ανωτατο τεχνολογικο εκπαιδευτικο ιδρυμα κρητης
σχολη διοικησησ και οικονομιασ
τμημα διοικησησ επιχειρησεων

Η Ασφάλεια των ηλεκτρονικών συναλλαγών στο διαδίκτυο

Πτυχιακή Εργασία

Μουρσελλά Ελευθερία
Α.Μ 3017

Επιβλέπων καθηγητής:

Ρομπογιαννάκης Ιωάννης

ΠΕΡΙΛΗΨΗ

Η πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω του διαδικτύου σε πολλές περιπτώσεις αναστέλλεται λόγω ζητημάτων ασφάλειας. Η ανασφάλεια και η αβεβαιότητα των χρηστών σχετικά με την εκτέλεση ηλεκτρονικών συναλλαγών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους εξάπλωσης του ηλεκτρονικού εμπορίου.Οι χρήστες προκειμένου να πραγματοποιήσουν τις αγορές τους στο διαδίκτυο, πρέπει να είναι σίγουροι ότι τα προσωπικά τους δεδομένα προστατεύονται κατάλληλα και ότι δεν πρόκειται να πέσουν θύματα απάτης.

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο την Ασφάλεια των ηλεκτρονικών συναλλαγών στο διαδίκτυο. Στα πλαίσια της εργασίας αυτής γίνεται μια προσπάθεια παρουσίασης των σημαντικότερων θεμάτων που σχετίζονται με την ασφάλεια στο ηλεκτρονικό εμπόριο.

Αρχικά παρουσιάζονται οι σημαντικότερες τεχνολογίες ασφάλειας που σχετίζονται με το ηλεκτρονικό εμπόριο. Αναλύονται οι δυνατότητες και οι περιορισμοί δύο σημαντικών τεχνολογιών για την ασφάλεια περιμέτρου, των firewalls και των συστημάτων ανίχνευσης εισβολών (Intrusion Detection System, IDS). Περιγράφεται το πρωτόκολλο SSL (Secure Sockets Layer) ένα από τα πιο διαδεδομένα πρωτόκολλα ασφαλείας . Επιπλέον περιγράφονται οι ηλεκτρονικές πληρωμές και οι δυνατότητες που προσφέρουν οι υποδομές δημοσίου κλειδιού στην ασφάλεια των ηλεκτρονικών συναλλαγών. Τέλος περιγράφεται το κινητό ηλεκτρονικό εμπόριο του οποίου οι υπηρεσίες απαιτούν μεγαλύτερη προστασία ασφάλειας από ότι οι υπηρεσίες του απλού ηλεκτρονικού εμπορίου.

Secure electronic Internet transactions

ABSTRACT

The realization of electronic transactions through the internet in many cases is postponed because of security matters. The insecurity and uncertainty of users in relation to performing electronic transactions are probably the most important restrictive reasons for the expansion of the electronic commerce. The users, in order to fulfill their purchases in the internet they have to be sure that their personal data is well protected and that they are not going to become victims of fraud.

This project is about security of the electronic transactions over the Internet. Throughout this project we will present the most important matters having to do with the security in electronic commerce is made.

At first the most important security technologies that are related to the electronic commerce are presented. The potentials and restrictions of two important technologies for the network security, that is, firewalls and Intrusion Detection System (IDS) are analyzed. The protocol SSL (Secure Sockets Layer), which can offer security in applications of electronic commerce, are described thoroughly. In addition the electronic payments and the potential offered by the Public Key Infrastructure (PKI) in electronic transactions are described. In conclusion mobile commerce is described whose services require greater security protection than the services of plain electronic commerce.

ΕΥΧΑΡΙΣΤΙΕΣ

Η πραγματοποίηση της παρούσας πτυχιακής καθώς επίσης και η ολοκλήρωση των σπουδών μου δεν θα ήταν εφικτή χωρίς την συμβολή κάποιων ανθρώπων που βοήθησαν με την καθοδήγηση τους.

Καταρχήν θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της πτυχιακής μου εργασίας κ.Ιωάννη Ρομπογιαννάκη για την ευκαιρία που μου έδωσε να ασχοληθώ με το θέμα αυτό καθως και για την αμέριστη βοήθεια και κατανόηση του καθ' όλη την διάρκεια της πραγματοποίησης αυτής της εργασίας.

Τέλος ,θα ήθελα να ευχαριστήσω τους γονείς μου και την θεία μου για την στήριξη και την βοήθεια τους τόσο οικονομική όσο και ηθίκη καθ' όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

Σχήματα

Πίνακες

• Εισαγωγή

Με την ολοένα και ταχύτερη ανάπτυξη των τεχνολογιών και των επικοινωνιών και ιδίως την ραγδαία, τα τελευταία χρόνια, ανάπτυξη του διαδικτύου, η φύση και η δραστηριότητα του εμπορίου έχει αλλάξει. Μια νέα μορφή εμπορίου, το ηλεκτρονικό εμπόριο (electroniccommerce) 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, 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 (ElectronicDataInterchange, EDI). Η Ηλεκτρονική Ανταλλαγή Δεδομένων δημιουργήθηκε στις αρχές της δεκαετίας του ’70 και είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέπει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα.

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 (electronicbusiness). 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, πολλές επιχειρήσεις, 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.

Το ηλεκτρονικό εμπόριο εμφανίζεται με δύο τύπους δραστηριότητας και τρεις μορφές. Ως προς τους τύπους, το ηλεκτρονικό εμπόριο διακρίνεται ανάμεσα στο έμμεσο ηλεκτρονικό εμπόριο**,**όπου η παραγγελία των προϊόντων γίνεται μέσω Η/Υ, τα οποία στη συνέχεια παραδίδονται στον πελάτη με φυσικό τρόπο χρησιμοποιώντας μεταφορικά και ταχυδρομικά μέσα, και τοάμεσο ηλεκτρονικό εμπόριο, όπου η παραγγελία, πώληση αλλά και παράδοση προϊόντων και υπηρεσιών γίνεται ηλεκτρονικά (π.χ. πώληση προγραμμάτων λογισμικού, παροχή πληροφόρησης κ.α). Από την άλλη πλευρά οι πιο συνηθισμένες μορφές ηλεκτρονικού εμπορίου ανάλογα με τα μέρη που εμπλέκονται σε μια ηλεκτρονική συναλλαγή αφορούν:

Επιχείρηση προς Καταναλωτή (BusinesstoConsumer, B2C)

> Είναι ίσως η πιο κλασσική μορφή ηλεκτρονικού εμπορίου, όχι όμως και η πιο διαδεδομένη. Αποτελεί το ηλεκτρονικό ανάλογο των καθημερινών συναλλαγών για αγορά προϊόντων ή χρήση υπηρεσιών. Η επιχείρηση-προμηθευτής διατηρεί έναν

διαδικτυακό τόπο (site) στον οποίο παρουσιάζει τα προϊόντα της ή/και τις υπηρεσίες της. Ο τόπος αυτός καλείται ηλεκτρονικό κατάστημα ή και e-shop.

Το ηλεκτρονικό κατάστημα αποτελείται από ιστοσελίδες που παρουσιάζουν τα προϊόντα ή τις υπηρεσίες του καταστήματος. Ο χρήστης-επισκέπτης και πιθανός καταναλωτής μπορεί να περιηγηθεί στις ιστοσελίδες του καταστήματος, να δει τα παρουσιαζόμενα προϊόντα, να επιλέξει τις αγορές του και στο τέλος να προχωρήσει στη διαδικασία πληρωμής και τελικής προμήθειας του προϊόντος.

Η πληρωμή γίνεται συνήθως μέσω πιστωτικών καρτών, ενώ η παράδοση της παραγγελίας γίνεται είτε μέσω ταχυδρομείου είτε, σε περιπτώσεις που η παραγγελία αφορά ηλεκτρονικό υλικό, υπάρχει η δυνατότητα ηλεκτρονικής παραλαβής.

Το ηλεκτρονικό εμπόριο έχει γνωρίσει αρκετή διάδοση στον τομέα του λιανικού εμπορίου. Χαρακτηριστικά τέτοια παραδείγματα είναι η πώληση βιβλίων, CD, πακέτων λογισμικού αλλά οι κλάδοι δραστηριοτήτων των εταιρειών ηλεκτρονικού εμπορίου δεν σταματούν εδώ. Στο διαδίκτυο υπάρχουν ακόμα και super-market που δίνουν τη δυνατότητα πραγματοποίησης on-line αγορών.

Σε ότι αφορά τις υπηρεσίες εδώ εντάσσονται οι δυνατότητες home-banking, δηλαδή πραγματοποίηση τραπεζικών συναλλαγών με τη χρήση υπολογιστή (πληρωμή λογαριασμών, δάνεια), κράτηση εισιτηρίων, δωματίων κλπ. Σημειώνεται ότι σχεδόν όλες οι μεγάλες αεροπορικές εταιρείες παρέχουν τη δυνατότητα κράτησης θέσεων από τον δικτυακό τους τόπο. Συγκεκριμένα η εταιρεία EasyJet κάνει πάνω από το 75% των κρατήσεων της on-line.

Επιχείρηση προς Επιχείρηση (Business to Business, B2B)

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει τη συνδιαλλαγή μεταξύ επιχειρήσεων. Πρόκειται για τον δυναμικότερο και ταχύτερα αναπτυσσόμενο κλάδο του ηλεκτρονικού εμπορίου. Οι συναλλαγές Επιχείρησης-προς-Επιχείρηση, περιλαμβάνουν τις καθιερωμένες συναλλαγές της επιχείρησης με τους προμηθευτές αλλά με πραγματοποίηση των προμηθειών με ηλεκτρονικό τρόπο.

Το ηλεκτρονικό εμπόριο επιτρέπει στις επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες των προμηθειών, το κόστος, την ταχύτερη αποστολή τους και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επίσης κάνει ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και την παροχή καλύτερης εξυπηρέτησης σε πελάτες. Η διαχείριση των επαφών με εταίρους (διανομείς, μεταπωλητές, μετόχους) της επιχείρησης γίνεται πολύ πιο αποτελεσματική. Κάθε αλλαγή μπορεί να ανακοινώνεται μέσα από μια ιστοσελίδα και το ηλεκτρονικό ταχυδρομείο, εκμηδενίζοντας την ανάγκη για ομαδικές επιστολές και άλλες δαπανηρές μορφές ειδοποίησης. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς, και η πραγματοποίηση ηλεκτρονικών πληρωμών, βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές περιορίζουν το ανθρώπινο λάθος, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών.

Δημόσιοι Φορείς προς το Κοινό (Governmenttoconsumer,G2C)

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει τη δυνατότητα πληροφόρησης, ανταλλαγής πληροφοριών και διεκπεραίωσης λειτουργιών μεταξύ των δημόσιων φορέων και των πολιτών. Οι πολίτες (επιχειρηματίες ή μη) χρησιμοποιούν το Διαδίκτυο για να πληροφορηθούν και να φέρουν σε πέρας γραφειοκρατικές διαδικασίες.

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει κυρίως δύο πλαίσια δραστηριοτήτων:

- Παροχή δυνατότητας στις επιχειρήσεις για διεκπεραίωση των συναλλαγών τους με το κράτος, με ηλεκτρονικό τρόπο.
- Παροχή δυνατότητας στους πολίτες για διεκπεραίωση των υποθέσεων τους με δημόσιες υπηρεσίες, με ηλεκτρονικό τρόπο. Αυτή η μορφή ηλεκτρονικού εμπορίου αναμένεται να γνωρίσει έκρηξη τα επόμενα χρόνια καθώς ολοένα και περισσότερες υπηρεσίες πληροφόρησης και ενημέρωσης παρέχονται από κρατικούς φορείς μέσω Διαδικτύου. Συγκεκριμένα αναμένεται να αναπτυχθούν ηλεκτρονικές συναλλαγές για τις πληρωμές κοινωνικής πρόνοιας και ιδιωτικών φόρων.

Οφέλη από το ηλεκτρονικό εμπόριο

Το ηλεκτρονικό εμπόριο αλλάζει ριζικά την παραδοσιακή θεώρηση της δοσοληψίας και γι' αυτό το λόγο, παρουσιάζει σημαντικά οφέλη σε ότι αφορά τόσο τους καταναλωτές όσο και τις επιχειρήσεις που το υιοθετούν. Ακολουθούν κάποια βασικά πλεονεκτήματα του ηλεκτρονικού εμπορίου που αφορούν τους καταναλωτές:

- Υπάρχει απεριόριστη δυνατότητα επιλογής προϊόντων.
- Οι καταναλωτές έχουν τη δυνατότητα να κάνουν άμεση σύγκριση τιμών στα προϊόντα που αγοράζουν.
- Παρέχεται η δυνατότητα χρήσης του καταστήματος και πραγματοποίησης συναλλαγών σε οποιαδήποτε ώρα, οποιασδήποτε μέρας.
- Εξοικονομείται ο χρόνος που πιθανόν να σπαταλούταν σε πολύωρη αναμονή για εξυπηρέτηση και στην εμπλοκή με γραφειοκρατικές διαδικασίες.
- Αίρονται οι γεωγραφικοί φραγμοί στις αγορές.
- Εξατομίκευση των πληροφοριών και των περιεχομένων του καταστήματος με βάση τις προτιμήσεις και τις ιδιαιτερότητες του πελάτη.
- Το κόστος των προϊόντων που πωλούνται μέσω Διαδικτύου είναι κατά γενικό κανόνα πολύ χαμηλότερο από τις τιμές του εμπορίου, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από μεγάλο μέρος του λειτουργικού κόστους ενός πραγματικού καταστήματος (ενοικίαση χώρου και «αέρα», ηλεκτρικό, νερό κλπ) και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.

Το ηλεκτρονικό εμπόριο προσφέρει σημαντικά οφέλη στις επιχειρήσεις, μερικά από τα οποία παρουσιάζονται παρακάτω:

- Κάθε εταιρεία που έχει ηλεκτρονική παρουσία μπορεί να διευρύνει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της online μπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της, ακόμα και στο εξωτερικό. Με άλλα λόγια, κάθε επιχείρηση που έχει ένα ηλεκτρονικό κατάστημα, είναι σαν να έχει υποκαταστήματα σε πολλές περιοχές και μάλιστα με ελάχιστο λειτουργικό κόστος.

- Κάθε εταιρεία που χρησιμοποιεί τις νέες τεχνολογίες, όπως το διαδίκτυο, γίνεται

εξ'ορισμού πιο ανταγωνιστική, αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και με δεδομένο το ότι σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω του διαδικτύου, το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρεία που θέλει να είναι ανταγωνιστική.

- Οι ηλεκτρονικές συναλλαγές επιτρέπουν την αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή. Αυτό σημαίνει πως κάθε εταιρεία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τα γούστα των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο.

Ασφάλεια στο Ηλεκτρονικό Εμπόριο

Μελέτες αναδεικνύουν ότι η πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω του διαδικτύου σε πολλές περιπτώσεις αναστέλλεται λόγω ζητημάτων ασφάλειας. Η ανασφάλεια και η αβεβαιότητα των χρηστών σχετικά με την εκτέλεση ηλεκτρονικών συναλλαγών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους εξάπλωσης του ηλεκτρονικού εμπορίου. Οι χρήστες προκειμένου να πραγματοποιήσουν τις αγορές τους στο διαδίκτυο, πρέπει να είναι σίγουροι ότι τα προσωπικά τους δεδομένα προστατεύονται κατάλληλα και ότι δεν πρόκειται να πέσουν θύματα απάτης.

Ο χρήστης που κάνει μια αγορά σε πραγματικό χρόνο (on-line) πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής του κάρτας δε θα υποκλαπεί. Κάθε φορά που συνδιαλέγεται δικτυακά με την τράπεζα 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 κανείς άλλος εκτός από τον πραγματικό παραλήπτη τους.

Συνήθεις απαιτήσεις ασφάλειας των χρηστών σε περιβάλλον ηλεκτρονικών δοσοληψιών είναι: η εμπιστευτικότητα (confidentiality*)* και η ακεραιότητα (integrity)των διακινούμενων μηνυμάτων, η αυθεντικοποίηση (authentication*)* τουαποστολέα, η μη-αποποίηση (nonrepudiation) αποστολής και λήψης μηνύματος, η διαθεσιμότητα (availability)του συστήματος και η χρονοσήμανση (timestamping)αποστολής ή λήψης ενός μηνύματος. Σημαντική συνεισφορά στην ικανοποίηση των απαιτήσεων αυτών έχουν εφαρμογές της επιστήμης της Κρυπτογραφίας. Για παράδειγμα, οι ψηφιακές υπογραφές *(*digital signatures*)* χρησιμοποιούνται για να επαληθεύσουν το φορέα αποστολής δεδομένων, και να διασφαλίσουν τη μη τροποποίηση και μη αποποίηση ενός μηνύματος. Η κρυπτογράφηση και αποκρυπτογράφηση *(*encryption/decryption*)* αξιοποιούνται για τη διατήρηση της εμπιστευτικότητας των δεδομένων της επικοινωνίας.

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο την Ασφάλεια των ηλεκτρονικών συναλλαγών στο διαδίκτυο. Στα πλαίσια της εργασίας αυτής γίνεται μια προσπάθεια παρουσίασης των σημαντικότερων θεμάτων που σχετίζονται με την ασφάλεια στο ηλεκτρονικό εμπόριο, όπως είναι οι τεχνολογίες ασφάλειας, οι ηλεκτρονικές πληρωμές καθώς και για το κινητό ηλεκτρονικό εμπόριο.

- **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.

Για να υπάρχει όμως ασφάλεια στις εφαρμογές ηλεκτρονικού εμπορίου απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου (web server). Ο εξυπηρετητής διαδικτύου πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης του πελάτη στον εξυπηρετητή του καταστήματος. Οι εξυπηρετητές διαδικτύου διαχειρίζονται και διανέμουν τις πληροφορίες στο διαδίκτυο.

- ***Πρωτόκολλο Ασφάλειας SSL***

Το SSL (SecureSocketLayer) 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 (dataencryption), υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή (serverauthentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (clientauthentication) μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης (CertificatesAuthorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Επιπλέον εξασφαλίζει την ακεραιότητα των δεδομένων (dataintegrity), εφαρμόζοντας την τεχνική των MessageAuthenticationCodes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Για κάθε

κρυπτογραφημένη συναλλαγή δημιουργείται ένα κλειδί συνόδου (sessionkey) 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 NetscapeCommunicationsCorporation 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 webbrowser της Netscape, τον NetscapeNavigator.

Ιούλιος 1995: Εκδόθηκε ο αντίστοιχος webbrowser της Microsoft, ο InternetExplorer, 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 defacto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων. Το HTTP (HyperTextTransferProtocol) είναι ένα πρωτόκολλο που φροντίζει τη μεταφορά και τον τρόπο μετάδοσης δεδομένων στο διαδίκτυο. Ωστόσο το SSLv.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 SSLv.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 NetscapeNavigator.

Μάιος 1996: Το SSL περνά στη δικαιοδοσία του InternetEngineeringTaskForce -IETF, ο οποίος δημιουργεί την ειδική ομάδα εργασίας TLSgroup και μετονομάζει την νέα έκδοση του SSL, σε TLS (TransportLayerSecurity).

Η ομάδα εργασίας TLSgroup καθιερώθηκε το 1996 για να τυποποιήσει το πρωτόκολλο TransportLayerSecurity. Η TLSgroup εργάστηκε πάνω SSLv.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 TLSgroup.

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.

Τρόπος λειτουργίας του SSL

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό
της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.

Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.

Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.

Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που

θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.

Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

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

Σχήμα 21Η διαδικασία της χειραψίας των δύο συσκευών σύμφωνα με το πρωτόκολλο SSL.

- **Αντοχή του SSL σε Γνωστές Επιθέσεις**

Επίθεση Λεξικού (DictionaryAttack)

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.

ΒίαιηΕπίθεση (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.

Επίθεση Επανάληψης (ReplayAttack)

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 replayattack. 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.

ΕπίθεσηΠαρεμβολής (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.

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.

- ## 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.

- ***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 ομοιόμορφο 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 (NetworkAddressTranslator), 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 (hostsecurity).

- **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.

- ## Ζητήματα Σχεδίασης των Firewalls

Η υλοποίηση ενός firewall δεν αποτελεί τετριμμένο θέμα και δεν παρέχεται ενσωματωμένη σε κανένα λειτουργικό σύστημα. Ο λόγος είναι ότι ένα firewall αποτελεί περισσότερο φιλοσοφία προστασίας και λιγότερο υλικό και λογισμικό που παρέχει πλήρη προστασία από κάθε εξωτερική απειλή. Υπάρχει μια αντίληψη ότι το firewall εξασφαλίζει την πλήρη προστασία ενός δικτύου απέναντι σε κάθε είδους απειλή. Η αντίληψη αυτή είναι τελείως λανθασμένη και μπορεί να οδηγήσει το διαχειριστή ασφάλειας ενός οργανισμού ηλεκτρονικού εμπορίου στην καταστροφική άποψη ότι με την εγκατάσταση ενός firewall είναι εγγυημένη η ασφάλεια του εσωτερικού δικτύου του οργανισμού την οποία διαχειρίζεται.

Η εγκατάσταση ενός firewall αποτελεί σημαντική σχεδιαστική απόφαση για τους παρακάτω λόγους:

- Η εγκατάσταση ενός firewall επιφέρει καθυστέρηση στο χρόνο απόκρισης των

προγραμμάτων που υλοποιούν τις υπηρεσίες που παρέχει η ιστοθέση.

- Η εγκατάσταση ενός firewall θα επιφέρει αναστάτωση, για κάποιο χρονικό διάστημα, στο προσωπικό του οργανισμού μέχρι αυτό να εξοικειωθεί με τις ήδη υπάρχουσες υπηρεσίες, που όμως τώρα θα υλοποιούνται με διαφορετικό τρόπο. Αυτό συμβαίνει επειδή δεν υλοποιούνται όλες ανεξαιρέτως οι υπηρεσίες διαμέσου του firewall με διαφανή τρόπο ως προς το χρήστη.

- Κατά την εγκατάσταση ενός firewall, οι υπηρεσίες δε θα μπορούν να παρέχονται στους χρήστες για περιορισμένο διάστημα κάτι το οποίο μπορεί επίσης να προκαλέσει προβλήματα.

- Απαιτείται συνεχής συντήρηση και ενημέρωση ενός firewall, καθώς προστίθενται νέες υπηρεσίες και απαξιώνονται παλαιότερες.

Εφόσον ληφθούν υπόψη τα παραπάνω και παρθεί η απόφαση για την εγκατάσταση ενός firewall, υπάρχουν ορισμένα σχεδιαστικά ζητήματα τα οποία θα πρέπει να αντιμετωπιστούν. Τα ζητήματα αυτά περιλαμβάνουν τα εξής:

- **Χρηστικότητα (usability) του firewall**: Τα firewalls χρησιμοποιούνται για να παρέχουν ασφάλεια στα δίκτυα. Το πιο ασφαλές δίκτυο είναι αυτό που δεν συνδέεται με κανένα άλλο δίκτυο, κάτι το οποίο προφανώς δεν είναι καθόλου αποδοτικό, αφού οι χρήστες του δικτύου δε θα μπορούν να έχουν πρόσβαση σε εξωτερικούς πόρους και ούτε οι κλασσικές εφαρμογές ηλεκτρονικού εμπορίου θα μπορούν να πραγματοποιούνται. Πρέπει συνεπώς να γίνουν συμβιβασμοί μεταξύ ασφάλειας και χρηστικότητας.

- **Εκτίμηση του κινδύνου**: Η διασύνδεση με εξωτερικό δίκτυο περιέχει κινδύνους. Επομένως απαιτείται η εκτίμηση της επίδρασης που θα έχει η εισβολή μιας εξωτερικής οντότητας που αποκτά πρόσβαση στο δίκτυο. Οπότε πρέπει η σχεδίαση του firewall να γίνει με τέτοιο τρόπο ώστε ζώνες διαφορετικού κινδύνου να προστατεύονται διαφορετικά.

- **Εκτίμηση των απειλών**: Κατά τη διασύνδεση του δικτύου ενός οργανισμού με άλλα δίκτυα, απαιτείται η εκτίμηση των απειλών από τις οποίες κινδυνεύει το δίκτυο. Αν πρόκειται για διασύνδεση με το εξωτερικό τμήμα του ίδιου οργανισμού, τότε το επίπεδο των απειλών είναι χαμηλό αφού πρόκειται για έμπιστους συνεργάτες. Εάν όμως πρόκειται για διασύνδεση με το διαδίκτυο, υπάρχουν σοβαρές απειλές.

- **Εκτίμηση του κόστους**: Προκειμένου ένας οργανισμός να αποκτήσει firewall, έχει δύο επιλογές: είτε να αγοράσει ένα εμπορικό προϊόν, είτε να το κατασκευάσει ο ίδιος ο οργανισμός. Για να πάρει όμως τη σωστή απόφαση ο οργανισμός πρέπει να υπολογίσει ακριβώς το κόστος υλοποίησης του firewall.

- **Τύπος firewall**: Υπάρχουν διάφοροι τύποι firewalls. Είναι προφανές ότι πρέπει να επιλεγεί ο κατάλληλος τύπος firewall, ο οποίος ικανοποιεί τις ανάγκες του οργανισμού.

- **Πολιτική Σχεδίασης των Firewalls**

Όπως προαναφέρθηκε, το firewall αποτελεί μια φιλοσοφία ασφάλειας και βοηθά στην υλοποίηση μιας ευρύτερης πολιτικής ασφάλειας που καθορίζει τις υπηρεσίες και την πολιτική προσπέλασης σε ένα δίκτυο.

Υπάρχουν γενικά δύο επίπεδα πολιτικής ασφάλειας που επηρεάζουν άμεσα το σχεδιασμό, την εγκατάσταση και τη χρήση ενός firewall:

- Η υψηλού επιπέδου πολιτική ή αλλιώς πολιτική πρόσβασης σε υπηρεσίες. Αυτή καθορίζει τα πρωτόκολλα της στοίβας TCP/IP και τις υπηρεσίες που θα πρέπει να επιτρέπονται ή να απαγορεύονται από το προστατευόμενο δίκτυο.
- Η χαμηλού επιπέδου πολιτική ή αλλιώς πολιτική σχεδίασης του φράγματος ασφάλειας. Αυτή περιγράφει το πώς λειτουργεί το φράγμα ασφαλείας και υλοποιεί τους περιορισμούς στα πρωτόκολλα TCP/IP και στις υπηρεσίες, όπως αυτοί υπαγορεύονται από την πολιτική πρόσβασης υψηλού επιπέδου.

Η πολιτική ασφάλειας του firewall πρέπει να είναι όσο το δυνατό πιο ευέλικτη, λόγω του ότι το διαδίκτυο συνεχώς αλλάζει, προσφέρει καινούργιες υπηρεσίες, μεθόδους και επιχειρηματικές δυνατότητες και συνεπώς οι ανάγκες του οργανισμού μπορεί να αλλάζουν με το χρόνο. Οι καινούργιες υπηρεσίες όμως, εγείρουν και καινούργια θέματα ασφάλειας τα οποία πρέπει να αντιμετωπίσει η πολιτική ασφάλειας των firewalls.

Πολιτική Πρόσβασης σε Υπηρεσίες

Η πολιτική πρόσβασης σε υπηρεσίες ενός οργανισμού αποτελεί επέκταση της γενικότερης πολιτικής του οργανισμού για την προστασία των πληροφοριακών του πόρων. Για να είναι ρεαλιστική η πολιτική πρόσβασης σε υπηρεσίες πρέπει να διασφαλίζει την προστασία του δικτύου από υπαρκτούς κινδύνους ασφάλειας, ενώ ταυτόχρονα να παρέχει στους χρήστες ικανοποιητική πρόσβαση στους πόρους του δικτύου.

Μια τυπική πολιτική είναι να επιτρέπεται μερική πρόσβαση των έξω προς το δίκτυο και επιπλέον αυτή η πρόσβαση να δίνεται μόνο όταν είναι απαραίτητο και μόνο σε συγκεκριμένους εξουσιοδοτημένους χρήστες των οποίων η ταυτότητα πιστοποιείται.

Για να είναι το firewall που θα υλοποιήσει την πολιτική πρόσβασης επιτυχημένο, πρέπει αυτή να είναι ρεαλιστική και να αντικατοπτρίζει το επίπεδο ασφάλειας που απαιτείται για το δίκτυο του οργανισμού. Ένας δικτυακός τόπος υψίστης ασφάλειας και απόρρητων δεδομένων δεν χρειάζεται καθόλου την ύπαρξη firewall γιατί απλούστατα δεν θα πρέπει καν να είναι συνδεδεμένος στο διαδίκτυο. Μια ρεαλιστική πολιτική πρόσβασης σε υπηρεσίες είναι εκείνη που παρέχει μια ισορροπία ανάμεσα στην προστασία του ιδιόκτητου δικτύου από γνωστούς κινδύνους ασφάλειας και τη διατήρηση της πρόσβασης των χρηστών του δικτύου σε εξωτερικούς πόρους όπως το διαδίκτυο. Γενικά υπάρχει συμβιβασμός μεταξύ της προσβασιμότητας και της ασφάλειας των πόρων του συστήματος.

Πολιτική Σχεδιασμού του Firewall

Η πολιτική σχεδιασμού του firewall ορίζει του κανόνες που χρησιμοποιούνται από το firewall για την υλοποίηση της πολιτικής πρόσβασης σε υπηρεσίες. Υπάρχουν δύο γενικές στρατηγικές που μπορεί να υλοποιεί ένα φράγμα ασφάλειας:

- Να επιτρέπει τη διέλευση πακέτων που αντιστοιχούν σε κάθε υπηρεσία εκτός και αν μια υπηρεσία απαγορεύεται ρητά.
- Να απαγορεύει τη διέλευση πακέτων κάθε είδους υπηρεσίας εκτός και αν αυτή επιτρέπεται ρητά.

Ένα firewall που ακολουθεί την πρώτη στρατηγική επιτρέπει να περάσει κάθε είδος κίνησης υπηρεσιών και πρωτοκόλλων του TCP/IP, με εξαίρεση εκείνες τις υπηρεσίες και τα πρωτόκολλα που χαρακτηρίζονται ως απαγορευμένα από την πολιτική πρόσβασης. Από τη σκοπιά της ασφάλειας αυτή η στρατηγική είναι λιγότερο επιθυμητή αφού προσφέρει πολλές οδούς παράκαμψης του firewall από επίδοξους εισβολείς.

Ένα firewall που ακολουθεί τη δεύτερη στρατηγική αρνείται να εξυπηρετήσει την κίνηση όλων των υπηρεσιών και πρωτοκόλλων του TCP/IP εκτός και αν αυτές χαρακτηρίζονται ρητά ως επιτρεπόμενες από την πολιτική πρόσβασης. Από τη σκοπιά της ασφάλειας αυτή η στρατηγική προτιμάται, αν και είναι δυσκολότερο να υλοποιηθεί.

Για να οδηγηθεί μια επιχείρηση σε μια πολιτική σχεδίασης του firewall και τελικά σε ένα ολοκληρωμένο σύστημα που υλοποιεί την πολιτική αυτή, καλό θα ήταν να ξεκινήσει ακολουθώντας τη δεύτερη στρατηγική. Στη συνέχεια ο σχεδιαστής ασφάλειας πρέπει να λάβει υπόψη του τα εξής:

- Ποιες υπηρεσίες του Internet σχεδιάζει η επιχείρηση να χρησιμοποιήσει (π.χ. Telnet, ftp).
- Πώς θα γίνεται η χρήση των υπηρεσιών (π.χ. σε τοπική βάση, διαμέσου του Internet, με χρήση dial-up υπηρεσίας από το σπίτι).
- Τι επιπρόσθετες ανάγκες και υπηρεσίες (π.χ. κρυπτογραφία) μπορούν να υποστηριχθούν.
- Πώς προσδιορίζεται η σχέση που συνδέει την ασφάλεια με τη λειτουργικότητα. Σε περίπτωση σύγκρουσης σε ποια από τις δύο έννοιες δίνεται προτεραιότητα.

