτρονικού εμπορίου. Η υποστήριξη της αυθεντικοποίησης εξυπηρετούμενου απαιτεί ξεχωριστά δημόσια κλειδιά και

πιστοποιητικά για κάθε εξυπηρετούμενο. Είναι λοιπόν φανερό ότι η αυθεντικοποίηση κάθε πελάτη στο ηλεκτρονικό εμπόριο είναι πρακτικά αδύνατη. Επίσης είναι πιο σημαντικό οι τελικοί καταναλωτές να μπορούν να ενημερώνονται σχετικά με την ταυτότητα των εμπόρων με τους οποίους συναλλάσσονται, παρά να απαιτείται ίδιος βαθμός ασφάλειας και από τους εμπόρους για τους καταναλωτές. Επιπλέον αφού ο αριθμός των εμπόρων-εξυπηρετητών διαδικτύου είναι πολύ μικρότερος από τον αριθμό των καταναλωτών-χρηστών, είναι ευκολότερο και πιο πρακτικό να εφοδιάζονται οι εξυπηρετητές με τα απαραίτητα δημόσια κλειδιά και πιστοποιητικά.

Σήμερα το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για Διαδίκτυο γενικά και το ηλεκτρονικό εμπόριο συγκεκριμένα. Αξίζει να σημειωθεί ότι αν όχι όλες, οι περισσότερες τράπεζες που προσφέρουν τις υπηρεσίες τους διαμέσου του διαδικτύου έχουν αναπτύξει την ασφάλεια των εφαρμογών ηλεκτρονικής τραπεζικής με βάση το πρωτόκολλο SSL.

Το πρωτόκολλο SSL χρησιμοποιείται συνήθως σε HTTP προϊόντα εξυπηρετητών και εξυπηρετούμενων. Για παράδειγμα, υπάρχουν αρκετοί HTTP εξυπηρετητές διαθέσιμοι οι οποίοι υποστηρίζουν το SSL. Από την πλευρά του εξυπηρετούμενου, σήμερα, οι περισσότεροι browsers ιστού υποστηρίζουν το SSL. Τα περισσότερα από αυτά τα προϊόντα υποστηρίζουν τον αλγόριθμο RC4 για κρυπτογράφηση και τα MD2 και MD5 για σύνοψη.

Μειονέκτημα της χρήσης του SSL αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του browser του εξυπηρετούμενου με τον HTTPS εξυπηρετητή. Η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίηση της SSL συνόδου. Πρακτικά οι χρήστες αντιλαμβάνονται λίγα δευτερόλεπτα καθυστέρηση μεταξύ της έναρξης σύνδεσης με τον HTTPS εξυπηρετητή και της ανάκτησης της πρώτης HTML σελίδας από αυτόν.

Transport Layer Security Protocol, TLS

Το Μάιο του 1996 το IETF δημιούργησε το πρωτόκολλο Transport Layer Security TLS WG για την ασφάλεια του επιπέδου μεταφοράς. Το Δεκέμβριο του 1996 ένα πρώτο έγγραφο TLS 1.0 κυκλοφόρησε ως Internet Draft. Το έγγραφο ήταν ουσιαστικά το ίδιο με τις προδιαγραφές του SSL 3.0. Γενικά η ομάδα εργασίας για τη δημιουργία του TLS είχε σαν στρατηγική της οι προδιαγραφές του TLS 1.0 να

βασίζονται κυρίως στο SSL 3.0, παρά σε άλλα πρωτόκολλα ασφάλειας επιπέδου μεταφοράς όπως SSL 2.0. Πρόσφατα, το Δεκέμβριο του 2005, η ομάδα εργασίας TLS group δημοσίευσε την έκδοση 1.1 του TLS.

Στο TLS 1.0 ενσωματώθηκε το SSL 3.0 με κάποιες μικρές τροποποιήσεις. Οι τροποποιήσεις αυτές αφορούσαν περισσότερο σημεία αποσαφήνισης. Η κύρια τροποποίηση που υποδείχθηκε για το SSL 3.0 ώστε να ενσωματωθεί στο TLS 1.0 είναι:

Το TLS record protocol και το TLS handshake protocol θα έπρεπε να διαχωρίζονται εντελώς και να καθορίζονται σαφώς σε σχετικά έγγραφα.

Οι διαφορές μεταξύ του TLS 1.0 και του SSL 3.0 δεν είναι ιδιαίτερα σημαντικές, αλλά είναι αρκετά κρίσιμες ώστε τα TLS 1.0 και SSL 3.0 να μη συνεργάζονται εύκολα. Ωστόσο το TLS 1.0 ενσωματώνει ένα μηχανισμό μέσω του οποίου μια υλοποίηση TLS μπορεί να γίνει συμβατή με το SSL 3.0.

Το πρωτόκολλο TLS είναι από μόνο του ένα στρωματοποιημένο πρωτόκολλο. Στο χαμηλότερο επίπεδο, το TLS record protocol λαμβάνει τα προς μετάδοση μηνύματα, κατακερματίζει τα δεδομένα σε διαχειρίσιμα τμήματα, προαιρετικά τα συμπιέζει, υπολογίζει και προσαρτά ένα MAC σε κάθε τμήμα, κρυπτογραφεί το αποτέλεσμα και το αποστέλλει. Επιπλέον το πρωτόκολλο αυτό εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το TLS record protocol όταν λάβει ένα πακέτο το αποκρυπτογραφεί, το επιβεβαιώνει, το αποσυμπιέζει, και το επανασυναρμολογεί πριν το μεταδώσει. Μια κατάσταση TLS σύνδεσης αποτελεί το λειτουργικό περιβάλλον του TLS record protocol. Αυτή καθορίζει τους αλγόριθμους συμπίεσης, κρυπτογράφησης και αυθεντικοποίησης μηνυμάτων, καθώς και τα κλειδιά που χρησιμοποιούνται για κρυπτογράφηση και αυθεντικοποίηση. Η σύνδεση αυτή (σύνδεση TLS), δημιουργείται κατά την εκτέλεση του TLS handshake protocol.

Στο υψηλότερο επίπεδο, το TLS handshake protocol χρησιμοποιείται για να συμφωνηθεί μια κατάσταση συνόδου μεταξύ του εξυπηρετητή και του εξυπηρετούμενου (πελάτη). Συγκεκριμένα προσδιορίζεται μια ταυτότητα συνόδου, μια προδιαγραφή κρυπτογραφίας, μια μέθοδος συμπίεσης και ένα κύριο κλειδί. Τα στοιχεία αυτά χρησιμοποιούνται για τη δημιουργία παραμέτρων ασφάλειας που θα χρησιμοποιηθούν από το TLS record protocol κατά την προστασία δεδομένων

εφαρμογών. Συγκεκριμένα το TLS handshake protocol αποτελείται από τρία υποπρωτόκολλα:

Το TLS change cipher spec protocol αποτελείται από ένα απλό μήνυμα Change_Cipher_Spec, το οποίο αποστέλλεται από τον πελάτη στον εξυπηρετητή κατά τη διάρκεια της χειραψίας, αφού έχουν συμφωνηθεί οι παράμετροι ασφάλειας.

Το TLS alert protocol χρησιμοποιείται για να αποστέλλει μηνύματα προειδοποίησης, τα οποία μεταβιβάζουν τη σημαντικότητα ενός μηνύματος προειδοποίησης και μια περιγραφή της προειδοποίησης αυτής. Οι προειδοποιήσεις είναι συνήθως μηνύματα προβλημάτων και λαθών που αφορούν κυρίως τη μετάδοση των μηνυμάτων.

Το TLS handshake protocol χρησιμοποιείται για να συμφωνηθεί μια κατάσταση συνόδου. Όταν ένας πελάτης και ένας εξυπηρετητής αρχίζουν για πρώτη φορά να επικοινωνούν επιλέγουν αλγόριθμους κρυπτογράφησης, προαιρετικά αυθεντικοποιούνται αμοιβαία και χρησιμοποιούν κρυπτογραφία δημοσίου κλειδιού για να παράγουν ένα κύριο μυστικό και τα αντίστοιχα κλειδιά συνόδου. Η ροή των μηνυμάτων που ο πελάτης και ο εξυπηρετητής ανταλλάσσουν μεταξύ τους είναι ουσιαστικά η ίδια, όπως του SSL handshake protocol.

Μετά την εκτέλεση του TLS handshake protocol ο πελάτης και ο εξυπηρετητής μπορούν να ανταλλάσσουν μηνύματα δεδομένων εφαρμογών με ασφάλεια. Τα μηνύματα αυτά μεταφέρονται μέσω του SSL Record protocol, αφού πρώτα κατακερματιστούν, συμπιεστούν, αυθεντικοποιηθούν και κρυπτογραφηθούν.

4^{ο} ΚΕΦΑΛΑΙΟ : ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

4.1 Ιστορία Κρυπτογράφησης

Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν 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 εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την 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 αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

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 επινόησαν 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, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του

οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλευθούν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια σς ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

- 3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 1450 π.Χ.: Γραμμική γραφή Α

- 1450 1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού (Σχήμα 2.2), που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που άνεσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι

πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι

Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

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. 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 (Εικόνα 2.3).

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο

Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκληθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA. Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το Μ-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών Μ-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.[1]

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

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. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

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.

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα είναι η χρήση της κβαντικής Φυσικής, όπως υποστηρίζει ο Νικολά Ζισίν, πρωτοπόρος της συγκεκριμένης τεχνολογίας στο Πανεπιστήμιο της Γενεύης. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην

πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε. Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή. Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

4.2 Μέθοδοι Κρυπτογράφησης

4.2.1 Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο

ασφαλές μέσο για την μετάδοση του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχτηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχτεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos του MIT (Massachusetts Institute of Technology).

4.2.2 Ασύμμετρη 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 του 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. Κάθε χρήστης, λοιπόν έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης

κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία 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.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ότι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής. Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί έναν υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με

το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

4.2.3 Μειονεκτήματα και Πλεονεκτήματα της Συμμετρικής και Ασύμμετρης Κρυπτογραφίας.

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέρθηκε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτικής του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, οι διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με

ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη. Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλοντα κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν,μιας και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στην περίπτωση που η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι, οι οποίοι θα αναλυθούν διεξοδικά παρακάτω.

4.3 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας.

- **DES (Data Encryption Standard).**

Το DES είναι το ακρωνύμιο των λέξεων Data Encryption Standard. Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit.Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή

MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

- **Triple-DES.**

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3(Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με τα τρία διαφορετικά κλειδιά.
- DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναιι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά. Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

- **DESX.**

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

- **AES (Advanced Encryption Standard).**

Το ακρωνύμιο AES προέρχεται από την φράση Advanced Encryption Standard. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES. Ο DES βρίσκεται ήδη πολλά χρόνια σε χρήση και από το 1998 το NIST δεν τον ανανεώνει.

- **DSS (Digital Signature Algorithm).**

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν τον επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α. Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

- **RC2, RC4, RC5**

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά απόθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές

για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

- **IDEA (International Data Encryption Algorithm)**

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο σε hardware όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτηταμε τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

- **Blowfish**

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια τηςύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

4.4 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

- RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p,q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε έναν

αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1)(q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό d, ώστε(ed-1) να διαιρείται από το (p-1)(q-1). Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα. Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα d από την δημόσια κλείδα e. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού n, δηλαδή των αριθμών p και q. Ο n είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς την κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στον χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = m^e \ mod \ n$, όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = c^d \ mod \ n$, όπου (n,d) η ιδιωτική κλείδα του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

4.5 Απλές Εφαρμογές της Κρυπτογραφίας

4.5.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση.

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου (privacy) μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα

δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στην δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση. Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου ότι οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

4.5.2 Εφαρμογές της Κρυπτογραφίας στην Πιστοποίηση Ταυτότητας και τις Ψηφιακές Υπογραφές.

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει πιστοποίηση ταυτότητας (authentication). Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων (integrity) και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας hash function και της ιδιωτικής κλείδας του αποστολέα.

- **Ψηφιακοί Φάκελοι (Digital Envelopes).**

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί.

Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με την δημόσια κλείδα της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

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

Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

4.6 Υποδομή Δημοσίου Κλειδιού

Ένα σημαντικό πρόβλημα που παρουσιάζεται στο ηλεκτρονικό εμπόριο και συγκεκριμένα στις ηλεκτρονικές συναλλαγές πληρωμής είναι η πιστοποίηση της ταυτότητας των οντοτήτων που λαμβάνουν μέρος στη συναλλαγή.

Σε μια συναλλαγή, τόσο ο πελάτης όσο και ο έμπορος πρέπει να είναι σε θέση να επιβεβαιώνουν την ταυτότητα του άλλου μέρους που λαμβάνει μέρος στη συναλλαγή. Δηλαδή πρέπει να μπορούν να επιβεβαιώνουν ότι το άλλο μέρος είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Η πρόσωπο με πρόσωπο ανθρώπινη συναλλαγή λύνει εύκολα αυτό το πρόβλημα, με οπτική αναγνώριση. Στις ηλεκτρονικές συναλλαγές, όμως, η πιστοποίηση δεν είναι τόσο απλή. Στις συναλλαγές μέσω διαδικτύου, η πιστοποίηση βασίζεται σε μια εφαρμογή της κρυπτογραφίας, τη «βεβαίωση». Η βεβαίωση αποτελεί ένα σχήμα σύμφωνα με το

οποίο έμπιστοι αντιπρόσωποι, όπως είναι οι αρχές πιστοποίησης, βεβαιώνουν την αυθεντικότητα αγνώστων αντιπροσώπων, ώστε αυτοί να θεωρούνται πλέον ως πιστοποιημένοι χρήστες. Η παραπάνω διαδικασία στηρίζεται στην έκδοση ψηφιακών πιστοποιητικών από την πλευρά των έμπιστων αντιπροσώπων. Η συγκεκριμένη τεχνική αναπτύχθηκε με στόχο να καταστεί δυνατή η διαδικασία της αναγνώρισης και πιστοποίησης σε μεγάλη κλίμακα.

Η κρυπτογραφία είναι στις μέρες μας κοινά αποδεκτή σαν το πλέον απαραίτητο εργαλείο ασφάλειας στο ηλεκτρονικό εμπόριο. Δύο σημαντικές εφαρμογές της κρυπτογραφίας είναι η κρυπτογράφηση και οι ψηφιακές υπογραφές. Η κρυπτογράφηση μπορεί να εξασφαλίσει ότι οι διακινούμενες πληροφορίες είναι εμπιστευτικές. Οι ψηφιακές υπογραφές βοηθούν στην επικύρωση της προέλευσης δεδομένων και επιβεβαιώνουν αν τα δεδομένα έχουν αλλοιωθεί. Περαιτέρω δυνατότητες προσφέρονται μέσω των υποδομών δημοσίου κλειδιού οι οποίες ενσωματώνουν ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα και αποδεικνύονται έτσι ικανές να υποστηρίξουν με ασφάλεια τις συναλλαγές ηλεκτρονικού εμπορίου που πραγματοποιούνται στο διαδίκτυο.

4.6.1 Πρωτόκολλα Πιστοποίησης Αυθεντικότητας

Πιστοποίηση αυθεντικότητας είναι η τεχνική με την οποία κάποιος πιστοποιεί ότι αυτός με τον οποίο επικοινωνεί είναι αυτός που πρέπει και όχι κάποιος άλλος.

Κατά την ίδρυση μιας συνόδου επικοινωνίας απαιτείται η αυθεντικοποίηση των ταυτοτήτων των επικοινωνούντων μελών, δηλαδή το κάθε μέλος αποδεικνύει την ταυτότητα του, προτού αρχίσει η ανταλλαγή πληροφοριών. Συγκεκριμένα στο ηλεκτρονικό εμπόριο είναι αναγκαίο να εξακριβωθεί η ταυτότητα του αποστολέα ενός ηλεκτρονικού εγγράφου. Όμως η εξακρίβωση της ταυτότητας μιας απομακρυσμένης οντότητας είναι αρκετά δύσκολη και απαιτεί σύνθετα πρωτόκολλα βασισμένα στην κρυπτογραφία.

Όταν ένας χρήστης επιθυμεί να εγκαταστήσει μια ασφαλή σύνδεση με ένα δεύτερο χρήστη, εκτελείται ένα πρωτόκολλο πιστοποίησης αυθεντικότητας και μόλις το πρωτόκολλο ολοκληρωθεί, ο κάθε χρήστης είναι σίγουρος για την ταυτότητα του άλλου.

Στα περισσότερα πρωτόκολλα εγκαθίσταται μεταξύ των δύο χρηστών ένα μυστικό κλειδί συνόδου (session key) για χρήση στην επερχόμενη συνομιλία. Στην πράξη, για λόγους απόδοσης, όλη η κίνηση δεδομένων κρυπτογραφείται χρησιμοποιώντας κρυπτογραφία μυστικού κλειδιού, ενώ η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται στα πρωτόκολλα πιστοποίησης αυθεντικότητας καθώς και για την κρυπτογράφηση των κλειδιών συνόδου.

Τα περισσότερα πρωτόκολλα πιστοποίησης αυθεντικότητας βασίζονται στην εξής αρχή: ο ένας χρήστης στέλνει στον άλλο ένα τυχαίο αριθμό, τον οποίο μετασχηματίζει με ένα ειδικό τρόπο και επιστρέφει το αποτέλεσμα. Τα πρωτόκολλα αυτά ονομάζονται πρωτόκολλα πρόκλησης-απόκρισης (challenge-response). Στη συνέχεια χρησιμοποιούνται οι εξής συμβολισμοί:

a, b: οι ταυτότητες των χρηστών A και B, αντίστοιχα.

Ri: οι προκλήσεις (τυχαίοι αριθμοί), όπου ο δείκτης συμβολίζει το χρήστη που προκαλεί.

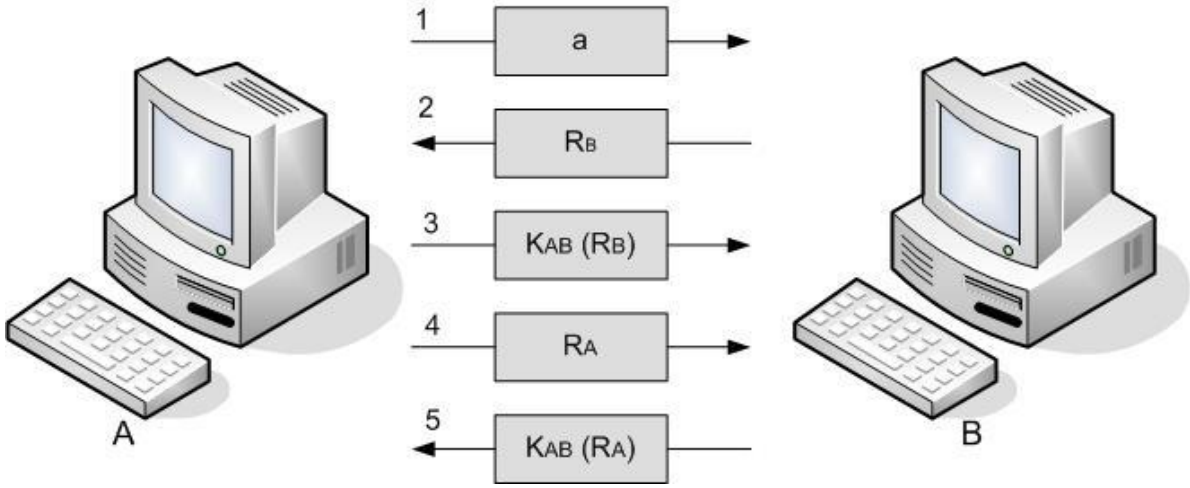
Ki: τα κλειδιά, όπου ο δείκτης συμβολίζει τον ιδιοκτήτη του κλειδιού.

Ks: το κλειδί συνόδου.

4.6.2 Πιστοποίηση Αυθεντικότητας Βασισμένη σε Μοιραζόμενο Μυστικό Κλειδί

Έστω δύο χρήστες, ο A και ο B, μοιράζονται ήδη ένα μυστικό κλειδί K_{AB}. Η συμφωνία για το μυστικό κλειδί μπορεί να επιτευχθεί μέσω τηλεφώνου ή με προσωπική συνάντηση των δύο χρηστών, αλλά σε καμιά περίπτωση μέσω του δικτύου.

Στο Σχήμα 6 φαίνεται η ακολουθία μηνυμάτων που ανταλλάσσουν οι δύο χρήστες μεταξύ τους.



Σχήμα 6: Αμφίδρομη πιστοποίηση αυθεντικότητας χρησιμοποιώντας ένα πρωτόκολλο πρόκλησης-απόκρισης.

Στο μήνυμα 1 ο χρήστης Α στέλνει την ταυτότητα του, a, στο χρήστη Β.

Ο χρήστης Β δε γνωρίζει αν το μήνυμα αυτό προέρχεται πράγματι από το χρήστη Α ή από έναν εισβολέα. Για αυτό επιλέγει μια πρόκληση, έναν μεγάλο τυχαίο αριθμό, R_B, και τον στέλνει στον Α ως μήνυμα 2.

Ο χρήστης Α κρυπτογραφεί το μήνυμα 2 με το κλειδί που μοιράζεται με τον Β και στέλνει το κρυπτογραφημένο κείμενο, $K_{AB}(R_B)$, στον Β ως μήνυμα 3. Όταν ο Β δει το κρυπτογραφημένο μήνυμα $K_{AB}(R_B)$, είναι σίγουρος ότι προέρχεται από τον Α, αφού κανείς άλλος δε γνωρίζει το κλειδί K_{AB}, και άρα κανείς δε θα μπορούσε να κατασκευάσει αυτό το μήνυμα εκτός από τον Α. Οπότε στο σημείο αυτό ο Β είναι σίγουρος ότι επικοινωνεί με τον Α.

Ο Α όμως, δεν γνωρίζει αν αυτός με τον οποίο επικοινωνεί είναι πράγματι ο Β. Ένας εισβολέας μπορεί να έχει υποκλέψει το μήνυμα 1 και να έχει στείλει αυτός το R_B. Για να μάθει ο Α με ποιον μιλάει, επιλέγει έναν μεγάλο τυχαίο αριθμό, R_A, και τον στέλνει στον Β ως μήνυμα 4.

Όταν ο Β απαντήσει με το $K_{AB}(R_A)$, ο Α γνωρίζει ότι μιλάει με τον Β. Στο σημείο αυτό ο Α μπορεί να επιλέξει ένα κλειδί συνόδου K_S και να το στείλει στον Β κρυπτογραφημένο με το K_{AB}.

4.6.3 Εγκατάσταση Μοιραζόμενου Κλειδιού

Στην προηγούμενη ενότητα οι δύο χρήστες μοιράζονταν ένα μυστικό κλειδί. Σε περίπτωση όμως που δύο χρήστες δεν έχουν μυστικό κλειδί και επιθυμούν να

επικοινωνήσουν με ασφάλεια μέσω του δικτύου, μπορούν να καθιερώσουν ένα τέτοιο κλειδί. Ένας τρόπος για να επιτευχθεί αυτό, θα ήταν να τηλεφωνήσει ο χρήστης Α στον Β και να του δώσει το κλειδί του. Αλλά στην περίπτωση αυτή ο Β δεν είναι σίγουρος ότι πρόκειται για τον Α και όχι για έναν εισβολέα. Θα μπορούσαν βέβαια να κανονίσουν από κοινού μια συνάντηση, όπου ο καθένας θα έφερνε το διαβατήριο του για πιστοποίηση της ταυτότητας του, συνήθως όμως κάτι τέτοιο δεν είναι γενικά εφικτό.

Υπάρχει ένα πρωτόκολλο που επιτρέπει σε δύο ξένους να επικοινωνήσουν με ασφάλεια εγκαθιστώντας ένα κοινό μυστικό κλειδί. Τα πρωτόκολλο αυτό ονομάζεται ανταλλαγή κλειδιού των Deffie-Hellman (Diffie-Hellman key exchange) και λειτουργεί ως εξής:

Οι χρήστες Α και Β έχουν συμφωνήσει σε δύο μεγάλους πρώτους αριθμούς n και g, όπου (n-1)/2 είναι επίσης πρώτος αριθμός. Οι αριθμοί αυτοί μπορεί να είναι δημόσιοι, έτσι είτε ο ένας χρήστης είτε ο άλλος μπορούν απλά να επιλέξουν τα n και g και να τα πουν στον άλλο ανοικτά.

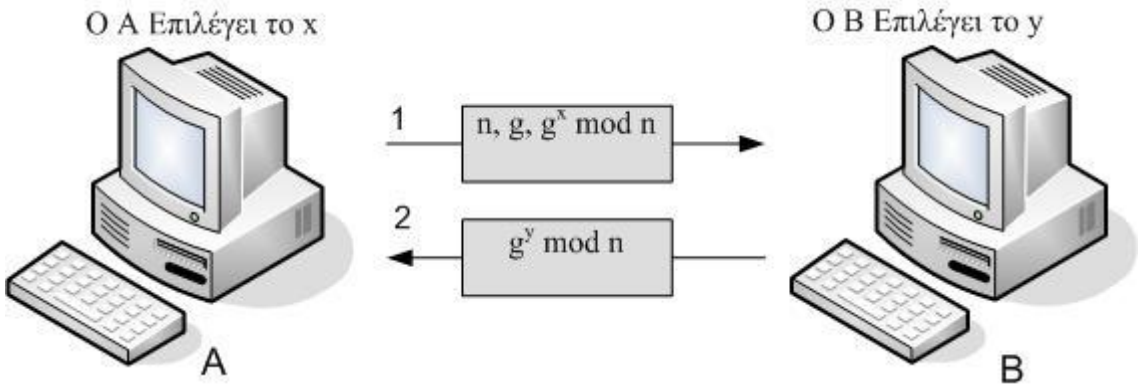
Στη συνέχεια ο Α επιλέγει ένα μεγάλο αριθμό, x, και τον κρατάει μυστικό. Όμοια ο Β επιλέγει ένα μεγάλο αριθμό, y.

