Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Μεσολογγίου

Σχολή Διοίκησης και Οικονομίας

Τμήμα Εφαρμογών Πληροφορικής στην Διοίκηση και Οικονομία

Πτυχιακή Εργασία

Θέμα:

Ασφάλεια στο Ηλεκτρονικό Εμπόριο και Προστασία Προσωπικών Δεδομένων

Επιβλέπων

Γαλάνη Ελένη

Σπουδαστής

Θαλασσινός Κωνσταντίνος
Α.Μ.: 10758

Μεσολόγγι 2006

Υπεύθυνη Δήλωση : Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος εφαρμογών πληροφορικής στην διοίκηση και οικονομία.

Πρόλογος

Το internet (διαδίκτυο) αποτελεί σήμερα τη μεγαλύτερη πηγή πληροφοριών παγκοσμίως και η οποία εξελίσσεται με ταχύτατους ρυθμούς. Τα άτομα που κάνουν χρήση της υπηρεσίας του internet είναι εκατομμύρια ενώ μέρα, με τη μέρα ο αριθμός αυτός αυξάνεται ραγδαία καθώς όλο και περισσότεροι εκφράζουν την επιθυμία τους για εισαγωγή στο χώρο του διαδικτύου.

Το παραπάνω αποτελεί παράγοντα προσέλκυσης για εταιρείες και επιχειρήσεις οι οποίες είτε θέλουν να διαφημίσουν τα προϊόντα τους είτε να δημιουργήσουν ένα ηλεκτρονικό κατάστημα για την πώλησή τους. Από την άλλη μεριά όμως υπάρχουν κάποιοι οι οποίοι επιθυμούν να υποκλέψουν τις επικοινωνίες που πραγματοποιούνται μεταξύ δύο συναλλασσόμενων του ηλεκτρονικού εμπορίου με απώτερο σκοπό την αποκομιδή στοιχείων (προσωπικά δεδομένα ή/και αριθμούς πιστωτικών καρτών) τέτοιων τα οποία θα πουλήσουν ή θα χρησιμοποιήσουν οι ίδιοι με σκοπό τα οικονομικά οφέλη.

Βασικός στόχος της παρούσας εργασίας είναι η αποτύπωση των συνθηκών που επικρατούν σήμερα στον ευαίσθητο τομέα της ασφάλειας του ηλεκτρονικού εμπορίου και της προστασίας των προσωπικών δεδομένων των ατόμων που κάνουν χρήση του.

Στην εισαγωγή αναφέρονται κάποια στοιχεία για το ηλεκτρονικό εμπόριο και μερικές από τις δραστηριότητες που περιλαμβάνει. Στο πρώτο κεφάλαιο, εξετάζεται η έννοια του ηλεκτρονικού εμπορίου, τα είδη και τους τύπους των προϊόντων που περιλαμβάνει καθώς και τα πλεονεκτήματα και μειονεκτήματα, ενώ κλείνει με την παρουσίαση των στόχων της ασφάλειας. Στο δεύτερο κεφάλαιο, παρουσιάζονται τα συστήματα ηλεκτρονικών πληρωμών και στο τέταρτο οι απαιτήσεις ασφάλειας. Αναφορά στην πολιτική ασφάλειας των πληροφοριακών συστημάτων γίνεται στο κεφάλαιο πέντε και ακολουθεί το κεφάλαιο έξι που ασχολείται με την επιστήμη της κρυπτογραφίας και το πώς μπορεί να χρησιμοποιηθεί για την προστασία των συναλλαγών μας. Τα είδη της κρυπτογραφίας, οι αλγόριθμοι που χρησιμοποιούνται καθώς οι απειλές που δέχεται περιλαμβάνονται στο κεφάλαιο αυτό. Ακόμα οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά στο ίδιο κεφάλαιο αποτελούν τρόπους απόδειξης ότι το άτομο που στέλνει τις πληροφορίες είναι αυτό που υποστηρίζει πως είναι. Τα πρωτόκολλα ασφαλής επικοινωνίας στο internet τα οποία συναντάμε στο κεφάλαιο οχτώ αποτελούν μερικούς ακόμα τρόπους προστασίας κατά τη διάρκεια των ηλεκτρονικών μας συναλλαγών. Στο έβδομο κεφάλαιο η παρουσίαση των αρχείων cookies είναι σημαντική καθώς αποτελούν τρόπο παραβίασης της ιδιωτικής μας ασφάλειας. Στο όγδοο κεφάλαιο η χρήση των μέσων προστασίας που ονομάζονται firewalls είναι μία καλή λύση για την προστασία των πληροφοριών που διέρχονται από και προς ένα δίκτυο. Το ένατο κεφάλαιο αναφέρεται στην έννοια των προσωπικών δεδομένων και στις ενέργειες που έχουν γίνει σε διεθνή, ευρωπαϊκό και ελληνικό νομοθετικό πλαίσιο για την προστασία τους. Στο τελευταίο κεφάλαιο γίνεται μελέτη της περίπτωσης ενός ηλεκτρονικού καταστήματος και στο αν πληρεί τις προϋποθέσεις ασφάλειας και προστασίας προσωπικών δεδομένων τοων πελατών της.

Περιεχόμενα

1 Εισαγωγή

Το internet εισβάλλει με τον καιρό όλο και περισσότερο σε διάφορους τομείς της ζωής μας. Ένας από αυτούς είναι και η οικονομία.

Η ανάγκη για Ηλεκτρονικό Εμπόριο προκύπτει από την απαίτηση των επιχειρήσεων και των κυβερνήσεων για καλύτερη χρήση της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών ώστε να βελτιωθούν οι σχέσεις αμφίδρομης επικοινωνίας με τους πελάτες/πολίτες/καταναλωτές, οι επιχειρηματικές διεργασίες και η ανταλλαγή πληροφοριών ενδο-επιχειρησιακά, αλλά και κυρίως μεταξύ των επιχειρήσεων.

Καθώς οι επιχειρηματικές δραστηριότητες που πραγματοποιούνται στον παγκόσμιο ιστό αυξάνονται, η ποσότητα των αγαθών, των υπηρεσιών και των πληροφοριών που ανταλλάσσονται φαίνεται πως διπλασιάζεται ή τριπλασιάζεται χρόνο με το χρόνο. Παρατηρείται ότι ακόμα και παραδοσιακές επιχειρήσεις προσπαθώντας να μη μείνουν πίσω στις εξελίξεις εισέρχονται στον εικονικό κόσμο του ηλεκτρονικού εμπορίου, έστω και με κάποια καθυστέρηση

Ο τρόπος αυτός εμπορίου συμβαδίζει με την εποχή και την ανάπτυξη της τεχνολογίας. Οι εταιρείες έχουν απλώσει τα δίχτυα τους και βομβαρδίζουν με διαφημίσεις, ανακαλύπτουν ευκολότερους, χρησιμότερους τρόπους συναλλαγών προς όφελός τους αλλά και προς όφελος των ηλεκτρονικών αγοραστών, πωλητών, ανθρώπων που το ηλεκτρονικό εμπόριο έγινε κομμάτι της ζωής τους.

Η εποχή, που κάποιος έπρεπε να πάει σε μια τράπεζα στις κανονικές εργάσιμες ώρες περιμένοντας στην ουρά για μια απλή κατάθεση ή για ένα δάνειο τείνει σιγά σιγά να εξαλειφθεί. Τώρα ο ηλεκτρονικός έλεγχος των τραπεζικών λογαριασμών, οι πληρωμές, η μεταφορά κεφαλαίων και άλλα πολλά γίνονται γρήγορα, εύκολα και άνετα μέσο του διαδικτύου.

Σύμφωνα με όλες τις ενδείξεις το ηλεκτρονικό εμπόριο θα συνεχίσει να αναπτύσσεται και, συνεπώς, πολλοί οργανισμοί θα αναγκαστούν, είτε να δικτυωθούν, είτε να κλείσουν.

Το Ηλεκτρονικό Εμπόριο προσφέρει τη δυνατότητα εκτέλεσης πράξεων για την ανταλλαγή προϊόντων ή υπηρεσιών μεταξύ δύο ή περισσότερων μερών με χρήση ηλεκτρονικών υπολογιστών και δικτύων υπολογιστών. Βασίζεται στην ηλεκτρονική επεξεργασία και μετάδοση δεδομένων, ήχου και εικόνων βίντεο. Η έννοια του ηλεκτρονικού εμπορίου περιλαμβάνει πολλές διαφορετικές δραστηριότητες όπως:

- ηλεκτρονική εμπορία αγαθών και υπηρεσιών,
- παράδοση ψηφιακού περιεχομένου (άϋλων αγαθών),
- ηλεκτρονική αγοραπωλησία μετοχών,
- ηλεκτρονική έκδοση φορτωτικών,
- εμπορικές δημοπρασίες,
- συλλογικές εργασίες σχεδίασης και τεχνικών μελετών,
- ενημέρωση από πηγές σε απευθείας σύνδεση,
- πωλήσεις απευθείας στον καταναλωτή και μεταγοραστική εξυπηρέτηση.