- **Αρχιτεκτονική των Firewalls**

Ένα από τα βασικά ζητήματα σχεδίασης είναι η επιλογή κατάλληλου τύπου firewall, ο οποίος ανταποκρίνεται στις ανάγκες του οργανισμού που επιθυμεί την εγκατάσταση του. Τα firewalls ανάλογα με το επίπεδο στο οποίο λειτουργούν και ανάλογα με το βαθμό λειτουργικότητας τους διακρίνονται σε φίλτρα πακέτων και πύλες εφαρμογών.

- **Φίλτρα Πακέτων**

Ένα φίλτρο πακέτων (ή firewall επιπέδου δικτύου) είναι μια δικτυακή συσκευή με πολλές θύρες που εφαρμόζει ένα σύνολο κανόνων σε κάθε εισερχόμενο πακέτο IP ώστε να αποφασίσει για το αν θα του επιτραπεί η διέλευση ή θα απορριφθεί. Τα πακέτα IP φιλτράρονται ανάλογα με τις πληροφορίες που βρίσκονται στην επικεφαλίδα τους (header), όπως:

- Τον αριθμό πρωτοκόλλου που δείχνει το είδος του πρωτοκόλλου που χρησιμοποιείται.
- Τη διεύθυνση IP του αποστολέα.
- Τη διεύθυνση IP του αποδέκτη.
- Το TCP ή UDPport προέλευσης.
- Το TCPή UDPport προορισμού.
- Άλλες πληροφορίες.

Γενικά τα φίλτρα πακέτων δεν έχουν μνήμη κατάστασης. Κάθε πακέτο IP εξετάζεται ξεχωριστά και ανεξάρτητα του τι συνέβη στο παρελθόν. Υπάρχουν όμως και μερικά πιο εξελιγμένα φίλτρα πακέτων που διατηρούν μια λίστα με τα δεδομένα κατάστασης των πακέτων που φτάνουν στο φίλτρο. Οι πληροφορίες των πακέτων που προηγήθηκαν, επιτρέπουν στα μελλοντικά πακέτα που αντιστοιχούν στην ίδια σύνοδο να περάσουν ή να απορριφθούν χωρίς πολλούς ελέγχους. Δηλαδή τα συγκεκριμένα φίλτρα πακέτων ελέγχουν συνόδους δικτύου και όχι μεμονωμένα πακέτα. Μια σύνοδος δικτύου αποτελείται από πακέτα τα οποία κινούνται και προς τι δύο κατευθύνσεις. Τα απλά φίλτρα πακέτων απαιτούν δύο κανόνες για κάθε σύνοδο: Έλεγχος πακέτων τα οποία κατευθύνονται από υπολογιστή προέλευσης προς υπολογιστή προορισμού, και έλεγχος πακέτων τα οποία επιστρέφουν από υπολογιστή προορισμού προς υπολογιστή προέλευσης. Τα εξελιγμένα φίλτρα πακέτων δεν απαιτούν την ύπαρξη του δεύτερου κανόνα.

Επιπλέον με βάση τις πληροφορίες των παλαιότερων πακέτων που μπορούν να αποθηκεύσουν τα εξελιγμένα φίλτρα, μπορούν να εξαχθούν στατιστικά στοιχεία σχετικά με την κίνηση των πακέτων.

Σχήμα 31 Τοποθέτηση ενός φίλτρου πακέτων μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου

Τα περισσότερα φίλτρα πακέτων συμπεριφέρονται και σαν δρομολογητές και ονομάζονται «δρομολογητές διαλογής». Ένας απλός δρομολογητής όταν δεχθεί ένα πακέτο, κοιτάζει την επικεφαλίδα του και εξετάζει τη διεύθυνση προορισμού. Αν ο δρομολογητής γνωρίζει πώς να στείλει το πακέτο τότε το δρομολογεί. Αν όμως δε γνωρίζει επιστρέφει το πακέτο στον αποστολέα. Ένας δρομολογητής διαλογής εξετάζει το πακέτο διεξοδικότερα. Έτσι δεν καθορίζει μόνο εάν το πακέτο μπορεί να δρομολογηθεί προς τον προορισμό του, αλλά και το αν πρέπει να δρομολογηθεί, εφαρμόζοντας την πολιτική ασφάλειας που έχει καθορίσει ο οργανισμός. Συνεπώς κάθε δρομολογητής διαλογής φιλτράρει τα πακέτα και επιπλέον τα δρομολογεί.

Ένα firewall επιπέδου δικτύου (φίλτρο πακέτου, δρομολογητής διαλογής) μπορεί να εμποδίσει ή να επιτρέψει συγκεκριμένους τύπους συνδέσεων, εφαρμόζοντας πάντα την πολιτική προσπέλασης του οργανισμού στον οποίο είναι εγκατεστημένο. Οι εξυπηρετητές που παρέχουν συγκεκριμένες υπηρεσίες συνδέονται σε κάποια ειδική θύρα (port). Έτσι προσδιορίζοντας τον κατάλληλο αριθμό θύρας (π.χ. το TCPport 23 Telnet συνδέσεις) μπορεί το firewall να επιτρέψει ή μη συγκεκριμένη σύνδεση. Για παράδειγμα μπορεί κάποιο firewall να επιτρέπει τις υπηρεσίες e-mail (port 25), FTP (FileTransferProtocol, port 21), και Telnet (port 23) και να εμποδίζει όλες τις υπόλοιπες συνδέσεις.

Τα συγκεκριμένα firewalls είναι ίσως τα πιο απλά στην υλοποίηση και χρησιμοποιούνται κυρίως σε δικτυακούς τόπους με μικρή πολυπλοκότητα. Παρουσιάζουν όμως κάποια μειονεκτήματα και για το λόγο αυτό αποφεύγονται σε μεγαλύτερους δικτυακούς τόπους.

- ***Πλεονεκτήματα και Μειονεκτήματα Φίλτρων Πακέτων (και Δρομολογητών Διαλογής)***

Τα σημαντικότερα πλεονεκτήματα των φίλτρων πακέτων και των δρομολογητών διαλογής είναι τα εξής:

- Το φιλτράρισμα πακέτων είναι φθηνή τεχνολογία.
- Το φιλτράρισμα πακέτων είναι μια διαφανής διεργασία για τους χρήστες: Επειδή τα firewalls αυτής της κατηγορίας δεν ασχολούνται καθόλου με το τμήμα δεδομένων του πακέτου, δεν είναι απαραίτητο οι χρήστες να μάθουν κάποιες ιδιαίτερες εντολές για να τα χειρίζονται.
- Τα firewalls αυτής της κατηγορίας εγκαθίστανται και διαμορφώνονται πολύ εύκολα.
- Η τεχνολογία των φίλτρων πακέτων και των δρομολογητών διαλογής δεν στηρίζεται στην κρυπτογραφία και έτσι μπορεί να εξαχθεί από τις ΗΠΑ ελεύθερα. Αυτό επιτρέπει την πώληση προϊόντων που χρησιμοποιούν τεχνολογία φιλτραρίσματος πακέτων σε όλο τον κόσμο.

Τα φίλτρα πακέτων και οι δρομολογητές διαλογής έχουν ορισμένες αδυναμίες και μειονεκτήματα. Η κυριότερη αδυναμία τους έγκειται στην πολυπλοκότητα της ορθής ρύθμισης και διαχείρισης των κανόνων φιλτραρίσματος. Ειδικότερα:

- Το να οριστούν σωστά οι κατάλληλοι κανόνες φιλτραρίσματος είναι μια δύσκολη και επιρρεπής σε λάθη διαδικασία.
- Η σειρά με την οποία πρέπει να εισαχθούν οι κανόνες φιλτραρίσματος παίζει σπουδαίο ρόλο και καθιστά ακόμη πιο δύσκολη την εύρεση ενός κατάλληλου συνόλου κανόνων.
- Πρέπει μερικές φορές να υπάρχουν εξαιρέσεις στους κανόνες φιλτραρίσματος, ώστε να επιτρέπονται μερικά είδη υπηρεσιών που κανονικά θα έπρεπε να παρεμποδιστούν. Οι εξαιρέσεις αυτές καθιστούν το σύνολο των κανόνων πολύπλοκο.

Κάθε firewall επιπέδου δικτύου αποφασίζει για κάθε πακέτο αν θα το προωθήσει ή θα το απορρίψει βασιζόμενο σε μη πιστοποιημένη πληροφορία. Οποιοσδήποτε σταθμός θα μπορούσε να προσποιηθεί ότι είναι κάποιος άλλος, αλλάζοντας την IP διεύθυνση προέλευσης στα πακέτα του. Το πρωτόκολλο IPSP (IPSecurityPolicy) προστατεύει από τέτοιου είδους επιθέσεις. Έτσι ένας δρομολογητής διαλογής χρησιμοποιώντας το πρωτόκολλο IPSP μπορεί να ρυθμιστεί ώστε να απορρίπτει κάθε πακέτο IP που δεν είναι κατάλληλα πιστοποιημένο από μια έγκυρη επικεφαλίδα πιστοποίησης.

- **Πύλες Εφαρμογών (ApplicationGateways)**

Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή να υλοποιήσει μια αυστηρότερη πολιτική ασφάλειας. Στο μοντέλο πελάτη/εξυπηρετητή η πύλη εφαρμογών είναι μια ενδιάμεση διεργασία που τρέχει μεταξύ του πελάτη που ζητάει μια συγκεκριμένη υπηρεσία και του εξυπηρετητή που παρέχει αυτή την υπηρεσία. Δηλαδή η πύλη εφαρμογών λειτουργεί ως εξυπηρετητής από τη σκοπιά του πελάτη και ως πελάτης από τη σκοπιά του εξυπηρετητή. Μια πύλη εφαρμογών μπορεί να λειτουργεί είτε στο επίπεδο εφαρμογής είτε στο επίπεδο μεταφοράς του TCP/IP.

Αν η πύλη λειτουργεί στο επίπεδο εφαρμογής ονομάζεται πύλη επιπέδου εφαρμογής (application-levelgateway) ή απλά πύλη εφαρμογών. Αντίστοιχα αν η πύλη λειτουργεί στο επίπεδο μεταφοράς ονομάζεται πύλη επιπέδου κυκλώματος (circuit-levelgateway).

Οι περισσότερες πύλες που χρησιμοποιούνται σε διατάξεις firewalls λειτουργούν στο επίπεδο εφαρμογής, είναι δηλαδή πληρεξούσιοι εξυπηρετητές (proxyservers).

Όταν ένας χρήστης που βρίσκεται στο εσωτερικό δίκτυο θέλει να επικοινωνήσει με μια υπηρεσία του εξωτερικού δικτύου, η πύλη εφαρμογών παρεμβάλλεται. Δηλαδή αντί ο χρήστης να επικοινωνήσει άμεσα με την υπηρεσία, επικοινωνεί με την πύλη εφαρμογών η οποία διαχειρίζεται παρασκηνιακά όλη τη μεταξύ τους επικοινωνία. Συγκεκριμένα όταν ένας

πελάτης συνδέεται με την πύλη εφαρμογών χρησιμοποιώντας ένα από τα πρωτόκολλα εφαρμογής του TCP/IP, όπως το Telnet ή το FTP, η πύλη του ζητά πληροφορίες όπως ένα όνομα εισόδου (login) και ένα κωδικό πρόσβασης (password) για την πιστοποίηση της ταυτότητας του. Αν η πύλη αναγνωρίσει και δεχτεί το χρήστη, ο χρήστης της δίνει το όνομα του απομακρυσμένου συστήματος (υπηρεσία) που επιθυμεί να προσπελάσει, η πύλη εφαρμογών συνδέεται για λογαριασμό του χρήστη με αυτό το απομακρυσμένο σύστημα και εγκαθιστά μια δευτερεύουσα σύνδεση. Στη συνέχεια μετάγει τα δεδομένα της εφαρμογής μεταξύ των δύο συνδέσεων.

Στην περίπτωση μιας πύλης εφαρμογών μπορεί η κίνηση δεδομένων να παρακολουθείται και επιπλέον να επιβληθούν εξειδικευμένοι περιορισμοί σχετικά με την κίνηση αυτών από και προς το ιδιωτικό δίκτυο με σκοπό να αποτραπεί η υποκλοπή πολύτιμων προγραμμάτων ή δεδομένων.

Σχήμα 32 Τοποθέτηση μιας πύλης εφαρμογών μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου

Η πύλη εφαρμογών φιλοξενείται σε ένα υπολογιστή γενικού σκοπού, ο οποίος ονομάζεται Bastionhost (ή υπολογιστής-οχυρό). Ο υπολογιστής-οχυρό απαιτείται να παρέχει μεγάλη ασφάλεια διότι αποτελεί το κύριο σημείο επικοινωνίας για τους χρήστες του εσωτερικού δικτύου. Επιπλέον επειδή ο υπολογιστής-οχυρό εκτίθεται σε άμεσες επιθέσεις από το διαδίκτυο θα πρέπει να είναι ρυθμισμένος με τέτοιο τρόπο ώστε να είναι ιδιαίτερα ασφαλής. Συνήθως το λειτουργικό σύστημα του bastionhost είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητες του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται. Έτσι μειώνεται η πιθανότητα ύπαρξης τυχόν «οπών ασφαλείας» και συνεπώς ενισχύεται η ασφάλεια του bastionhost.

- ***Πληρεξούσιοι Εξυπηρετητές (ProxyServers)***

Μια πύλη επιπέδου εφαρμογής που τρέχει σε ένα υπολογιστή-οχυρό συνήθως στεγάζει διάφορους proxyservers. Οι proxyservers χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Αν ένας χρήστης του ενδοεπιχειρησιακού

δικτύου θέλει να έχει πρόσβαση σε ένα συγκεκριμένο εξυπηρετητή εφαρμογής TCP/IP στο διαδίκτυο, πρέπει η εφαρμογή του εξυπηρετούμενου να εγκαταστήσει μια σύνδεση με τον proxyserver που τρέχει για αυτή τη συγκεκριμένη εφαρμογή στον υπολογιστή-οχυρό. Ο proxyserver με τη σειρά του πρέπει να πιστοποιήσει την αυθεντικότητα του χρήστη και να τον εξουσιοδοτήσει για πρόσβαση.

Μπορούν να χρησιμοποιηθούν διάφορα σχήματα πιστοποίησης αυθεντικότητας και εξουσιοδότησης. Το απλούστερο σχήμα είναι ο proxyserver να κρατά μια λίστα με διευθύνσεις IP που επιτρέπεται να συνδεθούν σε εξωτερικούς εξυπηρετητές εφαρμογών. Αυτό το σχήμα δεν είναι πολύ ασφαλές, αφού οποιοσδήποτε μπορεί να προσποιηθεί ότι έχει εξουσιοδοτημένη διεύθυνση IP. Ένα πιο ασφαλές σχήμα είναι η χρήση ισχυρών μηχανισμών πιστοποίησης αυθεντικότητας μεταξύ του χρήστη και του proxyserver.

Μετά την επιτυχή πιστοποίηση αυθεντικότητας και εξουσιοδότηση του χρήστη, ο proxyserver εγκαθιστά μια δεύτερη σύνδεση TCP/IP με τον εξυπηρετητή της εφαρμογής που ζητήθηκε. Ο εξυπηρετητής της εφαρμογής μπορεί να θέλει και αυτός με τη σειρά του να πιστοποιήσει την αυθεντικότητα του χρήστη. Αν και εδώ πιστοποιηθεί επιτυχώς η αυθεντικότητα του χρήστη και εξουσιοδοτηθεί, ο εξυπηρετητής της εφαρμογής αρχίζει να εξυπηρετεί την αίτηση. Από τη στιγμή αυτή και μετά ο proxyserver απλά μετάγει δεδομένα εφαρμογής μεταξύ των δύο συνδέσεων. Για κάθε πακέτο που ρέει από τον εσωτερικό εξυπηρετούμενο στον εξωτερικό εξυπηρετητή, ο proxyserver συνήθως αντικαθιστά τη διεύθυνση IP του αποστολέα με τη δική του διεύθυνση. Έτσι οι εσωτερικές διευθύνσεις IP που χρησιμοποιούνται στο ενδοεπιχειρησιακό δίκτυο είναι ολοκληρωτικά κρυμμένες και δεν εκτίθενται στο διαδίκτυο.

- ***Πλεονεκτήματα και Μειονεκτήματα Πυλών Εφαρμογών (και ProxyServers)***

Υπάρχουν αρκετά πλεονεκτήματα σχετικά με τη χρήση πυλών επιπέδου εφαρμογής γενικότερα και proxyservers ειδικότερα, μερικά από τα οποία είναι τα εξής:

- Παρέχουν μεγαλύτερη ασφάλεια: Τα firewalls αυτού του τύπου έχουν τη δυνατότητα προσθήκης μιας λίστας ελέγχου προσπέλασης για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης προτού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες.

- Επιπλέον τα συστήματα αυτού του τύπου παρέχουν μεγαλύτερη ασφάλεια αφού «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxyserver εμποδίζοντας έτσι την απευθείας σύνδεση.

- Υπάρχουν κάποιοι «έξυπνοι» proxyservers που λέγονται ApplicationLayerGateways (ALGs), οι οποίοι μπορούν να μπλοκάρουν συγκεκριμένα τμήματα ενός πρωτοκόλλου. Για παράδειγμα ένας (ALGs) για FTP μπορεί να διαχωρίζει την εντολή “put” από την εντολή “get”. Έτσι ένας οργανισμός μπορεί να επιτρέπει στους χρήστες του να «κατεβάζουν» αρχεία αλλά να μην αφήνει τους έξω να παίρνουν τα αρχεία των δικών του συστημάτων.

- Παρέχουν καλύτερη καταγραφή συμβάντων: Ένα βασικό χαρακτηριστικό των firewalls αυτής της κατηγορίας είναι ο on-line έλεγχος, ο οποίος επιτρέπει την παρακολούθηση της δραστηριότητας και την καταγραφή συγκεκριμένων γεγονότων.

Τα firewalls επιπέδου εφαρμογής έχουν ορισμένα μειονεκτήματα:

- Ένα firewall επιπέδου εφαρμογής απαιτεί ένα ξεχωριστό proxyserver για κάθε υπηρεσία δικτύου: Οι πύλες επιπέδου εφαρμογής επιτρέπουν μόνο εκείνα τα πρωτόκολλα και υπηρεσίες TCP/IP για τα οποία υπάρχει proxyserver. Για παράδειγμα αν ένα firewall φιλοξενεί proxyservers για Telnet και FTP, τότε μόνο η κυκλοφορία Telnet και FTP επιτρέπεται, ενώ όλες οι άλλες υπηρεσίες παρεμποδίζονται. Εάν απαιτείται η υποστήριξη κάποιας άλλης υπηρεσίας από το firewall, είναι αναγκαίο να προστεθεί ένας νέος proxyserver. Συνεπώς αν παρουσιαστεί μια νέα υπηρεσία στο Internet και το firewall δεν έχει τον αντίστοιχο proxyserver, οι χρήστες του δικτύου δεν θα έχουν τη δυνατότητα πρόσβασης σε αυτή την υπηρεσία.
- Δεν είναι πάντοτε διαφανή προς το χρήστη
- Είναι δυσκολότερα στην υλοποίηση
- Η ταχύτητα και η απόδοση των firewalls επιπέδου εφαρμογής δεν είναι τόσο ικανοποιητική όσο των firewalls επιπέδου δικτύου.

- **Υβριδικά Συστήματα Ασφάλειας**

Συνήθως η κατασκευή ενός firewall δε στηρίζεται μόνο σε μια από τις αρχιτεκτονικές που αναφέρθηκαν πιο πάνω. Για την κατασκευή ενός firewall συνδυάζονται τα firewalls επιπέδου δικτύου (φίλτρα πακέτων, δρομολογητές διαλογής) και τα firewalls επιπέδου εφαρμογής (πύλες εφαρμογών, proxyservers). Τα συνδυασμένα firewalls που προκύπτουν ονομάζονται υβριδικά συστήματα ασφάλειας και οδηγούν στην επίλυση συνδυασμένων προβλημάτων. Τα προς επίλυση προβλήματα εξαρτώνται από τις υπηρεσίες τις οποίες θέλει να προσφέρει ένας οργανισμός στους χρήστες, καθώς και από το επίπεδο του κινδύνου που είναι διατεθειμένος να δεχτεί.

Σε ένα υβριδικό σύστημα ασφάλειας, τα λαμβανόμενα πακέτα υπόκεινται πρώτα στον έλεγχο τον οποίο διενεργεί το firewall επιπέδου δικτύου. Ακολούθως τα πακέτα είτε απορρίπτονται, είτε διέρχονται και κατευθύνονται προς τον προορισμό τους, είτε προωθούνται σε κάποιο proxyserver για περαιτέρω επεξεργασία. Όταν το εσωτερικό δίκτυο ενός οργανισμού απαιτεί την ασφάλεια την οποία παρέχει ένα firewall επιπέδου εφαρμογής για ορισμένες υπηρεσίες και την ταχύτητα και ευελιξία ενός firewall επιπέδου δικτύου για ορισμένες άλλες υπηρεσίες, τότε βέλτιστη λύση αποτελεί ένα υβριδικό σύστημα ασφάλειας.

Ένα υβριδικό σύστημα ασφάλειας είναι σαφώς ακριβότερο, καθώς παρέχει μεγαλύτερη

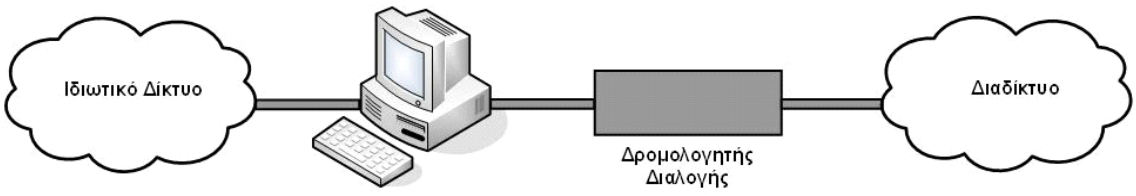
λειτουργικότητα και περισσότερα χαρακτηριστικά από ένα απλό firewall επιπέδου δικτύου.Τα εξής υβριδικά συστήματα ασφάλειας εφαρμόζονται σήμερα ευρέως στο διαδίκτυο:

- Διπλοσυνδεδεμένα Φράγματα Ασφάλειας (Dual-HomedFirewalls)
- Φράγματα Ασφάλειας Υπολογιστή Διαλογής (ScreenedHostFirewalls)
- Φράγματα Ασφάλειας Υποδικτύου Διαλογής (ScreenedSubnetFirewalls).

- ***Διπλοσυνδεδεμένα Φράγματα Ασφαλείας (Dual-HomedFirewalls)***

Τα διπλοσυνδεδεμένα firewalls αποτελούν καλύτερη εναλλακτική λύση σε σχέση με τα firewalls επιπέδου δικτύου, καθώς η πρόσβαση στο προστατευόμενο δίκτυο μπορεί να γίνει μόνο μέσω των proxyservers που τρέχουν στον υπολογιστή-οχυρό. Τα διπλοσυνδεδεμένα firewalls συνδυάζουν τόσο τα firewalls επιπέδου δικτύου, όσο και τα firewalls επιπέδου εφαρμογής, όπως κάθε υβριδικό σύστημα.

Ένα διπλοσυνδεδεμένο firewall αποτελείται από ένα υπολογιστή-οχυρό που είναι συνδεδεμένος και με τα δύο δίκτυα (ιδιωτικό δίκτυο και διαδίκτυο) και έχει απενεργοποιημένες τις δυνατότητες για προώθηση και δρομολόγηση IP. Αυτό σημαίνει ότι τα πακέτα IP από το ένα δίκτυο, το Internet, δε μπορούν να δρομολογηθούν άμεσα προς το εσωτερικό προστατευόμενο δίκτυο. Η IP κίνηση είναι πλήρως ελεγχόμενη, αφού τα συστήματα του εσωτερικού δικτύου και τα συστήματα του διαδικτύου δεν επιτρέπεται να επικοινωνήσουν άμεσα μεταξύ τους. Επιπλέον τοποθετείται και ένας δρομολογητής διαλογής μεταξύ του υπολογιστή-οχυρό και του διαδικτύου. Σκοπός του είναι να διασφαλίσει ότι κάθε πακέτο IP που φθάνει από το διαδίκτυο απευθύνεται με σωστό τρόπο στον υπολογιστή-οχυρό. Αν κάποιο πακέτο φθάνει με κάποια άλλη IP διεύθυνση προορισμού πρέπει να απορριφθεί.



Σχήμα 33 Ένα διπλοσυνδεδεμένο firewall.

Για λόγους απόδοσης μπορούν να χρησιμοποιηθούν περισσότεροι του ενός υπολογιστές-οχυρά, όπου όλοι θα είναι συνδεδεμένοι και στο εσωτερικό και στο εξωτερικό δικτυακό τμήμα.

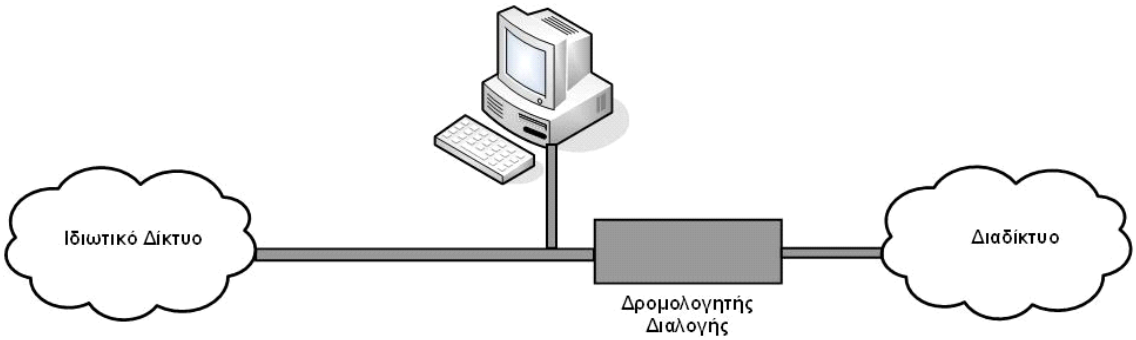
Το διπλοσυνδεδεμένο firewall είναι ένας απλός αλλά ασφαλής σχηματισμός. Η πρόσβαση στο ενδοεπιχειρησιακό δίκτυο μπορεί να περάσει μόνο από proxyservers που τρέχουν στον

υπολογιστή-οχυρό. Έτσι καμιά υπηρεσία δεν περνά εκτός από αυτές για τις οποίες υπάρχουν proxyservers. Με τον τρόπο αυτό υλοποιείται η πολιτική σχεδιασμού όπου κάθε υπηρεσία απαγορεύεται εκτός και αν αυτή ρητά επιτρέπεται.

Το διπλοσυνδεδεμένο firewall έχει το μικρότερο κόστος από τις τρεις υβριδικές αρχιτεκτονικές που εξετάζονται, αλλά παρουσιάζει ένα σοβαρότατο μειονέκτημα: Αποτελεί μοναδικό σημείοδυνητικής αποτυχίας στο δίκτυο, συνεπώς αν ένας κακόβουλος επιτιθέμενος εισβάλει σε αυτό, τότε όλο το δίκτυο εκτίθεται σε κίνδυνο. Επιπλέον υπάρχουν και κάποια πρακτικά προβλήματα στη χρήση αυτού του μηχανισμού που σχετίζονται με το ότι δεν υπάρχουν proxyservers για ιδιόκτητα εταιρικά TCP/IP πρωτόκολλα εφαρμογής, όπως τα LotusNotes, SQLnet και SAP.

- ***Φράγματα Ασφάλειας Υπολογιστή Διαλογής (ScreenedHostFirewalls)***

Ένα firewall υπολογιστή διαλογής παρέχει υπηρεσίες μέσω ενός υπολογιστή που είναι προσαρτημένος μόνο στο εσωτερικό δίκτυο. Στο σχηματισμό αυτό υπάρχει και ένας δρομολογητής διαλογής που συνδέει το εσωτερικό δίκτυο με το διαδίκτυο και πρέπει να είναι ρυθμισμένος έτσι ώστε να στέλνει όλη την κυκλοφορία IP που προέρχεται από το διαδίκτυο στην πύλη εφαρμογών που τρέχει στον υπολογιστή-οχυρό. Πριν όμως προωθήσει την κυκλοφορία IP σε αυτόν τον υπολογιστή, ο δρομολογητής διαλογής πρέπει να εφαρμόσει τους κανόνες φίλτρου πακέτων του. Μόνο η πληροφορία που είναι συμβατή με τους κανόνες διοχετεύεται στον υπολογιστή-οχυρό, ενώ όλη η άλλη πληροφορία απορρίπτεται. Συνεπώς οι πίνακες δρομολόγησης του δρομολογητή διαλογής πρέπει να προστατεύονται ισχυρά από εισβολή, διότι αν μια καταχώρηση στον πίνακα αλλάξει έτσι ώστε η κυκλοφορία να μην προωθείται στον υπολογιστή-οχυρό αλλά να στέλνεται απευθείας στο εσωτερικό δίκτυο, το firewall «αστοχεί».



Σχήμα 34 Ένας σχηματισμός firewall υπολογιστή διαλογής.

Ο μηχανισμός firewall υπολογιστή διαλογής είναι πιο ευέλικτος. Επιτρέπει στο δρομολογητή διαλογής να «περνάει» ορισμένες αξιόπιστες υπηρεσίες κατευθείαν στο εσωτερικό δίκτυο. Οπότε έχει τη δυνατότητα να επιτρέπει και στις υπηρεσίες για τις οποίες δεν υπάρχουν proxyservers, να περνάνε στο εσωτερικό δίκτυο, κάτι το οποίο δεν μπορούσε να

πραγματοποιήσει αρχιτεκτονική διπλοσυνδεδεμένων firewalls.

Επειδή η αρχιτεκτονική αυτή επιτρέπει και τη μεταφορά πακέτων από το Internet κατευθείαν στο εσωτερικό δίκτυο, ίσως φαίνεται πιο επικίνδυνη από την αρχιτεκτονική διπλοσυνδεδεμένων firewalls, η οποία δεν επιτρέπει σε κανένα πακέτο να περάσει απευθείας από το Internet στο εσωτερικό δίκτυο. Πρακτικά όμως η αρχιτεκτονική διπλοσυνδεδεμένων firewalls είναι επιρρεπής σε ενδεχόμενες αποτυχίες οι οποίες θα έχουν ως αποτέλεσμα τη μεταφορά πακέτων από το εξωτερικό προς το εσωτερικό δίκτυο. Από την άλλη πλευρά είναι ευκολότερο να αμυνθεί κανείς με τη χρήση ενός δρομολογητή ο οποίος παρέχει ένα περιορισμένο σύνολο υπηρεσιών, παρά με τη χρήση ενός υπολογιστή. Στις περισσότερες περιπτώσεις πάντως, η αρχιτεκτονική υπολογιστή διαλογής παρέχει μεγαλύτερη ασφάλεια και χρησιμότητα.