Ο χρήστης Α ξεκινάει στέλνοντας στο Β ένα μήνυμα που περιέχει τους εξής αριθμούς (n, g, g^x mod n) , όπως δείχνει το Σχήμα .

Ο χρήστης Β απαντά στέλνοντας στον Α ένα μήνυμα που περιέχει τον αριθμό g^y mod n.

Ο Α υψώνει τον αριθμό που πήρε από τον Β στην x-οστή δύναμη και παίρνει τον όρο $(g^y \text{ mod } n)^x$.

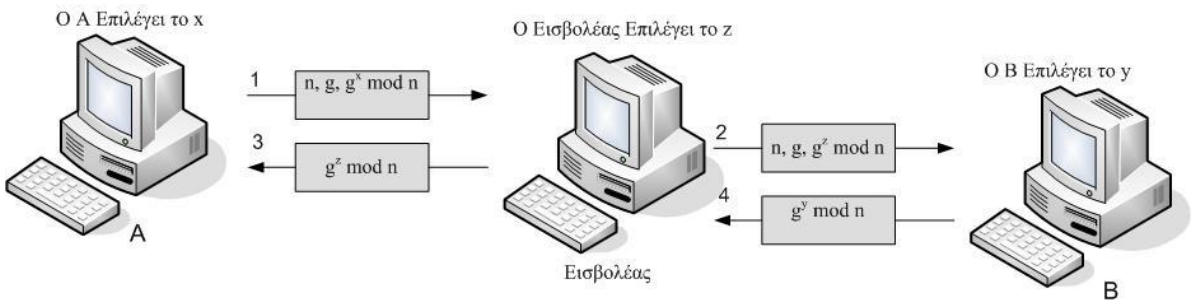
Ο χρήστης Β εκτελεί παρόμοια λειτουργία και παίρνει το $(g^x \text{ mod } n)^y$. Σύμφωνα με τους κανόνες της αριθμητικής modulo και οι δύο υπολογισμοί παράγουν το g^{xy} mod n. Έτσι ο Α και ο Β μοιράζονται τώρα το μυστικό κλειδί.



Σχήμα 7: Το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman.

Υπάρχει περίπτωση ένας εισβολέας να δει και τα δύο μηνύματα. Έτσι θα γνωρίζει τα n και g, όμως δε θα μπορεί να υπολογίσει τα x και y. Με δεδομένο μόνο το g^x mod n δε μπορεί να βρει το x. Δεν υπάρχουν πρακτικοί αλγόριθμοι για τον υπολογισμό διακριτών λογαρίθμων modulo.

Ο αλγόριθμος αυτός παρουσιάζει ένα μεγάλο πρόβλημα. Όταν ο χρήστης Β λαμβάνει την τριάδα (n, g, g^x mod n) δεν μπορεί να είναι σίγουρος ότι το μήνυμα αυτό προέρχεται από τον Α. Ένας εισβολέας μπορεί να εκμεταλλευτεί αυτό το γεγονός και να εξαπατήσει και τους δύο χρήστες Α και Β όπως φαίνεται στο Σχήμα 8: Ο Α στέλνει κανονικά το μήνυμα 1 που προορίζεται για τον Β. Ο εισβολέας υποκλέπτει το μήνυμα αυτό και στέλνει αντί αυτού στον Β το μήνυμα 2 (n, g, g^z mod n), όπου z είναι ο μυστικός αριθμός που επέλεξε ο εισβολέας. Επιπλέον ο εισβολέας στέλνει και ένα μήνυμα 3 πίσω στον Α. Αργότερα ο Β στέλνει το μήνυμα 4 προς τον Α, το οποίο ο εισβολέας επίσης υποκλέπτει και κρατάει.



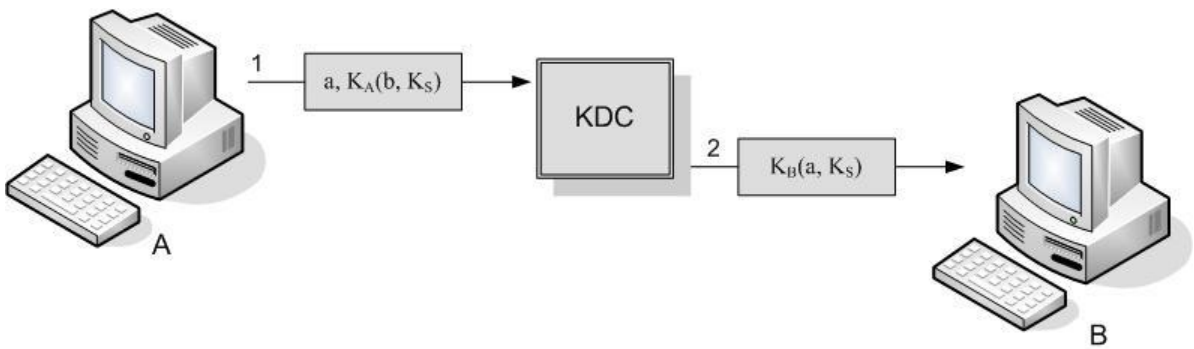
Σχήμα 8: Η επίθεση bucket brigade.

Έτσι ο Α υπολογίζει το μυστικό κλειδί g^{xz} mod n, το ίδιο κάνει και ο εισβολέας. Ο Β υπολογίζει το g^{yz} mod. Όμοια και ο εισβολέας. Οπότε ο Α νομίζει ότι μιλάει με τον Β και ο Β νομίζει ότι μιλάει με τον Α. Κάθε μήνυμα που στέλνεται από τον Α συλλαμβάνεται από τον εισβολέα, τροποποιείται και στη συνέχεια στέλνεται στον Β. Παρόμοια διαδικασία γίνεται για κάθε μήνυμα που στέλνεται από τον Β. Ο εισβολέας βλέπει τα πάντα και μπορεί να τροποποιεί όλα τα μηνύματα, ενώ οι χρήστες Α και Β έχουν την εντύπωση ότι έχουν ένα ασφαλές κανάλι επικοινωνίας. Η επίθεση αυτή ονομάζεται bucket brigade.

4.6.4 Πιστοποίηση Αυθεντικότητας με τη Χρήση Κέντρου Διανομής Κλειδιών

Σύμφωνα με την προηγούμενη ενότητα, για να επικοινωνήσει κάποιος με n άτομα χρειάζεται να έχει n κλειδιά. Για μεγάλο επικοινωνιακό φόρτο η διαχείριση κλειδιών είναι πρόβλημα.

Ένας διαφορετικός τρόπος προσέγγισης είναι η εισαγωγή ενός έμπιστου κέντρου διανομής κλειδιών (Key Distribution Center, KDC). Στο μοντέλο αυτό κάθε χρήστης έχει ένα απλό κλειδί το οποίο μοιράζεται με το κέντρο διανομής κλειδιών. Η πιστοποίηση αυθεντικότητας και η διαχείριση των κλειδιών συνόδου γίνεται με την μεσολάβηση του κέντρου διανομής κλειδιών. Το πρωτόκολλο αυτό παρουσιάζεται στο Σχήμα 9.



Σχήμα 9: Πιστοποίηση αυθεντικότητας με τη χρήση του κέντρου διανομής κλειδιών KDC.

Ο χρήστης Α επιλέγει ένα κλειδί συνόδου K_s, και λέει στο KDC ότι θέλει να μιλήσει στο χρήστη Β χρησιμοποιώντας το K_s. Το μήνυμα αυτό είναι

κρυπτογραφημένο με ένα μυστικό κλειδί K_A που μοιράζεται ο Α μόνο με το κέντρο διανομής κλειδιών (KDC).

Το κέντρο διανομής κλειδιών (KDC) αποκρυπτογραφεί το μήνυμα αυτό και εξάγει την ταυτότητα του Β και το κλειδί συνόδου. Στη συνέχεια κατασκευάζει ένα νέο μήνυμα που περιέχει την ταυτότητα του Α και το κλειδί συνόδου, το κρυπτογραφεί με το μυστικό κλειδί K_B που μοιράζεται με τον Β και το στέλνει στον Β.

Όταν ο Β αποκρυπτογραφήσει το μήνυμα, μαθαίνει ότι ο Α επιθυμεί να μιλήσει με αυτόν και επίσης γνωρίζει και το κλειδί συνόδου που ο Α θέλει να χρησιμοποιήσει. Με τον παραπάνω τρόπο η πιστοποίηση αυθεντικότητας πραγματοποιείται αξιόπιστα. Το κέντρο διανομής κλειδιών (KDC) γνωρίζει ότι το μήνυμα 1 προέρχεται από το χρήστη Α, εφόσον κανένας άλλος δεν είναι ικανός να το κρυπτογραφήσει με το μυστικό κλειδί του Α. Όμοια ο Β γνωρίζει ότι το μήνυμα 2 προέρχεται από το κέντρο διανομής κλειδιών (KDC), το οποίο εμπιστεύεται και επιπλέον κανένας άλλος δε γνωρίζει το μυστικό του κλειδί.

Το πρωτόκολλο αυτό παρουσιάζει ένα σημαντικό μειονέκτημα: Ένας εισβολέας μπορεί να αντιγράψει τα μηνύματα που αποστέλλονται μεταξύ των δύο χρηστών και να τα αναμεταδώσει. Το πρόβλημα αυτό ονομάζεται επίθεση επανάληψης (replay attack).

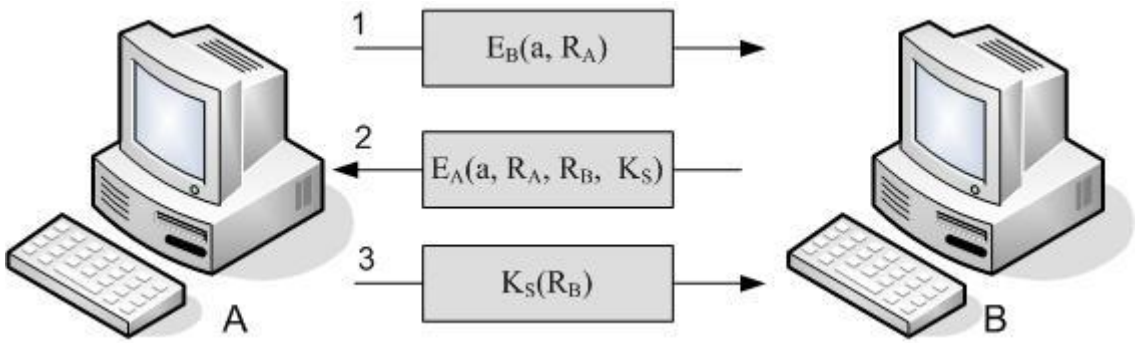
Μια λύση για το πρόβλημα αυτό είναι η τοποθέτηση χρονοσφραγίδας (timestamp) σε κάθε μήνυμα. Με αυτό τον τρόπο όταν κάποιος λάβει ένα παλιό μήνυμα μπορεί να το απορρίψει. Το πρόβλημα εδώ είναι ότι τα ρολόγια μέσα στο δίκτυο δεν είναι ποτέ συγχρονισμένα, έτσι υπάρχει σχεδόν πάντα κάποιο χρονικό διάστημα στο οποίο μια χρονοσφραγίδα θα παραμένει έγκυρη, ενώ δεν είναι. Ο εισβολέας μπορεί να επαναλάβει το μήνυμα κατά τη διάρκεια αυτού του διαστήματος.

Μια δεύτερη λύση είναι η τοποθέτηση ενός τυχαίου αριθμού nonce σε κάθε μήνυμα. Ο αριθμός αυτός είναι μοναδικός για κάθε μήνυμα. Ο χρήστης με αυτό τον τρόπο μπορεί να απορρίπτει κάθε μήνυμα που περιέχει ένα παλαιότερα χρησιμοποιούμενο nonce. Σε αυτή την προσέγγιση χρειάζεται μια λίστα που να αποθηκεύει όλα τα nonce για πάντα, γιατί κάποιος εισβολέας μπορεί να επιχειρήσει να επαναλάβει ένα μήνυμα που είχε σταλεί πριν από μεγάλο χρονικό διάστημα. Αυτή η λίστα συνεχώς θα μεγαλώνει δημιουργώντας πρόβλημα στην αποθήκευση της. Μπορούν βέβαια να συνδυαστούν οι χρονοσφραγίδες με τα

nonce, έτσι ώστε να υπάρχει όριο στα αποθηκευμένα nonce, αλλά με τον τρόπο αυτό το πρωτόκολλο γίνεται περισσότερο σύνθετο.

4.6.5 Πιστοποίηση Αυθεντικότητας με Χρήση Κρυπτογραφίας Δημοσίου Κλειδιού

Η πιστοποίηση της αμοιβαίας αυθεντικότητας μπορεί να επιτευχθεί και με τη χρήση κρυπτογραφίας δημοσίου κλειδιού. Δύο χρήστες, ο Α και ο Β, γνωρίζουν ο ένας το δημόσιο κλειδί του άλλου, και θέλουν να εγκαταστήσουν μια σύνοδο. Στη συνέχεια στη σύνοδο αυτή, θέλουν να χρησιμοποιήσουν κρυπτογραφία μυστικού κλειδιού που είναι πολύ γρηγορότερη σε σχέση με την κρυπτογραφία δημόσιου κλειδιού. Για το λόγο αυτό εκτελείται μια αρχική συναλλαγή όπου πιστοποιείται η αυθεντικότητα και των δύο πλευρών και επιπλέον καθορίζεται ένα κοινό μυστικό κλειδί συνόδου. Στο Σχήμα 10 φαίνονται τα μηνύματα που ανταλλάζουν οι δύο χρήστες για την περίπτωση αυτή.



Σχήμα 10: Πιστοποίηση αυθεντικότητας με χρήση κρυπτογραφίας δημοσίου κλειδιού.

Ο χρήστης Α ξεκινάει κρυπτογραφώντας την ταυτότητα του και ένα τυχαίο αριθμό R_A, χρησιμοποιώντας το δημόσιο κλειδί E_B του χρήστη Β.

Όταν ο Β λάβει το μήνυμα δε γνωρίζει αν προέρχεται από τον Α ή από κάποιον εισβολέα. Ο Β απαντάει στέλνοντας ένα μήνυμα που περιέχει τον R_A, ένα δικό του τυχαίο αριθμό R_B, και ένα προτεινόμενο κλειδί συνόδου K_S.Το μήνυμα αυτό, πριν το στείλει, το κρυπτογραφεί με το δημόσιο κλειδί E_A του Α.

Όταν ο Α πάρει το μήνυμα 2, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Μόλις δει τον R_A είναι σίγουρος ότι το μήνυμα προέρχεται από τον Β, διότι κανένας άλλος δε θα μπορούσε να αποκρυπτογραφήσει το μήνυμα 1 και να

καθορίσει τον R_A. Επιπλέον το μήνυμα πρέπει να είναι καινούργιο και όχι επανάληψη, εφόσον ο Α μόλις έστειλε στον Β τον R_A. Ο Α συμφωνεί για τη σύνοδο και στέλνει στον Β το μήνυμα 3.

Όταν ο Β δει το R_B κρυπτογραφημένο με το K_S καταλαβαίνει ότι σίγουρα ο Α πήρε το μήνυμα 2. Ένας εισβολέας δε μπορεί να κατασκευάσει το μήνυμα 3 εφόσον δε γνωρίζει ούτε το R_B ούτε το K_S και ούτε μπορεί να τα καθορίσει χωρίς το ιδιωτικό κλειδί του Α.

4.7 Ψηφιακές Υπογραφές

Η ανάπτυξη του Διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας, η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσομένων. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (μήνυμα ή κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα άτομα (εμπιστευτικότητα). Τα δεδομένα απαγορεύεται να αλλοιωθούν κατά τη μετάδοσή τους. Ο παραλήπτης θα πρέπει να λάβει τα δεδομένα που του στάλθηκαν, χωρίς αυτά να έχουν τροποποιηθεί στο ελάχιστο (ακεραιότητα). Σε μια τέτοια συναλλαγή, ο παραλήπτης πρέπει να είναι βέβαιος για την ταυτότητα του αποστολέα (αυθεντικότητα). Η συμμετοχή σε μία ηλεκτρονική συναλλαγή προϋποθέτει ότι τα εμπλεκόμενα μέρη δεν έχουν νόμιμο δικαίωμα να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

4.7.1 Η Έννοια της ψηφιακής υπογραφής.

Με τον όρο ηλεκτρονική υπογραφή δεν εννοούμε την αποτύπωση της ιδιόχειρης υπογραφής ούτε την μεταβίβασή της με ηλεκτρονικά μέσα, αλλά ένα ευρύτερο σύνολο μεθόδων υπογραφής για τον προσδιορισμό του συντάκτη του ηλεκτρονικού μηνύματος. Είναι μία μέθοδος τεκμηρίωσης με ηλεκτρονικά μέσα, που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις (εγγραφές δεδομένων σε μαγνητικά μέσα ηλεκτρονικού υπολογιστή, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής δεδομένων και της ηλεκτρονικής αλληλογραφίας), με σκοπό την διασφάλιση αφενός της γνησιότητας και της ακρίβειας του

περιεχομένου του ηλεκτρονικού εγγράφου και αφετέρου της εξατομίκευσης του εκδότη του εγγράφου αυτού. Για την δημιουργία και τις εφαρμογές της ηλεκτρονικής υπογραφής είναι δυνατόν να χρησιμοποιούνται σύγχρονες τεχνολογίες είτε υλικού (hardware) είτε λογισμικού (software) ηλεκτρονικών υπολογιστών, που επιλέγονται συνήθως από το πρόσωπο που επιδιώκει να αποκτήσει ηλεκτρονική υπογραφή, ώστε να προσδιορίζεται αξιόπιστα η ταυτότητά του στις ηλεκτρονικές συναλλαγές. Η ιδιόχειρη υπογραφή, που δεν είναι τεχνικά δυνατή στα ηλεκτρονικά έγγραφα, διότι λείπει η υλική ενσωμάτωση, υποκαθίσταται στην ηλεκτρονική επικοινωνία από την ηλεκτρονική υπογραφή. Υπάρχουν πολλοί τρόποι ηλεκτρονικής υπογραφής από την ατελέστερη μορφή των κωδικών (password) και των μυστικών κωδικών αριθμών (PIN) μέχρι τις πιο σύνθετες περιπτώσεις με χρήση κρυπτογραφικών ή βιομετρικών μεθόδων. Στην έννοια της ηλεκτρονικής υπογραφής περιλαμβάνεται και η ψηφιακή υπογραφή, η οποία δεν αποτελεί τίποτε περισσότερο από μία ασφαλή μέθοδο διαπίστωσης τόσο του εκδότη ηλεκτρονικού κειμένου, όσο και της γνησιότητας και του αναλλοίωτου αυτού.

Η ψηφιακή υπογραφή, όπως είδαμε, είναι μία μέθοδος κρυπτογράφησης ενός κειμένου, που εγγυάται την αυθεντικότητα και την μη αλλοίωση του κειμένου αυτού. Τα συστήματα παραγωγής ψηφιακής υπογραφής διαθέτουν τους κατάλληλους μηχανισμούς, ώστε να διασφαλίζεται ότι ένα έγγραφο είναι γνήσιο, ότι δημιουργήθηκε από τον υπογράφοντα και ενδεχομένως ότι ο χρόνος σύνταξης του εγγράφου είναι ο αναφερόμενος.

Τα κρυπτογραφικά συστήματα αποτελούνται από κρυπτογραφικούς αλγόριθμους, δηλαδή από ένα σύνολο μαθηματικών συναρτήσεων, που χρησιμοποιούνται στην κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Τα κυριότερα συστήματα κρυπτογράφησης είναι δύο: το συμμετρικό και το ασύμμετρο σύστημα κρυπτογράφησης. Το σύστημα που χρησιμοποιεί συμμετρικούς αλγόριθμους, όπως είναι το DES (Data Encryption Standard), διαθέτει το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, το οποίο είναι γνωστό τόσο στον αποστολέα όσο και στον παραλήπτη. Γι' αυτό το εν λόγω σύστημα είναι πρόσφορο για κλειστή ομάδα συναλλασσομένων και όχι για συναλλακτική επαφή με μεγάλο αριθμό συναλλασσομένων.

Το δεύτερο κρυπτογραφικό σύστημα, αυτό της ασύμμετρης κρυπτογράφησης,

χρησιμοποιεί ασύμμετρους αλγόριθμους (ασύμμετρη μέθοδος κρυπτογράφησης RSA). Για την θέση της ψηφιακής υπογραφής εφαρμόζεται ένας συνδυασμός δημοσίου και μυστικού κλειδιού.

Με την βοήθεια ενός ειδικού προγράμματος παράγεται καταρχάς μία σύντμηση του μεταβιβαζόμενου κειμένου, ένα είδος περίληψής του. Το συντμημένο αυτό κείμενο σφραγίζεται με το μυστικό κλειδί. Το μυστικό ιδιωτικό κλειδί είναι γνωστό μόνο στον αποστολέα του μηνύματος, ο οποίος το χρησιμοποιεί για την κρυπτογράφηση του μηνύματος. Το κλειδί αυτό αποθηκεύεται στον σκληρό δίσκο του υπολογιστή ή σε ειδική κάρτα ηλεκτρονικού υπολογιστή και ασφαλίζεται από τρίτους. Στην πράξη ασφαλίζεται συνήθως η κάρτα ηλεκτρονικού υπολογιστή με έναν αριθμό PIN. Ο συνδυασμός του μηνύματος με το μυστικό κλειδί αποτελεί την ψηφιακή υπογραφή του αποστολέα. Κατόπιν μεταδίδεται το κρυπτογραφημένο κείμενο στον παραλήπτη, ο οποίος το αποκρυπτογραφεί με την χρήση του δημοσίου κλειδιού του συντάκτη, το οποίο είτε αποστέλλεται στον παραλήπτη μαζί με το κρυπτογραφημένο κείμενο είτε ξεχωριστά είτε δημοσιεύεται σε έναν δημόσιο on line κατάλογο. Έτσι, ένα πρόγραμμα ελέγχου του παραλήπτη ξεκλειδώνει με το δημόσιο κλειδί το συντμημένο κείμενο και παράγει συγχρόνως μία δεύτερη σύντμηση του παραληφθέντος ηλεκτρονικού κειμένου. Αν τα δύο συντμημένα κείμενα είναι όμοια, πιστοποιείται η προέλευση του κειμένου από τον υπογράφοντα. Η ασύμμετρη κρυπτογραφική μέθοδος είναι προσφορότερη για τα ανοικτά δίκτυα, όπως το Ίντερνετ, ωστόσο δεν είναι κατάλληλη για μεταβίβαση εκτενών μηνυμάτων, επειδή είναι χρονοβόρα. Για τον λόγο αυτό για την αποστολή εκτενών μηνυμάτων ακολουθείται μία διαφορετική διαδικασία, κατά την οποία δημιουργείται πρώτα το «δακτυλικό αποτύπωμα» του κειμένου, εξάγεται δηλαδή το άθροισμα των bits, εκ των οποίων συγκροτείται το περιεχόμενο του κειμένου. Αυτό το «δακτυλικό αποτύπωμα» υπογράφεται στην συνέχεια, κρυπτογραφείται δηλαδή με την διαδικασία RSA. Ο αποστολέας κρυπτογραφεί έτσι την περίληψη του κειμένου αυτού μαζί με άλλα πρόσθετα δεδομένα, όπως ο τόπος και ο χρόνος της υπογραφής, με την χρήση του μυστικού κλειδιού. Ο παραλήπτης με την χρήση του δημόσιου κλειδιού αποκρυπτογραφεί το «δακτυλικό αποτύπωμα», ώστε να διαπιστώσει αν το περιεχόμενό του παρέμεινε αναλλοίωτο.

Άξιο αναφοράς είναι και το σύστημα του «ψηφιακού φακέλου», που αποτελεί συνδυασμό του συμμετρικού και του ασύμμετρου κρυπτογραφικού συστήματος.

Κατά το σύστημα αυτό κρυπτογραφείται το κείμενο από τον αποστολέα με έναν συμμετρικό αλγόριθμο και με την χρήση ενός σύντομου ασφαλούς κλειδιού, που καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και ονομάζεται γι' αυτό κλειδί συνεδρίας. Το κλειδί αυτό για ασφάλεια κρυπτογραφείται με έναν ασύμμετρο αλγόριθμο. Ο παραλήπτης του κειμένου πρέπει πρώτα να αποκρυπτογραφήσει το κλειδί συνεδρίας με το δημόσιο κλειδί και στην συνέχεια και το μήνυμα.

4.7.2 Η ψηφιακή υπογραφή ως υποκατάστατο της ιδιόχειρης υπογραφής στις ηλεκτρονικές συναλλαγές.

Για να θεωρηθεί η ψηφιακή υπογραφή ως υποκατάστατο της ιδιόχειρης, πρέπει να εξετασθεί αν αυτή πληρεί τις βασικές λειτουργίες της ιδιόχειρης υπογραφής, δηλαδή την αποδεικτική λειτουργία, την λειτουργία προσδιορισμού της ταυτότητας του εκδότη και την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου.