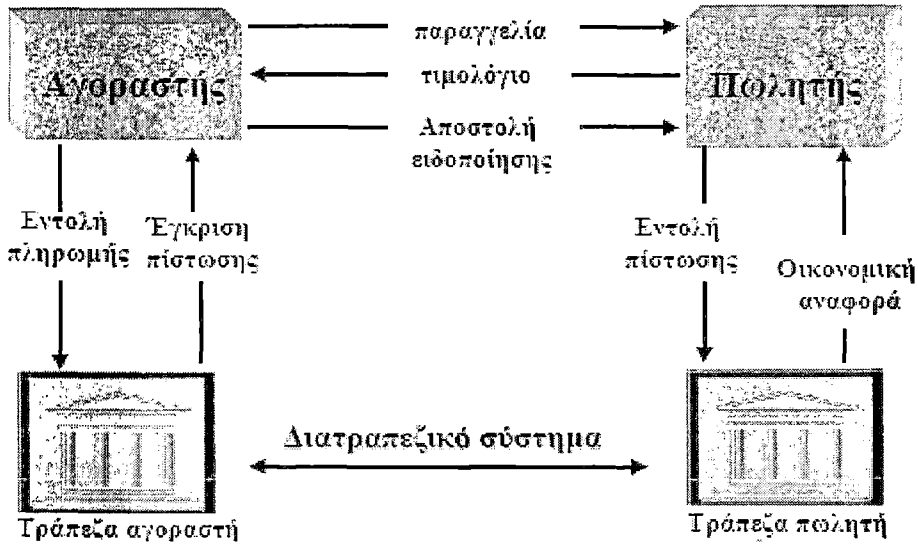
1.1 Τι είναι το ηλεκτρονικό εμπόριο

Ένας ορισμός του ηλεκτρονικού εμπορίου θα μπορούσε να εκφραστεί ως η χρήση των τηλεπικοινωνιακών μέσων για κάθε είδους εμπορικές συναλλαγές ή επιχειρηματικές δραστηριότητες μεταξύ επιχειρήσεων και ιδιωτών. Απλούστερα θα μπορούσαμε να πούμε ότι το ηλεκτρονικό εμπόριο είναι η πραγματοποίηση εμπορικών συναλλαγών μέσο δικτύου υπολογιστών.

Οι τεχνολογίες που χρησιμοποιούνται για την εφαρμογή του ηλεκτρονικού εμπορίου είναι η ηλεκτρονική ανταλλαγή δεδομένων (EDI), η ηλεκτρονική μεταφορά κεφαλαίων (EFT), το ηλεκτρονικό ταχυδρομείο (e-mail).

Συγκεκριμένα, η τεχνολογία EDI (Electronic Data Interchange) ή Ηλεκτρονική Μεταβίβαση Δεδομένων είναι μια τεχνολογία που επιτρέπει στις επιχειρήσεις να ανταλλάσσουν τα εμπορικά τους έγγραφα/ παραστατικά με ηλεκτρονικό τρόπο. Πιο απλά, το EDI είναι η διαδικασία ή μέθοδος της πραγματοποίησης συναλλαγών μεταξύ επιχειρήσεων, όπου τα δεδομένα της συναλλαγής περνούν από τον υπολογιστή της μίας επιχείρησης στον υπολογιστή της άλλης, χωρίς να χρειάζεται ανθρώπινη παρέμβαση για την ερμηνεία ή την αντιγραφή των στοιχείων αυτών. Για να υλοποιηθεί η αυτόματη αυτή μεταφορά, οι πληροφορίες θα πρέπει να είναι δομημένες σύμφωνα με προκαθορισμένη μορφή και κανόνες έτσι ώστε ο υπολογιστής να μπορεί να τις «μεταφράσει» στο μορφότυπο (format) των ενδοεπιχειρησιακών εφαρμογών για να ενημερώσει έτσι τα αρχεία ή τις βάσεις δεδομένων της συγκεκριμένης επιχείρησης.

Το σχήμα απεικονίζει την λειτουργία του συστήματος EDI



1.2 Επιχειρηματικές δραστηριότητες ηλεκτρονικού εμπορίου

Οι βασικότερες επιχειρηματικές διαδικασίες που εφαρμόζονται σήμερα στα πλαίσια της εμπορικής διαδικασίας περιλαμβάνουν:

- Προώθηση προϊόντος (marketing). Το marketing περιλαμβάνει μια σειρά από δραστηριότητες τόσο από την πλευρά του πωλητή προϊόντων και υπηρεσιών (π.χ. έρευνα αγοράς, σχεδιασμός προϊόντος, προώθηση και διαφήμιση προϊόντος κ.λ.π.) όσο και από την πλευρά του πιθανού αγοραστή (π.χ. επιλογή κατάλληλου προϊόντος, συλλογή πληροφοριών, επιλογή βέλτιστης προσφοράς κ.λ.π.).

- Επιβεβαίωση συνεργασίας (contracting). Για τη διεκπεραίωση αυτής της διαδικασίας απαιτούνται:

- από την πλευρά του αγοραστή, η συλλογή των προδιαγραφών του προϊόντος καθώς και άλλων όρων που σχετίζονται με τη συνεργασία με προμηθευτές (π.χ. μεταφοράς, παράδοσης και πληρωμής) και

- από την πλευρά του πωλητή, η διαπραγμάτευση για τους όρους συνεργασίας, η επεξεργασία των παραγγελιών σύμφωνα με τους συμφωνηθέντες όρους συνεργασίας κ.λ.π.

- Διαχείριση αποθεμάτων (logistics). Εδώ περιλαμβάνονται όλες οι λειτουργίες που στοχεύουν στη διάθεση των παραγγελθέντων προϊόντων στον αγοραστή σύμφωνα με τους όρους συνεργασίας. Λειτουργίες που περιλαμβάνονται στα πλαίσια αυτά αφορούν τη ζήτηση προϊόντων, τη μεταφορά, την υποδοχή και κατηγοριοποίηση των προϊόντων στην αποθήκη κ.λ.π.

- Διακανονισμός (settlement). Στη διαδικασία αυτή περιλαμβάνεται η τιμολόγηση προϊόντων και υπηρεσιών και η πληρωμή τους. Δεν πρόκειται απλώς για οικονομικό διακανονισμό αλλά για γενικότερο διακανονισμό των όρων συνεργασίας και εμπορικών εταίρων (π.χ. μπορεί να μη συντελείται μία απλή πληρωμή τιμολογίων αλλά και ο αμοιβαίος συμβιβασμός τους).

- Επικοινωνία με Δημόσιους Φορείς (interfacing with administration). Όλα τα μέρη που συμμετέχουν στα πλαίσια του διεθνούς επιχειρηματικού περιβάλλοντος πρέπει σε κάποια σημεία του εμπορικού κύκλου να έρθουν σε επαφή με δημόσιους φορείς, για διάφορους λόγους (π.χ. διεκπεραίωση εισαγωγών / εξαγωγών, εξόφληση φόρων κ.λ.π.)

1.3 Είδη ηλεκτρονικού εμπορίου

Ο βασικός διαχωρισμός σε κατηγορίες του ηλεκτρονικού εμπορίου, γίνεται με κριτήριο τις οντότητες που εμπλέκονται σε μια ηλεκτρονική συναλλαγή.

1.3.1 Ηλεκτρονικό εμπόριο από επιχειρήσεις προς καταναλωτές (Business-to-Consumer e-Commerce -B2C)

Η κατηγορία αυτή περιλαμβάνει κάθε είδος ηλεκτρονικής αγοράς στην οποία αλληλεπιδρά ένας οποιοσδήποτε καταναλωτής με μια εταιρία.
Έτσι έχει αναπτυχθεί μια ατελείωτη σειρά εφαρμογών που περιλαμβάνει μεταξύ άλλων και τα ακόλουθα:

υποστήριξη πελατών,
ηλεκτρονική δημοσιογραφία (εφημερίδες, περιοδικά),
ηλεκτρονική διανομή προϊόντων (π.χ. πληροφορίες, εφημερίδες, μουσική),
διαφήμιση,
ηλεκτρονικά καταστήματα - ηλεκτρονικές αγορές,
ηλεκτρονικές πληρωμές,
ηλεκτρονικές τράπεζες κ.α.

Οι επιχειρήσεις παρέχουν στους καταναλωτές online αγορές μέσα από το Internet, επιτρέποντας τους να αγοράζουν και να πληρώνουν τους λογαριασμούς τους online. Έτσι ο κάθε καταναλωτής μπορεί να παραγγέλνει πράγματα και να τα παραλαμβάνει στο σπίτι του, χωρίς να χρειαστεί πάει κάπου για να τα αγοράσει και για να τα πληρώσει. Αυτός ο τρόπος γλιτώνει χρόνο και από τους δύο συνναλασσόμενους.