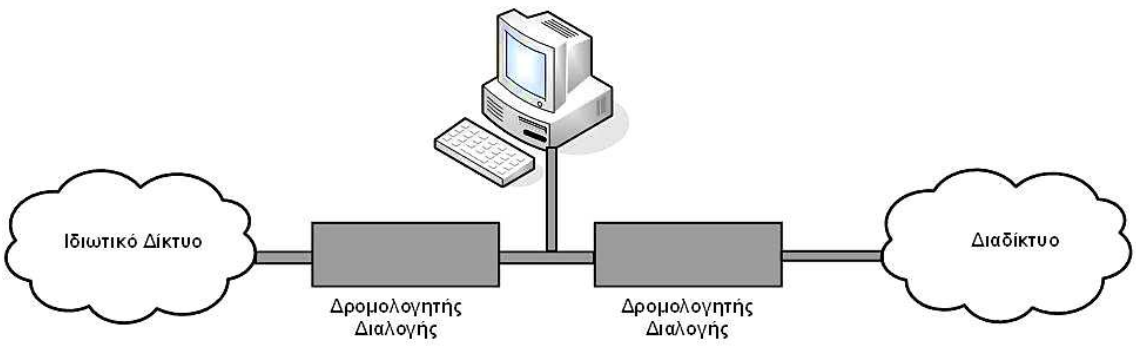
Η αρχιτεκτονική αυτή παρουσιάζει ένα σοβαρότατο μειονέκτημα: Βασίζεται σε δύο ξεχωριστές συσκευές ασφάλειας, το δρομολογητή διαλογής και τον υπολογιστή-οχυρό. Εάν κάποια από τις δύο αυτές συσκευές αποτύχει, τότε το δίκτυο εκτίθεται σε κίνδυνο. Αν για παράδειγμα ένας εισβολέας καταφέρει να παραβιάσει τον υπολογιστή-οχυρό, τότε θα έχει ελεύθερη πρόσβαση στο εσωτερικό δίκτυο. Ομοίως αν ο δρομολογητής εκτεθεί σε κίνδυνο, όλο το δίκτυο είναι πλέον ανασφαλές. Για αυτούς τους λόγους η πιο διαδεδομένη αρχιτεκτονική είναι η επόμενη.

- ***Φράγματα Ασφάλειας Υποδικτύου Διαλογής (ScreenedSubnetFirewalls)***

Ένα firewall υποδικτύου διαλογής αποτελείται από δύο δρομολογητές διαλογής με τον υπολογιστή-οχυρό να βρίσκεται ενδιάμεσα. Έτσι δημιουργείτε ένα εσωτερικό (περιμετρικό) υποδίκτυο διαλογής, ανάμεσα στο εσωτερικό και εξωτερικό δίκτυο.

Αυτή η αρχιτεκτονική εισάγει ένα επιπλέον επίπεδο ασφάλειας σε σχέση με την αρχιτεκτονική υπολογιστή διαλογής, προσθέτοντας το περιμετρικό υποδίκτυο το οποίο απομονώνει περισσότερο το εσωτερικό δίκτυο από το Internet.

Αυτό το περιμετρικό υποδίκτυο αναφέρεται και ως «αποστρατιωτικοποιημένη ζώνη» (DMZ-demilitarizedzone). Είναι δυνατό να υπάρχουν περισσότεροι του ενός υπολογιστές-οχυρά στο απομονωμένο αυτό δίκτυο για λόγους απόδοσης.



Σχήμα 35 Ένας σχηματισμός firewall υποδικτύου διαλογής.

Ο λόγος για τον οποίο προστίθεται ένα επιπλέον δίκτυο είναι ότι οι υπολογιστές-οχυρά αποτελούν τις πλέον ευπαθείς συσκευές του δικτύου, καθώς είναι τα συστήματα τα οποία κατεξοχήν μπορούν να δεχτούν επιθέσεις. Στην αρχιτεκτονική υπολογιστή διαλογής, ανάμεσα στον υπολογιστή-οχυρό και στο εσωτερικό δίκτυο δεν υπάρχει κανένας άλλος μηχανισμός άμυνας. Παραβιάζοντας κάποιος τον υπολογιστή-οχυρό μπορεί να έχει πλήρη πρόσβαση στο εσωτερικό δίκτυο. Η αρχιτεκτονική υποδικτύου διαλογής προσφέρει περισσότερη ασφάλεια, απομονώνοντας τον υπολογιστή-οχυρό στο περιμετρικό υποδίκτυο. Έτσι ακόμη και αν κάποιος εισβολέας αποκτήσει κάποια πρόσβαση στον υπολογιστή-οχυρό, θα έχει να αντιμετωπίσει ακόμη ένα δρομολογητή για μπορέσει να εισβάλει στο εσωτερικό δίκτυο.

Όπως έχει αναφερθεί, στο περιμετρικό υποδίκτυο περιλαμβάνονται δύο δρομολογητές διαλογής. Ο εσωτερικός δρομολογητής βρίσκεται μεταξύ του εσωτερικού δικτύου και του περιμετρικού υποδικτύου, ενώ ο εξωτερικός δρομολογητής βρίσκεται μεταξύ του περιμετρικού υποδικτύου και του εξωτερικού δικτύου, συνήθως του Internet.

Ο εσωτερικός δρομολογητής προστατεύει το εσωτερικό δίκτυο, τόσο από το Internet, όσο και από το περιμετρικό υποδίκτυο. Ο δρομολογητής αυτός αναλαμβάνει το μεγαλύτερο βάρος υλοποίησης του μηχανισμού φιλτραρίσματος πακέτων του firewall. Έτσι επιτρέπει να περάσουν μόνο επιλεγμένες υπηρεσίες από το εσωτερικό δίκτυο προς το Internet.

Ο εξωτερικός δρομολογητής προστατεύει τόσο το περιμετρικό υποδίκτυο όσο και το εσωτερικό δίκτυο από το Internet. Ο εξωτερικός δρομολογητής τείνει να επιτρέπει οτιδήποτε κατευθύνεται από το περιμετρικό υποδίκτυο προς τον εξωτερικό κόσμο. Σε γενικές γραμμές είναι απαραίτητο οι κανόνες οι οποίοι τίθενται για την προστασία των εσωτερικών μηχανών να συμφωνούν τόσο στον εσωτερικό όσο και στον εξωτερικό δρομολογητή. Οι μοναδικοί κανόνες φιλτραρίσματος πακέτων που εφαρμόζονται αποκλειστικά σε έναν εξωτερικό δρομολογητή, είναι αυτοί οι οποίοι προστατεύουν τον υπολογιστή-οχυρό και το εσωτερικό δίκτυο από το Internet.

Με αυτή την αρχιτεκτονική υποδικτύου διαλογής, το ιδιωτικό δίκτυο προστατεύεται ακόμη περισσότερο, αφού ένας επιτιθέμενος θα πρέπει να υπονομεύσει, όχι μόνο τον υπολογιστή-οχυρό αλλά και τους δρομολογητές για να φτάσει στο εσωτερικό δίκτυο. Έτσι δεν υπάρχει πλέον ένα και μοναδικό σημείο ευπάθειας το οποίο να θέτει σε κίνδυνο όλο το εσωτερικό δίκτυο.

- **Εγκατάσταση Firewall**

Η εγκατάσταση ενός firewall περιλαμβάνει μια σειρά διαδοχικά εκτελούμενων φάσεων. Αυτές είναι:

Σχεδιασμός Πολιτικής

Ο σχεδιασμός ενός firewall προϋποθέτει τον ακριβή προσδιορισμό των ορίων των διακριτών

περιοχών ασφάλειας του δικτύου, καθεμιά από τις οποίες λειτουργεί με βάση συγκεκριμένη πολιτική ασφάλειας. Στη συνέχεια επιλέγονται:

- Η βασική αρχιτεκτονική (αριθμός υπολογιστών, μέθοδοι συνδέσεων, λειτουργίες που εκτελούνται).
- Οι λειτουργίες που θα υλοποιηθούν (επίπεδο δικτύου, επίπεδο εφαρμογής, υβριδικός συνδυασμός).
- Το αρχιτεκτονικό σχέδιο του firewall (διπλοσυνδεδεμένο, με υπολογιστή διαλογής, με υποδίκτυο διαλογής).

Απόκτηση υλικού και λογισμικού για firewalls

Στη φάση αυτή εξασφαλίζεται η ύπαρξη του κατάλληλου εξοπλισμού (υλικό και λογισμικό), για να είναι δυνατή η εγκατάσταση, ο δοκιμαστικός έλεγχος, η λειτουργία και η επίβλεψη του firewall. Συγκεκριμένα εκτελείται:

- Προσδιορισμός των απαραίτητων τμημάτων υλικού (υπολογιστές, δρομολογητές, επεξεργαστές, μνήμη, δίσκος, κάρτες, καλώδια κλπ).
- Προσδιορισμός των απαραίτητων τμημάτων λογισμικού (λειτουργικά συστήματα, patches, devicedrivers, λογισμικό firewall, λογισμικό παρακολούθησης δικτύου).

Απόκτηση τεκμηρίωσης, εκπαίδευσης και υποστήριξης

Ανάλογα με τον επιλεγέντα αρχιτεκτονικό σχεδιασμό, πιθανότατα απαιτείται επιπρόσθετη εκπαίδευση και υποστήριξη από την προμηθεύτρια εταιρεία. Εάν ο οργανισμός δε διαθέτει εμπειρία στις τεχνολογίες που πρόκειται να υλοποιήσει, υπάρχει σοβαρό ενδεχόμενο να οδηγηθεί σε σφάλματα που θα μπορούσαν να προκαλέσουν καθυστέρηση στην εγκατάσταση, στη ρύθμιση και στη λειτουργία του firewall. Επιπλέον η συντήρηση του υλικού και του λογισμικού μπορεί να είναι τόσο περίπλοκη ώστε να απαιτείται εκπαίδευση και συνεχής υποστήριξη. Όλα αυτά πρέπει να μελετηθούν λεπτομερώς στη φάση αυτή.

Εγκατάσταση υλικού και λογισμικού

Στη φάση αυτή εγκαθίσταται και ρυθμίζεται το λειτουργικό σύστημα που θα υποστηρίξει το λογισμικό του firewall. Το λειτουργικό σύστημα περιλαμβάνει μόνο τις υπηρεσίες που είναι απαραίτητες για τη λειτουργία του firewall, ενώ όλες οι υπόλοιπες υπηρεσίες πρέπει να είναι απενεργοποιημένες. Στη συνέχεια το λογισμικό του firewall εγκαθίσταται στο επιλεγμένο υλικό για δοκιμαστικό έλεγχο.

Ρύθμιση της δρομολόγησης

Όταν ένα πακέτο φτάνει σε ένα δρομολογητή, ο δρομολογητής πρέπει να αποφασίσει για τη διάθεση του. Στόχοι του μηχανισμού δρομολόγησης είναι η απόδοση και η αξιοπιστία, όχι η υλοποίηση πολιτικής ασφάλειας.

Ρύθμιση των κανόνων φιλτραρίσματος πακέτων

Ο μηχανισμός φιλτραρίσματος ελέγχει το περιεχόμενο του πακέτου και με βάση ορισμένα κριτήρια και κανόνες υλοποιεί την πολιτική ασφάλειας αποφασίζοντας για την προώθηση ή απόρριψη του πακέτου. Εάν στην αρχιτεκτονική σχεδίαση περιλαμβάνονται και proxyservers, τότε πρέπει στη φάση αυτή να εγκατασταθεί το λογισμικό για κάθε υποστηριζόμενη υπηρεσία.

Ρύθμιση μηχανισμών καταγραφής και έγκυρης προειδοποίησης

Στη φάση αυτή πρέπει να γίνει επιλογή των περιπτώσεων φιλτραρίσματος πακέτων που θα καταγράφονται. Επιπλέον θα πρέπει να οριστούν εκείνα τα συμβάντα για τα οποία πρέπει να σημάνει συναγερμός.

Έλεγχος στο σύστημα firewall

Το σύστημα ελέγχεται στο περιβάλλον δοκιμών για τυχόν λάθη και ελλείψεις με χρήση συστημάτων ανίχνευσης εισβολής, σαρωτών θυρών (portsscanners), εργαλείων ανίχνευσης αδυναμιών, εργαλείων παραγωγής κίνησης στο δίκτυο και εργαλείων παρακολούθησης δικτύων. Επιπλέον εκτελούνται πιθανά σενάρια για επιβεβαίωση της ορθής λειτουργίας του firewall.

Εγκατάσταση του firewall

Αν το firewall πρόκειται να συνδέσει δύο ασύνδετα δίκτυα, τότε εγκαθίσταται σταδιακά. Αν το firewall πρόκειται να αντικαταστήσει ένα υπάρχον σύστημα, τότε το firewall εγκαθίσταται παράλληλα με τη λειτουργία του υπάρχοντος συστήματος, προσέχοντας πάντοτε να μην επηρεαστεί το παραγωγικό περιβάλλον λειτουργίας.

- **Συμπεράσματα**

Οι υποστηρικτές των firewalls τα θεωρούν σημαντικά, ως πρόσθετα μέτρα ασφάλειας, επειδή συγκεντρώνουν λειτουργίες ασφάλειας σε ένα και μόνο σημείο, απλοποιώντας την εγκατάσταση, τη ρύθμιση και τη διαχείριση.

Οι επικριτές των firewalls συνήθως επικαλούνται τη δυσκολία της χρήσης τους καθώς απαιτούν πολλές συνδέσεις και μηχανισμούς. Τους καταλογίζουν επίσης ότι αποτελούν εμπόδια στην ελεύθερη χρήση του Διαδικτύου. Ακόμη υποστηρίζουν ότι τα firewalls δημιουργούν μια ψευδαίσθηση ασφάλειας, οδηγώντας σε χαλάρωση των μέτρων ασφάλειας εντός του προστατευόμενου δικτύου.

Ωστόσο, όλοι συμφωνούν ότι τα firewalls είναι ισχυρά εργαλεία για την ασφάλεια των δικτύων, αλλά δεν αποτελούν πανάκεια για όλα τα προβλήματα ασφάλειας των δικτύων. Συνεπώς, δεν πρέπει να θεωρούνται ως υποκατάστατο μιας προσεκτικής διαχείρισης ασφάλειας μέσα σε ένα εσωτερικό δίκτυο.

Κάθε οργανισμός ηλεκτρονικού εμπορίου οφείλει να διαφυλάσσει τα προσωπικά δεδομένα των πελατών του και να λαμβάνει μέτρα ώστε αυτά να μην εκτίθονται σε μη εξουσιοδοτημένη πρόσβαση. Τα firewalls μπορούν να προσφέρουν αποτελεσματικές υπηρεσίες ελέγχου πρόσβασης για τα εσωτερικά δίκτυα των οργανισμών ηλεκτρονικού εμπορίου καθώς αποτελούν την πρώτη γραμμή άμυνας απέναντι σε εξωτερικές επιθέσεις. Συνεπώς τα firewalls αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο.

- ***ΣυστήματαΑνίχνευσηςΕισβολών (IntrusionDetectionSystems,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» (NetworkBasedIDS –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» (HostBasedIDS -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 (falsepositive), 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 (falsenegative), 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.

- **Δικτυακά Συστήματα Ανίχνευσης Εισβολών (NetworkBasedIDS –NIDS)**

Το δικτυακό σύστημα ανίχνευσης εισβολών συνήθως αποτελείται από δύο μέρη: τους αισθητήρες και τον σταθμό διαχείρισης-ανάλυσης. Οι αισθητήρες βρίσκονται στα τμήματα του δικτύου και παρακολουθούν για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος.

Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Λαμβάνουν όλη τη δικτυακή κίνηση (πακέτα) που διέρχεται από αυτούς και την αναλύουν. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στο σταθμό διαχείρισης-ανάλυσης. Ο σταθμός διαχείρισης-ανάλυσης πριν δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες, στον διαχειριστή του συστήματος μπορεί να πραγματοποιήσει επιπλέον ανάλυση.

Τα Δικτυακά συστήματα ανίχνευσης εισβολών χαρακτηρίζονται από ορισμένα πλεονεκτήματα, τα οποία τα καθιστούν πολύ αποτελεσματικά στη λειτουργία τους.

Πλεονεκτήματα

- Τα Δικτυακά συστήματα ανίχνευσης εισβολών λειτουργούν και ανιχνεύουν επιθέσεις σε πραγματικό χρόνο, οπότε προσφέρουν ταχύτατη ενημέρωση για την εξέλιξη μιας επίθεσης, ενώ μπορούν να προστατέψουν αυτόματα το δίκτυο πριν ακόμα γίνει ζημιά. Για παράδειγμα μπορεί να γίνει δυναμική ρύθμιση του firewall ώστε να σταματήσει τη σύνδεση με τη συγκεκριμένη IP από την οποία γίνεται η

επίθεση.

- Η εγκατάσταση του είναι απλή. Ένα Δικτυακό σύστημα ανίχνευσης εισβολών δεν απαιτεί μετατροπές στους server μιας επιχείρησης ή στους hosts για να εγκατασταθεί..

- Το δικτυακό σύστημα ανίχνευσης εισβολών δεν αποτελεί κρίσιμο παράγοντα για τη λειτουργικότητα του δικτύου, γιατί δε λειτουργεί ως δρομολογητής ή ως κάποια άλλη κρίσιμη συσκευή. Άρα τυχόν αποτυχία στο σύστημα ανίχνευσης εισβολών δε θα έχει σημαντική επίδραση στην επιχείρηση.

- Τα Δικτυακά σύστημα ανίχνευσης εισβολών ανιχνεύουν επιθέσεις που τα host-based συστήματα δεν μπορούν να ανιχνεύσουν, όπως π.χ. επιθέσεις που βασίζονται στα περιεχόμενα των IP πακέτων.

- Τα δικτυακά συστήματα ανίχνευσης εμποδίζουν τη διαγραφή των στοιχείων μιας επίθεσης από έναν επιτιθέμενο, αφού λόγω του ότι λειτουργούν σε πραγματικό χρόνο μπορούν να αποθηκεύουν τα στοιχεία αυτά σε ειδικούς χώρους. Έτσι ο επιτιθέμενος δεν μπορεί να διαγράψει τις αποδείξεις της επίθεσης του.

- Με τη σωστή τοποθέτηση τους (έξω από το προστατευόμενο δίκτυο) τα συστήματα ανίχνευσης εισβολών μπορούν να δουν επιθέσεις που προορίζονταν για το δίκτυο αλλά αποτράπηκαν από το firewall, και γενικότερα μπορούν να βοηθήσουν στη συλλογή πληροφοριών για το τι είδους προσπάθειες επίθεσης γίνονται στο δίκτυο, έτσι ώστε να υπάρξει η δυνατότητα καλύτερης διαμόρφωσης της πολιτικής ασφάλειας του δικτύου.

Μειονεκτήματα

Τα Δικτυακά συστήματα ανίχνευσης εισβολών παρουσιάζουν και αδυναμίες:

- Ένα Δικτυακό σύστημα ανίχνευσης εισβολών εξετάζει τη δικτυακή κίνηση μόνο στο τμήμα που είναι συνδεδεμένο. Δεν μπορεί να ανιχνεύσει μια επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου. Ένας μεγάλος οργανισμός για να καλύψει τις ανάγκες του σε δικτυακή κάλυψη, θα πρέπει να αγοράσει πολλούς αισθητήρες κάτι που σημαίνει επιπλέον κόστος.

- Τα Δικτυακά συστήματα ανίχνευσης εισβολών συνήθως χρησιμοποιούν ανάλυση signatures. Έτσι μπορούν να ανιχνεύσουν κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αδυνατούν να ανιχνεύσουν πιο πολύπλοκες επιθέσεις. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.

- Τα Δικτυακά συστήματα ανίχνευσης εισβολών δεν μπορούν να αναλύσουν κρυπτογραφημένες πληροφορίες μέσα σε ένα δίκτυο, οπότε και δεν μπορούν να ανιχνεύσουν τυχόν επιθέσεις και πληροφορίες σε κρυπτογραφημένη μορφή.

- **Συστήματα Ανίχνευσης Εισβολών Εγκατεστημένα σε Υπολογιστές (HostBasedIDS –HIDS)**

Τα HostBased συστήματα ανίχνευσης εισβολών ψάχνουν για ίχνη εισβολής στο τοπικό σύστημα του host. Συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό host, όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος.

Η συγκεκριμένη αρχιτεκτονική χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας.

Τα HostBased συστήματα ανίχνευσης εισβολών χαρακτηρίζονται με τη σειρά τους από ορισμένα πλεονεκτήματα, τα οποία τα καθιστούν αρκετά αποτελεσματικά στη λειτουργία τους.

Πλεονεκτήματα

- Τα HostBased συστήματα ανίχνευσης εισβολών συνήθως παρέχουν πολύ πιο λεπτομερείς πληροφορίες από ότι τα δικτυακά. Για παράδειγμα μπορούν να πουν τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι προσπάθησε να εκτελέσει μια επικίνδυνη εντολή.
- Τα HostBased συστήματα ανίχνευσης εισβολών έχουν μικρότερους falsepositive ρυθμούς από ότι τα δικτυακά συστήματα ανίχνευσης εισβολών. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο host είναι πολύ πιο εστιασμένο, παρά τα είδη κίνησης πακέτων που ρέουν στο δίκτυο.
- Σε ένα hostbased σύστημα είναι ευκολότερο να σχηματιστεί μια ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το loggingoff ενός επιτιθέμενου χρήστη.
- Τα HostBased συστήματα ανίχνευσης εισβολών μπορούν να χρησιμοποιηθούν και σε κρυπτογραφημένα περιβάλλοντα δικτύου, καθώς τα δεδομένα αποκρυπτογραφούνται μόλις εισάγονται στο σύστημα.

Μειονεκτήματα

- Τα HostBased συστήματα ανίχνευσης εισβολών έχουν τα ακόλουθα μειονεκτήματα:
- Τα hostbased συστήματα απαιτούν εγκατάσταση στη συγκεκριμένη συσκευή που θέλουμε να προστατέψουμε. Δηλαδή πρέπει να διαμορφώνονται και να ρυθμίζονται ξεχωριστά για κάθε σύστημα στο οποίο εγκαθίστανται πρώτη φορά, κάτι που δημιουργεί προβλήματα στο προσωπικό που τα διαχειρίζεται.

- Τα hostbased συστήματα είναι αρκετά ευάλωτα. Αγνοούν εντελώς το περιβάλλον του δικτύου, άρα ο χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των host που προστατεύονται.
- Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την οικονομική δυνατότητα να προστατέψουν ολόκληρο το δίκτυο τους με τη χρήση hostbased συστήματος.

- **Μοντέλα Εισβολών**

Τα συστήματα ανίχνευσης εισβολών προσδιορίζουν εάν κάποιες ενέργειες αποτελούν εισβολές, με βάση ένα ή περισσότερα μοντέλα εισβολών. Υπάρχουν τρία είδη μοντέλων:

Τα μοντέλα ανίχνευσης διαταραχών (anomalymodels) αποφαίνονται με βάση στατιστικά στοιχεία και ταξινομούν τις ενέργειες που είναι στατιστικά ασυνήθιστες ως ύποπτες. Τα μοντέλα κακής συμπεριφοράς (misusemodels) συγκρίνουν ενέργειες ή καταστάσεις με ακολουθίες που είναι ήδη γνωστό ότι αποτελούν εισβολές και τις ταξινομούν ως ύποπτες. Τα μοντέλα που βασίζονται στις προδιαγραφές (specification-basedmodels) ταξινομούν τις καταστάσεις που παραβιάζουν τις προδιαγραφές ως ύποπτες. Τα μοντέλα μπορεί να είναι είτε προσαρμοστικά, δηλαδή να αλλάζουν τη συμπεριφορά τους με βάση τις καταστάσεις των συστημάτων, είτε στατικά δηλαδή να μην τροποποιούνται κατά τη διάρκεια εκτέλεσης του συστήματος.

Στην πράξη τα μοντέλα συνδυάζονται συχνά και τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν συνδυασμό δύο ή τριών διαφορετικών τύπων μοντέλων.

- **Μοντέλα Ανίχνευσης Διαταραχών**

Τα μοντέλα ανίχνευσης διαταραχών θεωρούν ότι η απροσδόκητη συμπεριφορά αποτελεί τεκμήριο εισβολής. Δηλαδή υποθέτουν ότι κάθε επιθετική δραστηριότητα παρουσιάζει αναγκαστικά ανωμαλίες. Προφανώς καθιερώνεται ένα «προφίλ δραστηριότητας» στο οποίο η συμπεριφορά των χρηστών και των διεργασιών είναι η αναμενόμενη. Τα μοντέλα ανίχνευσης διαταραχών αναλύουν όλες τις καταστάσεις του συστήματος που διαφέρουν από το καθιερωμένο προφίλ και τις χαρακτηρίζουν ως επιθετικές. Με τον τρόπο που δουλεύουν τα μοντέλα αυτά παρουσιάζουν δύο προβλήματα:

Ασυνήθεις δραστηριότητες, που δεν έχουν χαρακτήρα εισβολής τις χαρακτηρίζουν ως επιθετικές (falsepositive).

Επιθετικές δραστηριότητες που δεν είναι ασυνήθεις, δεν τις χαρακτηρίζουν ως επιθέσεις (falsenegative).

Το δεύτερο πρόβλημα είναι ιδιαίτερα επικίνδυνο και πιο σοβαρό από το πρώτο πρόβλημα, αφού σκοπός των συστημάτων ανίχνευσης εισβολών είναι η ανίχνευση επιθέσεων.

Τα συστήματα ανίχνευσης διαταραχών είναι υπολογιστικά ακριβά, λόγω του κόστους του

ελέγχου και της συνεχούς ανανέωσης του προφίλ δραστηριότητας του συστήματος. Παρακάτω αναφέρονται τρία διαφορετικά μοντέλα ανίχνευσης διαταραχών.

- ***Μοντέλο Τιμών Κατωφλίου***

Το μοντέλο αυτό χαρακτηρίζει τις δραστηριότητες που γίνονται στο σύστημα ως επιθετικές ή μη, με βάση κάποιες καθορισμένες τιμές κατωφλίου (thresholdmetric). Το μοντέλο λειτουργεί ως εξής: Κάποιο συγκεκριμένο γεγονός αναμένεται να εμφανιστεί, σε δεδομένη χρονική περίοδο, κατ' ελάχιστο m και κατά μέγιστο n, όπου m και n συγκεκριμένες τιμές. Εάν κατά τη διάρκεια της συγκεκριμένης χρονικής περιόδου, το συγκεκριμένο γεγονός εμφανίζεται λιγότερο από m ή περισσότερο από n, τότε η συμπεριφορά θεωρείται διαταραγμένη.Ο καθορισμός των τιμών κατωφλίου αυξάνει την πολυπλοκότητα του μοντέλου.

- ***Μοντέλο Στατιστικών Ροπών***

Το μοντέλο αυτό χρησιμοποιεί στατιστικές ροπές. Ο αναλυτής γνωρίζει το μέσο και την τυπική απόκλιση (οι δύο πρώτες ροπές) και πιθανότατα άλλα μέτρα συσχέτισης (ροπές υψηλότερης τάξης). Αν οι τιμές βρίσκονται εκτός του αναμενόμενου διαστήματος γι' αυτή τη ροπή, η συμπεριφορά που αντιπροσωπεύουν οι τιμές θεωρείται διαταραγμένη. Επειδή η κατανομή (profile) της περιγραφής του συστήματος μπορεί να εμπεριέχει καθυστερήσεις, τα μοντέλα ανίχνευσης διαταραχών συνυπολογίζουν αυτές τις αλλαγές τροποποιώντας τους στατιστικούς κανόνες με βάση τους οποίους λαμβάνονται οι αποφάσεις. Επιπλέον η περιγραφή της κατανομής κάθε συστήματος ενημερώνεται σε τακτά χρονικά διαστήματα (π.χ. κάθε μέρα), με βάση τη συμπεριφορά που έχει παρατηρηθεί.

- ***Μοντέλο Πρόβλεψης Προτύπων***

Αυτό το μοντέλο ανίχνευσης εισβολών προσπαθεί να προβλέψει μελλοντικά γεγονότα με χρήση γεγονότων που έχουν ήδη συμβεί. Τα γεγονότα που προηγήθηκαν χρονικά έχουν θέσει το σύστημα σε μια συγκεκριμένη κατάσταση. Όταν συμβεί το επόμενο γεγονός, το σύστημα μεταβαίνει σε μια νέα κατάσταση. Προϊόντος του χρόνου μπορεί να αναπτυχθεί ένα σύνολο πιθανοτήτων μετάβασης. Όταν συμβεί ένα γεγονός που προκαλεί μια μετάβαση με μικρή πιθανότητα, το γεγονός κρίνεται διαταραγμένο. Οι διαταραχές δεν είναι πλέον βασισμένες σε στατιστικά των περιστατικών μεμονωμένων γεγονότων, αλλά σε ακολουθίες γεγονότων.

Το πρόβλημα στο μοντέλο αυτό είναι ότι διάφορα επιθετικά σενάρια που δεν έχουν προβλεφθεί από το σύστημα δε θα χαρακτηριστούν ως εισβολή. Δηλαδή αν μια ακολουθία γεγονότων A-B-E υπάρχει και είναι εισβολή, αλλά δε βρίσκεται στη βάση κανόνων, θα καταχωρηθεί απλά ως άγνωστη. Αυτό το πρόβλημα μπορεί να λυθεί μερικώς με το χαρακτηρισμό οποιοσδήποτε άγνωστου γεγονότος ως εισβολή (αυξάνοντας έτσι τον αριθμό falsenegatives). Στην φυσιολογική περίπτωση, ένα γεγονός χαρακτηρίζεται ως εισβολή εάν ταιριάζει με το αριστερό μέρος του κανόνα ανάλυσης και το δεξί μέρος είναι πολύ

διαφορετικό από το αποτέλεσμα της πρόβλεψης.

Υπάρχουν και πολλά πλεονεκτήματα σε αυτό το μοντέλο. Τα ακολουθιακά πρότυπα βασισμένα σε κανόνες μπορούν να ανιχνεύσουν ανώμαλες δραστηριότητες πολύ πιο εύκολα από άλλα μοντέλα. Επιπλέον τα συστήματα που κατασκευάζονται χρησιμοποιώντας αυτό το μοντέλο είναι ιδιαίτερα προσαρμόσιμα σε αλλαγές. Αυτό συμβαίνει γιατί τα λιγότερα καλά και αποτελεσματικά πρότυπα συνεχώς εξαλείφονται, ενώ παραμένουν μόνο τα πολύ ποιοτικά πρότυπα. Τέλος, οι ανώμαλες δραστηριότητες εντοπίζονται και αναφέρονται μέσα σε λίγα δευτερόλεπτα από τη στιγμή της λήψης της κρίσιμης πληροφορίας.

- **Μοντέλο Ανίχνευσης Κακής Συμπεριφοράς**

Η ανίχνευση κακής συμπεριφοράς (misusedetection) είναι η τεχνική για την αναζήτηση των καταστάσεων που γνωστό ότι είναι ανεπιθύμητες.

Η ανίχνευση κακής συμπεριφοράς απαιτεί τη γνώση όλων των ευπαθειών των συστημάτων που οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν. Το σύστημα ανίχνευσης εισβολών ενσωματώνει αυτή τη γνώση σε ένα σύνολο κανόνων. Ουσιαστικά το σύνολο αυτό περιέχει πρότυπα εισβολής. Οι κανόνες του συνόλου εφαρμόζονται στα γεγονότα που συμβαίνουν στο δίκτυο, ώστε να καθοριστεί εάν κάποια γεγονότα ταιριάζουν με κάποιους από τους κανόνες. Σε καταφατική περίπτωση συνάγεται ότι βρίσκεται σε εξέλιξη μια πιθανή εισβολή.

Τα συστήματα ανίχνευσης εισβολών που βασίζονται στο μοντέλο κακής συμπεριφοράς μοιάζουν πολύ με τα antivirus προγράμματα. Μπορούν να ανιχνεύσουν πολλά γνωστά πρότυπα εισβολής, αλλά δεν μπορούν να ανιχνεύσουν επιθέσεις που είναι άγνωστες στους δημιουργούς του συνόλου κανόνων. Οι άγνωστες επιθέσεις που έχουν διεξαχθεί, ή ακόμη και οι παραλλαγές γνωστών επιθέσεων, είναι δύσκολο να ανιχνευθούν. Με άλλα λόγια, τα μοντέλα κακής συμπεριφοράς προσπαθούν να αναγνωρίσουν γνωστές «κακές» συμπεριφορές.

Τα συστήματα ανίχνευσης εισβολών που βασίζονται στο μοντέλο κακής συμπεριφοράς χρησιμοποιούν συνήθως έμπειρα συστήματα για να αναλύσουν τα γεγονότα που συμβαίνουν στο δίκτυο και να εφαρμόσουν το σύνολο κανόνων σ’ αυτά.