Η ψηφιακή υπογραφή δύναται να αναπληρώσει την ιδιόχειρη υπογραφή στις ηλεκτρονικές συναλλαγές, καθώς πληρεί τις βασικές λειτουργίες που πληρεί και η τελευταία, δηλαδή:

- την αποδεικτική λειτουργία, στο μέτρο που συμπεραίνεται ότι το έγγραφο προέρχεται από τον υπογράφοντα με την βοήθεια του πιστοποιητικού που παρέχεται από τους παρόχους υπηρεσιών πιστοποίησης. Λειτουργίες πιστοποίησης επιτελούν οι πάροχοι υπηρεσιών πιστοποίησης, οι οποίες υπηρεσίες συνίστανται στην επιβεβαίωση της αυθεντικότητας του ιδιοκτήτη και των χαρακτηριστικών ενός δημόσιου κλειδιού με την έκδοση ενός πιστοποιητικού, μίας ηλεκτρονικής βεβαίωσης σχετικά με την ταυτότητα ενός ατόμου. Το παρεχόμενο πιστοποιητικό πρέπει να περιλαμβάνει ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, τα στοιχεία αναγνώρισης του Παρόχου Υπηρεσιών Πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος, το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί, εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε

δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος, ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, τον κωδικό ταυτοποίησης του πιστοποιητικού, την προηγμένη ηλεκτρονική υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που το εκδίδει, τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού και τυχόν όρια στο ύψος των συναλλαγών, για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

β)την λειτουργία προσδιορισμού της ταυτότητας του εκδότη, καθόσον τα κλειδιά της ψηφιακής υπογραφής παρέχονται από τους Παρόχους Υπηρεσιών Πιστοποίησης σε συγκεκριμένα πρόσωπα, με τα οποία συνδέονται συμβατικά.

- την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου, καθώς με την διαδικασία επαλήθευσης της ψηφιακής υπογραφής είναι δυνατή η διαπίστωση της αλλοίωσης ή όχι του περιεχομένου του ηλεκτρονικού εγγράφου, και
- την εγγυητική λειτουργία, επειδή ο αποστολέας ενός ηλεκτρονικού εγγράφου με την ψηφιακή του υπογραφή αναλαμβάνει την ευθύνη για την γνησιότητα και την ακρίβεια του περιεχομένου του εγγράφου.

4.7.3 Υπογραφές με Κρυπτογραφία Μυστικού Κλειδιού

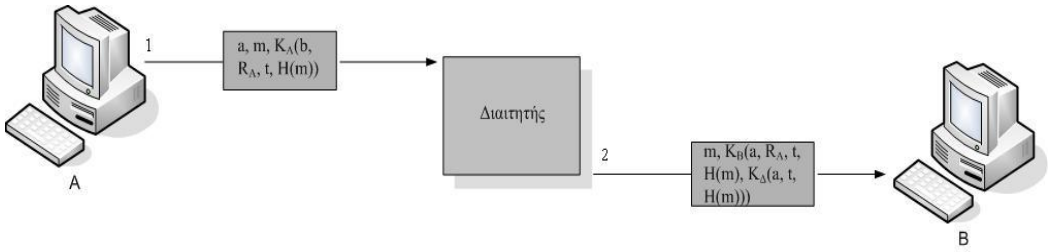
Στις υπογραφές με κρυπτογραφία μυστικού κλειδιού χρησιμοποιείται μια κεντρική εξουσία, η οποία υπογράφει και επιβεβαιώνει την ψηφιακή υπογραφή. Την εξουσία αυτή την ονομάζουμε «διαιτητή», διότι χρησιμοποιείται για να επιλύει διαφορές που μπορεί να προκύψουν. Ο διαιτητής γνωρίζει τα πάντα και τον εμπιστεύονται οι πάντες. Τονίζεται ότι η λειτουργία του όλου σχήματος βασίζεται στην εμπιστοσύνη που έχουν προς τον διαιτητή τα δύο μέρη που θέλουν να επικοινωνήσουν.

Υποθέτουμε πως ο χρήστης Α θέλει να επικοινωνήσει με τον χρήστη Β. Ο χρήστης Β με τη σειρά του θέλει κάποια μορφή εξασφάλισης σχετικά με την αυθεντικοποίηση της ταυτότητας του Α. Επίσης χρειάζεται να γνωρίζει, με κάποιο τρόπο, πως τα περιεχόμενα όλων των μηνυμάτων δεν έχουν μεταβληθεί (ακούσια ή εκούσια). Τέλος ο χρήστης Β θέλει ένα τρόπο εξασφάλισης των μηνυμάτων του

χρήστη Α ώστε να μην μπορεί κάποια στιγμή εκείνος να αρνηθεί το γεγονός ότι έχει στείλει τα συγκεκριμένα μηνύματα.

Κάθε χρήστης μοιράζεται ένα συμμετρικό κλειδί με τον διαιτητή. Το κλειδί αυτό το γνωρίζει μόνο ο συγκεκριμένος χρήστης και ο διαιτητής.

Όταν ο χρήστης Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο χρήστη Β, και δεν απαιτείται μυστικότητα, δηλαδή δεν ενδιαφέρει τον χρήστη Α αν το συγκεκριμένο μήνυμα διαβαστεί από κάποιον τρίτο, τότε εκτελείται η ακολουθία μηνυμάτων που απεικονίζεται στο Σχήμα 11.



Σχήμα 11: Ψηφιακές Υπογραφές χωρίς μυστικότητα.

Ο χρήστης Α υπολογίζει με χρήση ειδικού λογισμικού τη σύνοψη του μηνύματος m που θέλει να στείλει στον χρήστη Β, H(m). Στη συνέχεια δημιουργεί το K_A(b, R_A, t, H(m)), όπου με b παριστάνεται η ταυτότητα του Β, R_A είναι η πρόκληση από τον χρήστη Α και t μια χρονοσφραγίδα. Δηλαδή κρυπτογραφεί τη σύνοψη του μηνύματος H(m), και τα b, R_A, t, με το μυστικό κλειδί που μοιράζεται με τον διαιτητή. Έπειτα στέλλει στον διαιτητή την ταυτότητα του, a, το μήνυμα m σε καθαρή μορφή και το K_A(b, R_A, t, H(m)).

Όταν ο διαιτητής λάβει το μήνυμα 1, βλέπει ότι είναι από τον Α. Αποκρυπτογραφεί το μήνυμα 1 και στέλλει στον Β το μήνυμα 2. Το μήνυμα 2 περιέχει το μήνυμα m σε καθαρή μορφή και τα a, R_A, t, H(m), K_Δ (a, t, H(m)) κρυπτογραφημένα με το κλειδί K_B που μοιράζεται ο διαιτητής με τον Β. K_Δ είναι το κλειδί του διαιτητή.

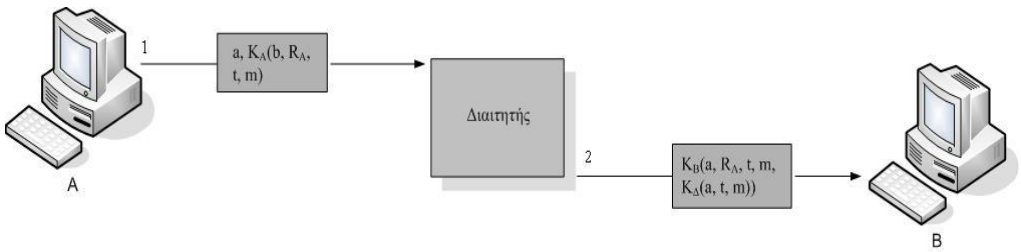
Ο Β μόλις λάβει το μήνυμα 2 υπολογίζει την σύνοψη μηνύματος εφαρμόζοντας στο μήνυμα m την ίδια συνάρτηση κατακερματισμού με τον αποστολέα, και ελέγχει αν αυτή είναι ίδια με την σύνοψη μηνύματος που περιέχεται κρυπτογραφημένη στο μήνυμα 2. Αν οι δύο συνόψεις ταυτίζονται, τότε το μήνυμα δεν τροποποιήθηκε από τη στιγμή που υπογράφηκε από τον διαιτητή και μετά.

Ο χρήστης Α δεν μπορεί να αργότερα να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα διότι ο Β έχει αποδείξεις: Είναι γνωστό ότι ο διαιτητής δεν μπορεί να

δεχθεί ένα μήνυμα από τον Α παρά μόνο αν αυτό είναι κρυπτογραφημένο με ΚΑ. Επιπλέον ο διαιτητής μόλις λάβει το μήνυμα 1 υπολογίζει την σύνοψη μηνύματος του m και ελέγχει αν αυτή είναι ίδια με την σύνοψη μηνύματος που περιέχεται κρυπτογραφημένη στο μήνυμα 1. Εφόσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά την αποστολή του, οι συνόψεις ταυτίζονται. Έτσι ο διαιτητής βεβαιώνει την αυθεντικότητα του μηνύματος και δεν υπάρχει πιθανότητα ένας εισβολέας να έστειλε στον διαιτητή ένα μήνυμα εκ μέρους του Α. Ο Β έχει ως αποδεικτικό στοιχείο για την ταυτότητα του Α το υπογεγραμμένο μήνυμα ΚΔ (a, t, H(m)), το οποίο προέρχεται από τον διαιτητή. Όταν ο διαιτητής, τον οποίο εμπιστεύονται όλοι, αποκρυπτογραφήσει το μήνυμα αυτό αποδεικνύετε ότι ο Α έστειλε κάποιο μήνυμα που έχει σύνοψη H(m) στον Β. Επιπλέον δεν μπορεί αργότερα ο Α να ισχυριστεί ότι έστειλε στον Β κάποιο άλλο μήνυμα με την ίδια σύνοψη H(m), διότι πρακτικά δεν υπάρχουν δύο διαφορετικά μηνύματα που να έχουν την ίδια σύνοψη μηνύματος.

Το πρωτόκολλο που περιγράφεται στο Σχήμα χρησιμοποιεί χρονοσφραγίδες για να αποτρέψει τυχόν επιθέσεις επανάληψης. Επιπλέον ο χρήστης Β μπορεί να ελέγχει όλα τα πρόσφατα μηνύματα ώστε να βλέπει αν το R_A χρησιμοποιήθηκε σε κάποιο από αυτά. Αν συμβαίνει κάτι τέτοιο το μήνυμα απορρίπτεται ως επανάληψη.

Όταν ο χρήστης Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο χρήστη Β, και απαιτείται μυστικότητα, δηλαδή ο χρήστης Α δε θέλει κανένας άλλος, εκτός από τον Β και τον διαιτητή, να διαβάσει το συγκεκριμένο μήνυμα, τότε εκτελείται η ακολουθία μηνυμάτων που απεικονίζεται στο Σχήμα 12.



Σχήμα 12: Ψηφιακές Υπογραφές με μυστικότητα.

Ο χρήστης Α δημιουργεί το $K_A(b, R_A, t, m)$, όπου m είναι το μήνυμα που θέλει να στείλει στον Β, και το στέλλει στον διαιτητή μαζί με την ταυτότητα του, a.

Όταν ο διαιτητής λάβει το μήνυμα 1, βλέπει ότι είναι από τον Α. Αποκρυπτογραφεί το μήνυμα 1 και στέλλει στον Β το μήνυμα 2. Το μήνυμα 2 περιέχει τα a, R_A, t, m,

K_{Δ} (a, t, m) κρυπτογραφημένα με το κλειδί K_B που μοιράζεται ο διαιτητής με τον Β.

Ο Β στη συνέχεια αποκρίνεται στην απαίτηση του Α.

Και σε αυτό το πρωτόκολλο ο χρήστης Α δεν μπορεί να αργότερα να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα διότι ο Β έχει τις ίδιες αποδείξεις με πριν.

Τα πρωτόκολλα ψηφιακής υπογραφής που απεικονίζονται στο Σχήμα και στο Σχήμα έχουν ουσιαστικά μόνο μια διαφορά: Στο πρωτόκολλο στο Σχήμα κρυπτογραφείται η σύνοψη του μηνύματος m, ενώ στο πρωτόκολλο στο Σχήμα κρυπτογραφείται το ίδιο το μήνυμα m. Το πρωτόκολλο που χρησιμοποιεί σύνοψη μηνύματος υπολογίζει πολύ πιο γρήγορα τις ψηφιακές υπογραφές σε σχέση με το πρωτόκολλο που χρησιμοποιεί κρυπτογραφία. Άρα εφόσον η κρυπτογραφία είναι μια αργή διαδικασία, στις περιπτώσεις που δεν απαιτείται μυστικότητα αλλά μόνο πιστοποίηση αυθεντικότητας, είναι προτιμότερο να χρησιμοποιείται το πρωτόκολλο που απεικονίζεται στο Σχήμα.

Με τα πρωτόκολλα αυτά (Σχήμα και Σχήμα) δύο χρήστες Α και Β μπορούν να επικοινωνούν μεταξύ τους χωρίς να χρειάζεται να μοιράζονται κάποιο κοινό κρυπτογραφικό κλειδί. Στις σημερινές εφαρμογές αυτό είναι αρκετά συνηθισμένο. Σε περίπτωση που δύο χρήστες θέλουν να επικοινωνήσουν, αλλά δεν υπάρχει αμοιβαία εμπιστοσύνη μεταξύ τους, το σχήμα αυτό μπορεί να δουλέψει αποτελεσματικά. Τα πρωτόκολλα αυτά μπορούν να χρησιμοποιηθούν και σε συναλλαγές ηλεκτρονικού εμπορίου, που λαμβάνουν χώρα στα πλαίσια ενός μεγάλου οργανισμού. Ο οργανισμός αυτός ελέγχει εταιρείες και χρήστες και τους δίνει την δυνατότητα να πραγματοποιούν ηλεκτρονικές συναλλαγές μεταξύ τους με βάση τα παραπάνω πρωτόκολλα. Στην περίπτωση αυτή ο χρήστης Α αντιπροσωπεύει τον αγοραστή, ο χρήστης Β τον πωλητή και ο ίδιος ο οργανισμός τον διαιτητή. Έτσι κάθε χρήστης-εταιρεία θα έχει ένα μυστικό κλειδί το οποίο θα γνωρίζει μόνο ο οργανισμός, και με το κλειδί αυτό θα μπορεί να κάνει ηλεκτρονικές συναλλαγές στα πλαίσια όμως του συγκεκριμένου οργανισμού.

4.7.4 Υπογραφές με Κρυπτογραφία Δημοσίου Κλειδιού

Ένα πρόβλημα που εμφανίζεται με τη χρήση κρυπτογραφίας μυστικού κλειδιού για τις ψηφιακές υπογραφές είναι ότι οι πάντες πρέπει να συμφωνήσουν ώστε να εμπιστεύονται μια συγκεκριμένη εξουσία, τον «διαιτητή». Επιπλέον ο διαιτητής

είναι σε θέση να διαβάζει όλα τα υπογεγραμμένα μηνύματα. Θα ήταν επομένως καλύτερα αν τα υπογεγραμμένα έγγραφα δεν απαιτούσαν μια έμπιστη κεντρική εξουσία. Η κρυπτογραφία δημοσίου κλειδιού μπορεί να αποτελέσει σημαντική συνεισφορά για τη λύση αυτού του προβλήματος.

Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής ψηφιακή υπογραφής. Η ψηφιακή υπογραφή αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι. Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί. Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να επιβεβαιώσει ότι το μήνυμα υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί. Εφόσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, μόνο αυτός θα μπορούσε να το χρησιμοποιήσει, για να υπογράψει κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό. Οπότε με την τεχνολογία της ασύμμετρης κρυπτογραφίας, διατηρώντας μυστικό το ένα κλειδί ως ιδιωτικό (δεδομένα δημιουργίας υπογραφής) και διανέμοντας ελεύθερα το άλλο κλειδί ως δημόσιο (δεδομένα επαλήθευσης υπογραφής), εξασφαλίζετε ότι όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να επαληθεύσουν μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού.

Συγκεκριμένα για να δημιουργηθεί μια ψηφιακή υπογραφή, απαιτούνται δύο βήματα:

1. Ο αποστολέας υπολογίζει με χρήση ειδικού λογισμικού μια σύνοψη H(m) του μηνύματος m.
2. Χρησιμοποιώντας το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη που προέκυψε. Η ασύμμετρα κρυπτογραφημένη σύνοψη μαζί με την πληροφορία προσδιορισμού του αλγόριθμου σύνοψης, αποτελεί την ψηφιακή υπογραφή του μηνύματος. Στη συνέχεια ο αποστολέας αποστέλλει αυτή τη ψηφιακή υπογραφή μαζί με το αρχικό μήνυμα στον παραλήπτη.

Το ιδιωτικό κλειδί του αποστολέα δεν χρησιμοποιείται για την κρυπτογράφηση του ίδιου του κειμένου, αλλά μόνο για τη δημιουργία της ψηφιακής υπογραφής, δηλαδή την κρυπτογράφηση της σύνοψης, η οποία επισυνάπτεται στα δεδομένα

που αποστέλλονται. Τα δεδομένα αυτά μπορεί να είναι είτε κρυπτογραφημένα, είτε μη κρυπτογραφημένα, ανάλογα με το επίπεδο μυστικότητας που είναι επιθυμητό. Ανεξαρτήτως πάντως της κρυπτογράφησης ή μη των δεδομένων, ο παραλήπτης μπορεί να συμπεράνει αν αυτά έχουν τροποποιηθεί και από πού αυτά προέρχονται, με τη βοήθεια του δημόσιου κλειδιού του αποστολέα. Συνολικά η επικύρωση της υπογραφής χρειάζεται τρία βήματα:

Το δημόσιο κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την αποκρυπτογράφηση της ψηφιακής υπογραφής και κατά συνέπεια της ανάκτησης της σύνοψης H(m) του αρχικού κειμένου m.

Ο παραλήπτης χρησιμοποιεί τον ίδιο αλγόριθμο κατακερματισμού με τον αποστολέα, για να παράγει μια σύνοψη του μηνύματος, όπως αυτό έχει φθάσει στα χέρια του.

Συγκρίνονται οι δύο συνόψεις, δηλαδή αυτή που δημιουργήθηκε από τον παραλήπτη, με αυτή που αποκρυπτογραφήθηκε στο πρώτο βήμα.

Οποιαδήποτε μεταβολή στα δεδομένα, θα έχει ως αποτέλεσμα τη διαφοροποίηση των συνόψεων. Με τον τρόπο αυτό ο παραλήπτης μπορεί να επιβεβαιώσει:

- Ότι τα δεδομένα δεν έχουν μεταβληθεί κατά τη διάρκεια της επικοινωνίας
- Ότι το δημόσιο και το ιδιωτικό κλειδί του αποστολέα είναι πράγματι ορθό ζεύγος.

Η επαλήθευση της οντότητας αποστολής και η ακεραιότητα των δεδομένων, αν και πολύ σημαντικά στοιχεία, δεν αποδεικνύουν υποχρεωτικά την ταυτότητα του ιδιοκτήτη του δημόσιου κλειδιού. Ο παραλήπτης του μηνύματος θέλει να είναι βέβαιος ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι. Ο οποιοσδήποτε θα μπορούσε να ζητήσει την έκδοση ενός ζεύγους κλειδιού υπό άλλο όνομα και στη συνέχεια να ανακοινώσει ότι το τάδε δημόσιο κλειδί είναι δικό του. Συνεπώς ο παραλήπτης θα πρέπει να διαθέτει περισσότερες και πραγματικά αξιόπιστες πληροφορίες για τον ιδιοκτήτη του κλειδιού. Η σημαντικότερη μέθοδος στην κατεύθυνση αυτή βασίζεται στην ύπαρξη μιας έμπιστης οντότητας που ονομάζεται Αρχή Πιστοποίησης (Certification Authority, CA) και εκδίδει ψηφιακά πιστοποιητικά (certificates).

Επιπρόσθετα στις υπογραφές αυτές, που χρησιμοποιούν κρυπτογραφία δημοσίου κλειδιού, ο παραλήπτης μπορεί να αποδείξει ότι ένα μήνυμα στάλθηκε από τον αποστολέα εφόσον το ιδιωτικό κλειδί του αποστολέα παραμένει μυστικό. Αν ο

αποστολέας αποκαλύψει το ιδιωτικό του κλειδί, ο καθένας θα μπορούσε να στείλει το συγκεκριμένο μήνυμα και έτσι ο παραλήπτης δε θα μπορεί να αποδείξει τίποτα. Υπάρχει όμως και το ενδεχόμενο ο αποστολέας να αποφασίσει να αλλάξει το κλειδί του. Κάτι τέτοιο είναι απόλυτα νόμιμο και συμβαίνει συχνά. Στην περίπτωση αυτή πάλι ο παραλήπτης δεν θα μπορεί να αποδείξει τίποτα, διότι θα έχει μια «παλιά ψηφιακή υπογραφή» που παράχθηκε με το παλιό κλειδί του αποστολέα. Επομένως φαίνεται και εδώ η ανάγκη ύπαρξης μιας αρχής που θα καταγράφει όλες τις αλλαγές κλειδιών και τις αντίστοιχες ημερομηνίες που έλαβαν χώρα οι αλλαγές.

4.8 Ψηφιακά Πιστοποιητικά (Certificates)

Η κρυπτογράφηση δημόσιου κλειδιού από μόνη της δεν μπορεί να εγγυηθεί την αυθεντικοποίηση των επικοινωνούντων μερών. Το μόνο που πραγματικά διασφαλίζει είναι ότι το δημόσιο και το ιδιωτικό κλειδί του αποστολέα είναι συμπληρωματικό ζευγάρι κλειδιών. Δεν υπάρχει καμιά εγγύηση για το ποιος είναι αυτός που κρατά το ιδιωτικό κλειδί. Ο παραλήπτης χρειάζεται σίγουρα κάποιες πιο αξιόπιστες πληροφορίες σχετικά με την ταυτότητα του ιδιοκτήτη του κλειδιού. Λύση στο πρόβλημα αυτό δίνει η ύπαρξη της Αρχής Πιστοποίησης (Certificate Authority, CA). Η CA είναι μια έμπιστη οντότητα η οποία εκδίδει πιστοποιητικά υπογεγραμμένα με το ιδιωτικό κλειδί της, τα οποία περιέχουν το όνομα και το δημόσιο κλειδί κάποιας οντότητας. Όταν ένας χρήστης θέλει να στείλει το δημόσιο κλειδί του σε κάποιον άλλο χρήστη, του στέλνει το πιστοποιητικό αυτό. Ο παραλήπτης του πιστοποιητικού, γνωρίζοντας το δημόσιο κλειδί της CA επιβεβαιώνει ότι το πιστοποιητικό είναι πράγματι υπογεγραμμένο από τη CA, άρα το δημόσιο κλειδί πρέπει όντως να είναι του συγκεκριμένου αποστολέα. Συνεπώς δεν είναι απαραίτητο ένας χρήστης να γνωρίζει τα δημόσια κλειδιά όλων των άλλων χρηστών. Αρκεί να γνωρίζει τα δημόσια κλειδιά κάποιων αρχών πιστοποίησης (CA) ώστε να είναι σε θέση να επιβεβαιώσει τη γνησιότητα των πιστοποιητικών που είναι υπογεγραμμένα από αυτές.

Η διαδικασία αυτής της αντιστοίχησης και δέσμευσης ενός δημόσιου κλειδιού σε μια οντότητα, καλείται πιστοποίηση (certification). Κατ' αναλογία, καλούνται πιστοποιητικά δημόσιου κλειδιού (public key certificates) ή απλά πιστοποιητικά,

τα ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση μιας οντότητας και τη συσχέτιση της με ένα δημόσιο κλειδί. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης, CA.

Τα πιστοποιητικά αυτά είναι τυποποιημένες ηλεκτρονικές βεβαιώσεις που εκδίδονται και υπογράφονται ηλεκτρονικά από την Αρχή Πιστοποίησης με σκοπό να πιστοποιήσουν την κατοχή συγκεκριμένου ζεύγους (ασύμμετρων) κρυπτογραφικών κλειδιών από ένα υποκείμενο και να περιγράψουν στοιχεία ταυτοποίησης του υποκειμένου αυτού. Επιτρέπουν δηλαδή την επαλήθευση του ισχυρισμού ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με τη χρήση ψεύτικου κλειδιού.

Ένα ψηφιακό πιστοποιητικό είναι μια δομή δεδομένων η οποία περιέχει:

- Το όνομα και πληροφορίες αναγνώρισης του υποκειμένου του πιστοποιητικού.
- Το δημόσιο κλειδί του υποκειμένου, δηλαδή του κατόχου του πιστοποιητικού (public key).
- Ένα μοναδικό αριθμό (serial number).
- Το όνομα της CA, δηλαδή της εκδότριας αρχής (issuer) του πιστοποιητικού.
- Την ψηφιακή υπογραφή της CA και τον αλγόριθμο (signature algorithm) που χρησιμοποιήθηκε.
- Την ημερομηνία έκδοσης (valid from) και λήξης (valid to) της ισχύος του πιστοποιητικού.

Η λειτουργία των πιστοποιητικών είναι απλοϊκή παρότι οι χρήσεις τους είναι εκτεταμένες και η παραγωγή τους στηρίζεται σε πολύπλοκες τεχνικές. Οργανισμοί πιστοποίησης αναλαμβάνουν να εκδώσουν πιστοποιητικό για ένα φορέα, ελέγχοντας την ορθότητα των στοιχείων του. Το πιστοποιητικό μεταφέρεται συνήθως μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής, ο παραλήπτης πρέπει να έχει το σωστό δημόσιο κλειδί του αποστολέα. Επίσης το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση του δημόσιου κλειδιού κάθε πλευράς στην άλλη πλευρά και για την χρήση του στην κρυπτογράφηση της επικοινωνίας. Το

πιστοποιητικό δε χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μια συναλλαγή. Αρκεί να σταλεί μια φορά κατά την έναρξη της σύνδεσης.