1.3.2 Ηλεκτρονικό εμπόριο από καταναλωτές/πολίτες προς κυβερνητικούς φορείς (Consumer/Citizen-to-Government e-Commerce -C2G)

Η κατηγορία αυτή περιλαμβάνει κάθε είδους αλληλεπίδραση μεταξύ ενός πολίτη και της κυβέρνησης, όπως φόροι κ.α. και η οποία αρχίζει να διευρύνεται και να κάνει πιο εύκολη τη ζωή των πολιτών, οι οποίοι έχαναν πολλές ώρες από τη ζωή τους περιμένοντας στις ουρές για να εξυπηρετηθούν.

Ανάμεσα στις πολλές υπηρεσίες που παρέχονται από τις κυβερνήσεις, πολλές από αυτές μπορούν να γίνουν μέσα από τα ηλεκτρονικά μέσα. Το να παρέχεις δημόσιες υπηρεσίες ηλεκτρονικά, όχι μόνο γλιτώνει τους πολίτες από το χάσιμο του χρόνου και τους παρέχει υψηλής ποιότητας υπηρεσίες, αλλά είναι και πιο αποδοτικό και αποτελεσματικό όσον αφορά το κόστος. Αυτές οι υπηρεσίες περιλαμβάνουν την πληρωμή των κυβερνητικών λογαριασμών, την απόδοση της επιστροφής φόρου, καταγραφή ψήφων, ανανέωση των διπλωμάτων οδήγησης, αλλαγή της προσωπικής διεύθυνσης κ.τ.λ.

1.3.3 Ηλεκτρονικό εμπόριο από επιχειρήσεις προς κυβερνητικούς φορείς (Business-to-Government e-Commerce - B2G)

Η κατηγορία αυτή καλύπτει κάθε είδος ηλεκτρονικής συναλλαγής μεταξύ κυβέρνησης και επιχειρήσεων, όπως π.χ. ηλεκτρονική ανακοίνωση προκηρύξεων. Αυτή η κατηγορία αναπτύσσεται σταδιακά και στο μέλλον προβλέπεται να δοθεί μεγαλύτερη βαρύτητα στις ηλεκτρονικές συναλλαγές των κυβερνήσεων με τις επιχειρήσεις.

Αυτός ο τρόπος εμπορίου συχνά περιγράφει τον τρόπο με τον οποίο οι κυβερνήσεις αγοράζουν προϊόντα και υπηρεσίες μέσω του Διαδικτύου.

1.3.4 Ηλεκτρονικό εμπόριο από επιχειρήσεις προς επιχειρήσεις (Business-to-Business e-Commerce - B2B)

Η κατηγορία αυτή περιλαμβάνει εταιρίες, που αλληλεπιδρούν προκειμένου να εκτελέσουν κάποιες λειτουργίες τους. Οι εταιρίες αυτές μπορούν να είναι:

Εταιρίες ξένες μεταξύ τους, που απλά χρησιμοποιούν το δίκτυο για την ηλεκτρονική διεξαγωγή των συναλλαγών τους.

Υποκαταστήματα ή τμήματα της ίδιας εταιρίας, που και πάλι χρησιμοποιούν το δίκτυο για τις συναλλαγές και για την επικοινωνία τους.

1.4 Τύποι Προϊόντων

Το ηλεκτρονικό εμπόριο Οι εφαρμογές παρέχουν τη δυνατότητα εύρεσης και ανάκτησης πληροφοριών, καθώς επίσης και συναλλαγές τεσσάρων τύπων προϊόντων: αγαθά, εργασίες, υπηρεσίες και άυλα αγαθά. Κάθε ένα από αυτά έχει ιδιαίτερα χαρακτηριστικά που καθιστούν χρήσιμη την εξέτασή τους, αφού η αντιμετώπισή τους σε μια εφαρμογή ηλεκτρονικού εμπορίου πρέπει να γίνεται με προσαρμογή στα ιδιαίτερα χαρακτηριστικά τους.

1.4.1 Αγαθά

Πρόκειται για φυσικά αντικείμενα, που έχουν παραχθεί σύμφωνα με κάποιες προδιαγραφές, που κατά κύριο λόγο τις ορίζει ο κατασκευαστής τους. Συνήθως συμπεριλαμβάνεται στην έννοιά τους και η μεταφορά από τον τόπο παραγωγής στον τόπο πώλησης.

Στην κατηγορία αυτή θα μπορούσαν να συμπεριληφθούν τα ακόλουθα:

- Είδη ένδυσης,
- Ανταλλακτικά κάθε είδους,
- Αυτοκίνητα,
- Υπολογιστές,
- Φαρμακευτικά προϊόντα... κλπ.

1.4.2 Εργασίες

Εδώ υπάγονται εργασίες ανάπτυξης ή κατασκευής αγαθών σύμφωνα με προδιαγραφές που θέτει ο πελάτης.

Παραδείγματα αποτελούν τα ακόλουθα:

- Προϊόντα λογισμικού,
- Ηλεκτρικές - υδραυλικές εγκαταστάσεις,
- Κατασκευές χώρων ... κλπ.

1.4.3 Υπηρεσίες

Η διάθεση και πώληση υπηρεσιών είναι συνήθως διαδικασίες αλληλοεξαρτώμενες.

Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν τα εξής:

- Δημόσιες, τουριστικές,
- Χρηματοοικονομικές, ψυχαγωγικές,
- Συμβουλευτικές υπηρεσίες
- Υπηρεσίες υγείας... κλπ.

1.4.4 Άϋλα αγαθά

Εδώ περιλαμβάνονται προϊόντα των οποίων η αξία δε συνδέεται άμεσα με το κόστος παραγωγής τους αλλά με το περιεχόμενο και τη χρήση τους. Η διανομή τους εξαρτάται άμεσα από κάποιο μέσο επικοινωνίας και συνδέονται άρρηκτα με την έννοια των δικαιωμάτων χρήσης.

Τέλος οι επιχειρηματικές διαδικασίες που σχετίζονται με αυτή την κατηγορία περιλαμβάνουν την αναπαραγωγή των προϊόντων κατόπιν σχετικής άδειας και όλες τις επικοινωνιακές διεργασίες που πρέπει να συντελεστούν για αυτό το σκοπό.

1.5 Πλεονεκτήματα ηλεκτρονικού εμπορίου

- Οι συναλλαγές πραγματοποιούνται 24 ώρες τη μέρα
- Η ταχύτητα των αγορών παρουσιάζει ενδιαφέρον καθώς ο χρόνος λήψης παραγγελιών, τιμολογίων και διάφορων πληροφοριών για τα προϊόντα είναι ελάχιστος.
- Σπάνια αντικείμενα όπως αντίκες και εξειδικευμένα είδη μπορούν να εντοπιστούν ευκολότερα με μια μηχανή αναζήτησης παρά με τον τηλεφωνικό κατάλογο
- Λόγω του ανταγωνισμού η κάθε επιχείρηση προσπαθεί να κερδίσει τους πελάτες, βελτιώνοντας όχι μόνο την ποιότητα των προϊόντων, αλλά και την παρουσίαση των προϊόντων, τις πληροφορίες που παρέχονται γι' αυτά με σκοπό να προσελκύσουν τον καταναλωτή.
- Ένα από τα μεγαλύτερα πλεονεκτήματα του internet είναι το μικρό κόστος εισόδου σε μία αγορά πράγμα το οποίο κάνει το διαδίκτυο να αποτελεί ένα σπουδαίο μέσο πωλήσεων
- Ο πελάτης μπορεί να διαλέξει αυτό που τον ενδιαφέρει από διάφορους προμηθευτές, χωρίς να τον απασχολεί η γεωγραφική θέση της επιχείρησης και να βρει μια πολύ συμφέρουσα προσφορά σε ελάχιστο χρόνο
- Οι λειτουργίες αναζήτησης του internet το κάνουν επίσης ένα καλό εργαλείο αγορών και παρότι η εφημερίδα αγορών μπορεί να μην έχει κατάλογο πωλήσεων για ένα σπίτι των δικών μας προδιαγραφών, στο διαδίκτυο υπάρχει πληθώρα.
- Χρήσιμη δυνατότητα των εξειδικευμένων καταστημάτων είναι η δυνατότητά τους να ειδοποιούν τον πελάτη, όταν κάτι για το οποίο ενδιαφέρεται βρέθηκε.
- Οι δημοπρασίες στο internet είναι ένας πολύ καλός τρόπος πωλήσεων καθότι η καταχώριση ενός είδους σε δημοπρασία είναι δωρεάν ενώ μερικές σελίδες δημοπρασιών εξειδικεύονται μόνο σε εξοπλισμό υπολογιστών ή συλλεκτικά αντικείμενα.
- Υπάρχει η δυνατότητα αλληλεπίδρασης πελατών με άλλους πελάτες σε ηλεκτρονικές κοινότητες, ανταλλαγή ιδεών και εμπειριών