Υπάρχει σαφής διαφορά μεταξύ της ανίχνευσης κακής συμπεριφοράς και της ανίχνευσης διαταραχών. Η ανίχνευση κακής συμπεριφοράς ανιχνεύει τις παραβιάσεις μιας πολιτικής. Η ανίχνευση διαταραχών ανιχνεύει τις παραβιάσεις του αναμενόμενου, οι οποίες θα μπορούσαν να παραβιάσουν ή να μην παραβιάσουν την πολιτική.

Μια ενδιαφέρουσα προσέγγιση σε αυτά τα συστήματα αποτελεί το σύστημα NIDES (NextGenerationIntrusionDetectionSystem), το οποίο βασίζεται τόσο στην ανίχνευση κακής συμπεριφοράς όσο και στην ανίχνευση διαταραχών. Ο ανιχνευτής διαταραχών χαρακτηρίζει τα γεγονότα ως επιθέσεις αν διαφέρουν πολύ από την αναμενόμενη συμπεριφορά. Για να το πετύχει αυτό, δημιουργεί προφίλ χρηστών που εξαρτώνται από πολλά διαφορετικά κριτήρια , περισσότερα από 30, όπως χρήση CPU, εντολές που χρησιμοποιήθηκαν, τοπική

δικτυακή δραστηριότητα, σφάλματα συστήματος κλπ. Τα προφίλ αυτά ανανεώνονται ανά περιοδικά διαστήματα. Ο ανιχνευτής κακής συμπεριφοράς του NIDES κωδικοποιεί γνωστές περιπτώσεις εισβολών και πρότυπα επιθέσεων. Η βάση των κανόνων μπορεί να αλλάζει για διαφορετικά συστήματα. Το πλεονέκτημα με το σύστημα αυτό είναι ότι έχουμε αυξημένες πιθανότητες να αναγνωρίσουμε μια εισβολή, αφού αν δεν την αναγνωρίσει ο ένας ανιχνευτής θα την εντοπίσει ο άλλος. Το NIDES όμως παρουσιάζει και κάποια μειονεκτήματα. Οι δύο ανιχνευτές που περιέχει το NIDES δε συνδέονται ισχυρά μεταξύ τους, αλλά ο καθένας εκτελεί τις δικές του λειτουργίες. Οποιεσδήποτε προσθήκες ή αφαιρέσεις από τη βάση κανόνων, πρέπει να λαμβάνουν υπόψη τις μεταξύ διαφορετικών κανόνων αλληλεξαρτήσεις. Επιπλέον το NIDES τρέχει σε σύστημα που δεν είναι το ίδιο με τα υπό παρακολούθηση συστήματα, κάτι που είναι επιπλέον κόστος.

- **Μοντέλο Ανίχνευσης Προδιαγραφών**

Η ανίχνευση προδιαγραφών αναζητά καταστάσεις που είναι γνωστό ότι δεν είναι επιθυμητές και όταν το σύστημα εισέρχεται σε μια τέτοια κατάσταση αναφέρεται μια πιθανή εισβολή.

Τα συστήματα ανίχνευσης εισβολών που βασίζονται στο μοντέλο προδιαγραφών αναζητούν ενέργειες εκτός των προδιαγραφών των βασικών προγραμμάτων. Κάθε πρόγραμμα διαθέτει ένα σύνολο κανόνων που διευκρινίζει τις επιτρεπτές ενέργειες. Εάν το πρόγραμμα προσπαθεί να προβεί σε οποιαδήποτε άλλη ενέργεια, ο μηχανισμός ανίχνευσης εισβολών αναφέρει πιθανή εισβολή. Αυτή η μέθοδος απαιτεί στο αρχικό στάδιο τη συλλογή προδιαγραφών για τα προγράμματα.

Η ανίχνευση που βασίζεται στις προδιαγραφές υπονοεί την υπόθεση ότι εάν όλα τα προγράμματα ακολουθούν τις προδιαγραφές τους, η πολιτική του συστήματος δεν μπορεί να παραβιαστεί.

Το μοντέλο ανίχνευσης προδιαγραφών βρίσκεται ακόμη στα αρχικά του στάδια. Μεταξύ των θετικών χαρακτηριστικών του μοντέλου αυτού είναι ότι εισβολές που χρησιμοποιούν άγνωστες επιθέσεις θα μπορούσαν να ανιχνευθούν, εφόσον βέβαια παραβιάζουν κάποιες προδιαγραφές.

Η ανίχνευση που βασίζεται στις προδιαγραφές ανιχνεύει τις παραβιάσεις των προδιαγραφών ανά πρόγραμμα. Υπάρχει η περίπτωση ένας επιτιθέμενος να επιτεθεί σε ένα σύστημα με τρόπο ώστε κανένα πρόγραμμα να μην παραβιάζει τις προδιαγραφές του, αλλά η συνδυασμένη επίδραση της εκτέλεσης όλων των προγραμμάτων κατά τη διάρκεια της επίθεσης να παραβιάζει την πολιτική ασφάλειας του συστήματος. Το μοντέλο ανίχνευσης με βάση τις προδιαγραφές δεν μπορεί προφανώς να ανιχνεύσει τέτοιου είδους επιθέσεις, αφού οι προδιαγραφές δεν παραβιάζονται. Το μοντέλο ανίχνευσης κακής συμπεριφοράς μπορεί να ανιχνεύσει τέτοια επίθεση, αναλόγως βέβαια με την πληρότητα του συνόλου κανόνων. Το μοντέλο ανίχνευσης με βάση τις διαταραχές θα μπορούσε επίσης να ανιχνεύσει την επίθεση, ανάλογα με το χαρακτηρισμό της αναμενόμενης συμπεριφοράς. Ουσιαστικά εάν η προδιαγραφή ενός προγράμματος είναι η ίδια η πολιτική ασφάλειας του, η βασισμένη σε προδιαγραφές ανίχνευση αποτελεί μια μορφή ενός συστήματος ανίχνευσης

κακής συμπεριφοράς.

- **Συστήματα Ανίχνευσης Εισβολών**

Στην παράγραφο αυτή μελετώνται δύο συστήματα ανίχνευσης εισβολών. Το πρώτο σύστημα είναι το NSM (NetworkSecurityMonitor). Το σύστημα αυτό εξετάζει απλώς την κυκλοφορία στο δίκτυο. ΤοδεύτεροσύστημαείναιτοDIDS (DistributedIntrusionDetectionSystem).

- **Παρακολούθηση της Κυκλοφορίας στο Δίκτυο για Εισβολές (NSM)**

Το NetworkSecurityMonitor – NSM είναι ένα σύστημα εντοπισμού εισβολών. Αποτελεί ένα networkbased σύστημα ανίχνευσης εισβολών. Δε χρησιμοποιεί τα στοιχεία ελέγχου από το host μηχάνημα, αλλά αντίθετα παρακολουθεί τη δικτυακή κίνηση για να εντοπίσει εισβολές. Από τη στιγμή που οι βασισμένες στο δίκτυο επιθέσεις είναι πλέον οι πιο διαδεδομένες, λόγω της εξάπλωσης του διαδικτύου, το NSM αποτελεί πολύτιμο εργαλείο στην ανίχνευση επιθέσεων.

Το NSM διαμορφώνει αρχικά μια κατανομή για την αναμενόμενη χρήση του δικτύου. Ακολούθως συγκρίνει την τρέχουσα χρήση του δικτύου με εκείνη της κατανομής. Αν η τρέχουσα χρήση διαφέρει από την αναμενόμενη, ερμηνεύεται ως διαταραχή. Δηλαδή το σύστημα αυτό ανιχνεύει επιθέσεις με βάση το μοντέλο ανίχνευσης διαταραχών, αφού οτιδήποτε αποκλίνει από το αναμενόμενο θεωρείται εισβολή. Συγκεκριμένα το NSM παρακολουθεί τη πηγή κίνησης του δικτύου, τον προορισμό και την παρεχόμενη υπηρεσία. Ορίζει μια μοναδική ταυτότητα σύνδεσης (connectionID) για κάθε σύνδεση. Στη συνέχεια συγκρίνει τα δεδομένα της κάθε σύνδεσης (π.χ. αριθμό πακέτων που στάλθηκαν κατά τη διάρκεια μιας καθορισμένης χρονικής περιόδου) με τα αναμενόμενα δεδομένα της σύνδεσης. Οποιοδήποτε δεδομένο εκτός του αναμενόμενου εύρους ερμηνεύεται ως διαταραχή.

Επιπλέον το σύστημα NSM καθορίζει ένα σύνολο ενεργειών, οι οποίες καταδεικνύουν επιθέσεις. Αν μια ενέργεια που πραγματοποιείται στο δίκτυο ταυτίζεται με μια ενέργεια του συνόλου, τότε το σύστημα αναφέρει επίθεση. Δηλαδή το σύστημα χρησιμοποιεί και το μοντέλο ανίχνευσης κακής συμπεριφοράς για ανίχνευση εισβολών στο δίκτυο. Συγκεκριμένα, ο αναλυτής του συστήματος NSM καταγράφει συγκεκριμένους κανόνες, με βάση τους οποίους συγκρίνεται η κίνηση του δικτύου. Οι κανόνες που χρησιμοποιήθηκαν αρχικά αφορούσαν τον έλεγχο για τυχόν υπερβολικό αριθμό προσπαθειών σύνδεσης, για τυχόν επικοινωνία ενός υπολογιστικού συστήματος με δεκαπέντε ή περισσότερα συστήματα ή για οποιαδήποτε προσπάθεια επικοινωνίας με ανύπαρκτο σύστημα.

Το πρωτότυπο σύστημα NSM αναπτύχθηκε στο UniversityofCaliforniaatDavis και εντόπιζε πολλές επιθέσεις. Όπως συμβαίνει σε όλα τα συστήματα ανίχνευσης εισβολών, το NSM κατέγραφε λανθασμένους συναγερμούς, όπως την πρόσβαση αποφοίτων του Πανεπιστημίου σε λογαριασμούς οι οποίοι είχαν παραμείνει ανενεργοί για μεγάλο χρονικό διάστημα.

Το σύστημα NSM είναι σημαντικό για αρκετούς λόγους:

Απετέλεσε τη βάση για ένα μεγάλο αριθμό συστημάτων ανίχνευσης εισβολών. Μάλιστα, έντεκα χρόνια από τη δημιουργία του χρησιμοποιούνταν σε πολλά συστήματα. Επιπλέον απέδειξε ότι η ανίχνευση εισβολών σε δίκτυο ήταν εφικτή σε πρακτικό επίπεδο.

Το NSM δεν είναι φανερό στον εισβολέα αφού παρακολουθεί παθητικά τη δικτυακή κίνηση. Επομένως δε μπορεί να τεθεί εκτός λειτουργίας ή να κινδυνέψουν τα δεδομένα του.

Η κίνηση στο δίκτυο χαρακτηρίζεται ολοένα και περισσότερο από κρυπτογραφημένη ροή μηνυμάτων με αποτέλεσμα η δυνατότητα ανάλυσης των περιεχομένων των πακέτων να μειώνεται. Όμως το NSM εξακολουθεί να είναι αποτελεσματικό διότι δεν εξετάζει τα περιεχόμενα της κίνησης αλλά πραγματοποιεί ανάλυση της ίδιας της κίνησης.

Το NSM μπορεί να χρησιμοποιηθεί σε οποιοδήποτε σύστημα, γιατί παρακολουθεί δικτυακή κίνηση με χρήση πρωτοκόλλων TCP, UDP, ICMP τα οποία είναι καθιερωμένα.

- **Συνδυασμένη Προσέγγιση (DIDS)**

Το σύστημα DistributedInstructionDetectionSystem – DIDS συνδυάζει τις δυνατότητες του NSM, με τη δυνατότητα παρακολούθησης εισβολών σε μεμονωμένα συστήματα. Δηλαδή χρησιμοποιεί τόσο την τεχνολογία networkbasedIDS, την οποία χρησιμοποιεί και το NSM, όσο και την τεχνολογία hostbasedIDS.

Το DIDS χρησιμοποιεί το συνδυασμό αυτό λόγω της διαπίστωσης της μη επάρκειας των παρακολουθήσεων που βασίζονταν αποκλειστικά στο δίκτυο και των παρακολουθήσεων που βασίζονταν αποκλειστικά στον υπολογιστή. Ένας εισβολέας που προσπαθεί να συνδεθεί με ένα σύστημα μέσω ενός λογαριασμού που δεν απαιτεί χρήση συνθηματικού δε θα ανιχνευόταν ως κακόβουλος από ένα σύστημα παρακολούθησης δικτύου. Ενδεχομένως οι μετέπειτα ενέργειες του να προκαλούσαν ένα σύστημα παρακολούθησης βασισμένο σε υπολογιστή να σημάνει συναγερμό εισβολής. Από την άλλη πλευρά ένα σύστημα ανίχνευσης βασισμένο σε υπολογιστή δε θα μπορούσε να ανιχνεύσει έναν εισβολέα ο οποίος επιχειρεί να συνδεθεί με ένα σύστημα παραπάνω από μια φορές μέσω telnet χρησιμοποιώντας κάθε φορά διαφορετικό όνομα σύνδεσης. Αντίθετα το βασισμένο στο δίκτυο σύστημα ανίχνευσης θα μπορούσε να ανιχνεύσει τις επαναλαμβανόμενες αποτυχημένες προσπάθειες σύνδεσης.

Το σύστημα DIDS χρησιμοποιεί ένα έμπειρο σύστημα το οποίο πραγματοποιεί την ανάλυση των δεδομένων. Το έμπειρο σύστημα είναι βασισμένο σε εντολές και είναι σε θέση να εξάγει συμπεράσματα, τόσο για μεμονωμένα συστήματα, όσο και για ολόκληρο το σύστημα που συμπεριλαμβάνει υπολογιστές και δίκτυο. Στη συνέχεια τα αποτελέσματα παρουσιάζονται στον υπεύθυνο του συστήματος ασφάλειας.

Πρόβλημα αποτελεί καθώς ένας εισβολέας κινείται από σύστημα σε σύστημα αλλάζοντας ταυτότητα. Για παράδειγμα ένας εισβολέας εισέρχεται στο πρώτο σύστημα ως χρήστης A και στο δεύτερο σύστημα ως χρήστης B. Οι μηχανισμοί βασισμένοι στον υπολογιστή δεν μπορούν να γνωρίζουν ότι ο χρήστης A και ο χρήστης B είναι ένας και έτσι δεν μπορούν να

συσχετίσουν τις ενέργειες αυτές. Όμως το έμπειρο σύστημα μπορεί να συμπεράνει ότι πρόκειται για τον ίδιο χρήστη. Για να είναι όμως δυνατή η συσχέτιση πρέπει κάθε χρήστης να έχει ένα μοναδικό αριθμό ταυτότητας δικτύου (NetworkIdentificationNumber – NID). Έτσι ο χρήστης A και B που είναι στην πραγματικότητα ο ίδιος χρήστης θα μοιράζονταν ένα κοινό NID.

Το έμπειρο σύστημα, ένα βασικό συστατικό στη λειτουργία του συστήματος DIDS, εξάγει πληροφορίες σχετικά με μια εισβολή από τα δεδομένα που λαμβάνει, με τη χρήση κάποιων κανόνων ενός μοντέλου ανίχνευσης εισβολών. Αυτό το μοντέλο περιλαμβάνει τα εξής επίπεδα:

Αρχικά συγκεντρώνει όλα τα δεδομένα για το δίκτυο και όλες τις πληροφορίες για τη δραστηριότητα των χρηστών.

Στο επίπεδο αυτό ορίζει ένα υποκείμενο που συγκεντρώνει όλα τα γεγονότα που σχετίζονται με ένα και μοναδικό χρήστη. Το NID αντιστοιχίζεται σε αυτό το υποκείμενο.

Το επίπεδο αυτό προσθέτει διάφορες συναφείς πληροφορίες. Για παράδειγμα χρονικά δεδομένα όπως ο χρόνος χρήσης του επεξεργαστή. Εάν ο χρήστης προσπαθήσει να συνδεθεί κάποια ώρα κατά την οποία δεν είχε προσπαθήσει ποτέ πριν να συνδεθεί συνάγεται το συμπέρασμα ότι πιθανό να αναφερόμαστε σε ύποπτο γεγονός.

Το επίπεδο αυτό ασχολείται με τις απειλές προς το δίκτυο, οι οποίες είναι συνδυασμοί διαφόρων γεγονότων. Μια απειλή είναι εξαπάτηση (abuse) εάν μεταβάλλεται η κατάσταση προστασίας του συστήματος. Παράδειγμα αποτελεί η μεταβολή ενός προστατευμένου από εγγραφή αρχείου, σε αρχείο το οποίο μπορεί να τροποποιηθεί από τον καθένα. Μια απειλή θεωρείται κακή συμπεριφορά (misuse) εάν παραβιάζει την πολιτική, χωρίς όμως να μεταβάλλει την κατάσταση του συστήματος. Παράδειγμα αποτελεί η αντιγραφή ενός απαγορευμένου αρχείου, που όμως το αντίγραφο αρχείο είναι προσιτό στον καθένα. Μια απειλή είναι ύποπτη πράξη (suspiciousact) αν δεν παραβιάζει την πολιτική, αλλά μπορεί να θεωρηθεί ότι είναι εντός του πεδίου ενεργειών για την προετοιμασία μιας επίθεσης.

Το επίπεδο αυτό βαθμολογεί την κατάσταση ασφάλειας του δικτύου, με βάση τις απειλές προς το σύστημα που αναπτύσσονται στο προηγούμενο επίπεδο. Έτσι δίνεται η δυνατότητα στον υπεύθυνο ασφάλειας του συστήματος να εντοπίσει γρήγορα τα προβλήματα.

Στο έμπειρο σύστημα κάθε κανόνας έχει μια σχετική αξία κανόνα (rulevalue). Η αξία κανόνα χρησιμοποιείται προκειμένου να υπολογιστεί η βαθμολογία. Ο υπεύθυνος ασφάλειας των συστημάτων ανατροφοδοτεί το έμπειρο σύστημα, ενώ σε περίπτωση ψευδών συναγερμών το έμπειρο σύστημα μειώνει την αξία που συνδέεται με τους κανόνες που οδήγησαν στον ψευδή συναγερμό.

- **Απόκριση στις Εισβολές (IntrusionResponse)**

Μετά την ανίχνευση μιας εισβολής, το επόμενο ζήτημα είναι το πώς μπορεί να

προστατευτεί το σύστημα που δέχτηκε την επίθεση. Στόχος είναι να αντιμετωπιστεί η αποπειραθείσα επίθεση με τρόπο ώστε να ελαχιστοποιείται η ζημιά, όπως προσδιορίζεται από την ισχύουσα πολιτική ασφάλειας. Μερικοί μηχανισμοί ανίχνευσης εισβολών μπορούν να αποτρέψουν τους εισβολείς. Σε αντίθετη περίπτωση, οι υπεύθυνοι ασφάλειας πρέπει να αποκριθούν στην επίθεση και να προσπαθήσουν να αποκαταστήσουν την οποιαδήποτε ζημιά προκλήθηκε.

- **Πρόληψη Περιστατικών**

Το βέλτιστο θα ήταν να ανιχνευτούν και να διακοπούν οι προσπάθειες εισβολής, πριν την επίτευξη του στόχου τους. Αυτό όμως απαιτεί επιμελή παρακολούθηση του συστήματος, συνήθως με ένα μηχανισμό ανίχνευσης εισβολών και τη λήψη μέτρων για την αντιμετώπιση της επίθεσης.

Η πρόληψη απαιτεί τον εντοπισμό της επίθεσης πριν από την ολοκλήρωση της. Ακολούθως λαμβάνονται μέτρα προκειμένου να αποτραπεί η ολοκλήρωση της επίθεσης.

Μια μέθοδος που πετυχαίνει πρόληψη των επιθέσεων είναι η απομόνωση των επιτιθέμενων σε μια περιορισμένη περιοχή. Οι επιτιθέμενοι τοποθετούνται σε ένα περιβάλλον ασφάλειας που είναι απομονωμένο από τα υπόλοιπα, έτσι ώστε η συμπεριφορά τους να μπορεί ελεγχθεί και να χειραγωγηθεί, όπου αυτό είναι απαραίτητο. Ταυτόχρονα όμως δίνεται η εντύπωση στους επιτιθέμενους ότι οι επιθέσεις τους έχουν πετύχει. Οι ενσωματωμένοι μηχανισμοί ασφάλειας του περιβάλλοντος ασφάλειας είναι σχεδιασμένοι ώστε να περιορίζουν την πρόσβαση στα αντικείμενα μέσα στο απομονωμένο περιβάλλον, περιορίζοντας με τον τρόπο αυτό τον επιτιθέμενο. Στους μηχανισμούς ανίχνευσης εισβολών μπορούν να ενσωματωθούν μέθοδοι που βασίζονται στη διαταραχή, έτσι ώστε να είναι εφικτή η παρακολούθηση σχετικών χαρακτηριστικών του συστήματος για τυχόν διαταραχές και την άμεση αντίδραση όταν οι διαταραχές εντοπίζονται σε πραγματικό χρόνο.

- **Χειρισμός των Εισβολών**

Όταν συμβεί μια εισβολή, η πολιτική ασφάλειας του συστήματος παραβιάζεται. Ο χειρισμός των εισβολών περιλαμβάνει την εκ νέου συμμόρφωση του συστήματος με την πολιτική ασφάλειας και τη λήψη μέτρων κατά του επιτιθέμενου, όπως αυτά καθορίζονται από την ισχύουσα πολιτική. Ο χειρισμός των εισβολών περιλαμβάνει έξι φάσεις:

- Προετοιμασία (preparation) για μια επίθεση: Στο βήμα αυτό πριν ανιχνευθεί οποιαδήποτε επίθεση, εγκαθίστανται οι διαδικασίες και οι μηχανισμοί για την ανίχνευση και την απόκριση στις επιθέσεις.
- Ταυτοποίηση (identification) μιας επίθεσης: Το βήμα αυτό διαμορφώνει τις υπόλοιπες φάσεις.
- Περιορισμός (containment) της επίθεσης: Το βήμα αυτό περιορίζει σε όσο το δυνατό μεγαλύτερο βαθμό τη ζημιά στο σύστημα.

- Εξουδετέρωση (eradication) της επίθεσης: Από αυτό το βήμα σταματά η επίθεση και παρεμποδίζονται περαιτέρω παρόμοιες επιθέσεις.
- Αποκατάσταση (recovery) από την επίθεση: Στο βήμα αυτό αποκαθίσταται η ασφαλής κατάσταση στο σύστημα σύμφωνα με την ισχύουσα πολιτική ασφάλειας.
- Συνεχής παρακολούθηση (follow-up) της επίθεσης: Αυτό το βήμα περιλαμβάνει τη λήψη μέτρων κατά του επιτιθέμενου, τον προσδιορισμό των προβλημάτων κατά τον χειρισμό του γεγονότος και καταγραφή των σχετικών εμπειριών που αποκτήθηκαν.

- ## Ηλεκτρονικές Πληρωμές

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 (electronicpayments) 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.

- ***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 αποτελείται από τα εξής βήματα όπως φαίνεται στο Σχήμα 41 Τυπική Συναλλαγή Πληρωμής.Σχήμα 41:

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.).

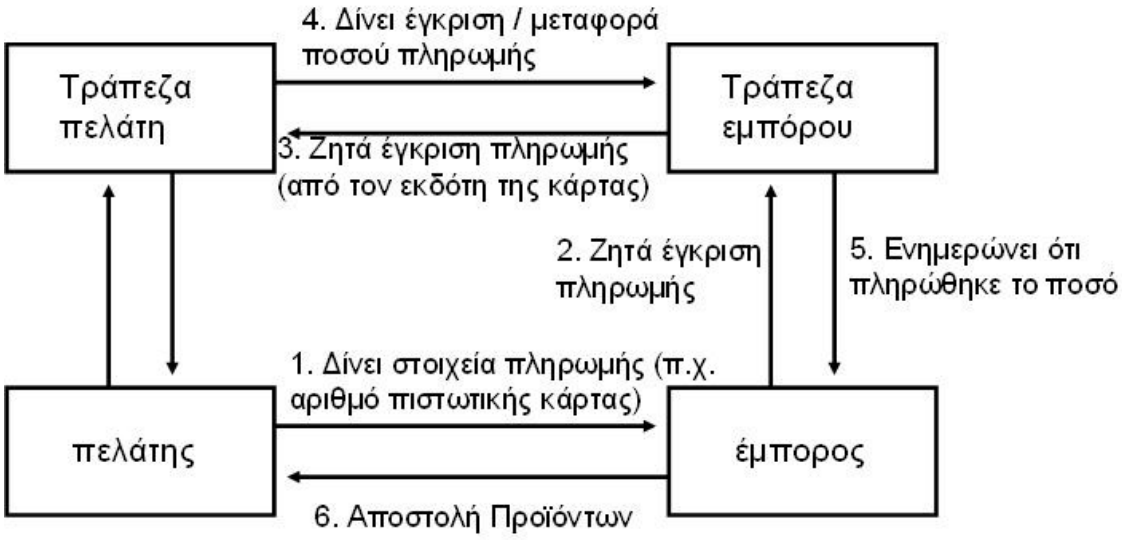
Ο έμπορος προωθεί τις πληροφορίες που έλαβε από τον πελάτη στην τράπεζα του, προκειμένου να εξακριβώσει την εγκυρότητα του τρόπου πληρωμής (π.χ. της πιστωτικής κάρτας).

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 41 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.

- **Σύγχρονες Μέθοδοι Πληρωμής**

- **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 (SecureSocketsLayer). Το πρωτόκολλο αυτό αναλύεται στην παράγραφο 2.1. Η χρησιμοποίηση webserver και webbrowser 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 (TrustedThirdParties – TTP). Μια TTP μεσολαβεί ανεξάρτητα στην όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή.

- **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 κεφαλαίο5.2. 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.

- **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 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.

- **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:

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.

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.

- **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 (κεφάλαιο 5) , 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 JavaCard.

- ***Ασφάλεια Ηλεκτρονικών Πληρωμών***

Η ανασφάλεια και η αβεβαιότητα των χρηστών σχετικά με την εκτέλεση ηλεκτρονικών αγορών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους εξάπλωσης του ηλεκτρονικού εμπορίου. Οι χρήστες προκειμένου να πραγματοποιήσουν τις αγορές τους στο διαδίκτυο, πρέπει να είναι σίγουροι ότι τα προσωπικά τους δεδομένα προστατεύονται κατάλληλα και ότι δεν πρόκειται να πέσουν θύματα απάτης. Είναι γνωστό ότι οι ηλεκτρονικές πληρωμές στο διαδίκτυο εισάγουν πρόσθετους κινδύνους σε σχέση με τις παραδοσιακές πληρωμές και άρα πρέπει να λαμβάνονται πρόσθετα μέτρα ασφάλειας.

Τα ηλεκτρονικά συστήματα πληρωμών αντιμετωπίζουν τα εξής επιπλέον προβλήματα:

- 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. έμπορας), οι οποίοι χρησιμοποιούν για απάτες τις πληροφορίες πληρωμής (π.χ. αριθμούς πιστωτικών καρτών) που τους δίνει ο πελάτης.

Τα γενικά χαρακτηριστικά που αναφέρονται παρακάτω αποτελούν τα συστατικά στοιχεία ασφαλείας που θα πρέπει να έχει ένα σύστημα ηλεκτρονικών πληρωμών:

Αυθεντικοποίηση Πληρωμής: Τόσο ο πληρωτής, όσο και ο δικαιούχος πληρωμής, θα πρέπει να αποδεικνύουν τις ταυτότητες τους, οι οποίες δεν είναι απαραίτητα ίδιες με τις αληθινές τους ταυτότητες. Η Αυθεντικοποίηση δεν υπονοεί ότι απαραίτητα η ταυτότητα του πληρωτή αποκαλύπτεται.

Ακεραιότητα Πληρωμής: Το σύστημα θα πρέπει να διασφαλίζει ότι τα δεδομένα της συναλλαγής πληρωμής δεν μπορούν να τροποποιηθούν από αναρμόδιους συμβαλλόμενους.

Έγκριση Πληρωμής: Το σύστημα θα πρέπει να εξασφαλίζει ότι δεν θα αποσυρθούν χρήματα από τον λογαριασμό του πελάτη, χωρίς τη ρητή άδεια του και ότι το καθορισμένο ποσό μπορεί να αποσυρθεί μόνο από εξουσιοδοτημένο συμβαλλόμενο.

Εμπιστευτικότητα Πληρωμής: Το σύστημα θα πρέπει να διασφαλίζει την προστασία των δεδομένων της συναλλαγής από τρίτους.

- **Υπηρεσίες Ασφάλειας Πληρωμών**

Ένα ηλεκτρονικό σύστημα πληρωμών, που χρησιμοποιείται στις συναλλαγές ηλεκτρονικού εμπορίου, 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.

Μη Ανίχνευση Θέσης: Προστατεύει από την κοινοποίηση της θέσης όπου γίνεται η συναλλαγή. Χρησιμοποιώντας μόνο ανωνυμία χρήστη, η IP διεύθυνση και το hostname του υπολογιστή, από τον οποίο στάλθηκε κάποιο μήνυμα ή 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 hostname του υπολογιστή δεν θα αποκαλυφθούν.

Μη Ανίχνευση Συναλλαγής Πληρωμής: Προστατεύει από τη σύνδεση δύοδιαφορετικών συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πελάτη. Ένας πληρωτής θέλοντας να διατηρήσει την ανωνυμία του, μπορεί να κρύβεται πίσω από ένα ψευδώνυμο, π.χ. μια

αριθμητική ταυτότητα. Εάν χρησιμοποιεί την ίδια ταυτότητα σε όλες τις συναλλαγές του, τότε η συμπεριφορά του μπορεί να παρατηρηθεί και σε συνδυασμό με άλλες πληροφορίες η ταυτότητα του μπορεί 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.

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.

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.

- **Ασφάλεια Ψηφιακού Χρήματος**

- **Κατηγορίες Ψηφιακού Χρήματος**

Γενικά υπάρχουν δύο ξεχωριστοί τύποι ηλεκτρονικού χρήματος (e-money): το ηλεκτρονικό χρήμα που προσδιορίζει την ταυτότητα του ιδιοκτήτη του (identifiede-money) και το ανώνυμο ηλεκτρονικό χρήμα (anonymouse-money), γνωστό επίσης και ως ψηφιακά μετρητά (digitalcash). 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 serialnumber. Είναι εύκολο να δημιουργηθεί ένα μεγάλο αρχείο στο οποίο θα καταχωρείται ποιος πελάτης έλαβε ποιους serialnumber 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.

- **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 serialnumber 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 (smartcards) 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 Observerchip 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.

- ***Άλλα Διαθέσιμα Συστήματα Ηλεκτρονικών Πληρωμών***

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.

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).

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.

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.

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.

Paypal

Το PayPal είναι μία επιχείρηση ηλεκτρονικού εμπορίου μέσω του οποίου επιτρέπονται οι πληρωμές ηλεκτρονικά και οι μεταφορές χρημάτων γίνονται μέσω του Διαδικτύου . Το PayPal χρησιμεύει ως μια ηλεκτρονική εναλλακτική λύση στις παραδοσιακές μεθόδους, όπως οι επιταγές και οι εντολές πληρωμών.

Ένας λογαριασμός PayPal μπορεί να χρηματοδοτηθεί με ηλεκτρονική πίστωση από ένα τραπεζικό λογαριασμό ή από μια πιστωτική κάρτα. Το PayPal είναι ένα παράδειγμα μιας πληρωμής σε υπηρεσίες διαμεσολαβήσεως, που διευκολύνει τον κόσμο κατά το ηλεκτρονικό εμπόριο.