Υπάρχουν δύο είδη πιστοποιητικών:

1) Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.
2) Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοση τους. Κατά την προσπάθεια σύνδεσης με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Λόγω της διαρκούς τεχνολογικής εξέλιξης, θεωρείται δεδομένη η εξασθένηση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών στο πέρασμα του χρόνου. Έτσι τα πιστοποιητικά δημοσίου κλειδιού που αναφέρονται σε τέτοια κρυπτογραφικά κλειδιά, εκδίδονται με προκαθορισμένη διάρκεια ισχύος (συνήθως από 1 έως 3 έτη), η οποία και αναγράφεται μέσα στα προκαθορισμένα για τον σκοπό αυτό πεδία τους.

4.8.1 Το Πιστοποιητικό X.509

Το πιο διαδεδομένο διεθνώς πρότυπο για τη σύνταξη ενός ψηφιακού πιστοποιητικού είναι το X.509 το οποίο αποτελεί Σύσταση (Recommendation) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Το πρότυπο X.509 διαθέτει αρκετά προκαθορισμένα πεδία για την αναγραφή των απαραίτητων πληροφοριών

(εκδότης, δημόσιο κλειδί υποκειμένου, διάρκεια ισχύος, κ.α.), καθώς και τη δυνατότητα να συμπεριλάβει επιπλέον εκτεταμένα πεδία (extensions) που καθορίζονται από τον εκδότη των πιστοποιητικών.

Το πρότυπο αυτό χρησιμοποιείται de facto στις περισσότερες εφαρμογές που κάνουν χρήση ψηφιακών πιστοποιητικών. Η Netscape υιοθέτησε το X.509 πρότυπο για την έκδοση των πιστοποιητικών που χρησιμοποιούνται στο Sockets Layer Protocol (SSL) πρωτόκολλο.

Τα πεδία του προτύπου X.509 φαίνονται στον Πίνακας 1.

Όνομα Πεδίου	Χρήση
Version	Η έκδοση του προτύπου X.509. Ορίζονται 3 εκδόσεις του X.509. Η έκδοση 1 δεν περιέχει τα πεδία issuer unique identifier, subject unique identifier τα οποία προστέθηκαν στην έκδοση 2, καθώς και το πεδίο extensions το οποίο προστέθηκε στην έκδοση 3.
serial number	Ένας μοναδικός ακέραιος που καθορίζεται από την Αρχή Πιστοποίησης για να αναγνωρίσει το πιστοποιητικό.
signature algorithm identifier	Το πεδίο αυτό αποτελείται στην ουσία από 2 πεδία, τα ονόματα των κρυπτογραφικών συναρτήσεων που συμμετέχουν, καθώς και από τις σχετικές παραμέτρους αυτών.
issuer name	Το όνομα της Αρχής Πιστοποίησης

period of validity	Αποτελείται από δύο ημερομηνίες, από την ημερομηνία ενεργοποίησης του πιστοποιητικού και από την ημερομηνία λήξης του πιστοποιητικού.
subject name	Το όνομα της οντότητας που πιστοποιείται.
algorithms	Το όνομα του κρυπταλγόριθμου που χρησιμοποιεί η οντότητα για να διαθέσει το δημόσιο κλειδί της.
parameters	Οι σχετικές παράμετροι που προσδιορίζουν τη λειτουργία του παραπάνω κρυπταλγόριθμου.
subject's public key	Το δημόσιο κλειδί της οντότητας που αναγνωρίζεται από το πεδίο subject name. Η οντότητα αυτή κατέχει το ιδιωτικό κλειδί.
issuer unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της Αρχής Πιστοποίησης για να ενισχύσει την αναγνώριση αυτής.
subject unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της οντότητας για να προσδώσει μοναδικότητα στο πιστοποιητικό, σε περίπτωση που το όνομα της οντότητας χρησιμοποιείται και για άλλο πιστοποιητικό.

extensions	Εδώ μπορούν να προστεθούν επιπλέον στοιχεία για να υποστηρίξουν ειδικές απαιτήσεις της εφαρμογής.
signature	Η ψηφιακή υπογραφή με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης επάνω σε όλες τις προαναφερθείσες πληροφορίες

Πίνακας 1: Πεδία του πιστοποιητικού X.509.

Η έκδοση ενός πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών, περιορίζεται σε συγκεκριμένες επιτρεπόμενες χρήσεις, οι οποίες προσδιορίζονται και από το σχετικό πεδίο subject unique identifier των πιστοποιητικών X.509 το οποίο δέχεται συγκεκριμένες προκαθορισμένες τιμές. Έχει επικρατήσει, τουλάχιστον στις περισσότερες σχετικές εφαρμογές στην Ευρώπη, να εκδίδεται σε ένα υποκείμενο ένα ξεχωριστό αναγνωρισμένο πιστοποιητικό για το ζεύγος κρυπτογραφικών κλειδιών που θα χρησιμοποιεί αποκλειστικά για τη δημιουργία αναγνωρισμένων υπογραφών με έννομες συνέπειες σε ηλεκτρονικά έγγραφα (με την ένδειξη μη αποκήρυξη – Non Repudiation) και ένα δεύτερο πιστοποιητικό (για άλλο ζεύγος κλειδιών) το οποίο θα χρησιμοποιείται για υπογραφές αυθεντικότητας δεδομένων ή και για υπογραφές ταυτοποίησης (με την ένδειξη Ψηφιακή Υπογραφή – Digital Signature). Στο δεύτερο αυτό πιστοποιητικό μπορούν να παρασχεθούν και δυνατότητες χρήσης των κλειδιών για απλή κρυπτογράφηση δεδομένων (με την πρόσθετη ένδειξη Κρυπτογράφηση κλειδιών-δεδομένων-Key/ Data Encipherment), αν και συνίσταται η χρήση τρίτου ξεχωριστού ζεύγους κλειδιών και αντίστοιχου πιστοποιητικού για τις εφαρμογές κρυπτογράφησης.

4.8.2 Υποδομή Δημοσίου Κλειδιού

Για να λειτουργήσει αποτελεσματικά η διαδικασία έκδοσης, υπογραφής και δημοσίευσης των ψηφιακών πιστοποιητικών είναι απαραίτητη μια υποδομή. Χωρίς την υποδομή αυτή είναι αμφίβολο αν οι κάτοχοι ψηφιακών πιστοποιητικών που

χρησιμοποιούν άλλους αλγόριθμους και πρότυπα (δηλαδή εκδίδονται από διαφορετικούς οργανισμούς) θα μπορούν να επικοινωνούν με ασφάλεια (security) και σιγουριά (assurance). Η υποδομή αυτή ονομάζεται Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure, PKI).

Η Υποδομή Δημοσίου Κλειδιού είναι ένας συνδυασμός λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που επιβεβαιώνουν και πιστοποιούν την εγκυρότητα της κάθε οντότητας που εμπλέκεται σε μια συναλλαγή με το Διαδίκτυο, και μπορούν να υποστηρίξουν με ασφάλεια τις συναλλαγές ηλεκτρονικού εμπορίου.

Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, σε εξυπηρετητές, σε λογισμικό χρηστών, καθώς επίσης και εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών αυτών.

Υπάρχουν οι κάποιες βασικές λειτουργίες – υπηρεσίες που είναι κοινές σε όλες τις Υποδομές Δημοσίου Κλειδιού και περιγράφονται παρακάτω:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημοσίου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ψηφιακές υπογραφές.

Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η κρυπτογραφία παρέχει ψηφιακές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο

οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Η Υποδομή Δημοσίου Κλειδιού έχει σκοπό τη διασφάλιση από κάθε πλευρά (Εμπιστευτικότητα, Ακεραιότητα, Μη Άρνηση Αποδοχής, Πιστοποίηση) των επικοινωνιών και των συναλλαγών στο Internet. Συγκεκριμένα η Υποδομή Δημοσίου Κλειδιού μπορεί να:

- επιτρέπει την ασφαλή επικοινωνία ανάμεσα σε οντότητες που δεν έχουν καμιά προηγούμενη γνωριμία ή εμπειρία μεταξύ τους.
- «δένει» μια οντότητα με ένα δημόσιο κλειδί, προσδίδοντας έτσι μια μορφή εμπιστοσύνης.
- χρησιμοποιεί ψηφιακά πιστοποιητικά.
- υποστηρίζει όλα τα γνωστά πρότυπα (standards) και είναι συμφωνημένη με την ισχύουσα νομοθεσία.

Η Υποδομή Δημοσίου Κλειδιού παρέχει το πλαίσιο μέσα στο οποίο εφαρμογές μπορούν να αναπτυχθούν και να λειτουργήσουν με ασφάλεια. Παραδείγματα τέτοιων εφαρμογών είναι η ασφαλής επικοινωνία μεταξύ των προγραμμάτων πλοήγησης και των εξυπηρετητών Web, οι συναλλαγές ηλεκτρονικού εμπορίου στο Internet, το ηλεκτρονικό ταχυδρομείο, η Ηλεκτρονική Ανταλλαγή Δεδομένων, κλπ.

4.8.3 Πάροχοι Υπηρεσιών Πιστοποίησης (ΠΥΠ)

Μια Υποδομή Δημοσίου Κλειδιού περιλαμβάνει έναν ή περισσότερους Πάροχους Υπηρεσιών Πιστοποίησης (ΠΥΠ). Οι Πάροχοι Υπηρεσιών Πιστοποίησης (Certification Service Providers - CSP) παλαιότερα αποκαλούνταν Έμπιστες Τρίτες Οντότητες (Trusted Third Parties – TTP), αλλά σήμερα στη βιβλιογραφία αναφέρονται ως ΠΥΠ αφού εκδίδουν, υπογράφουν, δημοσιεύουν και υποστηρίζουν τυποποιημένες ηλεκτρονικές βεβαιώσεις (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών τους.

Οι ΠΥΠ παρέχουν τεχνική αλλά και νομική υποστήριξη για θέματα που σχετίζονται με την παραγωγή και διανομή των απαιτούμενων διακριτικών διασφάλισης και επαλήθευσης μιας ηλεκτρονικής δοσοληψίας. Το βασικό έργο των ΠΥΠ είναι η άρτια οργάνωση των μηχανισμών διαχείρισης πιστοποιητικών. Οι ΠΥΠ είναι οντότητες-φορείς που πρωταρχικό σκοπό έχουν να πιστοποιούν τεχνικά και νομικά την αντιστοίχηση της ταυτότητας μιας οντότητας με ένα δημόσιο κλειδί το οποίο περιέχεται σε ένα πιστοποιητικό. Ουσιαστικά οι ΠΥΠ δραστηριοποιούνται για την παραγωγή, αποθήκευση, αποστολή και ανάκληση πιστοποιητικών για την υποβοήθηση στην επίτευξη ασφαλών ηλεκτρονικών επικοινωνιών.

Όπως αναφέρθηκε και προηγουμένως, η Αρχή Πιστοποίησης είναι αυτή που εκδίδει και υπογράφει τα ψηφιακά πιστοποιητικά. Ουσιαστικά μια Αρχή Πιστοποίησης λειτουργεί στα πλαίσια ενός ΠΥΠ.

Στα πλαίσια λειτουργίας του ένας ΠΥΠ περιλαμβάνει τα εξής:

Αρχή Πιστοποίησης (Certification Authority, CA): Η Αρχή Πιστοποίησης αποτελεί ένα έμπιστο τμήμα του οργανισμού ΠΥΠ και η λειτουργία της είναι η έκδοση και υπογραφή των τελικών πιστοποιητικών των υποκειμένων. Η ακεραιότητα λειτουργίας του ΠΥΠ συγκεντρώνεται στην CA.

Αρχή Εγγραφής (Registration Authority, RA). Η Αρχή Έγγραφής, ουσιαστικά παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ ενός χρήστη και του ΠΥΠ. Είναι το τμήμα του οργανισμού που είναι υπεύθυνο για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ταυτότητας ή του ρόλου ενός χρήστη ή μιας οντότητας όπως μιας εφαρμογής ή ενός εξυπηρετητή. Η RA προωθεί προς τη CA τις έγκυρες υποβληθείσες προς αυτήν αιτήσεις για τη δημιουργία των αντίστοιχων πιστοποιητικών.

Υπηρεσία Διαχείρισης Αιτημάτων Ανάκλησης (Revocation Management Service): Η υπηρεσία αυτή υποδέχεται, ελέγχει (σε συνεργασία με την Αρχή Εγγραφής) και διεκπεραιώνει τα αιτήματα - σε 24ωρη βάση, 7 μέρες την εβδομάδα – για ανάκληση, παύση ή επανεργοποίηση των πιστοποιητικών, συνεργαζόμενη με την Αρχή Πιστοποίησης για την κατάλληλη ψηφιακή υπογραφή των σχετικών εκδιδόμενων Λιστών Ανακληθέντων Πιστοποιητικών (Certificate Revocation Lists, CRL).

Υπηρεσία Δημοσίευσης (Dissemination & Revocation Status Service). Η υπηρεσία αυτή αναλαμβάνει τη δημοσίευση των Καταλόγων και των Λιστών Ανακληθέντων Πιστοποιητικών, καθώς και σχετικές ενημερώσεις ή κοινοποιήσεις προς τους συνδρομητές του ΠΥΠ.

Εκτός από τις παραπάνω υποχρεωτικές υπηρεσίες, οι οποίες προβλέπονται έμμεσα από τα σχετικά νομοτεχνικά πρότυπα, ένας ΠΥΠ μπορεί επίσης να παρέχει (προαιρετικά) και Υπηρεσίες Προμήθειας-Προετοιμασίας Φορέα (π.χ. έξυπνη κάρτα) για τους συνδρομητές (Subject Device Provision Service), Υπηρεσίες Χρονοσήμανσης ηλεκτρονικών εγγράφων (Time-Stamping Authority – TSA), Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων (Attribute Authority), Υπηρεσίες Ασφαλούς Αρχειοθέτησης εγγράφων (καλούμενες συχνά και ως Notary Services) κλπ.

Είναι επιτρεπτό για έναν ΠΥΠ να εκχωρεί σε τρίτους τη διεκπεραίωση μέρους ή ακόμη και του συνόλου των παραπάνω υπηρεσιών του. Εφόσον όμως ο ΠΥΠ εξακολουθεί να αναγράφεται στα εκδιδόμενα πιστοποιητικά ως Εκδότης, τότε διατηρεί ακέραια την ευθύνη του έναντι των τρίτων για οποιαδήποτε πράξη ή παράλειψη προξενεί ζημιά σε συνδρομητές.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των ΠΥΠ που είναι εγκατεστημένοι στην Ελλάδα.

Στα πλαίσια της λειτουργίας ενός ΠΥΠ απαιτείται η ανάπτυξη και δημοσίευση δύο βασικών κειμένων: της Πολιτικής Πιστοποιητικών και της Δήλωσης Πρακτικών Πιστοποίησης:

Η **Πολιτική Πιστοποιητικών** (Certificate Policy – CP) είναι ένα σύνολο συγκεκριμένων κανόνων οι οποίοι εξασφαλίζουν την εφαρμοσιμότητα ενός πιστοποιητικού. Περιλαμβάνει όλους τους ειδικότερους όρους έκδοσης και χρήσης που καθορίζει ο ΠΥΠ για τα ψηφιακά πιστοποιητικά. Όταν μια Αρχή Πιστοποίησης εκδίδει ένα πιστοποιητικό, ουσιαστικά δηλώνει προς το χρήστη του πιστοποιητικού ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί σε μια συγκεκριμένη οντότητα. Παρόλα αυτά, το όριο αποδοχής αυτής της διαβεβαίωσης της Αρχή Πιστοποίησης από το χρήστη πρέπει να αποτιμάται από αυτόν ανάλογα με το σκοπό και τις εφαρμογές που αυτό το πιστοποιητικό θα χρησιμοποιηθεί. Για παράδειγμα ένα πιστοποιητικό X.509 μπορεί να περιέχει ένα δείκτη προς μια

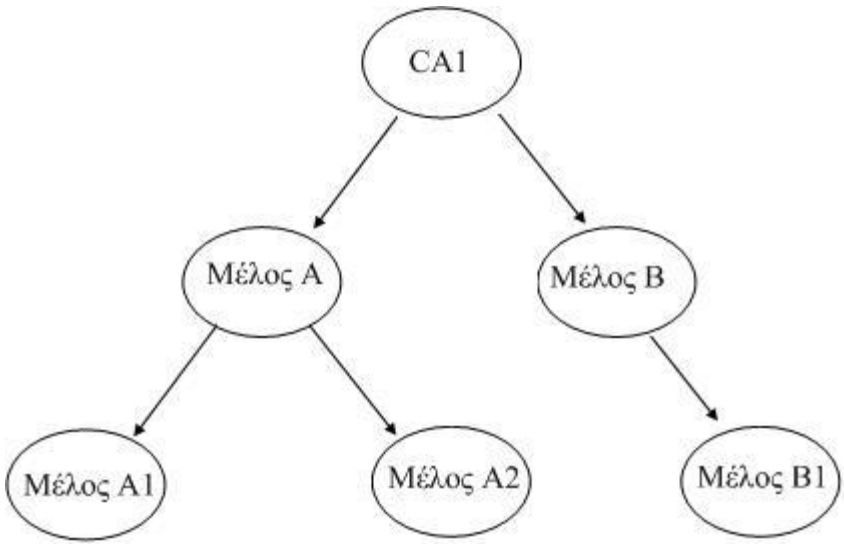
Πολιτική Πιστοποιητικών και ο δείκτης αυτός μπορεί να χρησιμοποιηθεί από το χρήστη για τη λήψη απόφασης αν πρέπει να εμπιστευθεί το συγκεκριμένο πιστοποιητικό για κάποιο συγκεκριμένο σκοπό. Η Πολιτική Πιστοποίησης πρέπει να είναι αποδεκτή τόσο από το δημιουργό ΠΥΠ όσο και από το χρήστη του πιστοποιητικού.

Η **Δήλωση Πρακτικών Πιστοποίησης** (Certification Practice Statement – CPS) είναι μια δήλωση όπου καταγράφονται οι πρακτικές που ακολουθεί μια Αρχή Πιστοποίησης για τη διαχείριση των πιστοποιητικών. Αποτελεί ένα λεπτομερέστατο έγγραφο, όπου αναφέρεται ο τρόπος διεκπεραίωσης των λειτουργικών διαδικασιών των συστημάτων που υποστηρίζουν υπηρεσίες ασφάλειας, οι ακολουθούμενες πρακτικές, καθώς και οι ενέργειες διανομής των πιστοποιητικών. Μια Δήλωση Πρακτικών Πιστοποίησης πρέπει να περιλαμβάνει λεπτομέρειες για τις ακολουθητέες διαδικασίες του κύκλου ζωής δημιουργίας και διαχείρισης πιστοποιητικών.

4.8.4 Μοντέλα Εμπιστοσύνης

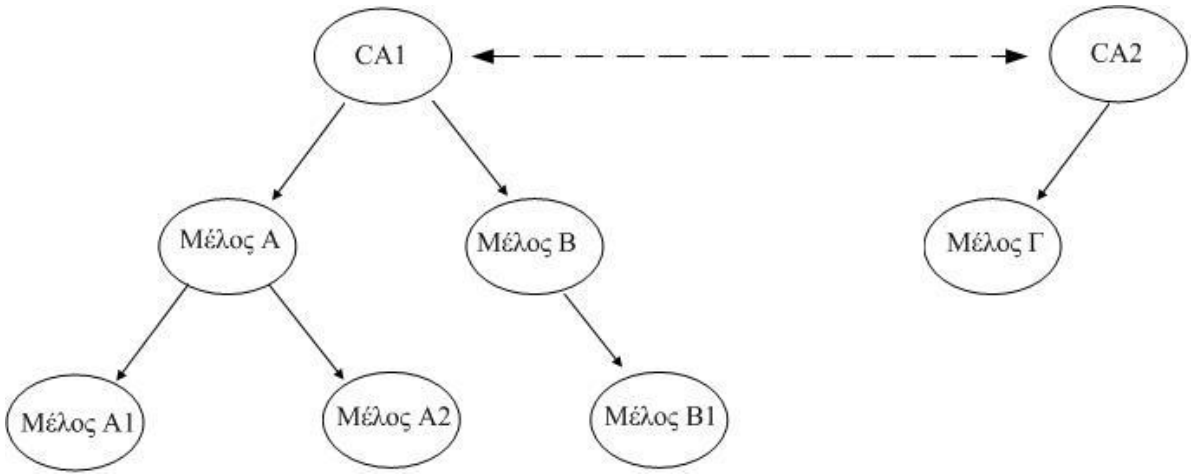
Τα μοντέλα εμπιστοσύνης καθορίζουν τους τρόπους με τους οποίους αλληλεπιδρούν οι οντότητες προκειμένου να διαπιστώσουν την εγκυρότητα ενός πιστοποιητικού. Μια Αρχή Πιστοποίησης μπορεί να δημιουργήσει ένα πιστοποιητικό για κάποιο μέλος, αλλά και το μέλος με τη σειρά του μπορεί να εγγυηθεί για κάποιο άλλο μέλος, δημιουργώντας πιστοποιητικό. Στο δέντρο που απεικονίζεται στο Σχήμα 13 φαίνεται ένα παράδειγμα όπου η Αρχή Πιστοποίησης (CA1) έχει πιστοποιήσει το μέλος Α και Β. Όλα τα πιστοποιητικά που έχουν εκδοθεί από την Αρχή Πιστοποίησης είναι αποδεκτά από όλα τα μέλη που συμμετέχουν στο PKI. Το μέλος Α αναλαμβάνει να πιστοποιήσει τα μέλη Α1 και Α2, και το μέλος Β πιστοποιεί το Β1. Τα μέλη Α1 και Α2 εμπιστεύονται το Α, οπότε μπορεί να εμπιστευθεί το ένα το πιστοποιητικό του άλλου. Εφόσον εμπιστεύονται τον Α, αυτόματα εμπιστεύονται και όλες τις οντότητες που βρίσκονται επάνω από το Α, στην περίπτωση μας την CA1. Το μέλος Β1 δέχεται το πιστοποιητικό του Α, αφού μέσω του Β, εμπιστεύεται την CA1.

Στην περίπτωση που το μέλος Β1 θέλει να επικοινωνήσει με το Α1, θα πρέπει να εμπιστευτεί το μέλος Β, την CA1 και το μέλος Α. Με άλλα λόγια, η εμπιστοσύνη υπάρχει αν υπάρχει δρόμος στο δέντρο από το μέλος Β1 στο μέλος Α1.



Σχήμα 13: Δέντρο Πιστοποίησης.

Στο Σχήμα 14 το μέλος Γ έχει πιστοποιητικό από μια άλλη Αρχή Πιστοποίησης την CA2. Στην περίπτωση που το Γ επιθυμεί να επικοινωνήσει με το μέλος Β, θα πρέπει ο Γ να ελέγξει αν δική του Αρχή Πιστοποίησης CA2, εμπιστεύεται την CA1 και αντίστροφα, ώστε να υπάρχει σύνδεση μεταξύ των δύο δέντρων πιστοποίησης.



Σχήμα 14: Διαπιστοποίηση

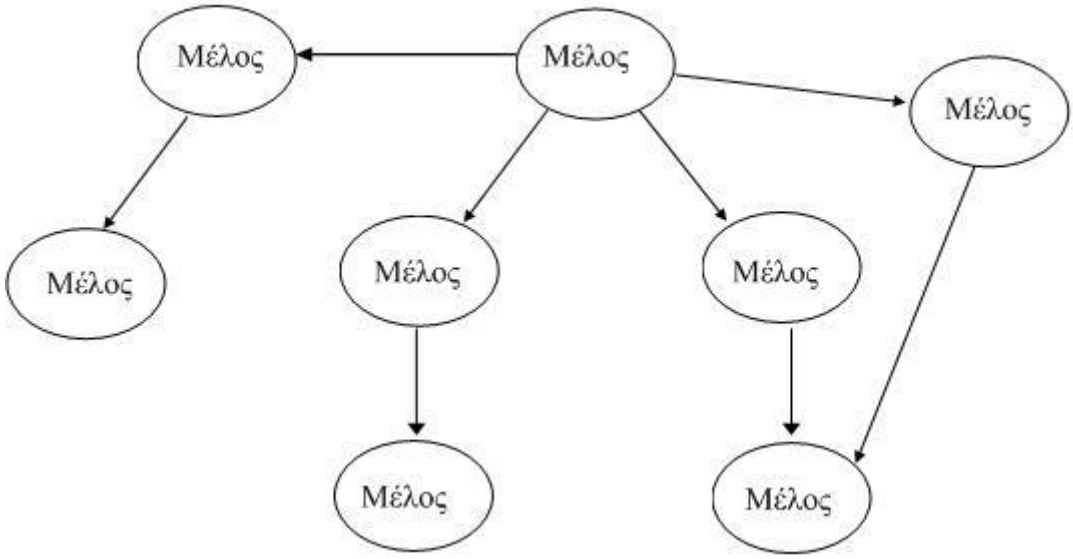
Η δυνατότητα των μελών να μπορούν να εκδίδουν πιστοποιητικά δημιουργεί ένα σημαντικότατο πρόβλημα. Το δέντρο αυξάνεται σε βάθος, με αποτέλεσμα να αυξάνεται και το πλήθος των παρεμβαλλόμενων οντοτήτων μεταξύ ενός μέλους και της Αρχής Πιστοποίησης. Αυτό σημαίνει ότι ο δρόμος πιστοποίησης μεταξύ δύο μελών μπορεί να γίνει ανεξέλεγκτα μεγάλος. Όπως είναι αναμενόμενο, η ασφάλεια ενός PKI θα φθίνει με την αύξηση του βάθους του δέντρου. Όσο

απομακρυσμένα είναι δύο μέλη, τόσο μικρότερη είναι και η εμπιστοσύνη στην αυθεντικότητα του πιστοποιητικού, αφού η ύπαρξη πολλών μελών στο ενδιάμεσο δίνει περισσότερες ευκαιρίες επίθεσης σε κάποιον επιτιθέμενο. Για το λόγο αυτό ορίζονται και μοντέλα όπου δεν επιτρέπεται τα μέλη να εκδίδουν πιστοποιητικά και να λειτουργούν ως Αρχής Πιστοποίησης. Έτσι τα μοντέλα εμπιστοσύνης διαχωρίζονται σε δύο κατηγορίες, στα επίπεδα και στα ιεραρχικά.