1.6 Μειονεκτήματα ηλεκτρονικού εμπορίου

- Το διαδίκτυο είναι ένα μέσο που δεν παρέχει το επιθυμητό επίπεδο ασφάλειας στις συναλλαγές, με αποτέλεσμα να μην ασφαλείς.
- Με τις αγορές στο internet δεν υπάρχει αμεσότητα με το αντικείμενο που θέλει να αγοράσει κάποιος. Η αγορά είναι εικονική. Ο πελάτης δεν μπορεί να πάει στο κατάστημα να αγγίξει τα εμπορεύματα.
- Επιβάρυνση με ένα ποσό για έξοδα συσκευασίας και αποστολής, αναμονή παραγγελίας.
- Πακέτα ανεπιθύμητου ταχυδρομείου από τους διαφημιστές,
- Αναγκαιότητα για ειδικούς διακομιστές Ιστού (Web servers) και άλλες υποδομές, επιπλέον των διακομιστών δικτύου (επιπρόσθετο κόστος)

1.7 Οι στόχοι της ασφάλειας στο ηλεκτρονικό εμπόριο

Η ασφάλεια διαδραματίζει έναν πολύ σημαντικό ρόλο στο ηλεκτρονικό εμπόριο, όμως από τη στιγμή που δεν είναι ικανοποιητική μπορεί να αποτελέσει καταστρεπτικό παράγοντα για τους συμμετέχοντες στο ηλεκτρονικό εμπόριο δηλαδή την επιχείρηση και τον καταναλωτή. Οι στόχοι της ασφάλειας στο ηλεκτρονικό εμπόριο είναι:

- Η προστασία της μυστικότητας του καταναλωτή στο σημείο της αγοράς
- Η προστασία της μυστικότητας των πληροφοριών των πελατών κατά τη διαδικασία αποθήκευση η επεξεργασίας
- Η προστασία την ταυτότητας των πελατών
- Η προστασία της επιχείρησης από απάτη, και την κατάχρηση
- Η προστασία των ενεργητικών πληροφοριών της επιχείρησης από την ανακάλυψη και κοινοποίηση
- Η εξασφάλιση της διαθεσιμότητας των συστημάτων και των διαδικασιών που απαιτούνται για τη διαδικασία της συνεργασίας του πελάτη με την επιχείρηση

Αυτοί οι στόχοι είναι μια αφετηρία για τη δημιουργία μιας καλής πολιτικής ασφάλειας.

1.8 Βασικοί όροι στην ασφάλεια τεχνολογιών πληροφοριακών συστημάτων (Τ.Π.Σ)

Μερικοί από τους πιο σημαντικότερους όρους που αναφέρονται στην ασφάλεια τεχνολογιών πληροφοριακών συστημάτων είναι οι ακόλουθοι:

- Αγαθό (asset)

Ονομάζεται κάτι το οποίο αξίζει να προστατευθεί.

- Ζημιά (harm)

Ονομάζεται ο περιορισμός της αξίας ενός αγαθού.

- Κίνδυνος (danger)

Ονομάζεται το ενδεχόμενο ένα αγαθό να υποστεί ζημιά.

- Ιδιοκτήτης ή χρήστης (owner/user) ενός αγαθού

Ονομάζεται το φυσικό ή νομικό πρόσωπο που κατέχει ή χρησιμοποιεί - αντίστοιχα - το αγαθό αυτό.

- Μέσο προστασίας (safeguard)

Ονομάζονται οι ενέργειες στις οποίες μπορεί να προβεί ο ιδιοκτήτης ή ο χρήστης ενός αγαθού προκειμένου να περιορίσει τον κίνδυνο να υποστεί ζημιά το αγαθό αυτό.

- Δεδομένα (data)

Είναι ένα σύνολο από σύμβολα που έχουν καταγραφεί.

- Πληροφορία (information)

Ονομάζονται τα δεδομένα τα οποία συνοδεύονται από τη σημασία (έννοιά) τους

- Υπολογιστικό σύστημα (IT system)

Ονομάζεται ένα συγκεκριμένο υπολογιστικό συγκρότημα, το οποίο εναι εγκατεστημένο σε συγκεκριμένες τοποθεσίες, πλαισιώνεται από συγκεκριμένο επιχειρησιακό περιβάλον και αποβλέπει στην εκπλήρωση συγκεκριμένων στόχων.

- Πληροφοριακό Σύστημα (information system)

Ονομάζεται ένα υπολογιστικό σύστημα μαζί με τις πληροφορίες τις οποίες επεξεργάζεται

- Ιδιοκτήτης πληροφορίας (information owner)

Ονομάζεται ο ιδιοκτήτης ενός αγαθού το οποίο έχει τη μορφή πληροφορίας.

- Ιδιοκτήτης συστήματος (system owner)

Ονομάζεται ο ιδιοκτήτης κάποιων υπολογιστικών πόρων.

- Εξουσιοδότηση (authorisation)

Ονομάζεται η διαδικασία κατά την οποία ο ιδιοκτήτης ενός αγαθού παρέχει - για συγκεκριμένο λόγο - κάποιο είδος δικαιώματος σε ένα πρόσωπο ή σε μια διαδικασία.

- Χρήστης (user)

Ονομάζεται μια οντότητα η οποία αξιοποιεί ένα μέρος ή το σύνολο ενός Πληροφοριακού Συστήματος.

- Υπηρεσία (service)

Ονομάζεται κάθε σύνολο λειτουργιών (functionalities) που παρέχονται σε κάποιο χρήστη από ένα υπολογιστικό σύστημα.

- Προσπέλαση (access)

Ονομάζεται η δυνατότητα χρήσης πληροφοριών ή υπολογιστικών πόρων ενός πληροφοριακού συστήματος.

- Προσπέλαση πληροφορίας (information access)

Ονομάζεται η δυνατότητα χρήσης συγκεκριμένων πληροφοριών από ένα πληροφοριακό σύστημα.

- Ακεραιότητα (integrity)

Ονομάζεται η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

- Ρήγμα ασφάλειας (breach of security)

Ονομάζεται η αποκάλυψη, μετατροπή ή παρακράτηση μιας πληροφορίας χωρίς εξουσιοδότηση.

- Παραβίαση (violation)

Ονομάζεται ένα γεγονός κατά τη διάρκεια του οποίου έχει παραβιαστεί το χαρακτηριστικό της αυθεντικότητας ή της διαθεσιμότητας ή της εμπιστευτικότητας ή της ακεραιότητας ή της συνέπειας.

- Επισφάλεια (hazard)

Ονομάζεται το ενδεχόμενο να συμβεί κάποια προσβολή

- Εξασφάλιση (assurance)

Ονομάζεται η βεβαιότητα ότι ένας ή περισσότεροι αντικειμενικοί σκοποί ή προδιαγραφές έχουν επιτευχθεί.

- Πολιτική (policy)

Ονομάζεται το σύνολο των κανόνων, μέτρων και διαδικασιών που καθορίζονται από τη διοίκηση ενός πληροφοριακού συστήματος και ορίζουν τους ελέγχους που απαιτούνται για την ασφάλεια των αγαθών του συστήματος.

- Οδηγίες (guidelines)

Ονομάζονται οι συστάσεις για τη λήψη ενεργειών, για την υιοθέτηση διαδικασιών, μεθόδων ή προτύπων, ή για την αγορά εξοπλισμού και οι οποίες πρέπει να πραγματοποιηθούν σε συγκεκριμένες περιστάσεις.

2 Συστήματα ηλεκτρονικών πληρωμών

Ταξινομούνται σύμφωνα με τη σχέση που υπάρχει ανάμεσα στο χρόνο που ο πελάτης θεωρεί την αγορά ως ολοκληρωμένη και το χρόνο που η αντίστοιχη χρηματική αξία λαμβάνεται πραγματικά από το λογαριασμό του. Μπορεί κανείς να διακρίνει:

2.1 Συστήματα προπληρωμής (Prepaid payment system)

Σε ένα σύστημα προπληρωμής, ένα συγκεκριμένο ποσό χρημάτων αφαιρείται από τον πελάτη χρεώνοντας για παράδειγμα τον τραπεζικό του λογαριασμό πριν γίνει οποιαδήποτε αγορά. Αυτό το χρηματικό ποσό μπορεί να χρησιμοποιηθεί αργότερα για πληρωμές. Στην κατηγορία αυτή εμπίπτουν έξυπνες κάρτες (smart cards) που στηρίζονται σε ηλεκτρονικά πορτοφόλια, ηλεκτρονικά μετρητά και συγκεκριμένες τραπεζικές επιταγές, όπως πιστοποιημένες επιταγές.

- Έξυπνες κάρτες (smart cards): οι κάρτες αυτές μοιάζουν με τις πιστωτικές αλλά έχουν ένα μικροτσίπ, στο οποίο αποθηκεύεται το ηλεκτρονικό χρήμα. Δηλαδή, στην κάρτα αυτή αποθηκεύονται η πίστωση, το χρέος και η αξία της.