Το PayPal εκτελεί την επεξεργασία των πληρωμών για online πωλήσεις, δημοπρασίες χώρων, καθώς και άλλους εμπορικούς χρήστες, για την οποία χρεώνει αμοιβή. Φορτίζει μερικές φορές επίσης τέλος συναλλαγής για τη λήψη χρημάτων (ένα ποσοστό του ποσού που απέστειλε συν ένα πρόσθετο σταθερό ποσό). Το επίπεδο των τελών εξαρτάται από το χρησιμοποιούμενο νόμισμα, την επιλογή πληρωμής που χρησιμοποιείται, τη χώρα του αποστολέα, τη χώρα του δικαιούχου, το ποσό που αποστέλλεται και τον τύπο του λογαριασμού του δικαιούχου. Επιπλέον, το eBay σε αγορές που γίνονται με πιστωτική κάρτα μέσω PayPal μπορεί να αναλάβει μια «αλλαγή του νομίσματος της συναλλαγής", αν ο πωλητής βρίσκεται σε άλλη χώρα, όπως και οι εκδότες πιστωτικών καρτών αυτόματα ενημερώνονται για τη χώρα προέλευσης του πωλητή.

- # Υποδομή Δημοσίου Κλειδιού

Ένα σημαντικό πρόβλημα που παρουσιάζεται στο ηλεκτρονικό εμπόριο και συγκεκριμένα στις ηλεκτρονικές συναλλαγές πληρωμής είναι η πιστοποίησητης 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. Οι βασικές αρχές της κρυπτογραφίας περιγράφονται

στο Παράρτημα. 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.

- ***Τι είναι κρυπτογραφία***

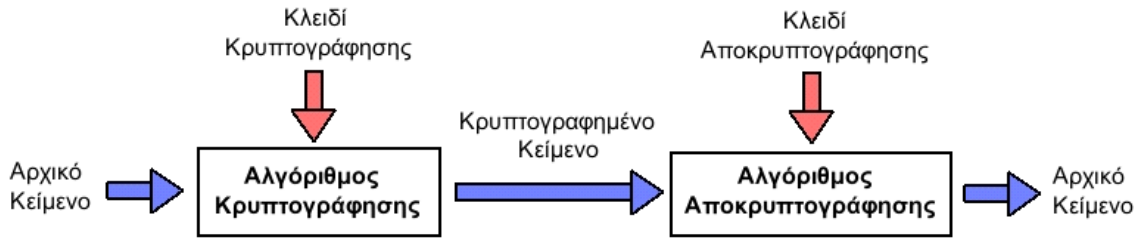
Ως κρυπτογραφία μπορεί να οριστεί ο επιστημονικός κλάδος που ασχολείται με τη μετατροπή των πληροφοριών, με σκοπό τη διαφύλαξη του απορρήτου τους. Σκοπός της είναι να διατηρήσει την ιδιωτικότητα ενός μηνύματος με το να κρατά την πληροφορία «κρυφή» από οποιοδήποτε άτομο, το οποίο δεν έχει ορισθεί ως αποδέκτης του μηνύματος ακόμα και αν έχει πρόσβαση στα κρυπτογραφημένα δεδομένα.

Κρυπτογράφηση (Encryption) είναι η διαδικασία κατά την οποία ένα μήνυμα μετατρέπεται σε τέτοια μορφή που να μην είναι κατανοητή για μη εξουσιοδοτημένους αποδέκτες. Το νέο μήνυμα που προκύπτει ονομάζεται κρυπτογράφημα (ciphertext). Η κρυπτογράφηση ενός μηνύματος πραγματοποιείται με τη χρήση μιας μαθηματικής συνάρτησης η οποία ονομάζεται κλειδί (key). Η ακριβώς αντίστροφη διαδικασία ονομάζεται αποκρυπτογράφηση (decryption) και οδηγεί στη δημιουργία του αρχικού πραγματικού μηνύματος (plaintext). Ένας εχθρός ή παρείσακτος (intruder) ακούει και αντιγράφει το κρυπτογράφημα, αλλά για να μπορέσει να το κατανοήσει πρέπει να γνωρίζει ή να σπάσει το κλειδί κρυπτογράφησης. Η τέχνη του σπασίματος κωδικών ονομάζεται κρυπτανάλυση.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με το κλειδί για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Παλαιότερα χρησιμοποιούσαν την κρυπτογράφηση αποκλειστικά για στρατιωτικούς σκοπούς. Στη σημερινή κοινωνία της πληροφορίας, η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης του απορρήτου των μηνυμάτων με όλα τα προφανή πλεονεκτήματα. Ως αποτέλεσμα, η σύγχρονη κρυπτογραφία είναι κάτι περισσότερο από απλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, και αποτελεί βασικό εργαλείο ασφάλειας στο ηλεκτρονικό εμπόριο. Για παράδειγμα, η πιστοποίηση αποτελεί εξίσου θεμελιώδη έννοια που συνδέεται άμεσα με την κρυπτογραφία. Όταν υπογράφεται ένα έγγραφο είναι απαραίτητο να υπάρχουν μηχανισμοί που να πιστοποιούν τον κάτοχο του εγγράφου. Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός συγκεκριμένου κλειδιού.Παρακάτω στο

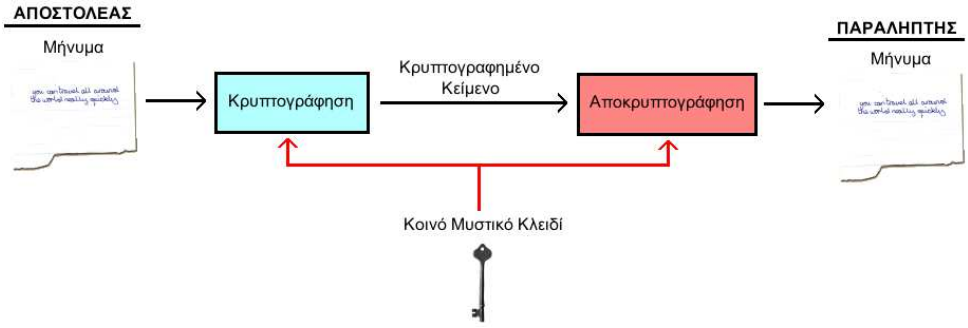
Σχήμα 51 βλέπουμε την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.



Σχήμα 51 Διαδικασία κρυπτογράφησης

- **Κρυπτογραφηση συμμετρικου κλειδιου**

Η κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography) βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης φαίνεται πιο παραστατικά στο Σχήμα 51 Κρυπτογράφηση συμμετρικού κλειδιού.



Σχήμα 52 Κρυπτογράφηση συμμετρικού κλειδιού.

- **Κρυπτογράφηση δημοσίου κλειδιού**

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

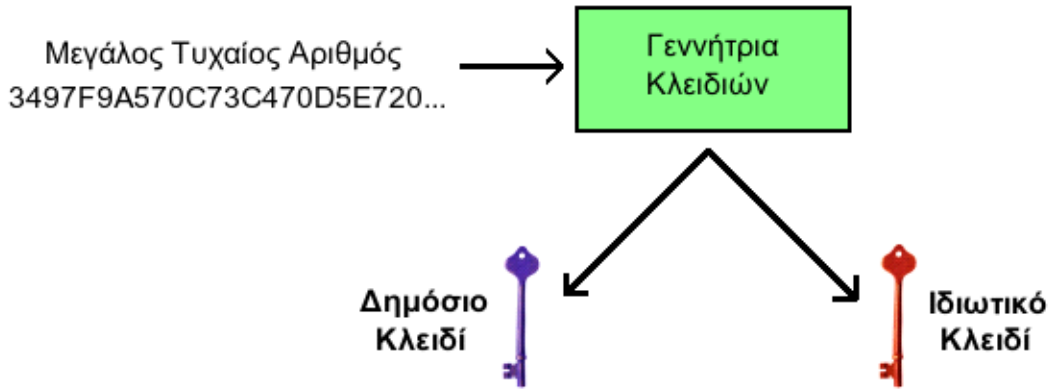
Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακέςαγορές κοκ).

- **Δημιουργία κλειδιών**

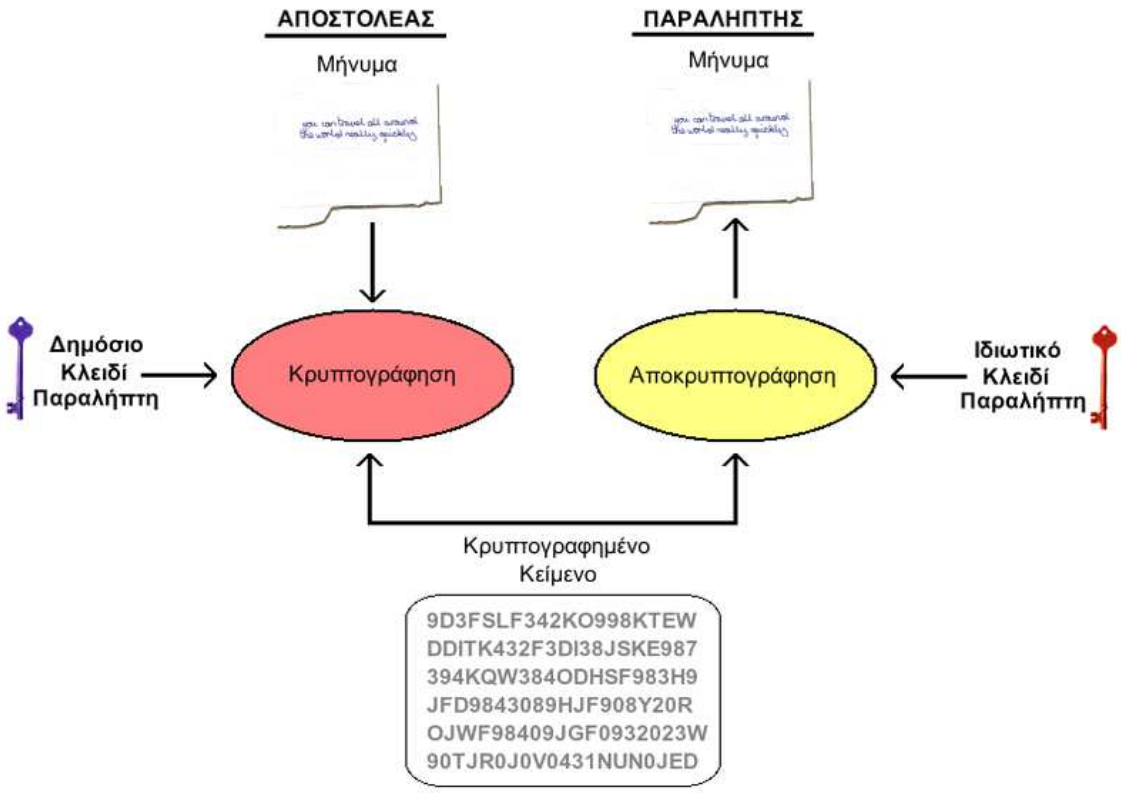
Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.



Σχήμα 53Δημιουργία κλειδιών

- **Εμπιστευτικότητα και Πιστοποίηση**

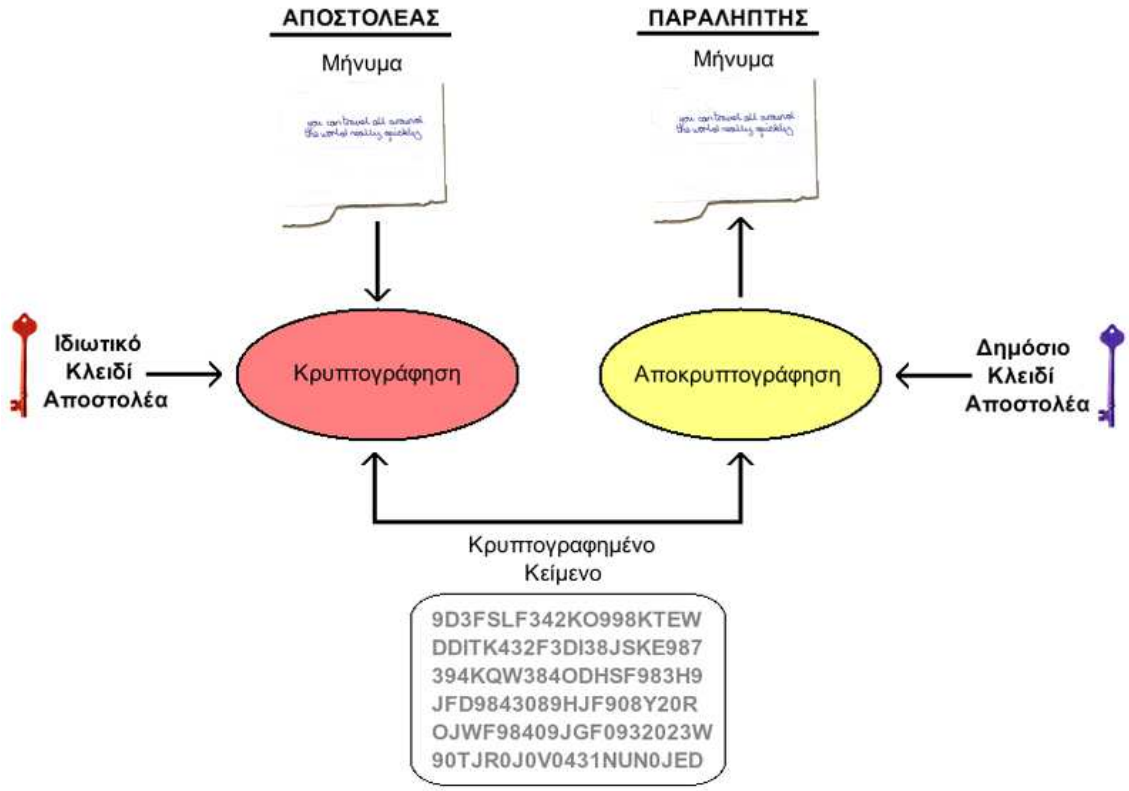
Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημενο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.



Σχήμα 54 Εμπιστευτικότητα

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα

είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



Σχήμα 55 Αυθεντικοποίηση

Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη τη διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

Οπότε συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

- ***Ψηφιακές Υπογραφές***

Για την απόδειξη της γνησιότητας ενός εγγράφου, χρησιμοποιούνται οι συμβατικές υπογραφές. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί. Στις συναλλαγές ηλεκτρονικού εμπορίου καθίσταται αναγκαία η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής

υπογραφής. Ο μηχανισμός της ηλεκτρονικής υπογραφής θα πρέπει να παρέχει απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των ανταλλασσόμενων μηνυμάτων. Απαιτείται δηλαδή ένα σύστημα μέσω του οποίου κάποιος θα μπορεί να στείλει ένα υπογεγραμμένο μήνυμα σε κάποιον άλλο με τέτοιο τρόπο ώστε:

Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας.

Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος.

Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

Οι ηλεκτρονικές υπογραφές που βασίζονται στην κρυπτογραφία ονομάζονται ψηφιακές υπογραφές. Η ψηφιακή υπογραφή εξαρτάται άμεσα από το μήνυμα το οποίο στέλνεται, είναι γνωστή μόνο στον αποστολέα αλλά μπορεί να επιβεβαιωθεί από τον καθένα. Η ψηφιακή υπογραφή θα πρέπει να είναι εύκολο να υπολογιστεί και να επιβεβαιωθεί από οποιονδήποτε ενδιαφερόμενο. Παράλληλα όμως θα πρέπει να είναι αδύνατο να αντιγραφεί.

Η ψηφιακή υπογραφή είναι άμεσα συσχετιζόμενη με το μήνυμα το οποίο στέλνεται και δεν είναι ποτέ η ίδια. Διαφορετικό μήνυμα σημαίνει άμεσα και διαφορετική ψηφιακή υπογραφή. Η «σύνδεση» της ψηφιακής υπογραφής με το περιεχόμενο του μηνύματος που υπογράφει εξασφαλίζει την ακεραιότητα των δεδομένων (dataintegrity). Δηλαδή διασφαλίζει ότι από τη στιγμή που ο αποστολέας υπέγραψε τα δεδομένα, αυτά δεν έχουν τροποποιηθεί.

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη σχήματα φαίνονται πιο παραστατικά αυτες οι ενέργειες.

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.

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

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

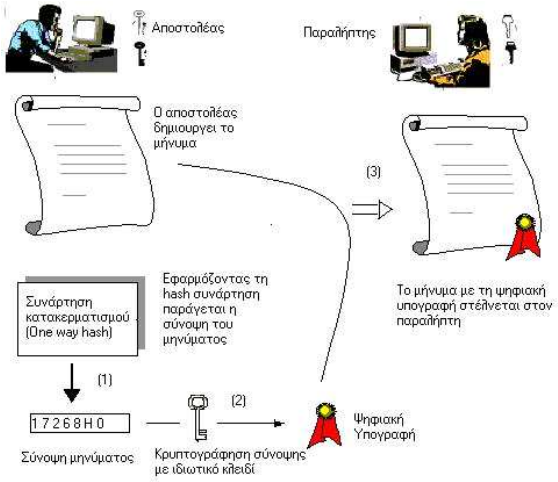
Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

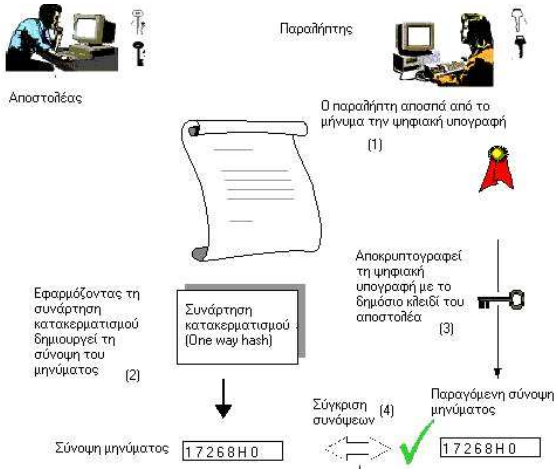
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

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

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



Σχήμα 56 Δημιουργία Ψηφιακής Υπογραφής



Σχήμα 57 Επαλήθευση Υπογραφής

- ***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 (CertificateAuthority, 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 (publickeycertificates) 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 (publickey).
- Ένα μοναδικό αριθμό (serialnumber).
- Το όνομα της CA, δηλαδή της εκδότριας αρχής (issuer) του πιστοποιητικού.
- Την ψηφιακή υπογραφή της CA και τον αλγόριθμο (signaturealgorithm) που χρησιμοποιήθηκε.
- Την ημερομηνία έκδοσης (validfrom) και λήξης (validto) 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:

- **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.
- **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.

- ## 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 defacto στις περισσότερες εφαρμογές που κάνουν χρήση ψηφιακών πιστοποιητικών. Η Netscape υιοθέτησε το X.509 πρότυπο για την έκδοση των πιστοποιητικών που χρησιμοποιούνται στο SocketsLayerProtocol (SSL) πρωτόκολλο.Παρακάτω στον Πίνακας 51φαίνονται τα πεδία του προτύπου X.509

Όνομα Πεδίου	Χρήση
Version	Η έκδοση του προτύπου X.509. Ορίζονται 3 εκδόσεις του X.509. Η έκδοση 1 δεν περιέχει τα πεδία issueruniqueidentifier, subjectuniqueidentifier 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 algo-rithm 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.
	Οι σχετικές παράμετροι που προσδιορίζουν τη λειτουργία του παραπάνω

	κρυπταλγόριθμου.
parameters	
subject's public key	Το δημόσιο κλειδί της οντότητας που αναγνωρίζεται από το πεδίο subjectname. 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 51 Τα πεδία του προτύπου 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 subjectuniqueidentifier 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 – NonRepudiation) 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 – DigitalSignature). Στο δεύτερο αυτό πιστοποιητικό μπορούν να παρασχεθούν και δυνατότητες χρήσης των κλειδιών για απλή κρυπτογράφηση δεδομένων (με την πρόσθετη ένδειξη Κρυπτογράφηση κλειδιών-δεδομένων-Key/ DataEncipherment),

αν και συνίσταται η χρήση τρίτου ξεχωριστού ζεύγους κλειδιών και αντίστοιχου πιστοποιητικού για τις εφαρμογές κρυπτογράφησης.

- ***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 (PublicKeyInfrastructure, 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.

- **Πάροχοι Υπηρεσιών Πιστοποίησης (ΠΥΠ)**

Μια Υποδομή Δημοσίου Κλειδιού περιλαμβάνει έναν ή περισσότερους Πάροχους Υπηρεσιών Πιστοποίησης (ΠΥΠ). Οι Πάροχοι Υπηρεσιών Πιστοποίησης (CertificationServiceProviders - CSP) παλαιότερα αποκαλούνταν Έμπιστες Τρίτες Οντότητες (TrustedThirdParties – 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:

- **ΑρχήΠιστοποίησης (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.

- **ΑρχήΕγγραφής (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 (RevocationManagementService)**. 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 (CertificateRevocationLists, CRL).

- **ΥπηρεσίαΔημοσίευσης (Dissemination&RevocationStatusService)**. 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 (SubjectDeviceProvisionService), Υπηρεσίες Χρονοσήμανσης ηλεκτρονικών εγγράφων (Time-StampingAuthority – TSA), Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων (AttributeAuthority), Υπηρεσίες Ασφαλούς Αρχειοθέτησης εγγράφων (καλούμενες συχνά και ως NotaryServices) 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.

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 (CertificatePolicy – 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.

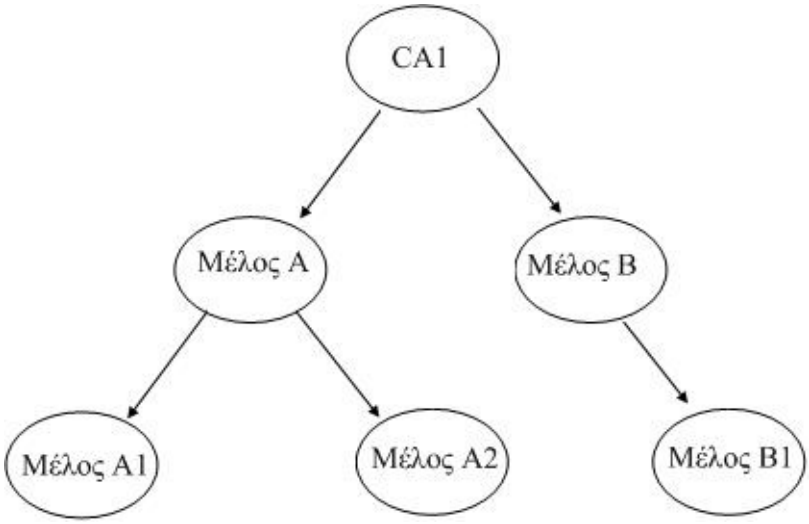
- Δήλωση Πρακτικών Πιστοποίησης (CertificationPracticeStatement – CPS) είναι μια δήλωση όπου καταγράφονται οι πρακτικές που ακολουθεί μια Αρχή Πιστοποίησης για τη διαχείριση των πιστοποιητικών. Αποτελεί ένα λεπτομερέστατο έγγραφο, όπου αναφέρεται ο τρόπος διεκπεραίωσης των λειτουργικών διαδικασιών των 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.

- **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 57 φαίνεται ένα παράδειγμα όπου η Αρχή Πιστοποίησης (CA1) έχει πιστοποιήσει το μέλος A και B. Όλα τα πιστοποιητικά που έχουν εκδοθεί από την Αρχή Πιστοποίησης είναι αποδεκτά από όλα τα μέλη που συμμετέχουν στο PKI. Το μέλος A αναλαμβάνει να πιστοποιήσει τα μέλη A1 και A2, και το μέλος B πιστοποιεί το B1. Τα μέλη A1 και A2 εμπιστεύονται το A, οπότε μπορεί να εμπιστευθεί το ένα το πιστοποιητικό του άλλου. Εφόσον εμπιστεύονται τον A, αυτόματα εμπιστεύονται και όλες τις οντότητες που βρίσκονται επάνω από το A, στην περίπτωση μας την CA1. Το μέλος B1 δέχεται το πιστοποιητικό του A, αφού μέσω του B, εμπιστεύεται την CA1.

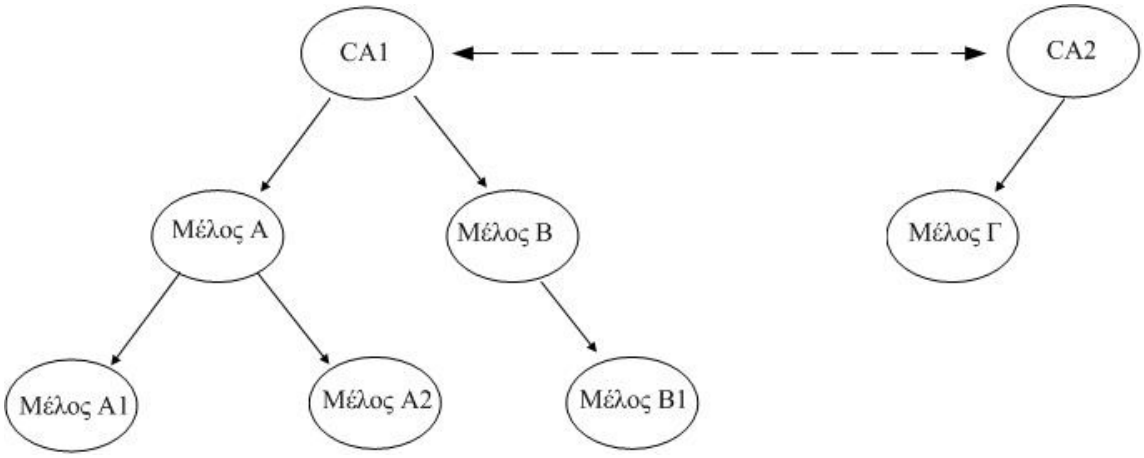
Στην περίπτωση που το μέλος B1 θέλει να επικοινωνήσει με το A1, θα πρέπει να εμπιστευτεί το μέλος B, την CA1 και το μέλος A. Με άλλα λόγια, η εμπιστοσύνη υπάρχει αν

υπάρχει δρόμος στο δέντρο από το μέλος Β1 στο μέλος Α1.



Σχήμα 58 Δέντρο Πιστοποίησης

Στο Σχήμα 58το 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.



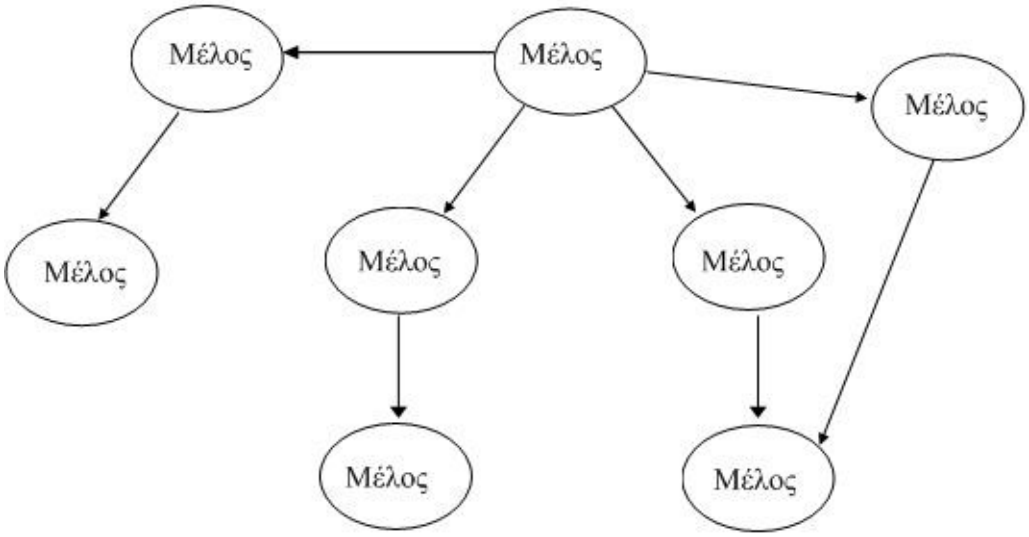
Σχήμα 59 Διαπιστοποίηση

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

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 (weboftrust), όπου ένα νέο μέλος μπορεί να γίνει μέλος του δικτύου εάν έχει συστηθεί από κάποιο υπάρχον μέλος.



Σχήμα 510 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 πιστοποιητικό.

Το δημοφιλές λογισμικό PrettyGoodPrivacy (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:

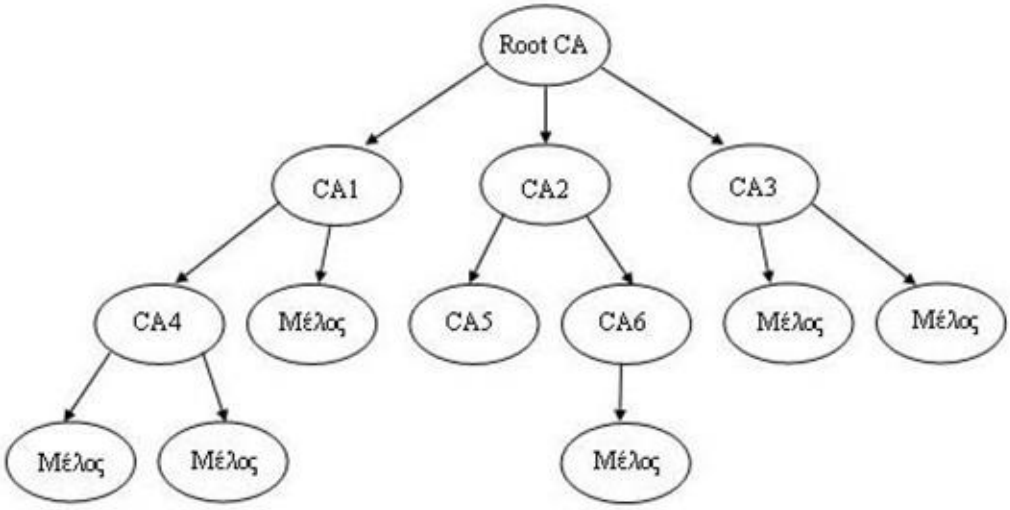
- ΑπολύτωςΈμπιστο (Completely Trusted).
- Μερικώς Έμπιστο (Marginally Trusted).
- Μη Έμπιστο (Untrusted).
- Άγνωστο (Unknown).

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 (CompletelyTrusted) κλειδιά ή από τρία μερικώς έμπιστα (MarginallyTrusted) 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 στοΣχήμα 510 βρίσκεται ο Θεμελιώδης Εκδότης Πιστοποιητικών (RootCertificationAuthority ή RootCA) 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 511 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 rootcertificate. Εξυπακούεται ότι αυτός ο Θεμελιώδης Εκδότης Πιστοποιητικών πρέπει να είναι απόλυτα έμπιστος.

- **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:

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.

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.

- **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 (serialnumber) σε μια Λίστα Ανακληθέντων Πιστοποιητικών (CertificateRevocationList, 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:

Στην περίπτωση που ο χρήστης υποψιαστεί ότι το ιδιωτικό του κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους, (αίτημα του χρήστη).

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.

- **Οργανισμοί Πιστοποίησης**

Στον Πίνακας 52φαίνονται 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 52 Οργανισμοί Πιστοποίησης.

Οι πολύ δημοφιλής browserInternetExplorer 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 InternetExplorer υιοθετούν το ITUstandard X.509 v.3.

- ***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 (InternationalOrganizationforStandardization), ITU (InternationalTelecommunicationUnion), ETSI (ElectronicTelecommunicationsStandardizationInstitute) 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 SecureSocketsLayer, 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 (smartcard) και της τρίτης ίσως σε μια ειδική προστατευόμενη συσκευή (tamperresistanthardware).

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.

• Έξυπνες Κάρτες (SmartCarts)

Τα τελευταία χρόνια η τεχνολογία έξυπνων καρτών (smartcards) εφαρμόζεται στο ηλεκτρονικό εμπόριο και παρέχει ένα ασφαλές περιβάλλον εκτέλεσης των ηλεκτρονικών συναλλαγών.