Επίπεδο Μοντέλο Εμπιστοσύνης

Το επίπεδο μοντέλο εμπιστοσύνης παρουσιάζεται στο Σχήμα 15.

Στο μοντέλο αυτό δεν υπάρχει καμιά οντότητα που να λειτουργεί αποκλειστικά ως Αρχή Πιστοποίησης. Έτσι, οποιαδήποτε οντότητα έχει το δικαίωμα να εκδώσει πιστοποιητικό για κάποια άλλη. Με αυτό τον τρόπο δημιουργείται ένα δίκτυο εμπιστοσύνης (web of trust), όπου ένα νέο μέλος μπορεί να γίνει μέλος του δικτύου εάν έχει συστηθεί από κάποιο υπάρχον μέλος.



Σχήμα 15: Επίπεδο Μοντέλο Εμπιστοσύνης.

Στο επίπεδο μοντέλο επικρατεί αναρχία. Μάλιστα ένα μέλος μπορεί να συσταθεί από περισσότερα από ένα μέλη. Αυτό μπορεί να χρησιμοποιηθεί ως μέτρο αξιολόγησης της εγκυρότητας του πιστοποιητικού. Όσο περισσότερα μέλη συστήνουν το νέο μέλος, τόσο θεωρητικά μικρότερη είναι η πιθανότητα να μην είναι έγκυρο το πιστοοιητικό.

Το δημοφιλές λογισμικό Pretty Good Privacy (PGP) υποστηρίζει το επίπεδο μοντέλο εμπιστοσύνης. Κάθε χρήστης του PGP διατηρεί μία λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί, η οποία καλείται keyring. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατό να φέρει έναν από τους εξής χαρακτηρισμούς:

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

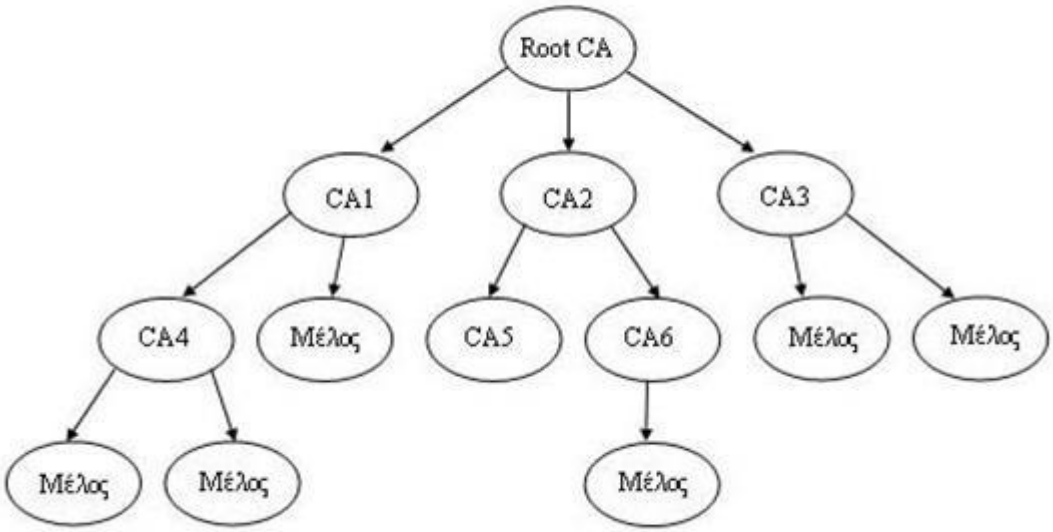
Το PGP επιτρέπει την ανταλλαγή keyrings, ενώ ο κάθε χρήστης έχει τη δυνατότητα να ρυθμίσει το επίπεδο εμπιστοσύνης για την αποδοχή ενός νέου κλειδιού. Δηλαδή, ο χρήστης μπορεί να θεωρήσει την οντότητα του κλειδιού έμπιστη, αν το κλειδί έχει ήδη υπογραφεί από δύο απολύτως έμπιστα (Completely Trusted) κλειδιά ή από τρία μερικώς έμπιστα (Marginally Trusted) κλειδιά.

Καθώς οι χρήστες ανταλλάσσουν keyrings σχηματίζουν έναν ιστό εμπιστοσύνης. Κάθε χρήστης αποτελεί αρχή πιστοποίησης του εαυτού του. Το απλό αυτό μοντέλο έχει επιτρέψει στο PGP να κερδίσει μία σχετικά μεγάλη αποδοχή στο Διαδίκτυο. Παρόλα αυτά, η Υποδομή Δημοσίου Κλειδιού του PGP δεν είναι κατάλληλη για εφαρμογές ηλεκτρονικού εμπορίου και για εφαρμογές που απαιτούν ισχυρή ταυτοποίηση.

Ιεραρχικό Μοντέλο Εμπιστοσύνης

Επειδή τα πιστοποιητικά δημοσίων κλειδιών που εκδίδει ένας ΠΥΠ προς τις ενδιαφερόμενες τελικές οντότητες, είναι και αυτά μια μορφή ηλεκτρονικών εγγράφων, επιβάλλεται να φέρουν και αυτά την ψηφιακή υπογραφή του εκδότη τους. Αυτό προϋποθέτει ότι και η ίδια η Αρχή Πιστοποίησης διαθέτει το δικό της ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού που και αυτό, με την σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Στην κορυφή της ιεραρχίας, όπως φαίνεται και στο Σχήμα 16 βρίσκεται ο Θεμελιώδης Εκδότης Πιστοποιητικών (Root Certification Authority ή Root CA) του ΠΥΠ. Ο Θεμελιώδης Εκδότης Πιστοποιητικών πιστοποιεί κάποιες Αρχές Πιστοποίησης, οι οποίες με τη σειρά τους μπορούν να πιστοποιήσουν κάποιες άλλες Αρχές

Πιστοποίησης. Στο τελευταίο επίπεδο οι Αρχές Πιστοποίησης πιστοποιούν τα μέλη του ΠΥΠ.



Σχήμα 16: Ιεραρχικό Μοντέλο Εμπιστοσύνης.

Σ' αυτήν την ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν το δημόσιο κλειδί και την ταυτότητα του χαμηλότερου επιπέδου. Σε κάθε πιστοποιητικό περιέχεται η υπογραφή του ανώτερου εκδοτικού οργανισμού που έχει δημιουργηθεί με το ιδιωτικό κλειδί αυτού. Από το σχήμα καταλαβαίνουμε ότι μια τέτοια ιεραρχική δομή μπορεί να εφαρμοστεί και στο εσωτερικό μεγάλων εταιριών. Το δημόσιο κλειδί του Θεμελιώδη Εκδότη Πιστοποιητικών δεν μπορεί να πιστοποιηθεί από κανέναν. Ο Εκδότης αυτός, εκδίδει πιστοποιητικό για τον εαυτό του που περιέχει το δημόσιο κλειδί του και την υπογραφή του με το ιδιωτικό του κλειδί, το οποίο καλείται root certificate. Εξυπακούεται ότι αυτός ο Θεμελιώδης Εκδότης Πιστοποιητικών πρέπει να είναι απόλυτα έμπιστος.

4.8.5 Διαδικασία Δημιουργίας Ψηφιακών Πιστοποιητικών

Η πρώτη διαδικασία που πραγματοποιείται σε μια τυπική εφαρμογή είναι η δημιουργία του ζεύγους κλειδιών της CA και η δημοσίευση του πιστοποιητικού της.

Κατά δεύτερο λόγο, λαμβάνει χώρα η διαδικασία δημιουργίας ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού του χρήστη. Το δημόσιο κλειδί θα κατατεθεί στην

Αρχή Εγγραφής μαζί με τα στοιχεία του χρήστη. Υπάρχουν δύο εναλλακτικές όπου μπορεί να δημιουργηθεί το ζεύγος κλειδιών:

1) Στο περιβάλλον του χρήστη. Στην περίπτωση αυτή το ρίσκο να αποκαλυφθεί το ιδιωτικό κλειδί είναι ελάχιστο, αφού ο μόνος γνώστης του κλειδιού είναι ο χρήστης. Ωστόσο αν το κλειδί χρησιμοποιείται για κρυπτογράφηση μηνυμάτων και όχι για αυθεντικοποίηση, η απώλεια του κλειδιού θα καταστήσει αδύνατη την αποκρυπτογράφηση των μηνυμάτων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί. Σε αυτή την εναλλακτική υποτίθεται πως ο χρήστης έχει την ικανότητα να δημιουργήσει μόνος του ένα κατάλληλο ζεύγος κρυπτογραφικών κλειδιών. Στην πράξη, ωστόσο, αυτό δεν συμβαίνει συχνά και κάποιος άλλος αναλαμβάνει τη δημιουργία του ζεύγους κλειδιών για τον χρήστη, όπως εξηγείται στην επόμενη εναλλακτική.
2) Στο περιβάλλον της Αρχής Εγγραφής ή Πιστοποίησης. Η δημιουργία του ζεύγους κλειδιών σε τοποθεσία διαφορετική από τον νόμιμο κάτοχο του ιδιωτικού κλειδιού έχει επίπτωση στην αυξημένη πολυπλοκότητα του μοντέλου επικοινωνίας. Αρχικά θα πρέπει να υπάρχει ένα ασφαλές κανάλι από το οποίο θα μεταφερθεί το ιδιωτικό κλειδί στον χρήστη. Επίσης ο βαθμός εμπιστοσύνης και οι απαιτήσεις ασφάλειας της Αρχής Εγγραφής θα είναι πολύ μεγαλύτερες, γιατί σε περίπτωση επιτυχούς επίθεσης εκτίθενται τα ιδιωτικά κλειδιά των χρηστών. Το πλεονέκτημα στην περίπτωση αυτή είναι η ασφαλής αποθήκευση του ιδιωτικού κλειδιού για να υπάρχει δυνατότητα ανάκτησης του αν ο χρήστης χάσει το κλειδί του. Επιπλέον πολλοί χρήστες δεν έχουν τη μαθηματική ικανότητα να δημιουργήσουν μόνοι τους ένα τέτοιο ζεύγος κρυπτογραφικών κλειδιών και η Αρχής Εγγραφής ή Πιστοποίησης το δημιουργεί για αυτούς.

Όποια εναλλακτική και να ακολουθηθεί, το ιδιωτικό κλειδί καταλήγει στο ασφαλές προσωπικό περιβάλλον του χρήστη το οποίο μπορεί να είναι ο σκληρός δίσκος, αποσπώμενος δίσκος ή έξυπνη κάρτα. Από τα τρία η ασφαλέστερη αποθήκευση είναι στην έξυπνη κάρτα, η οποία θεωρείται ανθεκτική σε εξωτερικές επεμβάσεις και έχει τη δυνατότητα να δημιουργεί τις ψηφιακές υπογραφές χωρίς να απαιτείται το ιδιωτικό κλειδί να μεταφερθεί σε λιγότερο ασφαλές περιβάλλον, όπως ο προσωπικός υπολογιστής του χρήστη.

Στη συνέχεια η Αρχή Εγγραφής, με κάποιο τρόπο, πιστοποιεί την ταυτότητα του χρήστη. Η διαδικασία αυτή περιέχει και χειρωνακτικές (manual) ενέργειες με σκοπό να πείσει ο χρήστης την Αρχή Εγγραφής πως είναι ακριβώς αυτός που ισχυρίζεται. Αφού η Αρχή Εγγραφής εξακριβώσει τα στοιχεία του χρήστη, συμπληρώνει τα στοιχεία που απαιτούνται για την έκδοση του πιστοποιητικού και τα στέλνει στην CA υπό μορφή τυποποιημένης αίτησης.

Έπειτα η CA δημιουργεί ένα πιστοποιητικό που περιέχει το δημόσιο κλειδί του χρήστη, μαζί με πληροφορίες της ταυτότητας του. Στη συνέχεια, η CA παράγει μια σύνοψη του μηνύματος από το πιστοποιητικό και υπογράφει τον κατακερματισμό με το ιδιωτικό της κλειδί, δημιουργώντας ένα υπογεγραμμένο πιστοποιητικό. Αφού δημιουργηθεί το πιστοποιητικό, μεταφέρεται στο χρήστη, είτε άμεσα, είτε μέσω της Υπηρεσίας Δημοσίευσης. Στη δεύτερη περίπτωση η Υπηρεσία αυτή δημοσιεύει το πιστοποιητικό σε κάποιο κατάλογο ο οποίος διατίθεται δημόσια. Από το δημόσιο κατάλογο όλα τα μέλη έχουν πρόσβαση όπου επιτρέπεται μόνο η ανάγνωση. Αντίθετα η CA έχει δυνατότητα πρόσβασης ανάγνωσης και εγγραφής.

Σημειώνεται πως υπάρχουν διαφορετικά επίπεδα στη διαδικασία πιστοποίησης που κυρίως εξαρτώνται από τη χρησιμοποιούμενη εφαρμογή. Για παράδειγμα μια πολυεθνική εταιρεία η οποία μεταφέρει, με ηλεκτρονικό τρόπο, κεφάλαια εκατομμυρίων δολαρίων καθημερινά έχει τελείως διαφορετικές απαιτήσεις ως τη γνησιότητα του (δημόσιου) κλειδιού της από ένα χρήστη που χρειάζεται ένα ψηφιακό πιστοποιητικό για να αποδεικνύει την γνησιότητα του (δημόσιου) κλειδιού του όταν στέλνει και λαμβάνει email.

Συνήθως για περιβάλλοντα υψηλής ασφάλειας, η διαδικασία προσκόμισης των δικαιολογητικών για την πιστοποίηση της ταυτότητας ενός χρήστη στην Αρχή Εγγραφής περιλαμβάνει χειρωνακτικές μεθόδους, με τρόπο που να είναι κοινωνικά αποδεκτός. Για παράδειγμα, οι βιομετρικές τεχνικές αποτελούν μια πολύ αποτελεσματική μέθοδο για αυτή την απαίτηση. Μπορεί λοιπόν η Αρχή Εγγραφής να υποβάλει το χρήστη σε μια διαδικασία «σκαναρίσματος» της κόρης ή της ίριδας του ματιού με σκοπό να πιστοποιήσει την ταυτότητα του. Είναι προφανές ότι για τις περισσότερες εφαρμογές – πλην ελαχίστων εξαιρέσεων – η διαδικασία αυτή δε θα είναι αποδεκτή από το χρήστη. Συνηθισμένα διαπιστευτήρια είναι η αστυνομική ταυτότητα, το δίπλωμα οδήγησης, το διαβατήριο. Τονίζεται ότι τα δικαιολογητικά αυτά εξαρτώνται άμεσα από την κρισιμότητα της εφαρμογής.

Επικοινωνία μεταξύ χρηστών

Θεωρούμε τη διαδικασία όπου ο χρήστης Α επιθυμεί να επικοινωνήσει με τον χρήστη Β. Η ασφαλής επικοινωνία απαιτεί αμοιβαία αυθεντικοποίηση των δύο μελών. Αρχικά ο χρήστης Α επικοινωνεί με τον χρήστη Β ή με τον δημοσιευμένο κατάλογο πιστοποιητικών, προκειμένου να λάβει το δημόσιο κλειδί του χρήστη Β. Στη συνέχεια εκτελεί τις ακόλουθες δύο ενέργειες:

Έλεγχος των στοιχείων του πιστοποιητικού. Ο χρήστης Α χρησιμοποιώντας το δημόσιο κλειδί της CA, αποκρυπτογραφεί το πιστοποιητικό του χρήστη Β και ελέγχει τα στοιχεία που περιγράφουν τον Β, καθώς και την επικαιρότητα του πιστοποιητικού. Αν δεν έχει δηλαδή παρέλθει η ημερομηνία λήξης του.

Έλεγχος ανάκλησης του πιστοποιητικού. Πολλές φορές λόγω κακής χρήσης του πιστοποιητικού ή λόγω υποψίας διαρροής του ιδιωτικού κλειδιού, το πιστοποιητικό μπορεί να λήξει πριν από την αναγραφόμενη ημερομηνία λήξης. Η τεχνητή αυτή λήξη ονομάζεται ανάκληση πιστοποιητικού. Στις λίστες ανακληθέντων πιστοποιητικών φαίνονται όλα τα πιστοποιητικά τα οποία έχουν ανακληθεί.

Μετά από την επιτυχή ολοκλήρωση των δύο παραπάνω ελέγχων και από τις δύο πλευρές, ακολουθεί το πρωτόκολλο αυθεντικοποίησης το οποίο βασίζεται στην κρυπτογραφία δημοσίου κλειδιού.

4.8.6 Διαδικασία Ανάκλησης Ψηφιακών Πιστοποιητικών

Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού μπορεί οποτεδήποτε να ανακληθεί οριστικά (revocation) ύστερα από αίτημα του ίδιου του τελικού χρήστη ή και από σχετική απόφαση του Εκδότη τους. Η ανάκληση ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του σειριακού αριθμού του πιστοποιητικού (serial number) σε μια Λίστα Ανακληθέντων Πιστοποιητικών (Certificate Revocation List, CRL) η οποία δημοσιεύεται σε τακτά χρονικά διαστήματα από την Υπηρεσία Ανάκλησης Πιστοποιητικών, αφού πρώτα υπογραφεί από τον ίδιο τον Εκδότη (CA) των πιστοποιητικών. Κάθε CA υπογράφει τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκδοθεί από την ίδια.

Η ανάκληση ενός πιστοποιητικού γίνεται σε δύο περιπτώσεις:

1) Στην περίπτωση που ο χρήστης υποψιαστεί ότι το ιδιωτικό του κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους, (αίτημα του χρήστη).
2) Στην περίπτωση που γίνει κακή χρήση του πιστοποιητικού από τον χρήστη, (απόφαση του Εκδότη).

Κακή χρήση ορίζεται η οποιαδήποτε χρήση του πιστοποιητικού πέραν της προβλεπόμενης. Η CA καθορίζει την χρήση των πιστοποιητικών. Όπως αναφέρθηκε προηγουμένως, ένα πιστοποιητικό μπορεί να χρησιμοποιείται για αυθεντικοποίηση ή για κρυπτογραφία.

Όταν η CA κρίνει ότι απαιτείται ανάκληση του πιστοποιητικού ενός χρήστη, η Υπηρεσία Ανάκλησης πιστοποιητικών ανανεώνει τη λίστα ανακληθέντων πιστοποιητικών και τη δημοσιεύει.

Κατά την επαλήθευση μιας υπογραφής, πρέπει κάθε χρήστης να συμβουλεύεται μία CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιον έλεγχο, εξαρτάται από τη σημασία του εγγράφου.

4.8.7 Οργανισμοί Πιστοποίησης

Στον Πίνακα 2 φαίνονται κάποιοι ενδεικτικοί οργανισμοί πιστοποίησης μαζί με τις αντίστοιχες ηλεκτρονικές διευθύνσεις τους.

Ενδεικτικοί Οργανισμοί Πιστοποίησης	Ηλεκτρονική Διεύθυνση
VeriSign	http://digitalid.verisign.com/
Thawte Digital Certificate Services	http://www.thawte.com/
Digital Signature Trust Co.	http://www.digsigtrust.com
Euro Trust A/S	http://www.eurotrust.dk

eSign Australia	http://www.esign.com.au/
The USERTRUST Network	http://www.usertrust.com/

Πίνακας 2: Οργανισμοί Πιστοποίησης.

Ο πολύ δημοφιλής browser Internet Explorer ενσωματώνει την τεχνολογία των πιστοποιητικών στις υλοποιήσεις του. Ο εν λόγω browser εμπιστεύεται την VerySign ως την έμπιστη, ανεξάρτητη αρχή που υπογράφει πιστοποιητικά. Τα πιστοποιητικά που χρησιμοποιεί ο Internet Explorer υιοθετούν το ITU standard X.509 v.3.

4.8.8 Η Σημερινή Πραγματικότητα

Το θέμα της διαλειτουργικότητας είναι ένα από τα πιο κρίσιμα ζητήματα που παραμένουν άλυτα ακόμη και σήμερα. Για να μπορεί μια PKI υποδομή να λειτουργεί ομαλά με οποιουδήποτε τύπου πιστοποιητικά και σε ολόκληρο τον κόσμο χρειάζεται να είναι συμφωνημένη με ένα μεγάλο πλήθος προτύπων, όπως π.χ. εκείνα των ISO (International Organization for Standardization), ITU (International Telecommunication Union), ETSI (Electronic Telecommunications Standardization Institute) αλλά και με διάφορα εθνικά πρότυπα, όπως για παράδειγμα το t-Scheme της Μεγάλης Βρετανίας.

Η πραγματικότητα έχει δείξει πως διαλειτουργικότητα υπάρχει μόνο σε απλές εφαρμογές (π.χ. πιστοποίηση ταυτότητας σε ένα δίκτυο υπολογιστών) ή πολύ περιορισμένου τύπου εφαρμογές (π.χ. χρήση του πρωτοκόλλου Secure Sockets Layer, SSL). Τα κατά τόπου πρότυπα δεν εγγυώνται πλήρη διαλειτουργικότητα καθώς χρειάζεται να γίνει εκτενέστατος έλεγχος για όλες τις περιπτώσεις συμβατότητας μεταξύ τους. Αυτό απαιτεί χιλιάδες εργατοώρες από εξειδικευμένο προσωπικό, κάτι που είναι ιδιαίτερα αποθαρρυντικό.

Ένας παράγοντας που συμβάλλει στην αύξηση της πολυπλοκότητας μιας τέτοιας υποδομής είναι οι διάφορες κατηγορίες πιστοποιητικών καθώς και το μέσο με το οποίο θα προσφέρονται αυτά στο χρήστη. Για παράδειγμα σήμερα υπάρχουν τρεις κύριες κατηγορίες ψηφιακών πιστοποιητικών, για πιστοποίηση ενός λογαριασμού ηλεκτρονικού ταχυδρομείου, για ηλεκτρονικές συναλλαγές και για ηλεκτρονική μεταφορά κεφαλαίων. Κάθε πιστοποιητικό από τα παραπάνω έχει διαφορετικές απαιτήσεις ασφάλειας. Για παράδειγμα ένα πιστοποιητικό της πρώτη κατηγορίας μπορεί να αποθηκευτεί σε μια δισκέτα, της δεύτερης κατηγορίας σε μια έξυπνη κάρτα (smart card) και της τρίτης ίσως σε μια ειδική προστατευόμενη συσκευή (tamper resistant hardware).

Μια υποδομή σαν την PKI είναι ένα τεράστιο και ιδιαίτερα ακριβό έργο, η επιτυχία του οποίου και τα αναμενόμενα κέρδη εμπεριέχουν σημαντικό ρίσκο. Εκτός από τον υλικοτεχνικό εξοπλισμό απαιτεί και μια εκτεταμένη τεχνολογική υποδομή, κυρίως όσον αφορά στα δίκτυα επικοινωνιών τα οποία υπάρχουν.

Η υλοποίηση και συντήρηση μιας τέτοιας υποδομής στηρίζεται κατά πολύ σε ανθρώπινες ενέργειες. Είναι δηλαδή απαραίτητο ένα εξειδικευμένο προσωπικό. Όμως το εξειδικευμένο προσωπικό, εκτός από το ότι είναι δύσκολο να βρεθεί στην σημερινή αγορά, κοστίζει ιδιαίτερα.

Είναι γεγονός ότι καθυστερεί η ανάπτυξη μιας πραγματικά παγκόσμιας υποδομής δημοσίου κλειδιού, η οποία θα προσφέρει όλα τα πλεονεκτήματα της χρήσης της κρυπτογραφίας δημοσίου κλειδιού. Η υφιστάμενη έλλειψη διαλειτουργικότητας στις εφαρμογές ηλεκτρονικών υπογραφών, το μεγάλο κόστος δημιουργίας και διατήρησης μιας ασφαλούς Υποδομής Δημοσίου Κλειδιού και ο μεγάλος επιχειρηματικός κίνδυνος της ανάπτυξης μιας τέτοιας υποδομής την στιγμή που δεν έχουν προσδιοριστεί σαφώς οι τελικές προδιαγραφές που θα επικρατήσουν, οδηγούν σε συγκράτηση και περιορισμό των σχετικών επενδύσεων και των πρωτοβουλιών για την ανάπτυξη συναφών εφαρμογών. Παράλληλα διατηρείται ένα κλίμα σύγχυσης και πλημμελούς ενημέρωσης των δυνητικών χρηστών των εφαρμογών ηλεκτρονικής υπογραφής, το οποίο δυσχεραίνει την ανάπτυξη της απαραίτητης σχετικής εμπιστοσύνης.