- Ηλεκτρονικές επιταγές (electronic checks): Κάθε ηλεκτρονική επιταγή έχει μια σειρά από νούμερα τα οποία την καθιστούν μοναδική. Συνοδεύεται με ψηφιακή υπογραφή και χρησιμοποιείται σαν ένα μήνυμα-εντολή για τη μεταφορά κεφαλαίων μεταξύ τραπεζικών λογαριασμών Οι ηλεκτρονικές επιταγές είναι πιο ασφαλείς διότι απαιτεί την κωδικοποίηση των απαραίτητων στοιχείων που διαβιβάζονται στον προμηθευτή ενώ υπάρχει δυνατότητα ελέγχου του διαθεσίμου ποσού του καταναλωτή πριν από την ολοκλήρωση της συναλλαγής.

2.2 Συστήματα άμεσης πληρωμής (Pay-now payment system)

Ο λογαριασμός του πελάτη χρεώνεται ακριβώς τη στιγμή της αγοράς. Στην κατηγορία αυτή ανήκουν συγκεκριμένες χρεωστικές κάρτες.

2.3 Συστήματα μεταπληρωμής (Pay-after payment system)

Ο τραπεζικός λογαριασμός του εμπόρου πιστώνεται με το ποσό της αγοράς πριν χρεωθεί ο λογαριασμός του πελάτη. Σε αυτή την κατηγορία ανήκουν οι πιστωτικές κάρτες.

- Πιστωτικές κάρτες (credit cards): Μέσω αυτού του συστήματος πληρωμών , ο καταναλωτής ταυτόχρονα με την παραγγελία δίνει τα στοιχεία της κάρτας του, όπως τον αριθμό και την ημερομηνία λήξης και ο προμηθευτής πληρώνεται από την τράπεζα του καταναλωτή. Για την αποφυγή παρεμβολής τρίτων προσώπων (κακόβουλων) αναπτύσσεται ένα σύστημα κρυπτογράφησης-αποκρυπτογράφησης που εγγυάται την ασφάλεια των συναλλαγών.

2.4 Τρίτη υπηρεσία πληρωμής

Η τρίτη υπηρεσία πληρωμής επιτρέπει τη μεταβίβαση χρημάτων σε έναν ηλεκτρονικό λογαριασμό και την πραγματοποίηση πληρωμών μέσω του λογαριασμού αυτού χωρίς να χρειάζεται να αποκαλυφθούν τα πραγματικά στοιχεία της πιστωτικής κάρτας ή του τραπεζικού λογαριασμού του πελάτη. Η δημοφιλέστερη από αυτές τις υπηρεσίες είναι η PayPal (που ανήκει στην eBay), αλλά υπάρχουν και άλλες, όπως οι Amazon.com Payments, Yahoo!, PayDirect και VeriSign Inc. Αυτές οι τρίτες υπηρεσίες πληρωμής δεν χρησιμοποιούνται αποκλειστικά σε δημοπρασίες. Μπορούν να χρησιμοποιηθούν για την αγορά προϊόντων από μικρές διαδικτυακές τοποθεσίες ή για την πραγματοποίηση κάποιας δωρεάς για διάφορους σκοπούς. Ουσιαστικά, μπορούν να χρησιμοποιηθούν ορισμένες από αυτές τις υπηρεσίες πληρωμής για να αποστολή χρημάτων σε οποιονδήποτε έχει λογαριασμό ηλεκτρονικού ταχυδρομείου.

2.4.1 Το Paypal

Το PayPal αναλαμβάνει να στείλει τα χρήματα στον πωλητή γνωστοποιώντας του μόνο το όνομα του καταναλωτή και την διεύθυνση μας (και όχι τα στοιχεία της κάρτας).

Το PayPal μεσολαβεί μεταξύ Πωλητή και Αγοραστή , διευκολύνοντας με ασφάλεια την διεκπεραίωση μια συναλλαγής γνωστοποιώντας στα αντισυμβαλλόμενα μέρη μόνο τα απαραίτητα στοιχεία για την ολοκλήρωση της "πληρωμής".

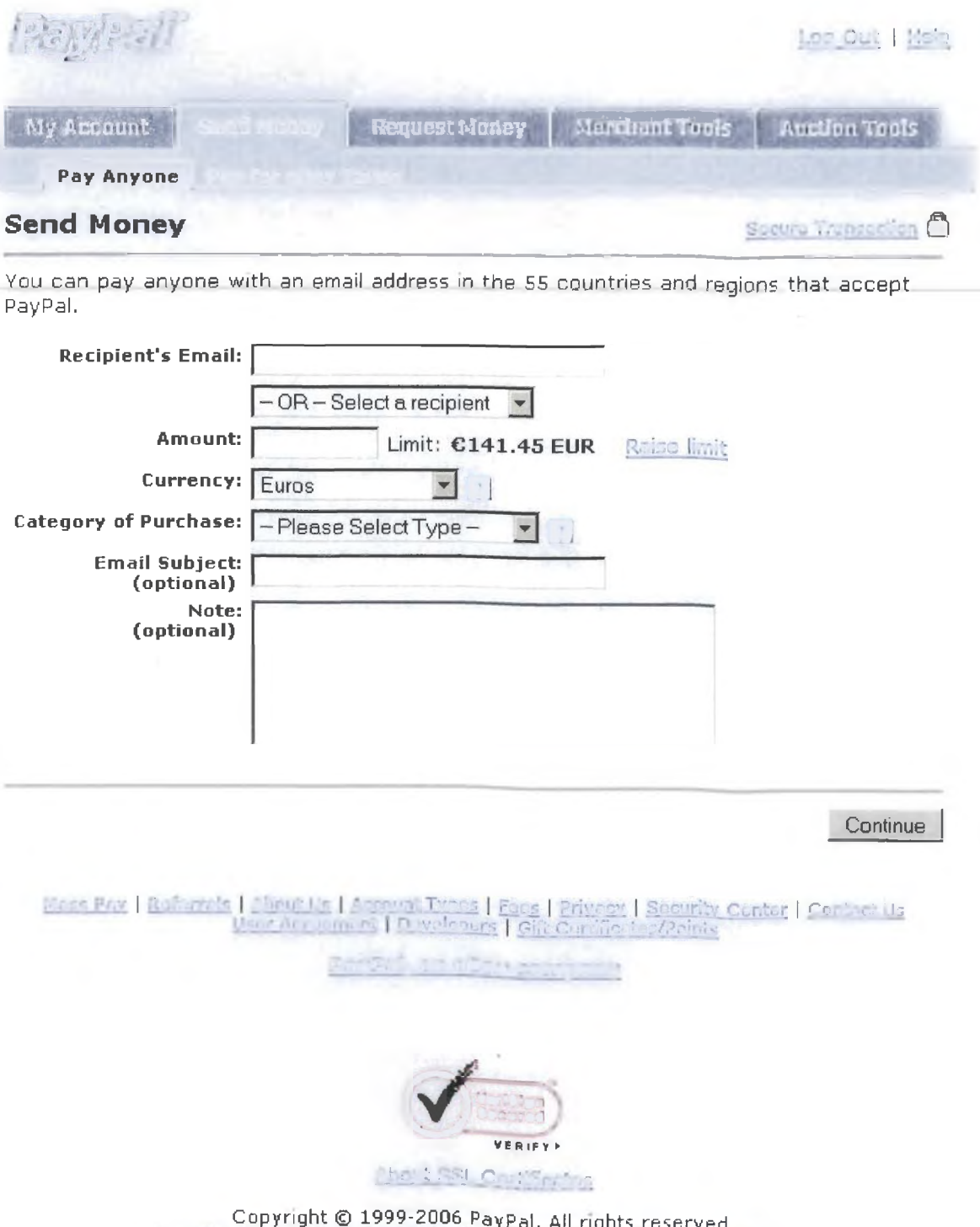
Από πλευράς ασφάλειας συναλλαγών είναι ότι καλύτερο υπάρχει αφού γίνεται γνωστοποίηση των στοιχείων της πιστωτικής κάρτας μόνο σε αυτή την υπηρεσία , χωρίς να χρειάζεται κάθε αγορά από ένα ηλεκτρονικό κατάστημα να κοινοποιούμε τα στοιχεία αυτά .

Εφαρμόζει πολλά προγράμματα - δικλείδες ασφαλείας και πιστοποίησης συστημάτων ασφαλείας , το όλο πλέγμα ασφάλειας έρχεται να ενισχύσει την ασφάλεια των συναλλαγών μας (δεν είναι τυχαίο ότι 60 εκατομμύρια καταναλωτών στον κόσμο το χρησιμοποιούν για τις συναλλαγές τους (πρόσφατα εξαγοράστηκε από την γνωστή εταιρεία δημοπρασιών ebay.com).