Η τεχνολογία των έξυπνων καρτών χρησιμοποιείται για την προσέγγιση και επίλυση προβλημάτων πρόσβασης, διαχείρισης και διακίνησης πληροφορίας σχεδόν σε όλους τους τομείς της οικονομίας και της κοινωνίας. Ένας από τους σημαντικότερους τομείς της οικονομίας, όπου η τεχνολογία των έξυπνων καρτών χρησιμοποιείται, είναι το ηλεκτρονικό εμπόριο. Ο ρόλος των έξυπνων καρτών εστιάζεται κυρίως στη διασφάλιση περιβάλλοντος εμπιστοσύνης στις συναλλαγές μεταξύ πολιτών και παροχέων υπηρεσιών στο ηλεκτρονικό εμπόριο.

Μια έξυπνη κάρτα είναι μια πλαστική ίση σε μέγεθος με μια πιστωτική κάρτα, στην οποία έχει ενσωματωθεί ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά. Το ολοκληρωμένο κύκλωμα μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή.

Ουσιαστικά οι έξυπνες κάρτες είναι μικροσκοπικοί υπολογιστές. Ανάμεσα στα βασικότερα πλεονεκτήματα που διαφοροποιούν την έξυπνη από την απλή κάρτα είναι ότι το ολοκληρωμένο κύκλωμα μπορεί να παρέχει μια ασφαλή δομή αποθήκευσης δεδομένων καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών, να υπολογίζει κρυπτογραφικές συναρτήσεις και να αντιλαμβάνεται άμεσα προσπάθειες παράνομης (ή λανθασμένης) πρόσβασης. Οι έξυπνες κάρτες αναπόφευκτα αλλάζουν το ηλεκτρονικό εμπόριο λόγω της επαναστατικής ευκολίας και αξιοπιστίας που προσφέρουν, όσον αφορά το πώς τα δεδομένα αποθηκεύονται, προσπελάζονται, επεξεργάζονται και μεταβάλλονται. Λόγω του υψηλού επιπέδου ασφάλειας που παρέχουν οι εν λόγω κάρτες μειώνεται σημαντικά η πιθανότητα απάτης.

Οι έξυπνες κάρτες παρέχουν δύο βασικές λειτουργίες: αυθεντικοποίηση, και αποθήκευση δεδομένων. Η αυθεντικοποίηση διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να αποκτήσουν πρόσβαση σε συστήματα και κτιριακές εγκαταστάσεις. Μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί και σαν φορητή συσκευή αποθήκευσης έχοντας τη δυνατότητα να αποθηκεύει ένα ευρύ σύνολο από δεδομένα διαφορετικού τύπου και για διαφορετικούς σκοπούς. Επιπλέον μπορεί να χρησιμοποιηθεί και ως ηλεκτρονικό πορτοφόλι και να αποθηκεύει χρήματα σε ποικίλα συναλλάγματα καθώς επίσης και πιστωτικά υπόλοιπα και άλλες μορφές αξιών.

Οι έξυπνες κάρτες λόγω της ενσωματωμένης τεχνολογίας τους, έχουν ποικίλες εφαρμογές στο ηλεκτρονικό εμπόριο. Μια έξυπνη κάρτα μπορεί να είναι μια πιστωτική ή χρεωστική κάρτα με υψηλότερο επίπεδο ασφάλειας από ότι οι μαγνητικές κάρτες. Ένας από τους πιο ασφαλείς τρόπους για τη διασφάλιση της προστασίας του ιδιωτικού κλειδιού είναι η αποθήκευση του σε μια έξυπνη κάρτα. Οι κάρτες αυτές, μπορούν να συνδεθούν σε ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί για κρυπτογράφηση ή για δημιουργία ψηφιακής υπογραφής. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να αποθηκευτεί στον υπολογιστή και ότι κάποιος για να έχει πρόσβαση στο ιδιωτικό κλειδί πρέπει να κλέψει την έξυπνη κάρτα. Αλλά ακόμα και σε αυτή την περίπτωση δεν θα μπορέσει να έχει πρόσβαση στο ιδιωτικό κλειδί διότι η έξυπνη κάρτα ζητά έναν κωδικό πρόσβασης (PIN) πριν δώσει το ιδιωτικό κλειδί. Επιπλέον η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί ως ηλεκτρονικό πορτοφόλι όπου αποθηκεύονται μονάδες χρήματος και στη συνέχεια ο κάτοχος της τη χρησιμοποιεί για τις ηλεκτρονικές αγορές του στο διαδίκτυο. Επίσης, οι έξυπνες κάρτες μπορούν να παρέχουν υψηλό επίπεδο αυθεντικοποίησης. Συγκεκριμένα μπορούν να αποθηκεύουν ψηφιακά πιστοποιητικά και συνεπώς να παρέχουν αυθεντικοποίηση στον κάτοχο τους κατά την πρόσβαση του σε κάποιο δίκτυο ή σύστημα. Λόγω της επεξεργαστικής δυνατότητας που έχουν, οι έξυπνες κάρτες μπορούν να δημιουργούν ζεύγος κλειδιών, να αποθηκεύουν το ιδιωτικό κλειδί και να δημιουργούν ψηφιακές υπογραφές με υψηλό επίπεδο ασφάλειας και αξιοπιστίας. Γενικά τα οφέλη που προσφέρουν οι έξυπνες κάρτες στο ηλεκτρονικό εμπόριο είναι πολλά και αναμφισβήτητα θα αλλάξουν ριζικά τις σχέσεις ανάμεσα σε καταναλωτές και οργανισμούς ηλεκτρονικού εμπορίου (εμπόρους).

- ***Ιστορία Έξυπνων Καρτών***

Η ιστορία της έξυπνης κάρτας είναι παράλληλη με την ανάπτυξη της τεχνολογίας των chip κατά τη διάρκεια των τελευταίων 40 ετών. Το 1969 παρουσιάστηκε στη Γαλλία, από τον δημοσιογράφο RolandMoreno, μία ιδέα για μία κάρτα με ενσωματωμένο κύκλωμα. Έτσι γεννήθηκε η έξυπνη κάρτα. Οι έξυπνες κάρτες αναπτύχθηκαν ανεξάρτητα στη Γερμανία (1967), στην Ιαπωνία (1970) και στις Η.Π.Α. (1972). Οι έξυπνες κάρτες άνθισαν τη δεκαετία του 1980.

Στο διάστημα 1982-84 η CartesBancaire (Ένωση Τραπεζικών Καρτών της Γαλλίας) έτρεξε το πρώτο πιλοτικό πρόγραμμα για έξυπνες κάρτες. Μετά την πολύ πετυχημένη δοκιμή, οι Γαλλικές τράπεζες εισήγαγαν τη χρήση των έξυπνων καρτών για τραπεζικές λειτουργίες στο ευρύ κοινό. Η χρήση αυτή είναι το πρώτο παράδειγμα δημόσιας λειτουργίας των έξυπνων καρτών για τραπεζικές λειτουργίες.

- ***Τεχνικά Χαρακτηριστικά***

Ο διεθνής οργανισμός τυποποίησης ISO (InternationalOrganizationforStandardization) χρησιμοποιεί τον όρο κάρτα ολοκληρωμένων κυκλωμάτων για να καλύψει όλες εκείνες τις συσκευές όπου ένα ολοκληρωμένο κύκλωμα περιλαμβάνεται μέσα σε ένα κομμάτι πλαστικό. Η κάρτα είναι διαστάσεων 85.6mmX 53.98mmX 0.76mm και είναι η ίδια με την τραπεζική κάρτα με τη μαγνητική λωρίδα, που χρησιμοποιείται ως όργανο πληρωμής για τις πολυάριθμες οικονομικές συναλλαγές.

Η κύρια περιοχή αποθήκευσης σε τέτοιες κάρτες είναι συνήθως Ηλεκτρονικά Διαγραφόμενη Προγραμματιζόμενη Μόνο-Ανάγνωσης Μνήμη (ElectricallyErasableProgrammableReadOnlyMenory, EEPROM), η οποία έχει τη δυνατότητα να ενημερώνει και να διατηρεί τα περιεχόμενα της. Τα νεώτερα chip έξυπνων καρτών ενσωματώνουν μερικές φορές μαθηματικούς συνεπεξεργαστές στο chip του μικροεπεξεργαστή, και έτσι είναι σε θέση να εκτελέσουν αρκετά σύνθετες ρουτίνες κρυπτογράφησης σχετικά γρήγορα. Για το λόγω αυτό χρησιμοποιούνται στο ηλεκτρονικό εμπόριο και εκτελούν λειτουργίες κρυπτογράφησης και δημιουργίας ψηφιακών υπογραφών.

Το chip μιας έξυπνης κάρτας έχει τη δυνατότητα να αποθηκεύσει πολύ περισσότερα στοιχεία από εκείνα που μπορεί να συγκρατήσει μια αντίστοιχη μαγνητική κάρτα, και όλα αυτά μέσα σε ένα εξαιρετικά ασφαλές περιβάλλον. Τα στοιχεία που καταχωρούνται στο chip μπορούν να προστατευθούν αποτελεσματικά από εξωτερική αλλαγή.

Στη συνέχεια περιγράφονται τα είδη έξυπνων καρτών:

Κάρτες μικροεπεξεργαστών (IntegratedCircuit (IC) MicroprocessorCards): Οι κάρτες με μικροεπεξεργαστή είναι οι κλασσικές έξυπνες κάρτες οι οποίες μπορούν να διαχειριστούν και να επεξεργαστούν τα δεδομένα που βρίσκονται αποθηκευμένα σε αυτές. Οι κάρτες αυτές, εκτός από CPU, διαθέτουν μνήμη μόνο ανάγνωσης (ReadOnlyMemory, ROM) για την αποθήκευση του λειτουργικού συστήματος της κάρτας, μνήμη RAM (RandomAccessMemory) για γρήγορη εκτέλεση υπολογισμών και μνήμη EEPROM για την αποθήκευση εφαρμογών και δεδομένων. Οι μικροεπεξεργαστές των καρτών αυτών έχουν

τη δυνατότητα να εκτελούν υπολογισμούς τοπικά μέσα στα κυκλώματα της κάρτας, καθώς επίσης και να τρέχουν μικρά προγράμματα υπολογισμών. Αυτές οι κάρτες χρησιμοποιούνται για ποικίλες μικρές εφαρμογές, ειδικά για εκείνες που ενσωματώνουν αλγόριθμους κρυπτογράφησης, πράγμα το οποίο απαιτεί το χειρισμό μεγάλων αριθμών.

Υπάρχουν κάποιες έξυπνες κάρτες οι οποίες εκτελούν περισσότερες από μια εφαρμογές και έχουν ανοικτά λειτουργικά συστήματα (Java, MULTOS). Οι κάρτες αυτές ονομάζονται έξυπνες κάρτες πολλαπλών εφαρμογών (multi-applicationsmartcards).

Κάρτες Μνήμης (IntegratedCircuit (IC) MemoryCards): Η κάρτα μικροεπεξεργαστών μπορεί να προσθέσει, να διαγράψει και γενικά να χειριστεί τις αποθηκευμένες σε αυτήν πληροφορίες, ενώ μια κάρτα μνήμης (π.χ. προπληρωμένη τηλεφωνική κάρτα) μπορεί να αναλάβει μόνο μια προκαθορισμένη λειτουργία: την αποθήκευση πληροφορίας. Οι κάρτες μνήμης δεν έχουν απολύτως καμιά δυνατότητα επεξεργασίας και χειρισμού πληροφοριών, ενώ η μνήμη τους δε μπορεί να ξεπεράσει (τουλάχιστον για τις υπάρχουσες τυποποιήσεις ISO) τα 4KB. Ακριβώς επειδή δεν έχουν μικροεπεξεργαστική ικανότητα, οι κάρτες μνήμης συγκαταλέγονται καταχρηστικά στις έξυπνες κάρτες.

Οι κάρτες αυτές στοιχίζουν οπωσδήποτε λιγότερο από τις κάρτες με μικροεπεξεργαστή, ωστόσο όμως υστερούν αρκετά στην ασφάλεια της πληροφορίας που συγκρατούν στο εσωτερικό τους. Εξαρτώνται άμεσα από την ασφάλεια του αναγνώστη καρτών (smartcardreader) για την επεξεργασία και είναι ιδανικές όταν οι απαιτήσεις ασφάλειας δεν προϋποθέτουν υψηλό επίπεδο ασφάλειας.

Οπτικές Κάρτες Μνήμης (OpticalMemoryCards): Οι οπτικές κάρτες μνήμης μπορούν να αποθηκεύουν μέχρι 4MB πληροφορίας. Βέβαια μόλις γραφτούν, τα στοιχεία δεν μπορούν να αλλάξουν ή να αφαιρεθούν. Κατά συνέπεια, αυτός ο τύπος κάρτας είναι ιδανικός για την φύλαξη αρχείων (π.χ. ιατρικά αρχεία ή e-books).

Οι έξυπνες κάρτες, ανάλογα με τον τρόπο επικοινωνίας τους με το εξωτερικό περιβάλλον, διακρίνονται στις εξής κατηγορίες:

Έξυπνες κάρτες με επαφή (contactcards). Μια έξυπνη κάρτα με επαφή χρειάζεται να τοποθετηθεί σε ένα αναγνώστη καρτών (cardreader) προκειμένου να διαβαστούν ήδη υπάρχουσες πληροφορίες ή να εισαχθούν νέες.

Ασύρματεςέξυπνεςκάρτες(contactless cards).Οι κάρτες αυτές έχουν ενσωματωμένη κεραία και έτσι μπορούν να επικοινωνούν με μια κεραία λήψης ασύρματα, χωρίς δηλαδή φυσική επαφή.

Υβριδικές και συνδυασμένες κάρτες (hybrid&combinationcards). Οι κάρτες αυτές ενσωματώνουν και τους δύο τρόπους μετάδοσης και συνεπώς, μπορούν να επικοινωνήσουν κατά περίπτωση, είτε με ασύρματο είτε με ενσύρματο τρόπο.

- **Αναγνώστες έξυπνων καρτών (smartcardreader)**

Το απαραίτητο εργαλείο για την σύνδεση του κόσμου των έξυπνων καρτών με τον ηλεκτρονικό υπολογιστή είναι ο αναγνώστης καρτών (smartcardreader). Οι πληροφορίες που διαθέτουν οι έξυπνες κάρτες δεν θα είχαν καμιά αξία, εάν δεν υπήρχαν οι αντίστοιχοι αναγνώστες έξυπνων καρτών.

Ο αναγνώστης έξυπνων καρτών αποτελεί τον «συνδετήρα» του αυστηρά προστατευμένου εσωτερικού των έξυπνων καρτών με τον έξω κόσμο. Ρόλος των συσκευών αυτών είναι η ανάγνωση των πληροφοριών που ενσωματώνουν οι έξυπνες κάρτες.

Δύο είναι οι κυριότερες κατηγορίες αναγνωστών έξυπνων καρτών. Η πρώτη είναι οι τερματικές συσκευές, οι οποίες απαρτίζονται από επιμέρους εξαρτήματα όπως πληκτρολόγιο, εκτυπωτή, οθόνη. Χαρακτηριστικά παραδείγματα της κατηγορίας αυτής είναι τα κινητά τηλέφωνα, τα καρτοτηλέφωνα, οι αυτόματοι πωλητές και οι αποκωδικοποιητές.

Δεύτερη κατηγορία είναι οι αναγνώστες-εγγραφείς έξυπνων καρτών, οι οποίοι δεν φέρουν εξοπλισμό αλλά συνδέονται με τερματικές συσκευές όπως Η/Υ, InfoKiosks, controllers.

- ***Χαρακτηριστικά Έξυπνων Καρτών***

Στον Πίνακας 61που ακολουθεί φαίνονται κάποια βασικά χαρακτηριστικά των έξυπνων καρτών που τις κάνουν ιδανικές για χρήση στο ηλεκτρονικό εμπόριο.

Κόστος	Το κόστος των καρτών αυτών ποικίλει ανάλογα με τη μνήμη και την επεξεργαστική τους ικανότητα.
Αξιοπιστία	Οι κατασκευαστές εγγυούνται 10.000 κύκλους εγγραφής/ανάγνωσης. Οι κάρτες που δηλώνονται ως συμβατές με τις προδιαγραφές του ISO 7816 πρέπει να πληρούν τις προϋποθέσεις που αυτό θέτει για τις έξυπνες κάρτες.
Διόρθωση Λαθών	Τα τρέχοντα λειτουργικά συστήματα καρτών (COS) κάνουν τον δικό τους έλεγχο για λάθη.
	EEPROM: 8K – 128Kbit. Με σύγχρονες τεχνικές συμπίεσης δεδομένων,

Χωρητικότητα Αποθήκευσης	το μέγεθος των δεδομένων που μπορεί να καταχωρηθεί σε μια κάρτα αυξάνει σημαντικά.
Ευκολία Χρήσης	Οι έξυπνες κάρτες είναι φιλικές προς τον χρήστη.
Ευπάθεια	Παρουσιάζουν ευπάθεια σε φυσική κατάχρηση, αλλά είναι κατά πολύ πιο ανθεκτικές από τις κάρτες μαγνητοταινίας.
Ασφάλεια	Οι έξυπνες κάρτες παρέχουν υψηλή ασφάλεια. Οι πληροφορίες που αποθηκεύονται μέσα τους είναι δύσκολο να αντιγραφούν ή να υποκλαπούν, αντίθετα με τις κάρτες μαγνητικής ταινίας που αντιγράφονται σχετικά εύκολα.

Πίνακας 61 Χαρακτηριστικά έξυπνων καρτών.

- ***Πλεονεκτήματα Έξυπνων Καρτών και Δυσκολίες στην Ανάπτυξη τους***

Οι έξυπνες κάρτες χρησιμοποιούνται σε μεγάλο βαθμό στο ηλεκτρονικό εμπόριο λόγω των πλεονεκτημάτων που παρέχουν. Τα κυριότερα πλεονεκτήματα των έξυπνων καρτών είναι τα εξής:

- Οι έξυπνες κάρτες μπορούν να κρυπτογραφούν τα δεδομένα που εμπεριέχονται στο chip τους, παρέχοντας ένα ιδιαίτερα σημαντικό επίπεδο ασφάλειας συγκριτικά με τις παραδοσιακές κάρτες.
- Η πρόσβαση με τις έξυπνες κάρτες είναι εφικτή και σε γεωγραφικές τοποθεσίες όπου η on-line επικοινωνία δεν είναι διαθέσιμη.
- Η σωστή χρήση των έξυπνων καρτών μειώνει την πιθανότητα εξαπάτησης ή υποκλοπής.
- Η έξυπνη κάρτα μπορεί να προσφέρει αυθεντικοποίηση στον κάτοχο της.

Στις έξυπνες κάρτες μπορεί να συνυπάρχουν πολλαπλές εφαρμογές. Κάθε αλλαγή των στοιχείων κάποιας εφαρμογής μπορεί να γίνεται ηλεκτρονικά και μετά την έκδοση της κάρτας, χωρίς να χρειάζεται να ακυρωθεί η κάρτα και να εκδοθεί νέα.

Μπορεί μεν τα πλεονεκτήματα από τη χρησιμοποίηση των έξυπνων καρτών να είναι σημαντικά, όμως μια σειρά άλλων θεμάτων καθυστερεί την υιοθέτηση τους. Οι κυριότερες δυσκολίες που καθυστερούν την ανάπτυξη των έξυπνων καρτών είναι:

- Το κόστος της έξυπνης κάρτας είναι σαφώς υψηλότερο από το αντίστοιχο των απλών μαγνητικών καρτών και αυξάνεται ακόμη περισσότερο στην περίπτωση των multi-applicationcards. Επιπλέον για τη χρησιμοποίηση των έξυπνων καρτών, ένα σημαντικό κόστος προστίθεται λόγω της αναγκαίας αγοράς αναγνώστη καρτών.
- Έλλειψη εξοπλισμού από πολίτες και μικρές εταιρείες.
- Το πλήθος των χρηστών αισθάνονται ότι οι τεχνολογίες έξυπνων καρτών δεν είναι αρκετά ώριμες και υπάρχει πιθανότητα να αλλάξουν στο κοντινό μέλλον.
- Μερικές κατηγορίες εργαζομένων-χρηστών θεωρούν ότι η χρήση των έξυπνων καρτών επιφέρει αλλαγές συνηθειών στην εργασία και υπάρχει φόβος επιβολής πρόσθετων ελέγχων με την εφαρμογή έξυπνων καρτών.
- Οι έξυπνες κάρτες μπορούν να μειώσουν την πρόσβαση και τους πόρους σε εκείνους που είναι τεχνολογικά αναλφάβητοι ή αδιάφοροι.
- Υπάρχει έλλειψη ενημέρωσης του κοινού και προκατάληψη στην αξιοποίηση και στην εμπορική εφαρμογή νέων τεχνολογιών.

• *Εφαρμογές στο Ηλεκτρονικό Εμπόριο*

Μια έξυπνη κάρτα λόγω της μορφής και της ενσωματωμένης τεχνολογίας, μπορεί να χρησιμοποιηθεί με ποικίλους τρόπους στο ηλεκτρονικό εμπόριο. Στη συνέχεια παρουσιάζονται οι βασικότερες εφαρμογές των έξυπνων καρτών στο ηλεκτρονικό εμπόριο:

Ηλεκτρονικό Πορτοφόλι

Η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί ως ηλεκτρονικό πορτοφόλι όπου αποθηκεύονται μονάδες χρήματος (π.χ. ψηφιακά νομίσματα) οι οποίες στη συνέχεια χρησιμοποιούνται για ηλεκτρονικές πληρωμές. Δηλαδή ο κάτοχος της έξυπνης κάρτας μπορεί να μεταφέρει από τον τραπεζικό του λογαριασμό ένα ποσό (σχετικά μικρό) στην έξυπνη κάρτα και στη συνέχεια να το χρησιμοποιήσει για πληρωμές. Όταν εξαντληθούν τα μετρητά, ο κάτοχος επαναλαμβάνει τη μεταφορά χρημάτων στο ηλεκτρονικό πορτοφόλι.

Παραδείγματα χρήσεων αποτελούν οι πληρωμές στο Internet, οι ελεγχόμενοι χώροι στάθμευσης, διόδια σε δρόμους, πληρωμή εισιτηρίου σε μέσα μαζικής μεταφοράς, αυτόματη πληρωμή φωτοτυπιών σε δημόσιες βιβλιοθήκες αλλά και αγορές καταναλωτικών ειδών σε κάθε είδους κατάστημα. Με αυτό τον τρόπο διευκολύνεται η άμεση είσπραξη του πληρωτέου ποσού.

Πιστωτικές Κάρτες

Μια έξυπνη κάρτα μπορεί να είναι πιστωτική ή χρεωστική κάρτα και ο νόμιμος κάτοχος της

μπορεί να τη χρησιμοποιεί για αγορές. Για παράδειγμα μπορεί να κάνει κάποιες αγορές στο διαδίκτυο και να χρησιμοποιήσει την έξυπνη κάρτα ως μέσο πληρωμής, δηλαδή να δώσει στον έμπορα τις απαραίτητες πληροφορίες για την κάρτα του (αριθμό, ημερομηνία έκδοσης, κλπ.) ώστε να μπορέσει να γίνει η πληρωμή. Οι έξυπνες κάρτες παρέχουν υψηλότερη ασφάλεια από ότι οι μαγνητικές κάρτες. Οι πληροφορίες που αποθηκεύονται μέσα στις έξυπνες κάρτες είναι δύσκολο να αντιγραφούν ή να υποκλαπούν, αντίθετα με τις κάρτες μαγνητικής ταινίας που αντιγράφονται σχετικά εύκολα.

Αποθήκευση Ιδιωτικού Κλειδιού

Οι έξυπνες κάρτες έχουν αποδειχθεί κατάλληλες και πολύ ασφαλείς συσκευές για την αποθήκευση ευαίσθητων δεδομένων όπως είναι τα ιδιωτικά κλειδιά. Οι κάρτες αυτές, μπορούν να συνδεθούν σε ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί για κρυπτογράφηση ή για δημιουργία ψηφιακής υπογραφής. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δε χρειάζεται ποτέ να αποθηκευτεί στον υπολογιστή και ότι κάποιος για να έχει πρόσβαση στο ιδιωτικό κλειδί πρέπει να κλέψει την έξυπνη κάρτα. Αλλά ακόμα και σε αυτή την περίπτωση δεν θα μπορέσει να έχει πρόσβαση στο ιδιωτικό κλειδί διότι η πρόσβαση στη μνήμη των έξυπνων καρτών προστατεύεται πάντα από ένα PIN και μόνο μετά την παρουσίαση του σωστού PIN η έξυπνη κάρτα επιτρέπει την πρόσβαση στη μνήμη της και άρα στα δεδομένα ασφάλειας που έχει αποθηκευμένα (ιδιωτικό κλειδί). Σε περίπτωση παρουσίασης λανθασμένων PIN, το chip εμποδίζει την περαιτέρω πρόσβαση στη μνήμη, προστατεύοντας έτσι τις πληροφορίες από αναρμόδια πρόσβαση.

Προηγμένες ηλεκτρονικές υπογραφές σε ηλεκτρονικά έγγραφα

Λόγω της επεξεργαστικής τους ικανότητας, οι έξυπνες κάρτες μπορούν να δημιουργούν ζεύγος κλειδιών και να αποθηκεύουν το ιδιωτικό κλειδί και τα ψηφιακά πιστοποιητικά με ασφάλεια.

Πολύπλοκα ολοκληρωμένα κυκλώματα μπορούν να ενσωματωθούν στις έξυπνες κάρτες και κατ’επέκταση πολύπλοκες πράξεις όπως η δημιουργία ψηφιακής υπογραφής μπορούν να εκτελούνται στην έξυπνη κάρτα με υψηλό επίπεδο ασφάλειας και αξιοπιστίας . Έτσι, οι κάτοχοί των έξυπνων καρτών, που πιστοποιούν την ταυτότητά τους με «αναγνωρισμένα πιστοποιητικά» να μπορούν να υπογράφουν ηλεκτρονικά έγγραφα με δικονομική αξία ίση με αυτήν της ιδιόχειρης υπογραφής τους στα έντυπα έγγραφα.

Πρόσβαση σε ανοικτά ή κλειστά δίκτυα

Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν ψηφιακά πιστοποιητικά (digitalcertificates) και άλλες πληροφορίες για τον έλεγχο του δικαιώματος πρόσβασης του χρήστη, ώστε να μπορεί να χρησιμοποιεί υπολογιστικά και δικτυακά συστήματα με ασφαλή τρόπο. Για παράδειγμα μια εταιρεία μπορεί να χρησιμοποιεί έξυπνες κάρτες για να ελέγχει ποιοι

μπαίνουν στο εταιρικό της δίκτυο.

- ***Άλλες Εφαρμογές***

Υγεία και Ασφάλιση

Μια από τις πιο ενδιαφέρουσες εφαρμογές εντοπίζεται στο χώρο της υγείας, όπου οι έξυπνες κάρτες χρησιμοποιούνται για την ασφαλή αποθήκευση στοιχείων ταυτότητας, και ιατρικών δεδομένων ενός ατόμου. Έτσι οι ιατρικές πληροφορίες είναι έγκαιρα και έγκυρα διαθέσιμες στους ασθενείς και ιατρούς.

Αντίστοιχη εφαρμογή μπορεί να αναπτυχθεί στο χώρο της κοινωνικής ασφάλισης όπου η έξυπνη κάρτα λειτουργεί ως φάκελος ασφαλισμένου με όλες τις πληροφορίες για τα στοιχεία του, τις ασφαλιστικές καλύψεις, τις συνταγογραφήσεις φαρμάκων κλπ.

Με τον τρόπο αυτό διευκολύνεται σημαντικά η ελεύθερη διακίνηση των ασθενών που μπορούν να ταξιδεύουν στο εσωτερικό και στο εξωτερικό φέροντας μαζί τους τον ασφαλιστικό και ιατρικό τους φάκελο.

Πέραν αυτού, οι έξυπνες κάρτες στον τομέα της υγείας χρησιμοποιούνται σε εφαρμογές ταυτοποίησης του ασθενούς και επαγγελματιών υγείας (ιατρών, νοσηλευτών κλπ), ηλεκτρονικών υπογραφών για την ακεραιότητα και την αυθεντικότητα των ιατρικών δεδομένων και κρυπτογράφησης των δεδομένων για τη διασφάλιση της εμπιστευτικότητας.

Έλεγχος πρόσβασης σε κτίρια

Μια έξυπνη κάρτα μπορεί να αποθηκεύσει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης (accesscontrol) σε κτίρια και εγκαταστάσεις, όπως πανεπιστήμια, νοσοκομεία, στρατιωτικές μονάδες, βιβλιοθήκες, λέσχες κλπ.

Για ανάγκες υψηλότερης ασφάλειας, π.χ. πρόσβαση σε συγκεκριμένες υπηρεσίες, μια έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά (π.χ. δακτυλικά αποτυπώματα, ίριδα του ματιού) του χρήστη.

GSM κάρτες

Η πιο διαδεδομένη χρήση της έξυπνης κάρτας είναι για την κινητή τηλεφωνία με τις γνωστές SIM (SubscriberIdentityModule) κάρτες.

Στις μεταφορές

Οι εφαρμογές στον τομέα των μεταφορών που μπορούν να προσφέρουν οι έξυπνες κάρτες

είναι οι εξής:

- Πληρωμή εισιτηρίου στις δημόσιες συγκοινωνίες.
- Πληρωμή διοδίων.
- Δικαιώματα parking.
- Κρατήσεις αεροπορικών εισιτηρίων, κρατήσεις σε ξενοδοχεία.
- Τεκμηρίωση κατόχου, ηλεκτρονικό διαβατήριο.

- ## Κινητό Ηλεκτρονικό Εμπόριο

Λόγω της ραγδαίας ανάπτυξης του εμπορίου στο Διαδίκτυο, το ηλεκτρονικό εμπόριο συχνά αναφέρεται σε αγορές από on-line καταστήματα του διαδικτύου, που είναι γνωστά ως δικτυακοί τόποι ηλεκτρονικού εμπορίου ή εικονικά καταστήματα. Παρόλα αυτά, το ηλεκτρονικό εμπόριο δε θα έπρεπε να συνδεθεί αποκλειστικά με την ύπαρξη μιας ιστοσελίδας όπου είναι δυνατή η πραγματοποίηση αγορών. Περιλαμβάνει κάθε είδους ηλεκτρονική επικοινωνία μέσω της οποίας μπορεί ο πελάτης να αναζητήσει κάποιο προϊόν και να πραγματοποιήσει μια συναλλαγή.

Επιπλέον λόγω της ταχύτατης ανάπτυξης της τεχνολογίας και των καλύτερων και αποδοτικότερων συστημάτων έγινε δυνατή η ασύρματη επικοινωνία πελατών που βρίσκονται σε κίνηση με τους δικτυακούς τόπους ακόμα και μέσω συσκευών που

καταλαμβάνουν ελάχιστο χώρο και δεν αποτελούν βάρος για τον πελάτη όπως είναι οι συσκευές κινητής τηλεφωνίας.

Η κατακόρυφη αύξηση των κινητών τερματικών που χρησιμοποιούνται τα τελευταία χρόνια, έδωσε έδαφος στην ταχύτατη ανάπτυξη του ηλεκτρονικού εμπορίου που διεξάγεται με την χρήση των παραπάνω συσκευών. Ο νέος τύπος των συγκεκριμένων ηλεκτρονικών συναλλαγών, ο οποίος διεξάγεται με τη χρήση κινητών συσκευών ονομάζεται κινητό ηλεκτρονικό εμπόριο (mobilecommerce). Με τον όρο αυτό ορίζεται οποιοδήποτε είδος εμπορικής συναλλαγής που γίνεται διαμέσου κινητού τηλεπικοινωνιακού δικτύου (mobiletelecommunicationnetwork), με τη χρήση ασύρματων φορητών συσκευών. Σημειώνεται πως οι ηλεκτρονικές συναλλαγές οι οποίες πραγματοποιούνται με τη χρήση ενός φορητού ηλεκτρονικού υπολογιστή ο οποίος είναι συνδεδεμένος με το διαδίκτυο μέσω ενός modem που χρησιμοποιεί ενσύρματο δίκτυο, δεν συμπεριλαμβάνονται στον ορισμό του κινητού ηλεκτρονικού εμπορίου.