5^{Ο} ΚΕΦΑΛΑΙΟ : ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Οι ηλεκτρονικές συναλλαγές έχουν γίνει πολύ σημαντικές στη ζωή του καταναλωτή. Τον βοηθούν να κάνει τις αγορές του και τις συναλλαγές του με δημόσιες υπηρεσίες και τράπεζες από όπου κ αν βρίσκεται οποιαδήποτε ώρα της ημέρας κ μέρα της εβδομάδας. Και αυτό γιατί η διαδικασία είναι πολύ απλή και η πρόσβαση είναι προσιτή σε όλους. Βασικό προτέρημα τους είναι ότι μπορούν να εξυπηρετηθούν όλες τις ώρες την ημέρας και μέρες της εβδομάδας, καθώς οι περισσότεροι πολίτες έχουν πλέον σύνδεση με το Internet και στο σπίτι και στο χώρο εργασίας τους, έτσι τους διευκολύνει κατά πολύ σε σύγκριση με τα συμβατικά καταστήματα λιανικής πώλησης και με την φυσική τους παρουσία σε δημόσιες υπηρεσίες, όπου απαιτείται μετακίνηση – η όποια μπορεί να διαρκέσει πολύ – και λειτουργούν μονό τις εργάσιμες ώρες και μέρες. Ακόμα, ψάχνοντας αυτό που αναζητάμε μέσω ενός online καταλόγου μπορεί να είναι πολύ ταχύτερο από την περιήγηση σε ένα φυσικό κατάστημα, όπως και η εξυπηρέτηση σε μία δημόσια υπηρεσία μπορεί να είναι χρονοβόρα. Επίσης η διαδικασία είναι πολύ απλή και η πρόσβαση είναι προσιτή σε όλους.

Οι ηλεκτρονικές συναλλαγές θα λέγαμε ότι χωρίζονται σε δυο κατηγορίες, α) στις συναλλαγές που κάνουμε με διάφορα ηλεκτρονικά καταστήματα, και β) σε αυτές που πραγματοποιούμε με δημόσιες υπηρεσίες και τράπεζες. Και οι δύο κατηγορίες έχουν μπει στην καθημερινότητα του καθενός και η λειτουργικότητά τους είναι σημαντική στην εξέλιξή τους.

5.1 Συναλλαγές με ηλεκτρονικά καταστήματα

Τα ηλεκτρονικά καταστήματα συγκαταλέγονται στις εφαρμογές της κατηγορίας επιχείρηση προς καταναλωτή και αποτελούν σημεία προώθησης και πώλησης αγαθών μέσω Internet. Ένα ηλεκτρονικό κατάστημα μπορεί να αναπαραστήσει και να εμπλουτίσει με νέες δυνατότητες τη λειτουργικότητα ενός νέου καταστήματος. Σε αρκετές περιπτώσεις, τα ηλεκτρονικά καταστήματα λειτουργούν ως υποκαταστήματα των υφισταμένων (φυσικών) καταστημάτων, ενώ σε άλλες περιπτώσεις αποτελούν τα μοναδικά σημεία πώλησης των προϊόντων μιας

επιχείρησης. Στόχος ενός ηλεκτρονικού καταστήματος δεν είναι μόνο η προβολή των προϊόντων αλλά και η εφαρμογή τεχνικών που προσδίδουν πρόσθετη αξία στην ηλεκτρονική παρουσία του εμπόρου και ωθούν τον πελάτη να προτιμήσει την ηλεκτρονική αγορά έναντι της παραδοσιακής. Από την πλευρά του εμπόρου, εξασφαλίζεται η ηλεκτρονική του παρουσία σε παγκόσμιο επίπεδο καθώς και η δημιουργία νέων καναλιών προώθησης και πώληση των προϊόντων. Επιπλέον, προκύπτουν νέα κανάλια επικοινωνίας με τους πελάτες αλλά και με άλλες επιχειρήσεις, καθιστώντας ακόμα πιο ισχυρή και άμεση την επαφή της επιχείρησης μαζί τους. Αυτοματοποιημένες διαδικασίες, που αφορούν την διαχείριση αποθεμάτων και την διανομή (μεταφορά και παράδοση) των προϊόντων, μπορούν να υιοθετήσουν και να συντελέσουν στην εξοικονόμηση κόστους για την επιχείρηση και κατ' επέκταση για τον ίδιο τον πελάτη.

Σε ένα μεγάλο ποσοστό, τα υπάρχοντα ηλεκτρονικά καταστήματα στο Internet διαθέτουν χαρακτηριστικά που αφορούν την προβολή και προώθηση των προϊόντων, την δυνατότητα άμεσης παραγγελίας και αγοράς αυτών είτε με αντικαταβολή είτε μέσω πιστωτικής κάρτας. Επίσης υιοθετούνται μέθοδοι για την αναγνώριση της ταυτότητας του πελάτη και σκιαγράφηση του προφίλ, όχι μόνο όσο αφορά τα προσωπικά του στοιχεία αλλά και τις αγοραστικές του συνήθειες. Με αυτόν τον τρόπο κάθε φορά που ο πελάτης αυτός επισκέπτεται το κατάστημα, μπορεί να δει κάποιες σελίδες διαμορφωμένες συμφωνά με τις απαιτήσεις και τη αγοραστική του συμπεριφορά κατά την τελευταία του επίσκεψη. Επιπλέον νέα προϊόντα και προσφορές που εμπίπτουν στις αγοραστικές τους συνήθειες προτείνονται στους συχνότερους επισκέπτες.

5.1.1 Γενιές ηλεκτρονικών καταστημάτων

Η ανάπτυξη των ηλεκτρονικών καταστημάτων και της αγοράς αυτών δεν επιτεύχθηκε από την μια μέρα στην άλλη, αλλά υπήρχε μια σταδιακή εξέλιξη μέσα από την οποία διαμορφώθηκαν 4 γενιές ηλεκτρονίων καταστημάτων:

1) Πρώτη γενιά Ηλεκτρονικών Καταστημάτων-Απλή παρουσία.
2) Δεύτερη γενιά Ηλεκτρονικών Καταστημάτων-Η δυνατότητα για παραγγελία.
3) Τρίτη γενιά Ηλεκτρονικών Καταστημάτων –Ολοκλήρωση με τα υπάρχοντα Πληροφορικά συστήματα.

4) Τέταρτη γενιά Ηλεκτρονικών Καταστημάτων-Πλήρεις και Ασφαλείς Υπηρεσίες.

- **Πρώτη γενιά Ηλεκτρονικών Καταστημάτων-Απλή παρουσία.**

Η πρώτη γενιά ηλεκτρονικών καταστημάτων έκανε την εμφάνιση της σχεδόν ταυτόχρονα με την ανάπτυξη του Word Wide Web. Οι επιχειρήσεις διαπιστώνοντας τις δυνατότητες που τους πρόσφερε το Internet προχώρησαν στην δημιουργία ηλεκτρονικών σελίδων, επιδιώκοντας αρχικά μια απλή παρουσία στον καινούργιο αυτόν χώρο προκειμένου να αυξήσουν τη φήμη και την πελατεία τους. Αργότερα, ανακαλύπτοντας την χρησιμότητα του Internet ως μέσο διαφήμισης και προσέλκυσης καινούργιων πελατών άρχισαν να επενδύουν αρκετά χρήματα προκειμένου να βελτιώσουν τις επαφές τους, δημιουργώντας, έτσι, πιο φιλικές και προσιτές web σελίδες.

- **Δεύτερη γενιά Ηλεκτρονικών Καταστημάτων-Η δυνατότητα για παραγγελία.**

Οι δυνατότητες παρουσίας, προβολής και διαφήμισης που προσέφεραν τα καταστήματα της πρώτης γενιάς, δεν ήταν αρκετές για την θεαματική αύξηση των πωλήσεων μιας επιχείρησης. Μετά από σχετικές έρευνες, μελέτες, και αναλύσεις της συμπεριφοράς των καταναλωτών διαπιστώθηκε ότι :

- Το Internet παρέχει μια μοναδική ευκαιρία διεξαγωγής marketing. Μέσω του διαδικτύου υπάρχει η δυνατότητα προσέγγισης μεγάλου αριθμού καταναλωτών, αλλά και το marketing και η στρατηγική προσέλκυση της επιχείρησης στοχεύει σε κάθε καταναλωτή ξεχωριστά, λόγω της ύπαρξης ενός χρήστη-καταναλωτή κάθε φορά μπροστά από την οθόνη του υπολογιστή.
- Οι πωλήσεις προϊόντων μπορούν να αυξηθούν σημαντικά εάν οι: καταναλωτές έχουν την δυνατότητα παραγγελιάς μέσω του Internet.
- Δεδομένου ότι μπορεί να γίνει παραγγελία προϊόντων μέσω Internet τότε αυτόματα μεγαλώνει και το εύρος της αγοράς κάθε επιχείρησης αφού υπάρχει η δυνατότητα να δέχεται και παραγγελίες (και επομένως να αποκτά καινούργιους πελάτες) από περιοχές στις οποίες μέχρι τώρα δεν υπήρχε φυσική παρουσία του καταστήματος. Η επιχείρηση επομένως μπορεί να

κάνει αισθητή την παρουσία της σε αγορές τις οποίες προηγουμένως ήταν πολύ δύσκολο ή ακόμη και αδύνατον να εισχωρήσει.

Βάσει των παραπάνω συμπερασμάτων διαμορφώθηκε μια καινούργια γενιά ηλεκτρονικών καταστημάτων, η οποία επιτρέπει στους καταναλωτές να παραγγέλνουν τα προϊόντα που επιθυμούν. Τα καταστήματα αυτά λειτουργούν παρασκηνιακά με τον εξής τρόπο:

1) Οι καταναλωτές κατά την πλοήγηση τους στο κατάστημα επιλεγούν τα προϊόντα της αρεσκείας τους, τα τοποθετούν σε εικονικά καλάθια και κατά την έξοδο τους από το κατάστημα προβαίνουν στην παραγγελία των προϊόντων.
2) Οι παραγγελίες αυτές αποστέλλονται στο ηλεκτρονικό γραμματοκιβώτιο της επιχείρησης .
3) Ο διαχειριστής του συστήματος λαμβάνει τις παραγγελίες, τις εκτυπώνει και τις προωθεί για διεκπεραίωση.

➢ **Τρίτη γενιά Ηλεκτρονικών καταστημάτων –Ολοκλήρωση με τα Υπάρχοντα Πληροφοριακά Συστήματα**

Η Τρίτη γενιά καταστημάτων εμφανίζεται στα μέσα του 1995 και εστιάζει στο θέμα της ολοκλήρωσης των ηλεκτρονικών καταστημάτων με το υπάρχον πληροφοριακό σύστημα των επιχειρήσεων. Εταιρείες που διέθεταν ηλεκτρονικά καταστήματα εγκατεστημένα στους υπολογιστές, προσπαθούσαν να βρουν ένα τρόπο ολοκλήρωσης και ομαλής συνύπαρξης και λειτουργίας των δύο συστημάτων. Οι επιχειρήσεις ήθελαν να εφαρμόσουν ένα σχήμα μέσα από το οποίο να καταχωρούνται απευθείας οι ηλεκτρονικές παραγγελίες (που γίνονται από το ηλεκτρονικό κατάστημα) στο πληροφοριακό τους σύστημα προκειμένου να διεκπεραιώνονται πιο γρήγορα και πιο άμεσα. Βέβαια μετά την εύρεση και υλοποίηση ενός τέτοιου μηχανισμού προέκυψαν κι άλλα θέματα όπως η αυτόνομη ενημέρωση της αποθήκης και η διαχείριση των προσφορών του ηλεκτρονικού καταστήματος από το υπάρχον Π.Σ, ενώ προέκυψε και το θέμα ηλεκτρονικής πληρωμής. Έτσι εμφανίστηκε μια καινούργια γενιά ηλεκτρονικών καταστημάτων, η οποία παρέχει τις παρακάτω λειτουργίες:

- Ηλεκτρονική προβολή και διαφήμιση
- Ηλεκτρονικές προσφορές και εκπτώσεις προϊόντων
- Ηλεκτρονική παραγγελία
- Ηλεκτρονική τιμολόγηση

- Φυσική παράδοση προϊόντος
- Ηλεκτρονική παράδοση προϊόντος (οπού επιτρέπει)
- Ηλεκτρονική πληρωμή.

- **Τέταρτη γενιά ηλεκτρονικών καταστημάτων – Ολοκληρωμένες και ασφαλείς υπηρεσίες**

Ένα χρόνο μετά την υλοποίηση και λειτουργία καταστημάτων τρίτης γενιάς, έκαναν την εμφάνιση τους τα ηλεκτρονικά καταστήματα τέταρτης γενιάς. Οι λειτουργίες των ηλεκτρονικών καταστημάτων επεκτείνονται και περιλαμβάνουν όλες τις λειτουργίες που προσφέρουν τα καταστήματα τρίτης γενιάς αλλά και κάποιες επιπλέον που αφορούν κυρίως θέματα ασφαλείας και αποδοτικής διαχείρισης της αποθήκης και των αποθεμάτων. Ορισμένες από τις καινούργιες λειτουργίες αφορούν:

- Ηλεκτρονική πληρωμή, ηλεκτρονικό πορτοφόλι
- Αυτοματοποιημένο υπολογισμό φορολογίας
- Ασφάλεια
- Έλεγχος αποθεμάτων
- Ευέλικτη κοστολόγηση
- Ανίχνευση προϊόντος
- Εξατομίκευση συμπεριφοράς καταναλωτή
- Επεκτασιμότητα – ολοκλήρωση

5.1.2 Λειτουργίες καταστήματος

Οι λειτουργίες ενός ηλεκτρονικού καταστήματος αφορούν τόσο τον έμπορο όσο και τον καταναλωτή. Έτσι το περιβάλλον ανάπτυξης μιας εφαρμογής ηλεκτρονικού καταστήματος θα πρέπει να ικανοποιεί τόσο τις απαιτήσεις των εμπόρων όσο και τις ανάγκες των καταναλωτών

α) Για τον επιχειρηματία

Όσον αφορά τη διαχείριση και διοίκηση του καταστήματος, πρέπει να παρέχονται τα ακόλουθα:

- Δημιουργία καταλόγου προϊόντων και διαχείρισης αυτού
- Υπολογισμός εξόδων αποστολής και παράδοσης προϊόντων

- Ανάλυση του προφίλ και της αγοραστικής συμπεριφοράς των καταναλωτών
- Δυνατότητα διαφήμισης
- Πολιτική τιμών και προώθηση προϊόντων

β) Για τον καταναλωτή

- Εγγραφή στο κατάστημα
- Πλοήγηση στο κατάστημα και αναζήτηση
- Καλάθι αγορών
- Εξατομικευμένο εμπόριο
- Χρήση εκπτωτικών κουπονιών
- Παραγγελιοληψία
- Ηλεκτρονική πληρωμή και ηλεκτρονικό πορτοφόλι

5.1.3 Οφέλη ηλεκτρονικών καταστημάτων

α) Οφέλη από την δραστηριοποίηση μια επιχείρησης στο Διαδίκτυο

Από την δραστηριοποίηση μιας επιχείρησης στο Διαδίκτυο προκύπτουν οφέλη τόσο για την επιχείρηση την ίδια όσο και για τους πελάτες τις επιχείρησης. Τα οφέλη για την ίδια την επιχείρηση συνοψίζονται στα εξής:

- **Συνεχής προβολή και λειτουργία της επιχείρησής**

Οι πελάτες μπορούν να επισκεφτούν τις σελίδες του ηλεκτρονικού καταστήματος 24 ώρες το 24ωρο, 365 ημέρες το χρόνο, να «ξεφυλλίσουν» τον ηλεκτρονικό κατάλογο των προϊόντων και να κάνουν τις αγορές τους με αντικαταβολή ή και με την πιστωτική τους κάρτα. Για την επιχείρησή αυτό σημαίνει ότι δεν χρειάζονται υπερωρίες προσωπικού ή διπλές βάρδιες, γιατί το ηλεκτρονικό κατάστημα δεν χρειάζεται προσωπικό.

- **Προβολή των προϊόντων της με ένα μοναδικό μέσο επικοινωνίας**

Το νέο αυτό μέσο μαζικής επικοινωνίας (Διαδίκτυο) μπορεί να συνδυάσει κείμενο, εικόνα, ήχο και video, αλλά και να αλληλεπιδράσει με τους πελάτες της επιχείρησης, επιτρέποντάς τους να κάνουν ερωτήσεις και αγορές από το σπίτι. Επίσης, το Διαδίκτυο, σε αντίθεση με τον τύπο, το ραδιόφωνο και την τηλεόραση, παρέχει τη δυνατότητα απεριόριστης χρήσης κειμένου, εικόνας, ήχου και video, με

κόστος χαμηλότερο από αυτό μιας ολοσέλιδης καταχώρισης σε κάποιο περιοδικό εθνικής εμβέλειας.

- **Μείωση των κρίκων της προμηθευτικής αλυσίδας**

Η μείωση των κρίκων της προμηθευτικής αλυσίδας έχει ως αποτέλεσμα τη γρηγορότερη και με μειωμένο κόστος εξυπηρέτηση του πελάτη σας. Ειδικά στην περίπτωση προϊόντων, όπως εκδόσεις, μουσικά ή άλλα CDs, ταινίες - video και λογισμικό, οι «ενδιάμεσοι» μπορούν να εξαλειφθούν. Χαρακτηριστικά παραδείγματα είναι τα www.books.gr (βιβλία), www.dvdcool.gr (DVDs), www.norton.com (λογισμικό).

- **Μειωμένα κόστη.**

Μείωση τιμών για τον πελάτη μπορεί να προκύψει και από τη μείωση του κόστους διαφήμισης, παραγωγής, αποθήκευσης, ακόμη και διανομής του προϊόντος (όταν αυτό διανέμετε απευθείας μέσω του Διαδικτύου). Ας δούμε πώς μπορούν να μειωθούν αυτά τα κόστη.

1) Κόστος μεταφοράς πληροφοριών

Το κόστος της μεταφοράς πληροφοριών σχετικών με τις τιμές, τα προϊόντα, το stock, τις ειδικές προσφορές κ.ά., σε οποιαδήποτε μορφή (κείμενο, ήχος, εικόνα, video), από την εταιρεία προς:

- Τον πελάτη
- Τους συνεργάτες
- Άλλες εταιρείες (προμηθευτές, κέντρα διανομής, άλλες εταιρείες στο εσωτερικό ή το εξωτερικό)

Τους πωλητές της ή διάφορα στελέχη της επιχείρησης ανά τον κόσμο είναι πολύ μικρότερο μέσω Διαδικτύου. Έτσι, η επιχείρηση μπορεί να βρίσκετε σε διαρκή επικοινωνία με τους συνεργαζόμενους οίκους του εξωτερικού, με τους πωλητές στην επαρχία και με τα στελέχη σε κάποιο συνέδριο, με κόστος πολύ μικρότερο από ότι θα απαιτούσε κάθε άλλη μορφή επικοινωνίας.

2) Κόστος έκδοσης καταλόγου προϊόντων

Το κόστος του τυπώματος, αλλά και της διανομής μειώνεται δραστικά, γιατί γίνεται με ηλεκτρονικό τρόπο. Επίσης, μειώνεται στο ελάχιστο το κόστος επανέκδοσης. Έτσι, ο κατάλογος προϊόντων είναι πάντα ενημερωμένος και δεν χρειάζεται η επιχείρηση να περιμένει να μαζευτούν πολλές αλλαγές, για να

αποφασίσει επανέκδοσή του, ούτε να καταφεύγετε σε πρόχειρες και ακαλαίσθητες λύσεις (διορθώσεις με στυλό, αυτοκόλλητα κλπ.).

3) Κόστος διατήρησης / απόκτησης πελατών

Το κόστος διατήρησης ενός πελάτη είναι χαμηλότερο από το κόστος απόκτησης νέων πελατών. Οι ευκολίες, οι υπηρεσίες και η εξατομικευμένη εξυπηρέτηση των επισκεπτών μέσω του ηλεκτρονικού καταστήματος αυξάνει τους πιστούς πελάτες, άρα μειώνει το συνολικό κόστος προώθησης και προβολής της εταιρείας. Το κλασικό παράδειγμα εξατομίκευσης δίνει το γνωστό βιβλιοπωλείο Amazon (www.amazon.com), το οποίο - μεταξύ άλλων - παρέχει στους πελάτες του τη δυνατότητα «αποθήκευσης» των επιθυμιών τους για μελλοντικές αγορές και καταγράφει τις αγορές τους, για να τους προτείνει παρεμφερή προϊόντα.

4) Συμπίεση του κόστους παραγωγής και διανομής προϊόντων

Ειδικά για τα προϊόντα που μεταφέρονται μέσω Διαδικτύου (βιβλία, λογισμικό, φωτογραφίες, μουσική, σχέδια, πληροφορίες) και τις υπηρεσίες (χρηματοοικονομικές, τραπεζικές, πληροφορίες για ιατρικά θέματα, συμβουλευτική επιχειρήσεων κ.ά.), το κόστος αναπαραγωγής μειώνεται δραστικά και το κόστος διανομής πρακτικά εξαλείφεται.

β) Οφέλη για τους πελάτες της επιχείρησης

- **Άμεση ικανοποίηση των πελατών**

Για ορισμένα προϊόντα η τεχνολογία επιτρέπει την άμεση (μέσω Διαδικτύου) παράδοση. Ο αγοραστής μπορεί να απολαύσει το προϊόν ακόμη και την ίδια στιγμή, όπως στην περίπτωση αγοράς ενός μουσικού κομματιού, μιας φωτογραφίας, ενός video clip, ενός άρθρου ή κάποιου λογισμικού. Αυτό αυξάνει την πιθανότητα να κάνουν οι πελάτες αγορές «της στιγμής», γιατί δεν χρειάζεται να βγουν από το σπίτι τους.

- **Μεγαλύτερη γκάμα προϊόντων για τον πελάτη**

Στην περίπτωση που ο επισκέπτης του ηλεκτρονικού καταστήματος μένει στην επαρχία, όπου οι επιλογές είναι λιγότερες από αυτές στις μεγάλες πόλεις, δεν εξυπηρετείται απλώς καλύτερα, αλλά βρίσκει και αυτό που θέλει. Από την άλλη μεριά, η επιχείρησή δεν περιορίζεται γεωγραφικά και αυξάνει την πελατεία της, χωρίς να επιβαρύνεται με το κόστος δημιουργίας νέων καταστημάτων.

- **Διευρυμένες επιλογές για τους πελάτες σε ανταγωνιστικές τιμές**

Τα δίκτυα και το Ηλεκτρονικό Εμπόριο δίνουν τη δυνατότητα σε όλες τις επιχειρήσεις - ανεξαρτήτως μεγέθους - να δραστηριοποιηθούν στην παγκόσμια αγορά. Από την άλλη πλευρά, οι αγοραστές των προϊόντων έχουν περισσότερες επιλογές, ακριβώς γιατί οι «προμηθευτές» των προϊόντων είναι περισσότεροι ανά γεωγραφική αγορά. Αυτό συμβαίνει, γιατί το κόστος έναρξης («ανοίγματος») και συντήρησης ενός ηλεκτρονικού καταστήματος είναι πολύ μικρό. Το αποτέλεσμα του αυξημένου ανταγωνισμού είναι είτε η βελτίωση της ποιότητας είτε η μείωση των τιμών.

- **24ωρη υποστήριξη των πελατών**

Χρησιμοποιώντας τις δυνατότητες του Διαδικτύου, η επιχείρηση μπορεί να προβάλλει μέσω του ηλεκτρονικού της καταστήματος:

- Ηλεκτρονικό κατάλογο προϊόντων
- Πληροφορίες για τη διαθεσιμότητα (stock) των προϊόντων, τα νέα μοντέλα, σχέδια, χρώματα κ.ά.
- Οδηγίες χρήσης, εγκατάστασης και συντήρησης των προϊόντων
- Λύσεις σε προβλήματα
- Απαντήσεις στις πιο συχνές ερωτήσεις και απορίες των πελατών σας
- Πληροφορίες για το στάδιο διεκπεραίωσης της παραγγελίας του πελάτη

Η παραπάνω πλήρης κάλυψη των αναγκών υποστήριξης των πελατών προσφέρεται 24 ώρες το 24ωρο, χωρίς την ύπαρξη προσωπικού.

- **Εξατομίκευση των υπηρεσιών σύμφωνα με τις ανάγκες κάθε πελάτη**

Το Ηλεκτρονικό Εμπόριο επιτρέπει την παρακολούθηση και καταγραφή του αγοραστικού προφίλ των πελατών με λεπτομέρεια. Έτσι, η επιχείρηση μπορεί να παρέχει σε κάθε πελάτη της εξατομικευμένα προϊόντα. Για παράδειγμα, πολλά ηλεκτρονικά βιβλιοπωλεία καταγράφουν τις αγοραστικές συνήθειες των πελατών τους και παρουσιάζουν σελίδες, ειδικά για αυτούς, με προϊόντα του ενδιαφέροντός τους.