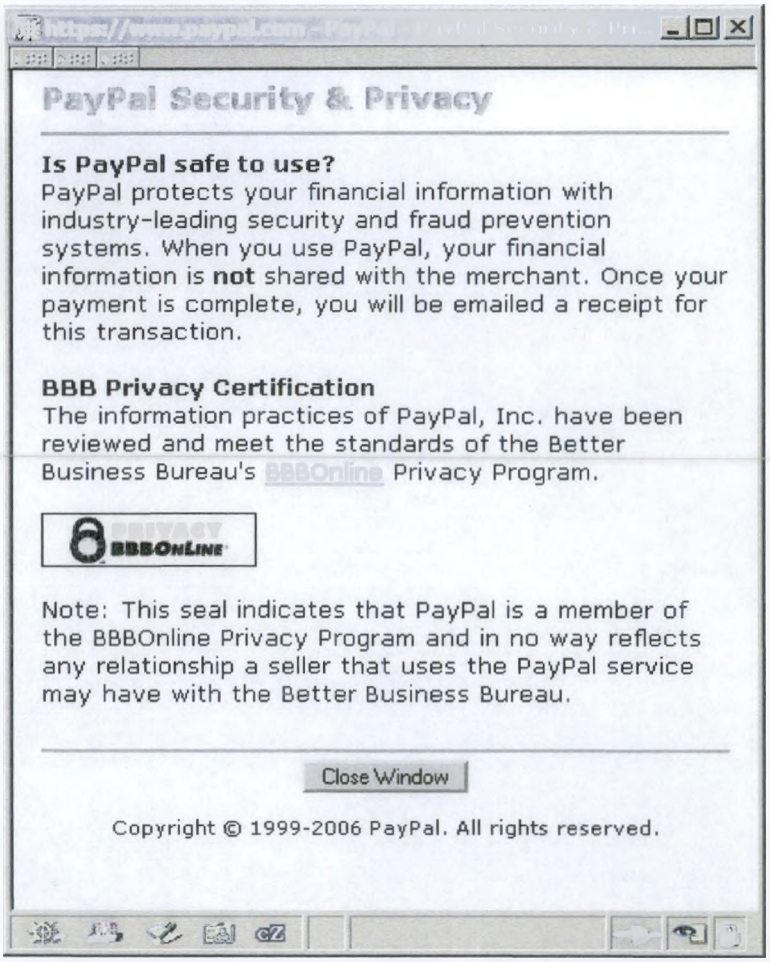
Η υπηρεσία είναι δωρεάν για τον καταναλωτή που θέλει να στείλει χρήματα.

Για τον πωλητή (ιδιοκτήτη ηλεκτρονικού καταστήματος, πωλητή δημοπρασίας κλπ) υπάρχει κάποιο κόστος συνήθως χαμηλότερο από τους άλλους εναλλακτικούς τρόπους πληρωμών . Το κόστος κυμαίνεται σήμερα σε 0.35 ευρώ + 3,4% επί της αξίας συναλλαγών (κοστολόγιο ιδιαίτερα φθηνό για μικρής αξίας συναλλαγές).

Παρακάτω υπάρχει μία απεικόνιση της ιστοσελίδας Paypal και της διαδικασίας αποστολής χρημάτων. Η αποστολή μπορεί να γίνει σε οποιονδήποτε από ένα σύνολο 55 χωρών. Παρατηρούμε ότι η ιστοσελίδα χρησιμοποιεί το πρωτόκολλο SSL και μάλιστα έχει πάρει πιστοποίηση από την εταιρεία Versign η οποία ειδικεύεται στο χώρο της ασφάλειας ενώ παράλληλα μας ενημερώνει ότι η συναλλαγή που πρόκειται να πραγματοποιηθεί είναι ασφαλής.



Εδώ βλέπουμε τις πληροφορίες που μας δίνει το PayPal σχετικά με την ασφάλεια και την προστασία των προσωπικών μας δεδομένων.



2.4.2 Είδη Λογαριασμών στο PayPal

- Personal Account

Ιδανικό για όσους θέλουν να στείλουν χρήματα , δηλαδή για χρήση αγορών . Αλλά και εάν σας στείλουν χρήματα (πχ έχετε δημοπρατήσει ένα προϊόν) πάλι είναι δωρεάν αλλά τα χρήματα αυξάνουν το υπόλοιπο στον λογαριασμό σας που είναι διαθέσιμο.

- Premier Account

Ιδανικό για όσους συστηματικά θα δέχονται πληρωμές (ιστοσελίδες , πωλητές δημοπρασιών)

- Business Account

Ιδανικό για όσους συστηματικά θα δέχονται πληρωμές (ιστοσελίδες , πωλητές δημοπρασιών)

3 Απαιτήσεις ασφάλειας

Για την αντιμετώπιση της ασφάλειας των ηλεκτρονικών συναλλαγών έχουν οριστεί κάποιες απαιτήσεις.

Οι βασικότερες από αυτές τις απαιτήσεις είναι οι ακόλουθες:

- Εμπιστευτικότητα (Confidentiality),
- Ακεραιότητα (Integrity),
- Αυθεντικότητα (Authentication) και η
- Δεσμευτικότητα (Non-refutability) ή αλλιώς η μη ύπαρξη δυνατότητας αποποίησης ευθύνης από τους συναλλασσόμενους (Non-repudiation)

Πολλές φορές χρησιμοποιούνται και οι όροι εξουσιοδότηση και εξασφάλιση όταν γίνεται αναφορά στις απαιτήσεις ασφάλειας.

Ακολουθεί ανάλυση των παραπάνω απαιτήσεων.

3.1 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητας εγγυάται ότι οι πληροφορίες δεν πρέπει να είναι διαθέσιμες ούτε αποκαλύπτονται στους μη εξουσιοδοτημένους χρήστες και παρέχει μηχανισμούς οι οποίοι θα πρέπει να προστατεύουν τα δεδομένα που αποστέλλονται από τους κακόβουλες χρήστες του διαδικτύου. Για την εξασφάλιση της εμπιστευτικότητας μπορεί να χρησιμοποιηθεί υβριδική κρυπτογραφία, δηλαδή ένας συνδυασμός συμμετρικής και ασύμμετρης κρυπτογραφίας. Κάθε χρήστης αποκτά ζεύγος ασύμμετρων κλειδιών (ιδιωτικό και δημόσιο) και παράγει τυχαίο συμμετρικό κλειδί, με το οποίο κρυπτογραφεί τα εμπιστευτικά δεδομένα του και το αποθηκεύει κρυπτογραφημένο με το δημόσιο κλειδί του. Για την ανάγνωση των εμπιστευτικών δεδομένων, ο χρήστης χρησιμοποιεί το ιδιωτικό του κλειδί για να ανακτήσει το συμμετρικό κλειδί, με το οποίο στη συνέχεια αποκρυπτογραφεί τα εμπιστευτικά δεδομένα. Ακόμα υπάρχει η περίπτωση τα δεδομένα να αποστέλλονται κρυπτογραφημένα και να αποκρυπτογραφούνται όταν παραληφθούν από το χρήστη για τον οποίον προορίζονται ώστε να μην είναι αναγνώσιμα από τους ενδιάμεσους κόμβους του δικτύου.

3.2 Ακεραιότητα (Integrity)

Τα αντικείμενα του συστήματος που σχετίζονται με το εκτελέσιμο λογισμικό και τα αντίστοιχα δεδομένα-πληροφορίες θα πρέπει να προστατεύονται αποτελεσματικά ως προς την ακεραιότητά τους, δηλαδή τη μη τροποποίησή τους από μη εξουσιοδοτημένες οντότητες. Συγκεκριμένα θα πρέπει να υπάρχουν οι απαραίτητοι μηχανισμοί έτσι ώστε τα δεδομένα να παραμένουν αναλλοίωτα κατά τη διάρκεια της μεταφοράς τους και αποθήκευσης τους στο διαδίκτυο.

3.3 Αυθεντικότητα (Authentication)

Αυθεντικοποίηση ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.
Η αυθεντικοποίηση αφορά επομένως τη διαδικασία κατά την οποία επαληθεύεται η δηλωθείσα ταυτότητα ενός λογικού υποκειμένου.

Γενικά, η αυθεντικοποίηση είναι η βασικότερη υπηρεσία ασφάλειας που μπορεί να προσφέρει ένα δίκτυο υπολογιστών καθώς αυτή παρέχει προστασία έναντι μη εξουσιοδοτημένων δοσοληψιών, εξασφαλίζοντας τη γνησιότητα ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την εγκυρότητα ενός τερματικού υπολογιστή.

3.3.1 Κατηγορίες αυθεντικοποίησης

Η διαδικασία της αυθεντικοποίησης αποτελεί την υποβολή πληροφοριών στο σύστημα που είναι εκ των προτέρων γνωστές αποκλειστικά και μόνο στο λογικό υποκείμενο και στο πληροφοριακό σύστημα. Γενικότερα η διαδικασία αυθεντικοποίησης περιλαμβάνει: α) την παροχή της πληροφορίας από ένα λογικό υποκείμενο στο σύστημα, β) την ανάλυση αυτής της πληροφορίας και γ) τον έλεγχο ότι πράγματι αυτή η πληροφορία σχετίζεται με το ίδιο λογικό υποκείμενο.