Λόγω της πανταχού παρουσίας (ubiquity) των κινητών τηλεφώνων (και των άλλων κινητών συσκευών), το κινητό ηλεκτρονικό εμπόριο υπόσχεται περισσότερες ευκαιρίες από ότι το παραδοσιακό ηλεκτρονικό εμπόριο. Ο καταναλωτής μπορεί να έχει πρόσβαση σε πληροφορίες, προϊόντα και υπηρεσίες ανά πάσα στιγμή και από οπουδήποτε, χωρίς να παίζει ρόλο η τοποθεσία στην οποία βρίσκεται (π.χ. να αγοράσει εισιτήρια για μια θεατρική παράσταση εν κινήσει, να πληρώσει για θέση στάθμευσης, να αγοράσει προϊόντα με χρήση κινητού τηλεφώνου, να κατεβάσει αρχεία πολυμέσων στο PDA (PersonalDataAssistant) του, να λάβει πληροφορίες όπως πρόγνωση καιρού και χρηματιστηριακές αξίες κοκ).

Οι υπηρεσίες κινητού ηλεκτρονικού εμπορίου απαιτούν μεγαλύτερη προστασία ασφάλειας από ότι οι υπηρεσίες του απλού ηλεκτρονικού εμπορίου, λόγω του ότι στην πρώτη περίπτωση όλες οι πληροφορίες και τα δεδομένα μεταφέρονται μέσω ασύρματων τηλεπικοινωνιακών δικτύων, τα οποία είναι πιο ευάλωτα σε επιθέσεις από ότι τα ενσύρματα δίκτυα. Συγκεκριμένα στο κινητό ηλεκτρονικό εμπόριο τα δεδομένα των συναλλαγών καθώς και τα προσωπικά δεδομένα των καταναλωτών είναι διαθέσιμα στον αέρα και ευάλωτα σε επιθέσεις κρυφακούσματος (eavesdropping) και όχι μόνο. Δηλαδή το κινητό ηλεκτρονικό εμπόριο έχει κάποιες επιπλέον απαιτήσεις ασφάλειας σε σχέση με το παραδοσιακό ηλεκτρονικό εμπόριο.

• *Ασύρματες Συσκευές*

Στο κινητό ηλεκτρονικό εμπόριο, ως κινητές τερματικές συσκευές δεν χρησιμοποιούνται αποκλειστικά τα κινητά τηλέφωνα. Υπάρχουν αρκετά είδη ασύρματων συσκευών που μπορούν να χρησιμοποιούν οι καταναλωτές ώστε να πραγματοποιούν ασύρματες συναλλαγές. Οι πιο διαδεδομένες ασύρματες συσκευές είναι:

- Κινητάτηλέφωνα (mobilephone).
- PDA (Personal Data Assistant).
- Έξυπνα τηλέφωνα (smartphone): τα έξυπνα τηλέφωνα συνδυάζουν την τεχνολογία PDA με τα κινητά τηλέφωνα σε μια συσκευή.

- Tablet PCs.
- Φορητοί υπολογιστές (Laptop).

Κάθε ασύρματη συσκευή έχει κάποια ιδιαίτερα χαρακτηριστικά τα οποία επηρεάζουν τη χρησιμότητα της. Τα χαρακτηριστικά αυτά είναι:

- Μέγεθος παρουσίασης πληροφοριών και χρωματική ανάλυση τους (colourofdisplay).
- Συσκευές εισόδου: διαθεσιμότητα πληκτρολογίου και ποντικού (mouse).
- Χωρητικότητα μνήμης και επεξεργαστική ισχύ.
- Δυνατότητα σύνδεσης στο δίκτυο.
- Υποστήριξη λειτουργικών συστημάτων (π.χ. PalmOS, MicrosoftPocketPC).
- Διαθεσιμότητα εσωτερικού αναγνώστη έξυπνων καρτών (internalsmartcartreader): για παράδειγμα για την κάρτα SIM το κινητό τηλέφωνο αποτελεί αναγνώστη έξυπνης κάρτας.

Με βάση τα παραπάνω χαρακτηριστικά, οι υπηρεσίες που λαμβάνουν οι τελικοί χρήστες ποικίλουν. Επιπλέον με βάση την τεχνολογία του δικτύου που χρησιμοποιείται για τη μεταφορά των πληροφοριών, η ικανότητα του εύρους ζώνης (bandwidthcapacity) ποικίλει και επηρεάζει το είδος των πληροφοριών που οι τελικοί χρήστες λαμβάνουν.

Στα κινητά τηλέφωνα, υπάρχουν τρεις λύσεις για την εσωτερική εισαγωγή των έξυπνων καρτών: singleSIM, dualchip και dualslot. SingleSIM είναι η λύση που είναι ευρέως διαδεδομένη σήμερα, όπου κάθε εμπιστευτική πληροφορία του χρήστη αποθηκεύεται σε μια έξυπνη κάρτα. Στο dualchip υπάρχουν δύο έξυπνες κάρτες σε ένα κινητό τηλέφωνο, μια για αυθεντικοποίηση του χρήστη στο πάροχο του δικτύου (networkoperator) και μια για υπηρεσίες προστιθέμενης αξίας όπως ασύρματες πληρωμές ή ψηφιακές υπογραφές. Το dualslot κινητό τηλέφωνο έχει μια κάρτα SIM και ένα slot για εξωτερική έξυπνη κάρτα φυσικού μεγέθους. Έτσι διαφορετικές κάρτες μπορούν να χρησιμοποιούνται η μια μετά την άλλη.

- ## Έξυπνα Τηλέφωνα (Smart Phones)

Με τον όρο έξυπνα τηλέφωνα περιγράφονται οι κινητές συσκευές οι οποίες παρέχουν δυνατότητες επόμενης γενιάς (nextgenerationcapabilities) όπως εφαρμογές java, έγχρωμη απεικόνιση και πολυφωνικούς ήχους κλήσης. Κάποια περιλαμβάνουν ενσωματωμένες κάμερες, δυνατότητα αποστολής και λήψης MMS (MultimediaMessagingService) ή λειτουργικά συστήματα όπως των PDA (IPalm, PockectPC).

Ένα από τα πιο κοινά χαρακτηριστικά των έξυπνων τηλεφώνων είναι οι έγχρωμες οθόνες

υψηλής ανάλυσης οι οποίες δίνουν τη δυνατότητα λήψης έγχρωμων γραφικών και φωτογραφιών.

Το πρότυπο J2ME (Javaformobiledevices) επιτρέπει τη λήψη παιχνιδιών και εφαρμογών κατευθείαν στο τηλέφωνο. Η εκτέλεση ενός προγράμματος Javaapplet στο ίδιο το τηλέφωνο αντί στον κεντρικό server παρέχει καλύτερα γραφικά, είναι πιο γρήγορη και πιο φθηνή, αφού δεν απαιτείται η μεταφορά πολλών δεδομένων στο δίκτυο.

Τα έξυπνα τηλέφωνα παρέχουν επίσης γρηγορότερες συνδέσεις για μετάδοση δεδομένων, σύνδεση στο διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου.

Ένα ιδιαίτερο χαρακτηριστικό στα έξυπνα τηλέφωνα αποτελεί η ιδέα της λειτουργίας τους ως PDA. Υπάρχουν τρία βασικά λειτουργικά συστήματα που μπορούν να ενσωματωθούν στις συσκευές αυτές: το Symbian, το PalmOS και το MicrosoftPocketPC.

- ## PDA (Personal Data Assistant)

Τα PDAs είναι μικρές φορητές υπολογιστικές συσκευές που παρέχουν δυνατότητες συγκρίσιμες με εκείνες ενός φορητού υπολογιστή αλλά σε πολύ μικρότερο μέγεθος. Τα σύγχρονα PDAs διαθέτουν έγχρωμες LCD οθόνες υψηλής ανάλυσης και ευκρίνειας, τεχνολογία touchscreen (αφής) όπου με ένα ειδικό πενάκι πραγματοποιούνται όλες οι λειτουργίες. Οι συσκευές αυτές διαθέτουν ενσωματωμένο modem/fax, ενώ για την επικοινωνία με άλλες συσκευές (π.χ. PC) παρέχουν τη δυνατότητα υπέρυθρης ζεύξης. Τα λειτουργικά συστήματα που κυριαρχούν είναι το EPOC της Symbian, το PalmOS και το MicrosoftPocketPC. Ο σχεδιασμός των λειτουργικών συστημάτων είναι ειδικός για κινητή (mobile) χρήση, δηλαδή είναι γρήγορα, σταθερά στη λειτουργία τους και εύκολα στο χειρισμό τους.

- ## Tablet PC

Τα TabletPCs είναι μια νέα μορφή φορητών υπολογιστών, εξοπλισμένα με οθόνες αφής, ασύρματη σύνδεση στο Internet και εφαρμογές ομιλίας και γραφής. Στα TabletPCs είναι δυνατή η εκτέλεση όλων των τυπικών υπολογιστικών δραστηριοτήτων γράφοντας κατευθείαν στη οθόνη τους, ή χρησιμοποιώντας το εικονικό πληκτρολόγιο που μπορεί να εμφανίσει αυτή.

Τα TabletPCs προσφέρουν μέγιστη φορητότητα ενώ ταυτόχρονα προσπαθούν να επιτύχουν εξαιρετική επεξεργαστική ισχύ αλλά και απόλυτη συνεργασία με τον χρήστη. Τα TabletPCs είναι εύκολα στο χειρισμό τους και προσφέρονται για πραγματοποίηση εφαρμογών κινητού ηλεκτρονικού εμπορίου.

- ## *Σύγκριση με το Ηλεκτρονικό Εμπόριο*

Σε σύγκριση με το ηλεκτρονικό εμπόριο, το κινητό ηλεκτρονικό εμπόριο παρουσιάζει τόσο πλεονεκτήματα όσο και μειονεκτήματα.

Τα πλεονεκτήματα του κινητού ηλεκτρονικού εμπορίου είναι:

- **Πανταχού παρουσία (ubiquity)**: η συσκευή που χρησιμοποιούν οι τελικοί χρήστες

(καταναλωτές) είναι κινητή, και έτσι μπορούν να έχουν πρόσβαση στις εφαρμογές κινητού ηλεκτρονικού εμπορίου σε οποιοδήποτε μέρος βρίσκονται και σε πραγματικό χρόνο.

- **Δυνατότητα πρόσβασης (accessibility)**: η δυνατότητα πρόσβασης είναι σχετική με την πανταχού παρουσία και σημαίνει ο τελικός χρήστης έχει δυνατότητα πρόσβασης οποιαδήποτε στιγμή και από οπουδήποτε.

- **Ασφάλεια (security)**: η ασύρματη συσκευή του χρήστη παρέχει ένα ιδιαίτερο επίπεδο ασφάλειας. Για παράδειγμα η κάρτα SIM (SubscriberIdentityModule) που τοποθετείται στο κινητό τηλέφωνο είναι μια έξυπνη κάρτα στην οποία αποθηκεύονται οι εμπιστευτικές πληροφορίες του χρήστη (π.χ. ιδιωτικό κλειδί αυθεντικοποίησης).

- **Εντοπισμός (localization)**: ο χειριστής δικτύου μπορεί να εντοπίσει εγγεγραμμένους χρήστες χρησιμοποιώντας ένα σύστημα ανίχνευσης θέσης, όπως το GPS (GlobalPositionSystem), ή μέσω της τεχνολογίας δικτύων GSM (GlobalSystemforMobileCommunication) ή UMTS (UniversalMobileTelecommunicationsSystem) και να προσφέρει υπηρεσίες βασισμένες στην τοποθεσία που βρίσκεται ο χρήστης (π.χ. τοπικές πληροφορίες για ξενοδοχεία, εστιατόρια).

- **Ευκολία (convenience)**: το μέγεθος και το βάρος των ασύρματων συσκευών, η δυνατότητα μεταφοράς τους σε οποιοδήποτε μέρος καθώς και η δυνατότητα πρόσβασης τους στο δίκτυο, τα κάνει να είναι το ιδανικό εργαλείο για την πραγματοποίηση προσωπικών αναγκών.

- **Προσωποποιημένες υπηρεσίες (personalization)**: οι ασύρματες συσκευές είναι συνήθως προσωπικές για κάθε χρήστη. Έτσι ο χρήστης είναι σε θέση να λαμβάνει πληροφορίες που σχετίζονται άμεσα με τις ανάγκες και τις επιθυμίες του.

Το κινητό ηλεκτρονικό εμπόριο παρουσιάζει τα ακόλουθα μειονεκτήματα:

- Οι ασύρματες συσκευές έχουν περιορισμένες ικανότητες (π.χ. χωρητικότητα μνήμης, επεξεργαστική ισχύς). Οι ικανότητες αυτές ποικίλουν μεταξύ των ασύρματων συσκευών και έτσι οι υπηρεσίες των χρηστών θα πρέπει να προσαρμόζονται αναλόγως.

- Οι ασύρματες συσκευές είναι πιο επιρρεπής στην κλοπή και στην καταστροφή. Αφού τα κινητά τηλέφωνα είναι προσωπικά και περιέχουν τις εμπιστευτικές πληροφορίες του χρήστη, θα πρέπει να προστατεύονται σύμφωνα με υψηλά πρότυπα ασφάλειας.

- Η επικοινωνία μέσω του αέρα ανάμεσα στην ασύρματη συσκευή και στο δίκτυο εισαγάγει πρόσθετους κινδύνους ασφάλειας (π.χ. κρυφάκουσμα).

- ***Ζητήματα Ασφαλείας***

Το κινητό ηλεκτρονικό εμπόριο δε θα είχε επιτυχία χωρίς την ύπαρξη ενός ασφαλούς περιβάλλοντος. Ακολουθούν κάποια ζητήματα σχετικά με την ασφάλεια των ασύρματων συναλλαγών:

- **Ασύρματη συσκευή**: τόσο η ασύρματη συσκευή όσο και οι εμπιστευτικές πληροφορίες του χρήστη που περιέχονται σε αυτήν πρέπει να προστατεύονται από μη εξουσιοδοτημένη χρήση. Για το λόγο αυτό χρησιμοποιούνται μηχανισμοί ασφάλειας οι οποίοι περιλαμβάνουν αυθεντικοποίηση του χρήστη (π.χ. με τη χρήση PIN ή κωδικού πρόσβασης) και ασφαλή αποθήκευση των εμπιστευτικών δεδομένων (π.χ. στην κάρτα SIM στο κινητό τηλέφωνο).

- **Ράδιο κανάλι**: η πρόσβαση στο τηλεπικοινωνιακό δίκτυο απαιτεί την προστασία των δεδομένων που μεταφέρονται. Συγκεκριμένα πρέπει να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των μεταφερόμενων δεδομένων. Επίσης, τα προσωπικά δεδομένα των χρηστών πρέπει να προστατεύονται από επιθέσεις τύπου κρυφακούσματος. Οι διαφορετικές τεχνολογίες ασύρματων δικτύων χρησιμοποιούν διαφορετικούς μηχανισμούς ασφάλειας οι οποίοι παρουσιάζονται στην επόμενη παράγραφο.

- **Εφαρμογές κινητού ηλεκτρονικού εμπορίου**: οι εφαρμογές κινητού ηλεκτρονικού εμπορίου, και ειδικά αυτές που περιλαμβάνουν πληρωμή, πρέπει να είναι ασφαλείς και να πιστοποιούν τον πελάτη, τον έμπορα και τον πάροχο δικτύου. Για παράδειγμα, σε μια συναλλαγή τόσο ο πελάτης όσο και ο έμπορας θέλουν να πιστοποιήσουν ο ένας την ταυτότητα του άλλου πριν πραγματοποιηθεί η πληρωμή. Επίσης ο πελάτης θέλει να είναι βέβαιος για την παραλαβή των προϊόντων ή των υπηρεσιών που θα πληρώσει. Επιπλέον πρέπει να διασφαλίζεται η αυθεντικοποίηση, η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών πληρωμής (π.χ. αριθμός πιστωτικής κάρτας), καθώς επίσης και η μη αποποίηση της συναλλαγής.

- ***Τεχνολογίες Ασφαλείας σχετικά με το Ασύρματο Ηλεκτρονικό Εμπόριο***

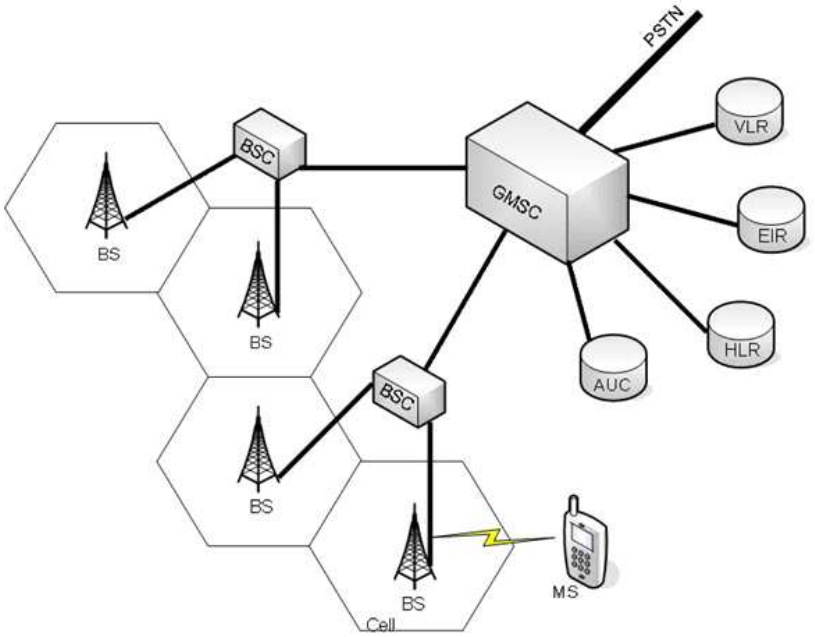
- **GSM(Global System for Mobile Communication)**

Το GSM είναι το πανευρωπαϊκό πρότυπο για την ψηφιακή κυψελωτή τηλεφωνία όπως αυτό έχει καθοριστεί από το Ευρωπαϊκό Ινστιτούτο Τυποποίησης των Τηλεπικοινωνιών (EuropeanTelecommunicationsStandardInstituteETSI) και εφαρμόζεται σε πάνω από 170 χώρες παγκοσμίως. Ο ρόλος του είναι η παροχή ενός τυποποιημένου τηλεπικοινωνιακού προτύπου. Η φιλοσοφία της κυψελωτής τηλεφωνίας είναι η χρήση πομποδεκτών χαμηλής ισχύος όπου οι συχνότητες θα μπορούσαν να επαναχρησιμοποιηθούν μέσα σε μια γεωγραφική περιοχή.

Σήμερα, τα GSM τηλέφωνα είναι ευρέως διαδεδομένα και για το λόγο αυτό θεωρούνται ως η κύρια συσκευή για εφαρμογές κινητού ηλεκτρονικού εμπορίου. Τα πρώτα χρόνια

λειτουργίας του GSM (αρχές τις δεκαετίας του 1990) οι συσκευές αυτές, εκτός από την τηλεφωνία, δεν είχαν κάποιες ιδιαίτερες ικανότητες. Καθώς όμως το κεντρικό δίκτυο GSM επεκτάθηκε, οι ασύρματες συσκευές αναβαθμίστηκαν και μπορούν να παρέχουν στους χρήστες τους τις ακόλουθες υπηρεσίες:

- SMS (ShortMessageService): επιτρέπει την αποστολή και λήψη μικρών μηνυμάτων μεταξύ κινητών τηλεφώνων.
- MMS (MultimediaMessagingService): υποστηρίζει τη μετάδοση δεδομένων εικόνας, ήχου, γραφικών και φωνής.
- WAP (WirelessApplicationProtocol): επιτρέπει την έκθεση πληροφορίας από το διαδίκτυο σε μια κινητή συσκευή.
- HSCSD (HighSpeedCircuitSwitchedData): επιτρέπει υψηλούς ρυθμούς μετάδοσης δεδομένων.



Σχήμα 71Δίκτυο GSM

Τα ασύρματα δίκτυα χρησιμοποιούν Σταθμούς Βάσης (BaseStationsBS) προκειμένου να καλύψουν με ραδιοσήματα μια συγκεκριμένη γεωγραφική περιοχή που ονομάζεται κυψέλη. Διάφοροι BSs ελέγχονται από ένα Ελεγκτή Σταθμού Βάσης (BaseStationControllerBSC). Διάφοροι BSCs συνήθως ελέγχονται από ένα Κινητό Κέντρο Μεταγωγής (MobileSwitchingCenterMSC).

Μια από τις κύριες δυσκολίες των ασύρματων δικτύων είναι το γεγονός ότι οι Κινητοί Σταθμοί (MobileStationMS, π.χ. τα κινητά τηλέφωνα) δεν έχουν μόνιμη σύνδεση στο ασύρματο δίκτυο. Για το λόγο αυτό το δίκτυο πρέπει να «ακολουθεί» τη θέση του κινητού συνδρομητή. Εκτελείται δηλαδή μια διαδικασία ενημέρωσης θέσης (locationupdate). Όταν ένας MS κινείται από την περιοχή θέσης (“locationarea” LA) που ελέγχει ένας BSC σε μια άλλη, ο MS κινεί μια διαδικασία ενημέρωσης θέσης. Αυτό πρακτικά σημαίνει ότι ο MS

λαμβάνει ένα νέο προσδιοριστικό θέσης (LAIdentifierLAI) για την τρέχουσα περιοχή θέσης.

Κάθε GSM συνδρομητής λαμβάνει ένα μοναδικό αναγνωριστικό που ονομάζεται Διεθνής Ταυτότητα Κινητού συνδρομητή (InternationalMobileSubscriberIdentityIMSI), ένα κινητό τηλέφωνο και ένα κλειδί αυθεντικοποίησης Ki. Αυτά τα δεδομένα αποθηκεύονται μόνιμα στον Καταχωρητή Θέσης Συνδρομητών (HomeLocationRegisterHLR) που αντιστοιχεί στο MSC όπου είναι εγγεγραμμένος ο συνδρομητής. Όμως ένας MS δε βρίσκεται πάντα μέσα στο διοικητικό χώρο του συγκεκριμένου MSC. Όταν ένας MS μετακινείται σε περιοχή κάποιου άλλου MSC, τα στοιχεία σχετικά με τον MS αποθηκεύονται προσωρινά στον Καταχωρητή Θέσης Επισκεπτών (VisitorLocationRegisterVLR) του τρέχοντος MSC.
Το GSM καθορίζει τις ακόλουθες υπηρεσίες ασφάλειας δικτύου, οι οποίες εξηγούνται αναλυτικά στις επόμενες παραγράφους:

- Εμπιστευτικότητα ταυτότητας συνδρομητή.
- Αυθεντικότητα ταυτότητας συνδρομητή.
- Εμπιστευτικότητα δεδομένων και σύνδεσης.

Υπάρχει διαφορά μεταξύ κινητού εξοπλισμού (MobileEquipmentME, π.χ. κινητό τηλέφωνο χωρίς κάρτα SIM) και κινητού σταθμού MS (π.χ. κινητή συσκευή με κάρτα SIM). Προφανώς, διαφορετικοί συνδρομητές μπορεί να χρησιμοποιούν τον ίδιο κινητό εξοπλισμό ΜΕ εάν εισάγουν ο καθένας τη δική του κάρτα SIM (σε διαφορετικές χρονικές στιγμές). Για να εξασφαλιστεί ότι καμιά κλεμμένη ή μη εξουσιοδοτημένη ασύρματη συσκευή δεν χρησιμοποιείται στο σύστημα, το Κέντρο Διαπίστωσης Αυθεντικοποίησης (AuthenticationCenterAUC), σε συνεργασία με τον HLR, ελέγχει τον κατάλογο με τις Διεθνείς Ταυτότητες Κινητού Εξοπλισμού (InternationalMobileEquipmentIdentityIMEI) πριν καθιερωθεί μια κλήση.

- **Εμπιστευτικότητα Ταυτότητας Συνδρομητή**

Για να προστατευτεί η ταυτότητα του συνδρομητή από τους ωτακουστές στο ραδιοκανάλι, το IMSI δε στέλνεται ποτέ σε καθαρή μορφή στον αέρα. Έτσι αντί για το IMSI χρησιμοποιείται μια προσωρινή αλλοίωση του, η προσωρινή ταυτότητα κινητού συνδρομητή (temporarymobilesubscriberidentityTMSI). Κατά την εγκατάσταση μιας σύνδεσης, ο MS στέλνει το προηγούμενο του TMSI στον VLR του τρέχοντος MSC, και λαμβάνει ως επιστροφή ένα νέο TMSI. Το νέο αυτό TMSI στέλνεται σε κρυπτογραφημένη μορφή ώστε να μην μπορεί να διαβαστεί από ωτακουστές.

- **Αυθεντικότητα Ταυτότητας Συνδρομητή**

Όταν ένας MS θέλει να πραγματοποιήσει μια κλήση, αρχικά ζητά ελεύθερο κανάλι από το BS. Όταν το κανάλι οριστεί, ο MS ζητά ενημέρωση θέσης. Το αίτημα αυτό δίνεται μέσω του BSC στο MSC. Έπειτα ο MSC ζητά από τον MS να πιστοποιηθεί, δηλαδή να αποδείξει ότι είναι αυτός που ισχυρίζεται. Η διαδικασία αυθεντικοποίησης που ακολουθείται είναι ένας μηχανισμός πρόκλησης - απόκρισης. Πληροφορίες για τα πρωτόκολλα αυθεντικοποίησης υπάρχουν στην παράγραφο 6.1.

Όπως αναφέρθηκε προηγουμένως, κάθε συνδρομητής έχει ένα κλειδί αυθεντικοποίησης Ki το οποίο αποθηκεύεται στον HLR, ή πιο συγκεκριμένα στο Κέντρο Διαπίστωσης Αυθεντικοποίησης AUC του HLR. Το AUC είναι η μόνη οντότητα στο δίκτυο που γνωρίζει το Ki, και άρα ο συνδρομητής πρέπει να την εμπιστεύεται. Το Ki αποθηκεύεται επίσης στην κάρτα SIM του MS, μαζί με τη Διεθνή Ταυτότητα Κινητού συνδρομητή IMSI και τον A3 αλγόριθμο αυθεντικοποίησης.

Για να πιστοποιηθεί η αυθεντικότητα του MS, η οντότητα επικύρωσης MSC/VLR του στέλνει έναν τυχαίο αριθμό RAND. Ο MS εφαρμόζει τον αλγόριθμο αυθεντικοποίησης A3, χρησιμοποιώντας ως εισόδους τα IMSI, RAND και Ki ,και υπολογίζει την 32 bit απάντηση SRES. Αφού μόνο ο HLR γνωρίζει το Ki , ο VLR μπορεί να λάβει από τον HLR ένα διάνυσμα αυθεντικοποίησης. Το διάνυσμα αυτό αποτελείται από το ζευγάρι (RANDj , SRESj), έτσι ώστε ο VLR να ελέγξει αν ο MS έχει στείλει την σωστή απάντηση στη συγκεκριμένη πρόκληση.

Όμως, αφού το TMSI είναι προσωρινή ταυτότητα, η οντότητα επικύρωσης MSC/VLR πρέπει να λάβει το IMSI από τον HLR. Αυτό προϋποθέτει ότι ο HLR. εμπιστεύεται τον VLR ότι δε θα κάνει κακή χρήση του IMSI.

Το σύστημα αυθεντικοποίησης στο GSM παρουσιάζει μια σημαντική αδυναμία: Απαιτεί την αυθεντικοποίηση μόνο του συνδρομητή και το δίκτυο δεν αυθεντικοποιείται. Κάτι τέτοιο είναι ευάλωτο σε επιθέσεις τύπου «άνθρωπος στη μέση» (man-in-the-middleattack).

- **Εμπιστευτικότητα Δεδομένων και Σύνδεσης**

Το Κέντρο Διαπίστωσης Αυθεντικοποίησης AUC υπολογίζει για κάθε συνδρομητή ένα κλειδί κρυπτογράφησης KC 64-bit, χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης A8. Για τον υπολογισμό αυτό, χρησιμοποιεί σαν εισόδους το IMSI, το κλειδί αυθεντικοποίησης Ki του συνδρομητή και τον ίδιο τυχαίο αριθμό RAND που χρησιμοποιείται για τον υπολογισμό του διανύσματος αυθεντικοποίησης.

Το διάνυσμα που περιέχει το κλειδί κρυπτογράφησης KC στέλνεται μαζί με το διάνυσμα αυθεντικοποίησης στην οντότητα επικύρωσης MSC/VLR, και επίσης αποθηκεύεται στην κάρτα SIM. Για την πραγματική κρυπτογράφηση των δεδομένων και της ομιλίας εφαρμόζεται ο αλγόριθμος A5. Η κρυπτογράφηση εκτελείται στον κινητό εξοπλισμό, επειδή η κάρτα SIM δεν έχει αρκετή επεξεργαστική ικανότητα ώστε να κρυπτογραφεί σε πραγματικό χρόνο. Είναι προφανές ότι ο συνδρομητής πρέπει να εμπιστεύεται τον VLR διότι αυτός γνωρίζει το κλειδί κρυπτογράφησης και άρα είναι σε θέση να διαβάζει όλα τα δεδομένα τα οποία στέλνει ή λαμβάνει ο συνδρομητής.

- **3G/UMTS**

Το σύστημα UMTS (UniversalMobileTelecommunicationsSystem) κατευθύνει την πορεία των τηλεπικοινωνιών προς την τρίτη γενιά ασύρματων τηλεπικοινωνιακών δικτύων. Το σύστημα αυτό προήλθε από περαιτέρω ανάπτυξη του GSM και έχει τη δυνατότητα να ανταποκριθεί στη συνεχώς αυξανόμενη ζήτηση των εφαρμογών του διαδικτύου και στη συνεχόμενη ζήτηση για νέα χωρητικότητα στα συνωστισμένα ασύρματα δίκτυα.

Το σύστημα UMTS (συχνά αναφέρεται W-CDMAwidebandcodedivisionmultipleaccess) είναι μια από τις πιο σημαντικές καινοτομίες στην τάση προς τα δίκτυα τρίτης γενιάς. Μπορεί να καλύψει ταχύτητες μέχρι και 2Mbps ανά χρήστη, επιτρέπει πολλές εφαρμογές να χρησιμοποιηθούν από πολλούς χρήστες, είναι σε παγκόσμια κοινή χρήση και κάνει αποδοτικότερη χρήση του φάσματος. Για τους λόγους αυτούς είναι κατάλληλο για εφαρμογές κινητού ηλεκτρονικού εμπορίου.

Η κύρια διαφορά του UMTS με το GSM είναι το δίκτυο πρόσβασης ραδιοσυχνοτήτων UTRAN (UniversalTerrestrialRadioAccessNetwork) το οποίο βασίστηκε στις ανάγκες της καινούργιας ραδιοτεχνολογίας W-CDMA, και χειρίζεται όλες τις ραδιοκυματικές λειτουργίες. Ο ορισμός του κεντρικού δικτύου (CoreNetworkCN), το οποίο είναι υπεύθυνο για τη μεταγωγή και τη δρομολόγηση των συνδέσεων προς τα εξωτερικά δίκτυα κλήσεων και δεδομένων, προήλθε από το GSM. Κάτι τέτοιο προικίζει το σύστημα με την καινούργια ραδιοκυματική τεχνολογία και με μια σφαιρική χρήση γνωστής και ενισχυμένης τεχνολογίας η οποία επιταχύνει και διευκολύνει την εισαγωγή της.

Τα κύρια συστατικά του GSM κεντρικού δικτύου μπορούν να εξελιχθούν ή να επαναχρησιμοποιηθούν στο UMTS σύστημα.