5.2 Συναλλαγές με Δημόσιες Υπηρεσίες και Τράπεζες

Οι ηλεκτρονικές συναλλαγές με τις δημόσιες υπηρεσίες μιας χώρας συγκαταλέγονται στην ηλεκτρονική διακυβέρνηση. Ως ηλεκτρονική διακυβέρνηση ορίζεται η αξιοποίηση των τεχνολογιών πληροφορικής και επικοινωνιών στις

δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες, ώστε να βελτιωθεί η παροχή δημοσίων υπηρεσιών και οι δημοκρατικές διαδικασίες καθώς και να ενισχυθεί η υποστήριξη των πολιτικών που ασκεί το δημόσιο.

Οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης κατατάσσονται σε πέντε επίπεδα.

- **Επίπεδο 1: Πληροφοριακές Υπηρεσίες.** Παρέχεται μόνο πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης της υπηρεσίας. Οι πληροφορίες αφορούν τα δικαιολογητικά που πρέπει να προσκομιστούν, τους φορείς που εμπλέκονται για την ολοκλήρωση της υπηρεσίας, τη σειρά εκτέλεσης των συναλλαγών που περιλαμβάνει η υπηρεσία κλπ.
- **Επίπεδο 2 : Επικοινωνιακές Υπηρεσίες.** Παρέχουν πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης της υπηρεσίας καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων κλπ) τα οποία οι χρήστες μπορούν να κατεβάσουν στον υπολογιστή τους, να τα τυπώσουν και να τα χρησιμοποιήσουν κατά τη συναλλαγή τους με το φορέα σε φυσικό επίπεδο.
- **Επίπεδο 3 : Διαδραστικές Υπηρεσίες.** Εκτός από πληροφορίες, προσφέρουν online φόρμες για συμπλήρωση και ηλεκτρονική αποστολή. Δεδομένου ότι περιλαμβάνουν online υποβολή στοιχείων από μέρους του χρήστη, προϋποθέτουν μηχανισμό αναγνώρισης, ταυτοποίησης και προστασίας των δεδομένων που αποστέλλει ο χρήστης της υπηρεσίας.
- **Επίπεδο 4 : Συναλλακτικές Υπηρεσίες.** Υποστηρίζουν λειτουργίες όπου ο χρήστης ολοκληρώνει τις συναλλαγές που περιλαμβάνει η υπηρεσία (π.χ. πληρωμή ΦΠΑ). Το ότι μία ηλεκτρονική υπηρεσία δίνει τη δυνατότητα ολοκλήρωσης οικονομικών συναλλαγών συνεπάγεται τη δυνατότητα της πλήρους αποκατάστασης της αντίστοιχης μη-ηλεκτρονικής υπηρεσίας.
- **Επίπεδο 5 : Πιστοποιημένες Υπηρεσίες.** Παρέχουν προσυμπληρωμένες φόρμες στον χρήστη στο βαθμό που επιτρέπεται από το νομικό πλαίσιο και τον ενημερώνουν για υπηρεσίες που τον αφορούν ανάλογα με το κοινωνικό και οικονομικό του προφίλ.

Σύμφωνα με το επίπεδο 4 κατά την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι πολύ πιθανό να υπάρχει ανάγκη εκτέλεσης κάποιας οικονομικής συναλλαγής. Επομένως, για να είναι εφικτή η ηλεκτρονική ολοκλήρωση μιας τέτοιας υπηρεσίας, απαιτείται η συνεργασία των φορέων της

Δημόσιας Διοίκησης με χρηματοπιστωτικά ιδρύματα. Η συνεργασία αυτή συνίσταται σε δύο βασικές ενέργειες (εκτός από απαιτήσεις ταυτοποίησης, απόδειξη εκτέλεσης πληρωμής κλπ) :

- Καταβολή του οικονομικού τμήματος για την λήψη μιας υπηρεσίας από τον ενδιαφερόμενο(πολίτη/επιχείρηση) με ηλεκτρονικό τρόπο – χρέωση του λογαριασμού του ενδιαφερόμενου.
- Ενημέρωση του φορέα - παρόχου της υπηρεσίας προς τον ενδιαφερόμενο για την καταβολή του οικονομικού τμήματος – πίστωση του λογαριασμού του φορέα – παρόχου της υπηρεσίας.

5.2.1 Μέθοδοι Ηλεκτρονικών Πληρωμών

Τα βασικά μέσα που έχουν υιοθετηθεί και χρησιμοποιούνται σήμερα σε εμπορικές κυρίως συναλλαγές για την εκτέλεση ηλεκτρονικών πληρωμών είναι:

- Πιστωτικές κάρτες
- Χρεωστικές κάρτες
- Κάρτες αποθηκευμένης αξίας
- Ηλεκτρονικές επιταγές
- Web Banking

Από τα παραπάνω μέσα, οι πιστωτικές κάρτες και οι υπηρεσίες Web Banking είναι τα πλέον διαδεδομένα.

Η χρήση της πιστωτικής κάρτα ως μέσου εκτέλεσης ηλεκτρονικών πληρωμών διασφαλίζει σημαντικά την αποδοχή και τη διάδοση της υπηρεσίας, καθώς οι πολίτες είναι ιδιαίτερα εξοικειωμένοι με τη χρήση της, λόγω κυρίως της χρησιμοποίησής της σε καθημερινές εμπορικές συναλλαγές. Το ίδιο ισχύει και στην περίπτωση των υπηρεσιών Web Banking περισσότερες τράπεζες προσφέρουν σχετικές υπηρεσίες στους πελάτες τους.

5.2.2 Εφαρμογές Δημόσιων Ηλεκτρονικών Πληρωμών

Η χρήση ηλεκτρονικών μέσων για την εκτέλεση οικονομικών συναλλαγών (ηλεκτρονικών πληρωμών) με τους φορείς της δημόσιας διοίκησης μπορεί να βρει πληθώρα σημείων εφαρμογής, όπως:

- Πληρωμή παραβόλων

- Παραβολή προστίμων, πχ. του Κώδικα Οδικής Κυκλοφορίας, φορολογικών παραβάσεων
- Πληρωμή τελών, πχ ύδρευσης και αποχέτευσης, κυκλοφορίας
- Πληρωμή λογαριασμών επιχειρήσεων κοινής ωφέλειας
- Καταβολή φόρων, πχ δημοτικών φόρων, φόρου εισοδήματος, φόρου προστιθέμενης αξίας
- Καταβολή ασφαλιστικών εισφορών
- Πληρωμή δαπανών υγείας από ασφαλιστικούς οργανισμούς

5.2.3 Ηλεκτρονικές Συναλλαγές Πολίτη – Κράτους

Η σχέση Πολίτη - Κράτους (Citizen-to-Government, C2G) αναφέρεται στην άμεση κατανάλωση ηλεκτρονικών υπηρεσιών από τον πολίτη για προσωπική του χρήση. Σε αυτές τις υπηρεσίες συμπεριλαμβάνονται η πληρωμή Φόρων όπως ο Φόρος Εισοδήματος, προστίμων, κλήσεων, παραβόλων αλλά και η είσπραξη χρηματικών ποσών από το κράτος όπως η επιστροφή λόγω εκκαθάρισης του Φόρου Εισοδήματος, έκτακτες ενισχύσεις, μισθοδοσίες και συντάξεις.

Τα όρια των σχέσεων αυτών συχνά είναι δυσδιάκριτα όταν η ίδια οντότητα αναλαμβάνει το ρόλο τόσο του πολίτη όσο και της επιχείρησης απέναντι στο κράτος. Παραδείγματος χάριν, στην περίπτωση φυσικού προσώπου επιτηδευματία, όπου το ίδιο πρόσωπο υποβάλλει και πληρώνει δηλώσεις Φόρου Εισοδήματος Φυσικού Προσώπου αλλά και δηλώσεις Φόρου Προστιθέμενης Αξίας.

Στις υπηρεσίες ηλεκτρονικής διακυβέρνησης, το κράτος αναλαμβάνει το ρόλο μιας «επιχείρησης», η οποία προσφέρει ένα πλήθος ηλεκτρονικών υπηρεσιών στους πολίτες. Στην προσπάθεια να μειώσει τη γραφειοκρατία της δημόσιας διοίκησης και να βελτιώσει την ποιότητα των παρεχόμενων υπηρεσιών, επιδιώκει, όσο και μια επιχείρηση, να προωθήσει τη χρήση και την αποδοχή των υπηρεσιών αυτών από ένα όλο και μεγαλύτερο ποσοστό πολιτών. Προσπαθεί δηλαδή να μετατρέψει τους ευκαιριακούς επισκέπτες των κυβερνητικών ιστοχώρων σε τακτικούς χρήστες των κυβερνητικών ηλεκτρονικών υπηρεσιών.

Σε αυτό το κλίμα, το κέντρο βάρους της σχέσης κράτους – πολίτη μετατοπίζεται από την ανταπόκριση του κράτους στις ανάγκες των πολιτών, στη θεώρηση των πολιτών ως πελάτες - υποψήφιους καταναλωτές. Κι ενώ στους e-πολίτες

συγκαταλέγονται κατηγορίες χρηστών όπως οι web-surfers που φαίνονται απρόθυμοι να αφήνουν ίχνη της ταυτότητάς τους στο διαδίκτυο ή οι ευκαιριακοί χρήστες των υπηρεσιών που βλέπουν με σκεπτικισμό την εκχώρηση προσωπικών δεδομένων σε τρίτους, οι e-πελάτες είναι συνήθως έμπειροι χρήστες του διαδικτύου οι οποίοι δε διστάζουν να συμπληρώνουν ηλεκτρονικές φόρμες με προσωπικά τους στοιχεία στο διαδίκτυο ειδικά όταν ο αποδέκτης των στοιχείων αυτών αποπνέει την εμπιστοσύνη ενός κυβερνητικού φορέα.

Αυτή η θεώρηση αποκτά ιδιαίτερο βάρος στο χώρο των ηλεκτρονικών οικονομικών συναλλαγών, όπου τα δεδομένα που ανταλλάσσονται μπορεί να είναι ευαίσθητα οικονομικά δεδομένα ή στοιχεία που ως αντικείμενο υποκλοπής μπορεί να προωθήσουν το οικονομικό έγκλημα.

Στον πίνακα που ακολουθεί καταγράφονται ενδεικτικά ορισμένα από τα σημεία στα οποία λαμβάνει χώρα οικονομική συναλλαγή μεταξύ του πολίτη και του ευρύτερου δημοσίου τομέα. Ο πίνακας που παρουσιάζεται έχει δημιουργηθεί λαμβάνοντας ως βάση την καταγραφή των υπηρεσιών του δημοσίου τομέα του Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας.

Η μία διάσταση (Τομέας) προσδιορίζει τον τομέα, στα πλαίσια του οποίου παρέχεται η υπηρεσία, και η άλλη διάσταση (Κατηγορία Υπηρεσιών) προσδιορίζει το είδος της υπηρεσίας. Η κατηγορία Κρατικό Εισόδημα (Income-generating) περιλαμβάνει τις υπηρεσίες που απαιτούν πληρωμές σε σταθερή βάση από τον πολίτη προς το κράτος (π.χ. φορολογία, ασφαλιστική εισφορά κτλ.). Η κατηγορία Εγγραφή-Καταχώρηση (Registration) περιλαμβάνει τις υπηρεσίες που απαιτούν πληρωμές προκειμένου να ολοκληρωθεί κάποια υπηρεσία σχετικά με καταγραφή (π.χ. εγγραφή σε μητρώο). Η κατηγορία Επιστροφή-Επίδομα (Returns) περιλαμβάνει τις υπηρεσίες που απαιτούν την παροχή κάποιας μορφής επιδόματος (χρηματικού ή μη χρηματικού) από κάποιο φορέα του δημοσίου προς τον πολίτη. Η κατηγορία Άδεια (Permits and licenses) περιλαμβάνει τις υπηρεσίες που απαιτούν την πληρωμής του πολίτη προς κάποιο φορέα του δημοσίου στα πλαίσια της έκδοσης κάποιας άδειας (π.χ. οικοδομική άδεια, άδεια οδήγησης κτλ.).

Κάθε κελί του πίνακα είναι χωρισμένο σε 2 μέρη, το πάνω-αριστερά μέρος αναφέρεται σε υπηρεσίες που παρέχονται σε τοπικό επίπεδο (τοπική αυτοδιοίκηση) ενώ το κάτω-δεξιά μέρος αναφέρεται σε υπηρεσίες που

παρέχονται σε κεντρικό επίπεδο (κεντρική διοίκηση). Με τη λέξη «Υπάρχουν» επισημαίνεται η ύπαρξη των υπηρεσιών. Στην τελευταία στήλη παρουσιάζονται αθροιστικά τα σύνολα των υπηρεσιών.

Κατηγορία Υπηρεσιών / Τομέας	Κρατικό Εισόδημα (Income-generating)	Εγγραφή, Καταχώρηση (Registration)	Επιστροφή, Επίδομα (Returns)	Άδεια (Permits and licenses)	Σύνολο υπηρεσιών ανά τομέα
Κατάσταση πολιτών		Υπάρχουν	Υπάρχουν	Υπάρχουν	1 / 7
Άμυνα, Ασφάλεια, Δικαιοσύνη			Υπάρχουν	Υπάρχουν / Υπάρχουν	1 / 4
Υγεία, Κοινωνική Ασφάλιση	Υπάρχουν		Υπάρχουν / Υπάρχουν	Υπάρχουν / Υπάρχουν	20 / 10
Οικονομία, Ανάπτυξη	Υπάρχουν / Υπάρχουν		Υπάρχουν / Υπάρχουν	Υπάρχουν / Υπάρχουν	80 / 6
Δημόσια Έργα, Περιβάλλον				Υπάρχουν / Υπάρχουν	2 / 1
Σύνολο υπηρεσιών ανά κατηγορία υπηρεσιών	2 / 8	0 / 1	7 / 5	95 / 14	104 / 28

Πίνακας 3: Οικονομικές Συναλλαγές Πολίτη Κράτους

Στον τομέα **Κατάσταση πολιτών**, πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία της **Άδειας** (π.χ. Ανανέωση Άδειας Παραμονής) ενώ σε κεντρικό επίπεδο συναντάμε πληρωμές τόσο στην κατηγορία της **Εγγραφής, Καταχώρησης** (π.χ. Έκδοση Διαβατηρίου) όσο και στην κατηγορία **Επιστροφή, Επίδομα** (π.χ. Έξοδα Κηδείας).

Στον τομέα **Άμυνα, Ασφάλεια, Δικαιοσύνη**, πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία της **Άδειας** (π.χ. Χορήγηση Πιστοποιητικού Εισαγγελικής Αρχής) ενώ σε κεντρικό επίπεδο συναντάμε πληρωμές τόσο στην κατηγορία της **Επιστροφής, Επιδόματος** (π.χ. Επίδομα Στράτευσης) όσο και στην κατηγορία **Άδεια** (π.χ. Εξαγορά στρατιωτικών υποχρεώσεων).

Στον τομέα **Υγεία, Κοινωνική Ασφάλιση**, πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία της **Επιστροφής** (π.χ. Επίδομα τυφλότητας, Επίδομα βαριάς νοητικής καθυστέρησης) και στην κατηγορία της **Άδειας** (π.χ. Χορήγηση Άδειας Άσκησης Επαγγέλματος Ιατρού) ενώ σε κεντρικό επίπεδο συναντάμε πληρωμές στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Πληρωμή ασφαλιστικών εισφορών εργαζομένου), στην κατηγορία **Επιστροφή, Επίδομα** (π.χ. Χορήγηση Επιδόματος Κυοφορίας και Λοχείας) και στην κατηγορία **Άδεια** (π.χ. Χορήγηση πιστοποιητικών υγείας).

Στον τομέα **Οικονομία, Ανάπτυξη**, πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Πληρωμή Δημοτικού Φόρου), στην κατηγορία **Επιστροφή, Επίδομα** (π.χ. Χορήγηση οικοπέδου σε ακτήμονες) και στην κατηγορία **Άδεια** (π.χ. Άδεια ίδρυσης & λειτουργίας Γυμναστηρίου, Τέλη ύδρευσης). Σε κεντρικό επίπεδο, πληρωμές συναντάμε στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Πληρωμή ΦΠΑ), στην κατηγορία **Επιστροφή, Επίδομα** (π.χ. Χορήγηση Δελτίου κοινωνικού τουρισμού) και στην κατηγορία **Άδεια** (π.χ. Έκδοση Άδειας κυκλοφορίας μοτοποδηλάτου).

Στον τομέα **Δημόσια Έργα, Περιβάλλον**, πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία **Άδεια** (π.χ. Οικοδομική Άδεια, Επανασύνδεση ηλεκτρικού ρεύματος) και σε κεντρικό επίπεδο στην κατηγορία **Άδεια** (π.χ. Σημείωμα Καταβολής Τέλους Έγκρισης Τύπου Μηχανήματος Έργων).

5.2.4 Ηλεκτρονικές Συναλλαγές Επιχείρησης – Κράτους

Η σχέση Επιχείρησης-Κράτους (Business-to-Government, B2G) αναφέρεται στη χρήση ηλεκτρονικών υπηρεσιών τόσο από επιχειρηματίες, επιχειρήσεις και εταιρίες για εμπορικούς σκοπούς (κερδοσκοπικούς ή μη) όσο και από το κράτος για αγορά προϊόντων και υπηρεσιών από επιχειρήσεις. Τέτοιες υπηρεσίες μπορεί να είναι η πληρωμή Φόρων όπως ο Φόρος Εισοδήματος Νομικών Προσώπων, ο Φόρος Προστιθέμενης Αξίας (ΦΠΑ), ο Φόρος Μισθωτών Υπηρεσιών (ΦΜΥ), η

πληρωμή ασφαλιστικών εισφορών, προστίμων αλλά και η είσπραξη χρηματικών ποσών από το κράτος ως αποτέλεσμα εμπορικής συναλλαγής.

Στον πίνακα που ακολουθεί καταγράφονται ενδεικτικά ορισμένα από τα σημεία στα οποία λαμβάνει χώρα οικονομική συναλλαγή μεταξύ της επιχείρησης και του ευρύτερου δημοσίου τομέα. Ο πίνακας που παρουσιάζεται έχει δημιουργηθεί λαμβάνοντας ως βάση την καταγραφή των υπηρεσιών του δημοσίου τομέα του Πλαισίου Ηλεκτρονικής Διακυβέρνησης και Διαλειτουργικότητας.

Η μία διάσταση (Τομέας) προσδιορίζει τον τομέα, στα πλαίσια του οποίου παρέχεται η υπηρεσία, και η άλλη διάσταση (Κατηγορία Υπηρεσιών) προσδιορίζει το είδος της υπηρεσίας. Κάθε κελί του πίνακα είναι χωρισμένο σε 2 μέρη, το πάνω-αριστερά μέρος αναφέρεται σε υπηρεσίες που παρέχονται σε τοπικό επίπεδο (τοπική αυτοδιοίκηση) ενώ το κάτω-δεξιά μέρος αναφέρεται σε υπηρεσίες που παρέχονται σε κεντρικό επίπεδο (κεντρική διοίκηση). Με τη λέξη «Υπάρχουν» επισημαίνεται η ύπαρξη των υπηρεσιών. Στην τελευταία στήλη παρουσιάζονται αθροιστικά τα σύνολα των υπηρεσιών.

Κατηγορία Υπηρεσιών / Τομέας	Κρατικό Εισόδημα (Income-generating)	Εγγραφή, Καταχώρηση (Registration)	Επιστροφή, Επίδομα (Returns)	Άδεια (Permits and licenses)	Σύνολο υπηρεσιών ανά τομέα
Άμυνα, Ασφάλεια, Δικαιοσύνη				Υπάρχουν	4 / 0
Υγεία, Κοινωνική Ασφάλιση	Υπάρχουν			Υπάρχουν / Υπάρχουν	20 / 7
Οικονομία, Ανάπτυξη	Υπάρχουν / Υπάρχουν			Υπάρχουν / Υπάρχουν	40 / 5
Δημόσια Έργα, Περιβάλλον				Υπάρχουν / Υπάρχουν	1 / 1
Σύνολο υπηρεσιών ανά κατηγορία υπηρεσίας	2 / 8	0 / 0	0 / 0	63 / 5	65 / 13

Πίνακας 4: Οικονομικές Συναλλαγές Επιχείρησης – Κράτους

Στον τομέα **Άμυνα, Ασφάλεια, Δικαιοσύνη** πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία της **Άδειας** (π.χ. Χορήγηση Άδειας σύστασης και έγκρισης καταστατικών Εταιρείας).

Στον τομέα **Υγεία, Κοινωνική Ασφάλιση** πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία της **Άδειας** (π.χ. Χορήγηση άδειας λειτουργίας Εργαστηρίων φυσικοθεραπείας, οδοντοτεχνικών εργαστηρίων, μονάδων αδυνατίσματος, διαιτολογικών γραφείων, εργαστηρίων αισθητικής κτλ.) ενώ σε κεντρικό επίπεδο συναντάμε στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Εργοδοτική Εισφορά) και στην κατηγορία **Άδεια** (π.χ. Χορήγηση πιστοποιητικών υγείας)

Στον τομέα **Οικονομία, Ανάπτυξη** πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Πληρωμή Δημοτικού Φόρου) και στην κατηγορία **Άδεια** (π.χ. Άδεια σύστασης και έγκρισης καταστατικών ανωνύμων εταιριών, Χορήγηση άδειας λειτουργίας υποκαταστήματος σχολής οδηγών, Διαγραφή Α.Ε.). Σε κεντρικό επίπεδο πληρωμές συναντάμε στην κατηγορία **Κρατικό Εισόδημα** (π.χ. Πληρωμή Φορολογίας Εισοδήματος Επιχείρησης, Πληρωμή ΦΠΑ) και στην κατηγορία **Άδεια** (π.χ. Χορήγηση Άδειας Ίδρυσης Φροντιστηρίων).

Στον τομέα **Δημόσια Έργα, Περιβάλλον** πληρωμές συναντάμε σε τοπικό επίπεδο στην κατηγορία **Άδεια** (π.χ. Οικοδομική Άδεια, Επανασύνδεση ηλεκτρικού ρεύματος) και σε κεντρικό επίπεδο στην κατηγορία **Άδεια** (π.χ. Σημείωμα Καταβολής Τέλους Έγκρισης Τύπου Μηχανήματος Έργων).

5.2.5 Πλεονεκτήματα Ηλεκτρονικών Συναλλαγών με Δημόσιες Υπηρεσίες

Τα πλεονεκτήματα για τον πολίτη και τις επιχειρήσεις που συναλλάσσονται ηλεκτρονικά με τις δημόσιες υπηρεσίες είναι:

- Μείωση των διοικητικών βαρών, που συνεπάγεται η αυτοπρόσωπη παρουσία τους κατά τις συναλλαγές τους με τους φορείς του Δημοσίου.
- Μείωση του λειτουργικού κόστους της διοίκησης των δημόσιων υπηρεσιών.
- Περιορίζεται δραστικά ο χρόνος ολοκλήρωσης των διοικητικών διαδικασιών.
- Απαλλάσσει πολίτες και επιχειρηματίες από χρονοβόρες και γραφειοκρατικές διαδικασίες.

- Διαφάνεια των συναλλαγών μεταξύ πολιτών/επιχειρήσεων και δημόσιων υπηρεσιών.
- Δημιουργία και διάχυση της ψηφιακής γνώσης προς όλο τον πληθυσμό της χώρας.

5.2.6 Ηλεκτρονικές Συναλλαγές με Τράπεζες – e-Banking

Η ραγδαία εξάπλωση του internet έχει δημιουργήσει αρκετές νέες κατηγορίες υπηρεσιών. Μια από τις σημαντικότερες και πιο χρήσιμες είναι το e-banking, μέσω του οποίου είναι δυνατή η πραγματοποίηση τραπεζικών συναλλαγών από το σπίτι, το γραφείο ακόμα και το κινητό μας τηλέφωνο.

Στα πρώτα του βήματα το internet χρησίμευε μόνο για τη σύνδεση υπολογιστών με κύριο σκοπό την ανταλλαγή αρχείων. Στις μέρες μας η παραπάνω κατάσταση έχει μεταβληθεί σημαντικά, καθώς μια νέα γενιά υπηρεσιών έχει κάνει την εμφάνιση της. Μια από αυτές τις υπηρεσίες είναι το e-banking μέσω του οποίου ο χρήστης έχει τη δυνατότητα να πραγματοποιεί συναλλαγές με την τράπεζα του από την οθόνη οποιουδήποτε υπολογιστή.

Καθώς η συγκεκριμένη υπηρεσία υφίσταται αρκετά χρόνια έχει απαλχθεί από τα προβλήματα που ταλάνισαν τις πρώτες εκδοχές της ενώ υποστηρίζεται μεγάλος αριθμός λειτουργιών. Πλέον ο χρήστης έχει τη δυνατότητα, εκτός από στατιστικά στοιχεία για το λογαριασμό του, να κάνει μεταφορές χρημάτων σε άλλους λογαριασμούς, να ελέγχει την πορεία των πιστωτικών καρτών του, καθώς και να πληρώνει λογαριασμούς διαφόρων ειδών, όπως το λογαριασμό της ΔΕΗ. Παράλληλα, δεν είναι λίγες οι τράπεζες που προσφέρουν υπηρεσίες προστιθεμένης αξίας, όπως παρακολούθηση χαρτοφυλακίου ή δημιουργία ηλεκτρονικών αναφορών σχετικά με τις καταθέσεις του πελάτη.