Για την εφαρμογή ελέγχων αυθεντικοποίησης υπάρχουν τέσσερις βασικοί τρόποι. Αυτοί είναι:

- Τύπος I

Κάτι που το λογικό υποκείμενο γνωρίζει (π.χ ένα συνθηματικό)

- Τύπος II

Κάτι που το λογικό υποκείμενο κατέχει (π.χ ψηφιακό πιστοποιητικό ή έξυπνη κάρτα)

- Τύπος III

Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (π.χ σύστημα αναγνώρισης φωνής)

- Τύπος IV

Κάτι που προσδιορίζει τη τοποθεσία που βρίσκεται το λογικό υποκείμενο (π.χ διεύθυνση IP)

3.3.2 Συνθηματικά

Τα συνθηματικά αποτελούν το συνηθέστερο μέσο αυθεντικοποίησης. Συνθηματικό (password) είναι η πληροφορία η οποία σχετίζεται με ένα λογικό υποκείμενο και η οποία επιβεβαιώνει την ταυτότητα του λογικού υποκειμένου. Η διάδοση της χρήσης των συνθηματικών βασίζεται στα εξής πλεονεκτήματα:

- Είναι απλά στη λειτουργία τους και επομένως έχουν περιορισμένη σχεδιαστική πολυπλοκότητα
- Έχουν χαμηλό κόστος
- Παρέχουν ικανοποιητικό βαθμό προστασίας

Από την άλλη πλευρά τα μειονεκτήματα που παρουσιάζονται είναι:

- Η τυχαία αποκάλυψη του συνθηματικού
- Η αποκάλυψη του συνθηματικού με συστηματικό τρόπο (δοκιμή όλων των πιθανών συνδυασμών των αλφαριθμητικών χαρακτήρων συγκεκριμένου μεγέθους)
- Η αποκάλυψη του συνθηματικού κατά τη διάρκεια της μετάδοσής του

Για λόγους ασφαλείας ορισμένα συστήματα τηρούν ένα μετρητή για την καταγραφή των αποτυχημένων προσπαθειών πρόσβασης από τους χρήστες και στην περίπτωση όπου ένας χρήστης ξεπεράσει το επιτρεπόμενο όριο των αποτυχημένων προσπαθειών πρόσβασης στο σύστημα, τότε αυτομάτως ο λογαριασμός του κλειδώνεται.

Ορισμένα κριτήρια για την επιλογή και χρήση συνθηματικών από τους χρήστες ενός συστήματος έτσι ώστε να είναι όσο το δυνατό πιο ασφαλές είναι:

- Μήκος συνθηματικού (να ορίζεται πάντα ένα ελάχιστο μήκος για τα συνθηματικά)
- Μορφότυπο συνθηματικού (να αποτελείται από συνδυασμούς γραμμάτων, αριθμών και ειδικών χαρακτήρων)
- Αποφυγή εύκολων συνθηματικών (π.χ ονόματα, λέξεις από λεξικά)
- Αλλαγή συνθηματικών (να πραγματοποιείται κατά τακτά χρονικά διαστήματα αλλαγή του συνθηματικού)

3.4 Δεσμευτικότητα (Non-refutability)

Συχνά απαιτείται ο καταλογισμός της ευθύνης για την αποστολή ή παραλαβή ενός μηνύματος. Δηλαδή, είναι απαραίτητο σε ορισμένες περιπτώσεις ο αποστολέας ή παραλήπτης ενός μηνύματος να μη μπορεί να έχει τη δυνατότητα αποποίησης της ευθύνης ότι δε συμμετείχε στην εν λόγο αποστολή ή παραλαβή του συγκεκριμένου μηνύματος. Ένας μηχανισμός αντιμετώπισης του προβλήματος αυτού του είδους είναι με τη χρήση ψηφιακών υπογραφών (digital signatures) που υλοποιούνται με τη βοήθεια κρυπτογραφικών συστημάτων.

Πολλές φορές χρησιμοποιούνται και οι όροι εξουσιοδότηση και εξασφάλιση όταν γίνεται αναφορά στις απαιτήσεις ασφάλειας.

3.5 Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση αφορά την αναγνώριση και στη συνέχεια της παραχώρησης των δικαιωμάτων από τον ιδιοκτήτη προς το χρήστη. Ένα παράδειγμα είναι ότι ο πελάτης ουσιαστικά εξουσιοδοτεί την επιχείρηση για να ελέγξει τον αριθμό της πιστωτικής του κάρτας και συνεπώς να επιβεβαιώσει την ύπαρξη ή όχι του ανάλογου αντικρίσματος που έχει η κάρτα στη τράπεζα.

3.6 Εξασφάλιση (Assurance)

Η εξασφάλιση ουσιαστικά αναφέρεται στην ύπαρξη εμπιστοσύνης ανάμεσα στα συναλλασσόμενα μέρη έτσι ώστε η συναλλαγή να ολοκληρώνεται επιτυχώς χωρίς κανένα πρόβλημα. Για αυτό το λόγο ο πελάτης άλλωστε έχει την ανάγκη να γνωρίζει αν ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος.

4 Πολιτική ασφάλειας πληροφοριακών συστημάτων

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων αν και μπορεί να διαφέρει σημαντικά από επιχείρηση σε επιχείρηση, περιλαμβάνει γενικά το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων της επιχείρησης. Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη της επιχείρησης, στις δραστηριότητές τους που έχουν σχέση με τα πληροφοριακά συστήματα που καλύπτει η πολιτική.

Στην πολιτική ασφάλειας δηλαδή, καθορίζονται οι στόχοι της ασφάλειας καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο, επομένως κάθε πολιτικής ασφάλειας πληροφοριακών συστημάτων είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας.

Η εφαρμογή μιας πολιτικής ασφάλειας σε μια επιχείρηση έχει δεσμευτικό χαρακτήρα για όλα τα μέλη. Αυτό σημαίνει ότι η τήρηση των διαδικασιών και οδηγιών που επιβλέπει η πολιτική ασφάλειας και η εφαρμογή των μέτρων που προδιαγράφονται σε αυτήν, είναι υποχρεωτική για όλους τους χρήστες των πληροφοριακών συστημάτων.

4.1 Οδηγίες, διαδικασίες και μέτρα προστασίας

Οι πολιτικές ασφάλειας δηλώνουν τους στόχους για την ασφάλεια των πληροφοριακών συστημάτων και τα γενικά μέσα για την επίτευξή τους, ενώ οι οδηγίες που περιλαμβάνονται στην πολιτική ασφάλειας, αποσκοπούν στη δημιουργία του κατάλληλου πλαισίου για την επίτευξη των στόχων της πολιτικής ασφάλειας. Οι διαδικασίες δίνουν συγκεκριμένες κατευθύνσεις για την υλοποίηση και εφαρμογή των οδηγιών της πολιτικής.

Τέλος μια πολιτική ασφάλειας συνοδεύεται από ένα σύνολο μέτρων προστασίας ή αντιμέτρων ή μέτρων ασφάλειας όπως αλλιώς λέγονται, η εφαρμογή των οποίων παρέχει στα πληροφοριακά συστήματα το επίπεδο ασφάλειας που προσδιορίζεται στην πολιτική ασφάλειας. Η πολιτική ασφάλειας μαζί με το σύνολο των μέτρων προστασίας αποτελούν το σχέδιο ασφάλειας για τα πληροφοριακά συστήματα μιας επιχείρησης.

4.2 Εμπλεκόμενοι στην ανάπτυξη πολιτικών ασφάλειας

Η ανάπτυξη της πολιτικής ασφάλειας των πληροφοριακών συστημάτων μιας επιχείρησης βασίζεται στην καταγραή των απαιτήσεων ασφάλειας, με βάση τις οποίες διαμορφώνονται οι στόχοι της ασφάλειας, και στον προσδιορισμό των τρόπων για την επίτευξη των στόχων αυτών. Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές όπως:

- Οι χρήστες των πληροφοριακών συστημάτων
- Η διοίκηση της επιχείρησης που επιθυμεί την απρόσκοπτη χρήση των πληροφοριακών συστημάτων στις λειτουργίες της επιχείρησης
- Οι πελάτες της επιχείρησης, εφόσον δεδομένα που τους αφορούν αποτελούν συνιστώσα του πληροφοριακού συστήματος
- Το νομικό και ρυθμιστικό πλαίσιο στο οποίο λειτουργεί η επιχείρηση

4.3 Τι πρέπει να πληρεί μία πολιτική ασφάλειας για να είναι καλή;

Τα βασικά χαρακτηριστικά μιας καλοσχεδιασμένης πολιτικής είναι τα ακόλουθα:

- Θα πρέπει να μπορεί να είναι εφαρμόσιμη από το διαχειριστή και να βασίζεται σε κοινά αποδεκτές μεθόδους.
- Θα πρέπει να είναι υλοποιήσιμη με τη χρήση διάφορων διαθέσιμων εργαλείων.
- Θα πρέπει να καθορίζει με σαφήνεια τα όρια ευθύνης όλων των μελών του οργανισμού (χρήστες, διαχειριστές, διευθυντές κ.λπ.).