Η αρχιτεκτονική ασφαλείας του UMTS σχεδιάστηκε προσεκτικά ώστε να διορθώσει τις αδυναμίες ασφάλειας του GSM συστήματος. Τα κυριότερα προβλήματα του GSM δημιουργούνται από δύο γεγονότα: α) η αυθεντικοποίηση είναι μονόδρομη (δηλ. ο MS δεν αυθεντικοποιεί το δίκτυο, αλλά μόνο το δίκτυο αυθεντικοποιεί τον MS) και β) η κρυπτογράφηση είναι προαιρετική. Στο UMTS η αυθεντικοποίηση είναι αμοιβαία, και η κρυπτογράφηση υποχρεωτική, εκτός αν ο MS και το δίκτυο συμφωνήσουν ότι θέλουν μια μη κρυπτογραφημένη σύνδεση. Επιπλέον πάντα χρησιμοποιείται προστασία ενάντια στην τροποποίηση των μεταδιδόμενων δεδομένων, καθώς επίσης λαμβάνονται μέτρα για την αποφυγή επιθέσεων τύπου επανάληψης. Το UMTS χρησιμοποιεί νέους αλγόριθμους κρυπτογράφησης και πιο μεγάλου μήκους κρυπτογραφικά κλειδιά. Έτσι, το UMTS δεν έχει κάποια προφανή προβλήματα ασφάλειας.

- **WLAN**

Τα Ασύρματα Τοπικά Δίκτυα WLAN (WirelessLocalAreaNetworks) δεν αποτελούν μια νέα τεχνολογία. Παρέχουν σύνδεση Ethernet χωρίς καλώδια γεγονός που επιτρέπει στους χρήστες να έχουν υψηλής ταχύτητας πρόσβαση σε ένα δίκτυο δεδομένων όπως το διαδίκτυο ή το εσωτερικό δίκτυο μιας εταιρείας με χρήση ραδιοσυχνοτήτων. Αυτό παρέχει ένα σημαντικό πλεονέκτημα σε σχέση με τα δίκτυα GSM και UMTS καθώς δεν απαιτείται η συνδρομή και άδεια χρήσης από τον παροχέα του δικτύου.

Σημαντική εξάπλωση παρουσιάζει το πρότυπο της IEEE 802.11 και ιδιαίτερα τα πρότυπα 802.11b, το οποίο παρέχει ταχύτητες μετάδοσης έως 11Mbps και 802.11g το οποίο παρέχει ταχύτητες μετάδοσης έως 52Mbps. Τα πρότυπα αυτά είναι σύμφωνα με την Ευρωπαϊκή νομοθεσία για τη χρήση των συχνοτήτων στη ζώνη ISM (Industrial, Scientific, Medical Band) των 2.4GHz, σε αντίθεση με το πρότυπο 802.11a το οποίο χρησιμοποιεί τη ζώνη των 5GHz.

Τα 802.11b και 802.11g έχουν γνωρίσει και εξακολουθούν να γνωρίζουν ιδιαίτερη εξάπλωση από την εμφάνιση τους. Οι αριθμοί των συσκευών αυτής της τεχνολογίας έχουν αυξηθεί σημαντικά τα τελευταία χρόνια σε παγκόσμιο επίπεδο. Ταυτόχρονα τα διαθέσιμα σημεία πρόσβασης, σημεία δηλαδή όπου παρέχονται υπηρεσίες μέσω αυτής της τεχνολογίας, αυξάνουν επίσης με ραγδαίους ρυθμούς. Η διείσδυση των νέων αυτών τεχνολογιών στις ασύρματες συσκευές (π.χ. κινητά τηλέφωνα, PDAs, φορητοί υπολογιστές) ευνοεί την ανάπτυξη του κινητού ηλεκτρονικού εμπορίου.

Τα μέρη από τα οποία αποτελείται ένα WLAN είναι τα εξής:

- Ένα σημείο πρόσβασης AP (AccessPoint) ικανό να υποστηρίζει πολλούς πελάτες.
- Μια κάρτα πρόσβασης WLAN (π.χ. μια κάρτα PCMCIA (Personal Computer Memory Card International Association) που μπορεί να εισαχθεί σε ένα φορητό υπολογιστή).

Ένα σημαντικό ζήτημα για όλα τα ασύρματα δίκτυα είναι η ασφάλεια, δηλαδή ο έλεγχος της πρόσβασης στις υπηρεσίες και τις υποδομές, η ταυτοποίηση των χρηστών καθώς και η ακεραιότητα και η εμπιστευτικότητα των δεδομένων των χρηστών.

Αναφορικά με την ακεραιότητα και την εμπιστευτικότητα των δεδομένων καθώς μεταβιβάζονται μέσω του αέρα, οπότε και είναι εύκολο σε κακόβουλους χρήστες να «ακούν» τα δεδομένα αυτά, η αρχική πρόταση στο 802.11 ήταν η χρήση του WEP (WiredEquivalentPrivacy). Στο WEP χρησιμοποιείται κωδικοποίηση με στατικά κλειδιά των 40 ή 128 bits και για την κωδικοποίηση των δεδομένων και για την ταυτοποίηση των πελατών. Το πρόβλημα με το WEP είναι ότι μπορεί σχετικά εύκολα να παραβιαστεί δίνοντας τη δυνατότητα σε κακόβουλους χρήστες να προσπελάσουν τα δεδομένα των χρηστών ή να αποκτήσουν πρόσβαση στην υποδομή χωρίς να έχουν το δικαίωμα. Ταυτόχρονα η χρήση στατικών κλειδιών κάνει δύσκολη τη μεταβολή τους καθώς θα πρέπει να ενημερωθούν όλα τα AccessPoint αλλά και οι συσκευές των χρηστών. Έτσι με δεδομένα κλειδιά για μεγάλο χρονικό διάστημα, αργά ή γρήγορα το σύστημα είναι δυνατό να παραβιαστεί.

Σε πολλές περιπτώσεις η ασφάλεια που προσφέρει το WEP ενισχύεται με τη χρήση του προτύπου 802.1X ή με την υλοποίηση Εικονοκών Ιδιωτικών Δικτύων (VirtualPrivateNetworkVPN) πάνω από το ασύρματο δίκτυο. Ενδιαφέρον παρουσιάζει η περίπτωση του 802.1X. Στο πρωτόκολλο αυτό ο χρήστης διαθέτει το σχετικό λογισμικό στη συσκευή του. Ο χρήστης ζητά από το δίκτυο μέσω του ExtensibleAuthenticationProtocol (EAP) πάνω από το 802.1X να του δοθεί άδεια να συνδεθεί στο δίκτυο. Στην περίπτωση του 802.11, τα σημεία πρόσβασης είναι τα AccessPoint. Τα AccessPoint δεν κρατούν κάποια λίστα με τους χρήστες, αλλά προωθούν την αίτηση σε έναν εξυπηρετητή ταυτοποίησης. Ο εξυπηρετητής αυτός αναζητά στην κατάλληλη βάση δεδομένων τα στοιχεία του χρήστη καθώς και τα δικαιώματα πρόσβασης που αυτός έχει. Ο τρόπος με τον οποίο γίνεται η ταυτοποίηση του χρήστη είναι γενικά επιλογή της κάθε εφαρμογής καθώς το EAP παρέχει τη δυνατότητα ταυτοποίησης μέσω χρήσης ονόματος και συνθηματικού (username/password), πιστοποιητικών (certificates) μέσω ειδικής έξυπνης κάρτας, συσκευής USB ή άλλου αρχείου. Όλη η διαδικασία ταυτοποίησης πραγματοποιείται μέσω κρυπτογραφημένου καναλιού παρέχοντας ασφάλεια στα δεδομένα που ανταλλάσσονται.

Στην περίπτωση που πιστοποιηθεί η δυνατότητα πρόσβασης του χρήστη, ο εξυπηρετητής ταυτοποίησης ενημερώνει το AccessPoint να επιτρέψει τη σύνδεση στο χρήστη. Ταυτόχρονα παρέχει στο AccessPoint και στο τερματικό του χρήστη ένα προσωρινό κλειδί WEP, μέσω του οποίου πραγματοποιείται η κωδικοποίηση του καναλιού επικοινωνίας του χρήστη, παρέχοντας ασφάλεια καθ'όλη τη διάρκεια της σύνδεσης.

- **WAP (Wireless Application Protocol)**

Το WAP (WirelessApplicationProtocol) προσδιορίζει ένα περιβάλλον εφαρμογών και πρωτοκόλλων δικτύου για ασύρματες συσκευές όπως είναι τα κινητά τηλέφωνα, τα PDAs, οι φορητοί υπολογιστές.

Το WAP αποτελεί μια τεχνολογία η οποία παρέχει ένα μηχανισμό για την έκθεση πληροφορίας από το διαδίκτυο σε μια κινητή συσκευή. Αυτό γίνεται μεταφράζοντας την πληροφορία αυτή σε ένα format κατάλληλο για να εμφανίζεται στις οθόνες των κινητών συσκευών. Το WAP αποτελεί ένα ανοικτό standard, που υλοποιήθηκε από το WAPForum, και στα πάνω από 500 μέλη του συμπεριλαμβάνονται μερικές από τις μεγαλύτερες εταιρείες όπως η Nokia, η Ericsson, η Motorola κ.ά.

Το WAP (πρωτόκολλο ασύρματων εφαρμογών) είναι ο «μηχανισμός» που έρχεται να ενώσει το διαδίκτυο με τις ασύρματες συσκευές, ανοίγοντας το δρόμο για το κινητό ηλεκτρονικό εμπόριο. Συγκεκριμένα το WAP περιέχει σε σμίκρυνση ένα πρόγραμμα πλοήγησης στο διαδίκτυο και είναι ενσωματωμένο στις περισσότερες ασύρματες συσκευές (και στα κινητά τηλέφωνα τρίτης γενιάς). Έτσι επιτρέπει σε όλους τους χρήστες να έχουν άμεση πρόσβαση στο διαδίκτυο, κάθε στιγμή, και από οποιοδήποτε σημείο και αν βρίσκονται.

Οι WAP υπηρεσίες που προσφέρονται ποικίλουν από απλή αποστολή μηνυμάτων και διαχείριση κλήσεων, υπηρεσίες ηλεκτρονικού ταχυδρομείου (e-mail), μέχρι συναλλαγές κινητού ηλεκτρονικού εμπορίου και ολοκληρωμένες τραπεζικές υπηρεσίες (mobilebanking).

- ***Συστήματα Κινητών Πληρωμών (m-paymentsystems)***

Λόγω των ιδιαίτερων χαρακτηριστικών των ασύρματων συσκευών και των ασύρματων τηλεπικοινωνιακών δικτύων, τα συστήματα ασύρματων ηλεκτρονικών πληρωμών διαφέρουν από αυτά των παραδοσιακών ηλεκτρονικών πληρωμών. Στη συνέχεια κατηγοριοποιούνται τα συστήματα ασύρματων ηλεκτρονικών πληρωμών σύμφωνα με τον τρόπο που αποθηκεύει χρήματα ο πελάτης:

- Softwareelectroniccoins: ηλεκτρονικό χρήμα αποθηκευμένο σε ασύρματη συσκευή σε μορφή αρχείου.
- Hardwareelectroniccoins: ηλεκτρονικό χρήμα αποθηκευμένο σε ασύρματη συσκευή, σε μια έξυπνη κάρτα.
- Backgroundaccount: ηλεκτρονικό χρήμα αποθηκευμένο σε απομακρυσμένο λογαριασμό μιας έμπιστης τρίτης οντότητας.

Software electronic coins

Στην περίπτωση αυτή, αποθηκεύεται νομισματική αξία σε μια ασύρματη συσκευή και έτσι ο πελάτης έχει πλήρη έλεγχο των χρημάτων του όπου και αν βρίσκεται και ότι και αν κάνει. Ένα ηλεκτρονικό νόμισμα αντιπροσωπεύεται ως ένα αρχείο που περιέχει, μεταξύ άλλων πληροφοριών, την αξία του, τον σειριακό του αριθμό, την περίοδο ισχύος του και την

υπογραφή της εκδότριας τράπεζας. Λόγω του ότι τα software ηλεκτρονικά νομίσματα είναι εύκολο να αντιγραφούν, η εγκυρότητα τους βασίζεται στη μοναδικότητα του σειριακού τους αριθμού. Έτσι όταν ο πελάτης μεταφέρει ηλεκτρονικά νομίσματα στον έμπορα για την αγορά προϊόντων ή υπηρεσιών, ο έμπορας τα προωθεί στην εκδότρια τράπεζα η οποία κάνει έλεγχο μήπως τα νομίσματα αυτά έχουν ξανά ξοδευτεί (doublespendingtest). Σε περίπτωση που τα νομίσματα έχουν ξανά ξοδευτεί, απορρίπτονται. Αλλιώς, εισάγεται ο σειριακός αριθμός των νομισμάτων στη βάση δεδομένων ελέγχου της τράπεζας και τα χρήματα πιστώνονται στον λογαριασμό του έμπορα.

Η παραγωγή και αποθήκευση ηλεκτρονικών νομισμάτων παρουσιάζει ένα πρόβλημα. Λόγω των περιορισμένων δυνατοτήτων των ασύρματων συσκευών, τα ηλεκτρονικά νομίσματα πρέπει να παραχθούν και να αποθηκευτούν εξωτερικά και στη συνέχεια να μεταφορτωθούν στην ασύρματη συσκευή. Μια λύση είναι να γίνει η παραγωγή και αποθήκευση των νομισμάτων σε κάποιο ηλεκτρονικό υπολογιστή (homePC), και όταν χρειαστεί να γίνει η μεταφόρτωση τους στην ασύρματη συσκευή.

Hardware electronic coins

Στην περίπτωση αυτή, αποθηκεύεται νομισματική αξία σε μια έξυπνη κάρτα, που είναι τοποθετημένη στην ασύρματη συσκευή. Εδώ τα ηλεκτρονικά νομίσματα είναι αποθηκευμένα με ασφάλεια στη έξυπνη κάρτα και για το λόγο αυτό αντιπροσωπεύονται σαν ένας απλός αριθμητικός μετρητής. Προκειμένου να γίνει η πληρωμή, η έξυπνη κάρτα του πελάτη και ο εξυπηρετητής πληρωμής του έμπορα, αυθεντικοποιούν ο ένας τον άλλο και δημιουργούν ένα ασφαλές κανάλι μεταξύ τους. Τότε τα ηλεκτρονικά χρήματα μπορούν να μεταφερθούν από τον πελάτη στον έμπορα με ασφάλεια.

Background account

Στην περίπτωση αυτή τα χρήματα αποθηκεύονται σε έναν απομακρυσμένο λογαριασμό μιας έμπιστης τρίτης οντότητας. Ανάλογα με το συγκεκριμένο σύστημα πληρωμής, ο λογαριασμός μπορεί να είναι λογαριασμός πιστωτικής κάρτας ή τραπεζικός λογαριασμός. Για να γίνει η πληρωμή, πρώτα ο πελάτης στέλνει μηνύματα αυθεντικοποίησης και εξουσιοδότησης στον έμπορα, μέσω των οποίων η έμπιστη τρίτη οντότητα προσδιορίζει τον πελάτη και ελέγχει την έγκριση πληρωμής. Αν όλα πάνε καλά, αφαιρείται από τον λογαριασμό του πελάτη το συγκεκριμένο ποσό πληρωμής και πιστώνεται στο λογαριασμό του έμπορα.

Υπάρχουν πολυάριθμα συστήματα πληρωμής που ανήκουν σε αυτή την κατηγορία. Διαφέρουν μεταξύ τους ως προς φύση της έμπιστης τρίτης οντότητας και τη λειτουργία κατά την οποία στέλνονται τα μηνύματα αυθεντικοποίησης και εξουσιοδότησης. Για παράδειγμα, σε κάποιες περιπτώσεις τα δεδομένα αυτά στέλνονται καθαρά στον αέρα (π.χ. εξουσιοδότηση πιστωτικής κάρτας), χωρίς να παρέχουν οποιαδήποτε ασφάλεια ενάντια στους ωτακουστές. Σε άλλες περιπτώσεις οι πληροφορίες αυτές κρυπτογραφούνται και υπογράφονται ψηφιακά, παρέχοντας έτσι ασφάλεια, εμπιστευτικότητα και ανωνυμία του

πελάτη.

-
-
-
-
-
-
- **Πηγές**

1. Νίκος Κύρλογλου, “Σύντομος Οδηγός για το Ηλεκτρονικό Εμπόριο.
2. ΤΜΗΥΠ – Πανεπιστήμιο Πατρών, “Κεφάλαιο 1 – e-Επιχειρείν και e-Εμπόριο”.
3. Παναγιώτης Κυριακούλια, “Ηλεκτρονικό Εμπόριο και Απασχόληση: Δυνατότητες και Προοπτικές”.
4. Χρήστος Ι. Μπούρος, “Ηλεκτρονικό Εμπόριο”, Πανεπιστήμιο Πατρών, Τμήμα Μηχανικών Η/Υ και Πληροφορικής.
5. Βογιατζής Σωτήριος, “Πράκτορες Λογισμικού και Ηλεκτρονικό Εμπόριο”.
6. Καρέλη – Μανώλη – Μεσογείτη, “Ηλεκτρονικό Εμπόριο και Απασχόληση”.
7. Strategic International SA, “Μύθοι & Πραγματικότητα για το e-Commerce στην Ελλάδα”, June 2001.
8. Ομάδα Εργασίας Δ1 του ebusinessforum, “Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα - Αλληλεπίδραση και προοπτικές”, Ιούνιος 2003.
9. Ομάδα Εργασίας Δ1 του ebusinessforum, “Ενδεικτικός Κατάλογος Νομοθεσίας για τις Ηλεκτρονικές Συναλλαγές”, Μάιος 2003.
10. Ομάδα Εργασίας Ε2 του ebusinessforum, “Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης (Τεχνική & Νομική Προσέγγιση)”, Μάρτιος 2004.
11. Dumortier, Kelm, Nilsson, Skouma, Van Eecke, “The legal and market aspects of electronic signatures”, Study for the European Commission.
12. Αλέξανδρος Χαρίτση, “Ασφάλεια Δικτύων και Δεδομένων και Συνεπαγόμενο Κόστος”, Ιούλιος 2003.
13. Χαράλαμπος Λιναρδάκης, “Η Επίδραση της Νομοθεσίας στο Ηλεκτρονικό Εμπόριο
14. Χάρης Μανιφάβας,Σημειώσεις από το μάθημα Άσφαλεια Πληροφοριακών Συστημάτων’’,Τμήμα Εφ. Πληροφορικής και Πολυμέσων,ΤΕΙ Κρήτης 2008-2009
15. Θόδωρος Κ. Πανάγου, “E-Commerce”, Ιανουάριος 2004.
16. Δρ. Κωνσταντίνος Αντωνής, “Προστασία Επικοινωνιών - SSL”, 2003.
17. Δρ. Χρήστος Κ. Γεωργιάδης, “Προβλήματα Ασφάλειας στο Ηλκετρονικό Εμπόριο”, Ε-Επιχειρείν – Πανεπιστήμιο Θεσσαλίας.
18. Γκάδολος Ιωάννης, “Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών”, 1998.
19. Τζούραλη – Κολοκοτρώνης, “ Ασφαλής Διαδικτυακή Διακίνηση”.
20. Panko, “Corporate Computer and Network Security”, 2004.
21. David Wagner - Bruce Schneier “Analysis of the SSL 3.0 protocol”, 1997.
22. Jon Edney – William A. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i”.
23. Μάγκος Εμμανουήλ, “ Ασφάλεια στο WorldWideWeb”, 1997.
24. Βώρος Άγγελος, Γαροφαλάκης Γιάννης, Δεστούνης Παναγιώτης, Κάππος

Παναγιώτης, Σακκόπουλος Ευάγγελος, Τζήμας Γιάννης, “Τεχνολογίες Διαδικτύου”, Πανεπιστήμιο Πατρών, Σεπτέμβριος 2002.
25. Ομάδα Εργασίας Στ-3 του ebusinessforum, “Εμπιστοσύνη και Ασφάλεια σε ένα κινητό και γρήγορο δικτυακό περιβάλλον”, Αύγουστος 2004.
26. Μαρία Μπένου, Βικτωρία Σκουλαρίδου, Διομήδης Σπινέλλης, “Οδηγός Ασφαλούς Πλοήγησης στο Διαδίκτυο”, Οικονομικό Πανεπιστήμιο Αθηνών.
27. Δριμάλας Θεόδωρος, “Ασφάλεια Ιδιωτικού Δικτύου”, ΤΕΙ Πειραιά, Δεκέμβριος 2002.
28. Δρ. Πόνης Τ. Σταύρος, “Υποδομή Ηλεκτρονικού Εμπορίου”, Αθήνα 2005.
29. ΓεώργιοςΛεοντιάδης, “E – CommerceSETSecureElectronicTransaction”, Εθνικό
30. Ομάδα Εργασίας 2 (Α’ Κύκλου) του ebusiness forum, “Επιχειρησιακή Δικτύωση και Ηλεκτρονικό Εμπόριο”, Ιούλιος 2001.
31. Ded Shinder, “Protect your Web Servers with SSL”, November 2005.
32. Δημήτριος Βογιατζής, “Εισαγωγή στο Διαδίκτυο”, 2004.
33. Γιώργος Κουτέπας, “Ασφάλεια και Διαχείριση Δικτύων”, Δεκέμβριος 2005.
34. Tom Syroid, “Web Server Security”.
35. Yona Hollander, “The Future of Web Server Security, Why your Web site is still vulnerable to attack”.
36. Indian Computer Emergency Response Team, “Web Server Security Guidelines”, August 2004.
37. Steven M. Bellovin, “Web Servers and Security”, October 2005.
38. Θόδωρος Κομνηνός, Παύλος Σπυράκης, “Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων” Εκδόσεις Ελληνικά Γράμματα.
39. Στέφανος Γκρίτζαλη, Σωκράτης Κ. Κάτσικα, Δημήτρης Γκρίτζαλη, “Ασφάλεια Δικτύων Υπολογιστών, Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης” Έκδόσεις Παπασωτηρίου.
40. Πομπόρτσης Ανδρέας – Παπαδημητρίου Γεώργιος, “Ασφάλεια Δικτύων Υπολογιστών”, Εκδόσεις Τζιόλα.
41. Ανδρέα Σουρής – Δημήτρης Πατσός – Νίκος Γρηγοριάδης, “Ασφάλεια της Πληροφορίας”, Εκδόσεις Νέων Τεχνολογιών.
42. LincolnD. Stein, Επιμέλεια Δ. Γκαρμπολάς, “Ασφάλεια Δικτύων Web: Ένας Βήμα Μάγκος Εμμανουήλ, “Ασφάλεια Υπολογιστών και Προστασία Δεδομένων”, Ιόνιο Πανεπιστήμιο, 2006.
43. Σταύρος Κ. Λαδάς, “Κατασκευή ενός προσωπικού χαμηλού κόστους Firewall”, Πανεπιστήμιο Μακεδονίας.
44. Steven M. Bellovin, “Distributed Firewalls”, November 1999.
45. Marcus J. Ranum, “Thinking About Firewalls”, Trusted Information Systems, Inc. Glenwood, Maryland.
46. Terry Gray, “Firewalls: Friend or Foe?”, February 2003.
47. David W Chadwick, “Network Firewall Technologies”, IS Institute, University of Karl Forster, “Why Firewalls Fail to Protect Web Sites”, Lockstep Systems, Inc.
48. Nelly Delessy-Gassant, Eduardo B. Fernandez, Saeed Rajput, and Maria M. Larrondo-Petrie, “Patterns for Application Firewalls”, Florida Atlantic University.
49. Laurent Constantin, “Firewalls”, March 1999.
50. Mark-Anthony Takla, “Firewalls”, Spring 2004.
51. Αν. Καθ. Π. Γεωργιάδης, “Ασφάλεια Υπολογιστικών Συστημάτων”, Φερβουάριος 2005.
52. Παναγιώτης Γεωργαντάς, “Ασφάλεια Διαδικτυακών Υπηρεσιών”, Εθνικό Μετσόβιο Πολυτεχνείο.
53. Τσακαλίδης, Συρμακέσης, Μαρκέλλου, Ρήγκου, Μαρκέλλος, Ψαράς, Κολοκούρη,

"Ε - Επιχειρείν", Πανεπιστήμιο Πατρών, 2002.
54. Βασιλική Στρακαντούνα, "Επεξεργασία Προσωπικών Δεδομένων και Προστασία της Κωνσταντίνος Α. Παπανικήτα, "Επισκόπηση μεθόδων προστασίας και ανίχνευσης εισβολών σε κατανεμημένα συστήματα ασύρματων επικοινωνιών", Εθνικό Μετσόβιο Πολυτεχνείο, Σεπτέμβριος 2005.
55. Καθ. Παύλος Σπυράκης, "Αναχαιτίστε τους εισβολείς", Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών.
56. Admin, "Intrusion Detection Systems", February 2005.
57. Ricky M. Magalhaes, "Host-Based IDS vs Network-Based IDS", July 2004.
58. Robert J. Shimonski, "What You Need to Know About Intrusion Detection Systems", November 2002.
59. Ομάδα Εργασίας Ε-3 του ebusinessforum, "Ηλεκτρονικές Πληρωμές: Προβλήματα και Προοπτικές", Ιανουάριος 2004.
60. Βέρρη Ανδρονίκη, Γώγογλου Αικατερίνη, Μάρκος Άγγελος, "Ηλεκτρονικό Χρήμα, Ηλεκτρονικές Συναλλαγές, Ηλεκτρονικό Πορτοφόλι, Έξυπνες Κάρτες, W3C", Πανεπιστήμιο Μακεδονίας, 2002.
61. Knud Böhle, "Integration of Electronic Payment Systemsinto B2C Internet-Commerce– Problems and Perspectives", April 2002.
62. Thomi Pilioura, "Electronic Payment Systems on Open Computer Networks: A Survey".
63. Ed Mayo, "Consumers, Digital Cash and Electronic Payment", March 2004.
64. Robert Chesnut, "The e-Commerce Safety Guide".
65. S.W. Smith, "WebALPS: A Survey of E-Commerce Privacy and Security Applications". Cynthia Ruppel, Linda Underwood-Queen, Susan J. Harrington, "E-commerce: The Roles of Trust, Security, and Type of Ecommerce Involvement".
66. Κωνσταντίνος Μαργαρίτης, "Εισαγωγή στο Ηλεκτρονικό Εμπόριο και τις Κατανεμημένες Εφαρμογές", Σεπτέβριος 2004.
67. Κωνσταντινίδου Αλένα, "Ηλεκτρονικό Εμπόριο", Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα, Τμήμα Πληροφορικής.
68. Ανδρέου Πέτρος, Πέππα Ηλέκτρα, Παπακωνσταντίνου Κωνσταντίνα, "Ηλεκτρονικό Εμπόριο (e-commerce)", Πανεπιστήμιο Αιγαίου, 2002.
69. Ομάδα Εργασίας Α-3 του ebusinessforum, "Η Υποδομή για την Ηλεκτρονική Επιχείρηση και τις Ηλεκτρονικές Αγορές", Ιούλιος 2001.
70. Κωνσταντίνος Α. Κωτσοκάλης, "Συντονισμός Εργασιών για Διεκπεραίωση Μετσόβιο Πολυτεχνείο, Ιούνιος 2005.
71. Σανίνας Κωνσταντίνος, "Ιδιωτική και Ανώνυμη Αυθεντικοποίηση Χρήστη σε Κινητά Δίκτυα", Φεβρουάριος 2004.
72. Σωκράτης Κ. Κάτσικας, "Ο ρόλος της Υποδομής Δημόσιου Κλειδιού στην ανάπτυξη ηλεκτρονικών αγορών", Πανεπιστήμιο Αιγαίου.
73. Δημήτρης Π. Λέκκα, "Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας: Λειτουργικά, Αρχιτεκτονικά και Οργανωτικά ζητήματα", Πανεπιστήμιο Αιγαίου, Ιανουάριος 2002.
74. Εθνική Επιτροπή Τηλεπικοινωνιών και ταχυδρομείων (ΕΕΤΤ),Ψηφιακές Υπογραφές
75. Ομάδα Εργασίας Γ3 του ebusinessforum, "Έξυπνες Κάρτες", Οκτώβριος 2002.
76. Νίκος Κύρλογλου, "Ασύρματες Έξυπνες Κάρτες μιας Χρήσης", Απρίλιος 2003.
77. Πιτυρίγκας Ευριπίδης, "Ανάπτυξη Εφαρμογής Μηχανογράφησης Οφθαλμιατρείου Με Ζιάκα Ευαγγελία – Μπασιούκα Αθηνά, "SmartCarts", Τμήμα Μηχανικών Η/Υ Τηλεπικοινωνιών και Δικτύων.
78. Ομάδα Εργασίας ΟΕ Ε4 του ebusinessforum, "Κινητές και Ασύρματες Εφαρμογές

στις Μεταφορές και στην Εφοδιαστική", Ιανουάριος 2004.
79. Ομάδα 17 Κρητικάκου Βασιλική, Κρασοπούλου Παναγιώτα, Παρδάλη Βασιλική, και Ομάδα 24 Μήλεση Θεοδώρα, Σταυρουλάκη Μαρία, Ταλάντη Ιωάννα, "Κινητό Ηλεκτρονικό Επιχειρείν", Ιανουάριος 2003.
80. Ομάδα Εργασίας OB5 του ebusinessforum, "Κινητό Ηλεκτρονικό Εμπόριο", Ιούλιος 2002.
81. Μπάσιος Χρήστος, "Mobile Payment: Βασικές αρχές και εφαρμογές", Εθνικό Μετσόβιο Πολυτεχνείο, Ιούλιος 2004.
82. Κοτσομύτη Αγγελική - Μάρκου Ρέα - Πετράκη Ελένη, "Στρατηγική στο χώρο του Κινητού Ηλεκτρονικού Επιχειρείν", Οικονομικό Πανεπιστήμιο Αθηνών.
83. Dominik Haneberg, Alexander Kreibich, Wolfgang Reif, Kurt Stenzel, " Design for Trust: Security in M-Commerce".
84. Suresh Chari, Parviz Kermani, Sean Smith, and Leandros Tassiulas, "Security Issues in M-Commerce: A Usage-Based Taxonomy".
85. Λάζαρος Μεράκος, "Δίκτυα Κινητών Επικοινωνιών, Σύγχρονες Τάσεις", Τμήμα Πληροφορικής & Τηλεπικοινωνιών, Πανεπιστήμιο Αθηνών, Οκτώβριος 2004.
86. Scarlet Schwiderski-Grosche, Heiko Knospe, "Secure M-Commerce".
87. Ηλίας Τσουμελέας, "Ασφάλεια Τηλεπικοινωνιών", Εθνικό Μετσόβιο Πολυτεχνείο, Δήμητρα Χ. Σκούτα, "Κινητό Ηλεκτρονικό Επιχειρείν, M-Commerce", Εθνικό Μετσόβιο Πολυτεχνείο, Σεμπτέβριος 2004.
88. Blerim Rexha, Siemens AG, "Increasing User Privacy in Online Transactions with X.509 v3 Certificate Private Extensions and Smartcards", Seventh IEEE International Conference on E-Commerce Technology (CEC'05).
89. Seokwon Yang, Stanley Y. W. Su, Herman Lam, "A Non-Repudiation Message Transfer Protocol for E-commerce", 2003 IEEE International Conference on E-Commerce Technology (CEC'03).
90. Βικιπαίδεια,Κρυπτογραφία,Συμμετρική και Ασύμετρη κρυπτογράφηση,SSL
91. Λουκία Ι. Τζιοβάνη,Ασφάλεια στο ηλεκτρονικό εμπόριο, Εθνικό Μετσόβιο Πολυτεχνείο
92.
93. N. Ferguson; B. Schneier (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.
94. J. Katz; Y. Lindell (2007). Introduction to Modern Cryptography. CRC Press. ISBN 1-58488-551-3.
95. A. J. Menezes; P. C. van Oorschot; S. A. Vanstone (1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7.
96. IEEE 1363: Standard Specifications for Public-Key Cryptography
97. Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.
98. Σημειώσεις
99. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών,ΑΔΑΕ
100.