Σημαντικό ρόλο εξάπλωσης του e-banking παίζει η εδραίωση παγκόσμια αποδεκτών προτύπων ασφαλείας, που έχει επιτευχτεί τα τελευταία χρόνια. Καταυτόν τον τρόπο τόσο η τράπεζα όσο και ο τελικός χρήστης-πελάτης δε χρειάζεται να ανησυχούν για ενδεχόμενη διαρροή «ευαίσθητων» στοιχείων, όπως αριθμοί πιστωτικών καρτών ή λογαριασμών. Παράλληλα, σημαντικό είναι ότι στη συντριπτική πλειοψηφία των περιπτώσεων δεν υπάρχει κόστος χρησιμοποίησης των υπηρεσιών. Αν και, όπως προαναφέρθηκε, το e-banking δεν αποτελεί μια νέα υπηρεσία στις χώρες του εξωτερικού, στην Ελλάδα ανάλογες υπηρεσίες άρχισαν

να είναι διαθέσιμες στο ευρύ κοινό τα τελευταία επτά χρόνια. Ευθύς εξ αρχής, η αποδοχή των περισσότερων τραπεζών (ειδικά όσων διαθέτουν διεθνή παρουσία με καταστήματα σε πολλές χώρες του εξωτερικού) ήταν ιδιαίτερα θερμή. Ταυτόχρονα, ικανοποιητικός ήταν και ο αριθμός των Ελλήνων που έχουν εκδηλώσει ενδιαφέρον, ενώ αξίζει να σημειωθεί ότι ο αριθμός αυξάνεται διαρκώς.
Από τα παραπάνω στοιχεία γίνεται αντιληπτό ότι υπάρχουν όλα τα απαραίτητα συστατικά για την επιτυχία μιας δύσκολης (λόγω του οικονομικού χαρακτήρα των συναλλαγών) υπηρεσίας, όπως το Internet Banking. Λαμβάνοντας δε υπόψη την αδιαμφισβήτητη ευκολία και ασφάλεια της συγκεκριμένης υπηρεσίας (είναι δυνατή για παράδειγμα η μεταφορά χρημάτων από τον υπολογιστή οποιουδήποτε Internet Cafe), εύκολα μπορούμε να καταλήξουμε στο συμπέρασμα ότι κάθε χρήστης έχει τη δυνατότητα να πραγματοποιήσει τραπεζικές συναλλαγές κάθε είδους εύκολα και με ασφάλεια οπουδήποτε και αν βρίσκεται.
Η υπηρεσία e-banking απευθύνεται σε όλους τους πελάτες των τραπεζών, δηλαδή σε φυσικά και νομικά πρόσωπα. Σκοπός των τραπεζών είναι όλο και περισσότεροι πελάτες να χρησιμοποιούν αυτήν την υπηρεσία για τις τραπεζικές συναλλαγές τους. Με τον τρόπο αυτό δίνεται η δυνατότητα στο δίκτυο να απαλλαγεί από συναλλαγές ρουτίνας μετατρέποντας παράλληλα το κατάστημα σε ένα συμβουλευτικό χώρο τραπεζικών προϊόντων και υπηρεσιών.
Οι πελάτες λοιπόν που επιθυμούν να χρησιμοποιούν το e-banking το μόνο που έχουν να κάνουν είναι να συμπληρώσουν μια αίτηση η οποία διαφέρει ανάλογα με το αν ο πελάτης είναι φυσικό ή νομικό πρόσωπο.
Αναλυτικότερα, οι εφαρμογές του e-banking είναι:

1) Ενημέρωση: Θα μπορούσαμε να πούμε πως με μια ματιά μπορεί κάποιος να ενημερωθεί για τα υπόλοιπα των λογαριασμών που διατηρεί σε κάποιο τραπεζικό κατάστημα όσο και των πιστωτικών καρτών του άπλα με την είσοδό του στην αντίστοιχη υπηρεσία. Επίσης πολύ εύκολα μπορεί να δει αναλυτικά όλες τις κινήσεις που έχει διεκπεραιώσει κατά τη διάρκεια ενός συγκεκριμένου διαστήματος. Ακόμα, δυνατότητα ενημέρωσης παρέχεται και για την κατάσταση άυλων τίτλων, προθεσμιακών καταθέσεων, αναλυτική παρουσίαση και αποτίμηση του προσωπικού χαρτοφυλακίου μετοχών με βάση της τελευταίας συνεδρίασης του Χ.Α.Α.και ενημέρωση

για την εκτέλεση των εντολών αγοραπωλησίας μετοχών, ώστε να μπορεί ο χρήστης να προβεί σε intra-ray πώληση μετοχών σε περίπτωση αγοράς,

2) Διαχείριση λογαριασμών: Με αυτήν την υπηρεσία δίνεται η δυνατότητα στον ιδιώτη ή στον επιχειρηματία χρήστη να μεταφέρει χρήματα σε λογαριασμούς δικούς του ή σε λογαριασμούς τρίτων σε άλλες τράπεζες έχοντας μειωμένη προμήθεια κατά 50% σε σχέση με το κατάστημα. Μπορεί αν θέλει να στείλει εμβάσματα σε άλλες τράπεζες μέσω του συστήματος DIASTRANSFER και το κυριότερο μπορεί να πληρώσει τις δόσεις πιστωτικών καρτών και λογαριασμούς δημοσίου, όπως, για παράδειγμα, αν ο χρήστης έχει υποβάλλει τη φορολογική του δήλωση μέσω της υπηρεσίας Taxisnet μπορεί να πληρώσει το Φ.Π.Α. μέσω του e-banking. Τέλος, γίνεται εξόφληση λογαριασμών ΔΕΗ και ΟΤΕ.

3) Ακόμα, μπορούν να ορίσουν, να μεταβάλλουν και να ανακαλέσουν πάγιες εντολές, να παραγγείλουν καρνέ επιταγών, να αλλάξουν τα προσωπικά τους στοιχεία, να δηλώσουν απώλεια της κάρτας όπως και να κάνουν αίτηση για έκδοση οποιασδήποτε πιστωτικής κάρτας.

Πλεονεκτήματα του E-Banking

- Εξοικονομούν χρόνο χωρίς να απαιτείται η παρουσία του πελάτη στην τράπεζα.
- Πραγματοποιούν με ασφάλεια τις συναλλαγές τους από το δικό τους χώρο.
- Απολαμβάνουν άμεση και ποιοτική εξυπηρέτηση.
- Υπάρχει δυνατότητα να επιλέξουν μέσα από πληθώρα εναλλακτικών προτάσεων και λύσεων.
- Χαμηλό έως μηδενικό κόστος διεκπεραίωσης τραπεζικών συναλλαγών.
- Δυνατότητα διενέργειας σύγχρονων τραπεζικών και χρηματιστηριακών συναλλαγών υπό τις καλύτερες τεχνολογικά συνθήκες.
- Προσφέρει 24 ώρες τη μέρα και 7 μέρες την εβδομάδα υπηρεσίες εφόσον θα έχουν πρόσβαση στο διαδίκτυο.
- Δίνει τη δυνατότητα να ταξιδεύουν ελευθέρα χωρίς να ανησυχούν για το αν θα έχουν πρόσβαση στο λογαριασμό τους.

Μειονεκτήματα του E-Banking

- Μερικές φορές προκειμένου να εγγραφούν στην υπηρεσία μπορεί να πάρει αρκετό καιρό να αποκτηθεί κωδικός πρόσβασης.
- Μπορεί να πάρει αρκετό καιρό να μάθει ο πελάτης να χρησιμοποιεί το σύστημα του e-banking.
- Αλλαγές που ίσως κάνει η τράπεζα μπορεί να προκαλέσει σύγχυση ή καθυστερήσεις.
- Οι πελάτες μπορεί να ανησυχούν για την ασφάλεια ή την ακρίβεια.
- Υπάρχουν ερωτήσεις και αμφιβολίες για το αν έχει γίνει η συναλλαγή ή όχι.
- Υπάρχει περίπτωση το σύστημα να είναι μπλοκαρισμένο ή να έχει μεγάλη κίνηση και η εισαγωγή στο σύστημα να μην είναι δυνατή.

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

Στην παρούσα πτυχιακή εργασία αναλύθηκε το ηλεκτρονικό εμπόριο και πιο συγκεκριμένα οι ηλεκτρονικές συναλλαγές. Με τον όρο ηλεκτρονικό εμπόριο εννοούμε την αγοραπωλησία προϊόντων και υπηρεσιών μέσω του Internet και διακρίνεται σε πέντε κατηγορίες: 1) Business-to-Government, όπου πραγματοποιούνται συναλλαγές μεταξύ κυβέρνησης και επιχειρήσεων, 2) Government-to-Citizen, δηλαδή οι συναλλαγές μεταξύ πολίτη και κυβέρνησης, 3) Business-to-consumer, όπου ένας καταναλωτής συναλλάσσεται με μια επιχείρηση μέσω του διαδικτύου, 4) Consumer-to-Consumer, όπου ένας καταναλωτής απευθύνεται συνήθως μέσω αγγελιών σε άλλους καταναλωτές – πιθανούς αγοραστές του προϊόντος ή της υπηρεσίας, και 5) Business-to-Business, όταν δύο επιχειρήσεις συναλλάσσονται μεταξύ τους.

Στην αρχή του ηλεκτρονικού εμπορίου οι πληρωμές δεν γίνονταν ηλεκτρονικά αλλά με άλλους, χρονοβόρους και μη λειτουργικούς τρόπους (π.χ. κατάθεση στην τράπεζα). Έτσι, δημιουργήθηκαν τα συστήματα ηλεκτρονικών πληρωμών. Με τον όρο ηλεκτρονικές πληρωμές εννοούμε κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες, ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις, οι οποίες εκτελούνται με τη μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Σήμερα, ηλεκτρονικές συναλλαγές μπορούν να γίνουν μέσω τηλεφώνου, μέσω διαδικτύου και μέσω κινητής τηλεφωνίας. Ο καταναλωτής – πολίτης μπορεί να κάνει τις συναλλαγές του με διάφορους τρόπους, όπως με πιστωτική κάρτα, ηλεκτρονικές επιταγές, ηλεκτρονικό πορτοφόλι.

Ένα ηλεκτρονικό σύστημα πληρωμών δεν είναι ασφαλές εάν δεν περιλαμβάνει κάποιες υπηρεσίες ασφαλείας όπως το να προστατεύει τον καταναλωτή από ανωνυμία, δηλαδή να μην γίνεται γνωστή η ταυτότητά του, και αυτό επιτυγχάνεται με την υπηρεσία μη ανίχνευσης θέσης όπου εξασφαλίζει ότι η διεύθυνση IP και το Host name του υπολογιστή του δεν αποκαλύπτονται. Πρέπει επίσης να προστατεύει από τη σύνδεση δύο διαφορετικών συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πελάτη με την υπηρεσία μη ανίχνευσης συναλλαγής πληρωμών η οποία κρύβει με λίγα λόγια τη σύνδεση μεταξύ συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πληρωτή. Ακόμα, τα δεδομένα της

συναλλαγής θα πρέπει να προστατεύονται από την κοινοποίησή τους σε τρίτους, ακόμα και σε κάποιους εμπλεκόμενους, όπως να μην αποκαλύπτονται τα στοιχεία της πιστωτικής του κάρτας στον έμπορα. Επίσης, με την υπηρεσία μη αποκήρυξη των μηνυμάτων της συναλλαγής πληρωμής προστατεύεται και ο έμπορας και ο καταναλωτής έτσι ώστε να μην μπορούν αργότερα να αποκηρύξουν την προέλευση ή την παραλαβή μηνυμάτων. Τέλος, πρέπει να εμποδίζει τους ωτακουστές ή τους ανέντιμους συμμετέχοντες να επαναχρησιμοποιήσουν τα μηνύματα που ανταλλάχθηκαν σε μια συναλλαγή πληρωμής με την υπηρεσία μη επανάληψης μηνυμάτων συναλλαγής. Τα συστήματα ηλεκτρονικών πληρωμών που χρησιμοποιούνται ευρέως στο διαδίκτυο είναι το CyberCash, το DigiCash, το SET (Secure Electronic Transactions), το Millicent, το Mondex και το CAFE.

Η πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω του Διαδικτύου σε πολλές περιπτώσεις αναστέλλεται όμως λόγω ζητημάτων ασφάλειας. Η ανασφάλεια και η αβεβαιότητα των χρηστών σχετικά με την εκτέλεση των ηλεκτρονικών συναλλαγών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους της εξάπλωσης του ηλεκτρονικού εμπορίου. Υπάρχουν, βέβαια, διάφοροι κίνδυνοι στο διαδίκτυο οι οποία όμως εάν οι πολίτες είναι ενημερωμένοι και οι επιχειρήσεις σωστά ασφαλισμένες δεν δημιουργούν προβλήματα στις συναλλαγές. Η προσπάθεια απόσπασης προσωπικών στοιχείων (Phising), οι κλοπές λογαριασμών και οι ιοί είναι μερικοί από αυτούς τους κινδύνους, που όμως εάν οι πολίτες είναι προσεκτικοί δεν θα χρειάζεται να νιώθουν φόβο.

Ωστόσο, όσο προσεκτικός και να είναι ένας χρήστης δεν αρκεί στο να μην υποκλαπούν τα προσωπικά του στοιχεία. Το γεγονός ότι για να πραγματοποιηθούν συναλλαγές μέσω διαδικτύου πρέπει τα δίκτυα των οργανισμών ηλεκτρονικού εμπορίου να είναι συνδεδεμένα στο διαδίκτυο τα καθιστά ευάλωτα σε επιθέσεις. Πρέπει να φυλάσσουν τα προσωπικά δεδομένα των πελατών τους γιατί περιέχονται πολλά ευαίσθητα προσωπικά δεδομένα. Με λίγα λόγια πρέπει να ασφαλίσουν την περίμετρο του ιδιωτικού τους δικτύου. Αυτό πετυχαίνεται με την εφαρμογή των Firewalls (φράγματα ασφαλείας) και των συστημάτων ανίχνευσης εισβολών IDS. Τα Firewalls ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο με απώτερο σκοπό την προστασία του δικτύου, ουσιαστικά είναι ένα «τείχος» ασφάλειας μεταξύ του μη ασφαλούς δημόσιου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και

αξιόπιστο. Τα συστήματα ανίχνευσης εισβολών (IDS) αποτελούν ένα ισχυρό εργαλείο για την ασφάλεια δικτύων, το οποίο συμπληρώνει τη λειτουργία των συστημάτων firewalls. Στην ουσία αυτά τα συστήματα προσπαθούν να ανιχνεύσουν οποιαδήποτε παράνομη δραστηριότητα στοχεύει σε δικτυακούς και υπολογιστικούς πόρους.

Ακόμη, πρέπει να πρέπει να είναι ασφαλείς και οι Web εξυπηρετητές (Web Servers). Ο web εξυπηρετητής πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης (web browser) του πελάτη στον εξυπηρετητή του καταστήματος. Οι επιθέσεις στους Web εξυπηρετητές είναι συχνό φαινόμενο γιατί μέσω αυτών διανέμονται όλες οι πληροφορίες στο διαδίκτυο. Συνήθως, για να είναι ακόμη πιο ασφαλή τα δίκτυα των οργανισμών χρησιμοποιούνται τα firewalls σε συνδυασμό με τους web εξυπηρετητές.

Κάτι ακόμη που πρέπει να ασφαλίσουν οι οργανισμοί είναι η ασφάλεια των Web εφαρμογών. Η Web εφαρμογή είναι μια εφαρμογή η οποία έχει σχεδιαστεί ώστε να πραγματοποιεί συγκεκριμένες διεργασίες, να επιτυγχάνει συγκεκριμένους στόχους και να εξάγει στον χρήστη την επιθυμητή πληροφορία ή αποτέλεσμα η οποία όμως είναι προσβάσιμη με έναν φυλλομετρητή (web browser) μέσω του internet ή κάποιου τοπικού δικτύου. Η ασφάλεια των Web εφαρμογών είναι πολύ σημαντική γιατί πρέπει να αυθεντικοποιείται η ταυτότητα του χρήστη όταν εισέρχεται στο σύστημα, να υπάρχει εμπιστευτικότητα των προσωπικών του στοιχείων, όπως επίσης να είναι πάντα διαθέσιμη στους χρήστες. Υπάρχουν πολλοί εχθροί, απειλές και επιθέσεις προς τις Web εφαρμογές όπως οι Crackers, η κλοπή δεδομένων και οι επιθέσεις μεταμφίεσης. Ο σχεδιασμός και η ανάπτυξη ασφαλών web εφαρμογών προϋποθέτει ότι πρέπει να εφαρμοστεί ασφάλεια και στα τρία στρώματα: Δικτύου (Network), Host και Εφαρμογής (Application).

Πιο συγκεκριμένα, οι εφαρμογές ηλεκτρονικού εμπορίου αποτελούν αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων και της πλαστοπροσωπίας. Με την κρυπτογραφία και πιο συγκεκριμένα με τα πρωτόκολλα ασφαλείας που ενσωματώνονται σε αυτήν αντιμετωπίζονται εύκολα. Το πιο διαδεδομένο πρωτόκολλο ασφαλείας είναι το πρωτόκολλο SSL.

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική

συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, μέχρι να αποκρυπτογραφηθεί.

Μία παραδοσιακή μέθοδος κρυπτογράφησης είναι η συμμετρική κρυπτογραφία η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κ.λπ).

Η ασύμμετρη κρυπτογραφία (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρήσουν την πληροφορία ασφαλή. Ο πιο γνωστός αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο DES ενώ υπάρχουν και ο Triple-DES, ο DESX κ.ά. Στην ασύμμετρη κρυπτογράφηση πιο συχνά συναντούμε τον αλγόριθμο RSA.

Μια άλλη τεχνολογία που παρέχει ασφάλεια είναι η ηλεκτρονική υπογραφή. Η ηλεκτρονική υπογραφή είναι μία μέθοδος τεκμηρίωσης με ηλεκτρονικά μέσα, που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις με σκοπό την διασφάλιση αφενός της γνησιότητας και της ακρίβειας του περιεχομένου του ηλεκτρονικού εγγράφου και αφετέρου της εξατομίκευσης του εκδότη του εγγράφου αυτού. Ουσιαστικά εγγυάται την αυθεντικότητα και την μη αλλοίωση

του κειμένου που αποστέλλεται. Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Ο Πάροχος Υπηρεσιών Πιστοποίησης παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού. Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού.

Σήμερα οι επιχειρήσεις ολοένα και περισσότερο εκσυγχρονίζουν την τεχνική τους υποδομή και αξιοποιούν τις σύγχρονες τεχνολογίες στην παραγωγική τους διαδικασία. Ειδικότερα, φροντίζουν για την αξιοποίηση της χρήσης του διαδικτύου στις συναλλαγές τους. Συνεπώς αναμένεται ότι η αύξηση των ηλεκτρονικά παρεχόμενων υπηρεσιών και η ένταξη σε αυτές των οικονομικών συναλλαγών από πλευράς των δημοσίων οργανισμών, θα αξιοποιηθεί από τις επιχειρήσεις.

Βλέπουμε ήδη ότι τα περισσότερα ηλεκτρονικά καταστήματα τηρούν τους κανόνες ασφαλείας και αναπτύσσουν τις λειτουργίες τους. Ενώ αρχικά είχαν απλή παρουσία στο διαδίκτυο χωρίς να προσφέρουν υπηρεσίες ηλεκτρονικών συναλλαγών, τώρα πια τα περισσότερα καταστήματα προσφέρουν τα προϊόντα τους ηλεκτρονικά. Τα πλεονεκτήματα για μια επιχείρηση είναι πολλά, όπως μείωση των κρίκων της προμηθευτικής αλυσίδας και την συνεχή προβολή και λειτουργία της. Για τους πελάτες της η 24ωρη υποστήριξη και λειτουργία της όπως επίσης και οι διευρυμένες επιλογές για τους πελάτες σε ανταγωνιστικές τιμές είναι κάποιοι από τους λόγους που προτιμούν να κάνουν τις συναλλαγές τους ηλεκτρονικά.

Τέλος, η ενημέρωση των επιχειρήσεων και η κατάλληλη εκπαίδευση των στελεχών τους αναφορικά με τη χρήση των ηλεκτρονικά παρεχόμενων υπηρεσιών του δημοσίου τομέα, αναμένεται να δώσει σημαντική ώθηση στη χρήση τους. Οι οικονομικές συναλλαγές αποτελούν ένα από τα βασικότερα και πλέον χρονοβόρα σκέλη της συναλλαγής μεταξύ δημόσιων οργανισμών, πολιτών και επιχειρήσεων. Λαμβάνοντας υπόψη την αναμενόμενη διευκόλυνση, την αποφυγή μετακινήσεων, την εξοικονόμηση χρόνου της δημόσιας διοίκησης, την εξοικονόμηση χρόνου των συναλλασσόμενων, την ασφάλεια, την ασφάλεια, την ενίσχυση της διαφάνειας και την καταπολέμηση της διαφθοράς που παρέχουν οι ηλεκτρονικές συναλλαγές, η ανάπτυξη για τη λειτουργία ολοκληρωμένων ηλεκτρονικών υπηρεσιών στις οικονομικές συναλλαγές μεταξύ δημόσιων φορέων, πολιτών και επιχειρήσεων, καθίσταται σήμερα αναγκαία περισσότερο από ποτέ, ιδιαίτερα σε διαλειτουργικότητα με τα πληροφοριακά συστήματα της δημόσιας διοίκησης.

Κλείνοντας λοιπόν αναφέρουμε ότι ο μοναδικός τρόπος για να κρατήσεις έναν υπολογιστή ασφαλή είναι να τον κλειδώσεις σε ένα δωμάτιο χωρίς καμία απολύτως επαφή με το εξωτερικό περιβάλλον. Ο κίνδυνος όμως στις ηλεκτρονικές συναλλαγές δε διαφέρει από τους κινδύνους των καθημερινών απλών συναλλαγών μας. Με λίγη προσοχή όμως από τις επιχειρήσεις και τους πελάτες μέσω αυτής της τεχνολογίας θα μπορέσουμε να κάνουμε τη ζωή μας ευκολότερη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Boaz B., (2005). Authenticated Key Exchange and the SSL Protocol.
- Hayoz M., (2003). Introducing SSL.
- Αγγελούδης Στέλιος, «Ηλεκτρονικό εμπόριο», Notizie, No6, Ιταλία 2000
- Douglas E. Comer (1996), Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet, Αθήνα: Κλειδάριθμος.
- Αλεξανδρίδου Ε., (2004). Ηλεκτρονικό Εμπόριο και Προστασία Καταναλωτή.
- Γκάδολος Ι., (1998). Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών.
- Βογιατζής Σ., (2002). Πράκτορες Λογισμικού και Ηλεκτρονικό Εμπόριο.
- ΕΕΤΤ, (2002). Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής.
- Ηλεκτρονικό εμπόριο, Δουκίδης Γ., Θεμιστοκλής Μ., Δράκος Β., Παπαζαγειροπούλου Ν., Οικονομικό Πανεπιστήμιο Αθηνών Εκδόσεις νέων τεχνολογιών.
- Ηλεκτρονικό εμπόριο, Αρσένης Πασχόπουλος και Παναγιώτης Σκαλτσάς, εκδόσεις Κλειδάριθμος 2 έκδοση ενημερωμένη με τις τελευταίες εξελίξεις 2001.
- Λυραντωνάκης Α., «Το ηλεκτρονικό εμπόριο στο Internet:Ανάγκη για μια κοινή γλώσσα συνεννόησης», Ευρωενωσιακό Οικονομικό Δελτίο Διοικήσεως Επιχειρήσεων, Αθήνα, Ιανουάριος-Φεβρουάριος 1999
- Κρασοπούλου Παναγιώτα, «Τα πλεονεκτήματα του ηλεκτρονικού εμπορίου», Ευρωενωσιακό Οικονομικό Δελτίο Διοικήσεως Επιχειρήσεων, Αθήνα,14 Αυγούστου 2003.
- Δρ. ΓΕΩΡΓΙΑΔΗΣ Χρ., «Προβλήματα Ασφάλειας στο Ηλκετρονικό Εμπόριο», Ε-Επιχειρείν – Πανεπιστήμιο Θεσσαλίας
- ΚΑΤΣΙΚΑΣ Σωκ., «Ο ρόλος της Υποδομής Δημόσιου Κλειδιού στην ανάπτυξη ηλεκτρονικών αγορών», Πανεπιστήμιο Αιγαίου.
- «Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων», Τμήμα Πληροφορικής και Τηλεπικοινωνιών, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2004-2005.

- Παναγιωτόπουλος Π., Δραγώνας Γ., Σκούρλας Χ.,(2001), Τηλεπληροφορική και Δίκτυα Υπολογιστών, Αθήνα: Εκδόσεις Νέων Τεχνολογιών.
- «Θεωρία Πληροφορίας και Κωδικοποίησης», Ελληνικό Ανοικτό Πανεπιστήμιο, Σχολή Θετικών Επιστημών και Τεχνολογίας, Πάτρα 2002.
- ΕΕΤΤ, (2002). Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής.
- Ομάδα Εργασίας Ε2 του ebusiness forum, (2003). Δεκάλογος για τις Ηλεκτρονικές Υπογραφές και τα Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης.

ΔΙΑΔΙΚΥΤΟ

www.taxheaven.gr

www.ermis.gov.gr

www.wikipedia.org

thezocalo.blogspot.com

www.asxetos.gr

www.saferinternet.gr

www.eexi.gr

www.go-online.gr

www.e-businessforum.gr

www.ebusiness-lab.gr

www.e-yliko.gr

www.techblog.gr

www.eett.gr