Τα συστατικά που ορίζουν μία καλή πολιτική ασφαλείας είναι τα ακόλουθα:

- Οδηγίες αγοράς υπολογιστικών συστημάτων, οι οποίες προσδιορίζουν τα απαιτούμενα ή προτεινόμενα χαρακτηριστικά ασφαλείας. Αυτές οι οδηγίες, πρέπει να αποτελούν μέρους ενός ευρύτερου πλαισίου πολιτικής αγοράς υπολογιστικών συστημάτων.
- Διαφύλαξη του απορρήτου του χρήστη σε θέματα όπως παρακολούθηση του ηλεκτρονικού ταχυδρομείου, προσπέλαση των αρχείων των χρηστών κλπ.
- Καθορισμός δικαιωμάτων πρόσβασης, ώστε να αποφευχθεί η απώλεια ή η αλλοίωση των δεδομένων, προσδιορίζοντας κοινά αποδεκτές οδηγίες χρήσης για όλες της κατηγορίες χρηστών. Θα πρέπει να δίνονται οδηγίες για εξωτερικές συνδέσεις, συνδέσεις συσκευών στο δίκτυο καθώς και εγκατάσταση νέου λογισμικού.
- Θα πρέπει να ξέρει ο καθένας το ρόλο του και τις ευθύνες που αυτό συνεπάγεται, έτσι ώστε να μπορεί εύκολα κάποιος να απευθυνθεί στον αντίστοιχο αρμόδιο σε περίπτωση κάποιου προβλήματος.
- Πιστοποίηση των χρηστών με την χρήση μιας αποδοτικής πολιτικής χρήσης λέξεων κλειδιών (passwords) και καθορισμός οδηγιών πρόσβασης στους δικτυακούς πόρους του οργανισμού από απομακρυσμένο σημείο.
- Καθορισμός της διαθεσιμότητας των πόρων του συστήματος. Θα πρέπει να καθορίζονται οι ώρες λειτουργίας του συστήματος καθώς και ο απαιτούμενος χρόνος για τη συντήρηση του. Επίσης θα πρέπει να καταγράφονται πληροφορίες

που αφορούν τα σφάλματα και τα προβλήματα που παρουσιάστηκαν κατά το χρόνο λειτουργίας του συστήματος.

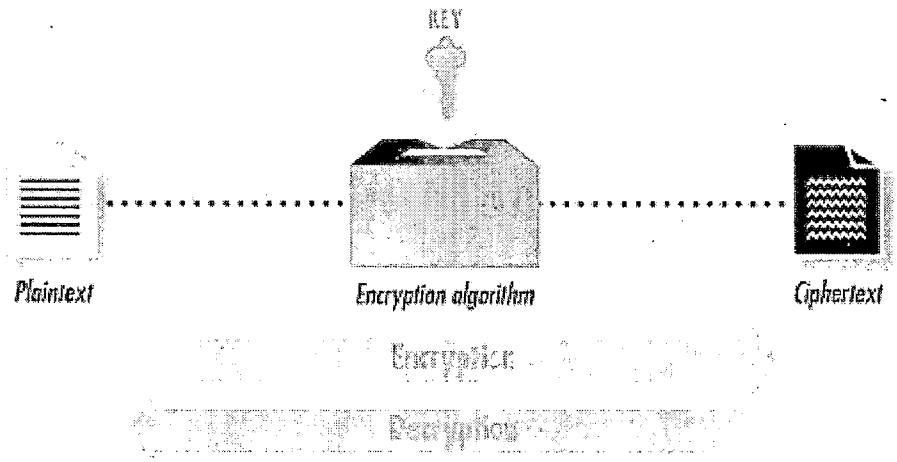
- Ένα πληροφοριακό σύστημα και μια πολιτική συντήρησης του δικτύου όπου θα καθορίζεται πότε, πως και από ποιόν θα γίνεται η συντήρησή του. Στο σημείο αυτό είναι σημαντικό να αποφασιστεί αν θα επιτρέπεται η συντήρηση από απόσταση και αν ναι πως θα ελέγχεται η πρόσβαση.
- Ο τρόπος με τον οποίο καταγράφονται και δημοσιοποιούνται οι παραβιάσεις. Θα πρέπει εκτός από τον τύπο της παραβίασης (π.χ. privacy και ασφάλεια, εσωτερική και εξωτερική) να ορίζει και σε ποιους απευθύνεται η αναφορά. Η δυνατότητα της ανώνυμης αναφοράς αυξάνει την πιθανότητα γνωστοποίησης μιας παραβίασης.
- Παροχή πληροφοριών στους χρήστες, το προσωπικό και τη διοίκηση για κάθε τύπο παραβίασης της πολιτικής ασφαλείας. Οδηγίες για το χειρισμό καταστάσεων σε περίπτωση παραβίαση της ασφάλειας και την ελεγχόμενη ενημέρωση τρίτων φορέων σε τέτοιες περιπτώσεις. Συμβατότητα της πολιτική ασφάλειας με την εκάστοτε νομοθεσία και τους κανονισμούς.

Όταν αποφασιστεί η πολιτική ασφαλείας που θα ακολουθηθεί θα πρέπει να γνωστοποιηθεί στους χρήστες, το προσωπικό και τη διοίκηση. Αυτοί με τη σειρά τους θα πρέπει να την διαβάσουν και να την κατανοήσουν και τέλος να δηλώσουν εάν την αποδέχονται ή όχι. Είναι βασικό η πολιτική ασφαλείας να έχει την αποδοχή όλων.

5 Κρυπτογραφία

Η κρυπτογραφία (cryptography) ως επιστήμη της ασφαλούς επικοινωνίας προσφέρει διάφορες τεχνικές για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Σε ένα σύστημα κρυπτογράφησης, το αρχικό μήνυμα (plaintext) μετασχηματίζεται σε κρυπτογράφημα (ciphertext), δηλαδή σε ένα μήνυμα το οποίο είναι μη-αναγνώσιμο από τρίτους (εκτός από τον επιδιωκόμενο παραλήπτη). Οι μετατροπές κρυπτογράφησης – αποκρυπτογράφησης (encryption-decryption) γίνονται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός αρκετά μεγάλου αριθμού, του κλειδιού κρυπτογράφησης (key). Προκειμένου να επιτευχθεί εμπιστευτικότητα των πληροφοριών των ηλεκτρονικών συναλλαγών χρησιμοποιείται κρυπτογράφηση, δημοσίου (ασύμμετρή κρυπτογραφία) ή ιδιωτικού κλειδιού (συμμετρική κρυπτογραφία).

Απεικόνιση μια απλής διαδικασίας κρυπτογράφησης με κλειδί



5.1 Συμμετρική κρυπτογράφηση (Symmetric key encryption)

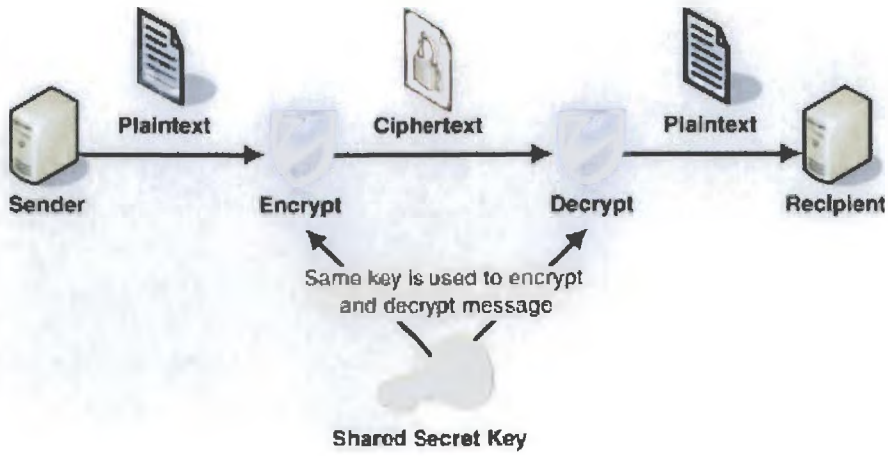
Η κρυπτογράφηση ιδιωτικού κλειδιού ή συμμετρική κρυπτογράφηση βασίζεται σε ένα κοινό κλειδί το οποίο διαμοιράζεται μεταξύ των συναλλασσομένων μερών. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των μηνυμάτων . Ο Kerberos και το Data Encryption Standard είναι οι πλέον παραδοσιακές τεχνολογίες ιδιωτικού κλειδιού.

Η συμμετρική κρυπτογραφία έχει ως μοναδικό σκοπό της τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών και είναι κατάλληλη για μετατροπές μεγάλου όγκου δεδομένων επειδή οι υπολογισμοί που απαιτεί εκτελούνται πολύ γρήγορα.

Το βασικό πρόβλημα της κρυπτογράφησης του τύπου αυτού αφορά τη δημιουργία, την αποθήκευση και την μετάδοση του μυστικού κλειδιού (key management). Συγκεκριμένα:

- Και τα δύο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί.
- Κάθε χρήστης θα πρέπει να έχει τόσα μυστικά κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται.
- Δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μερών. Από την στιγμή που δύο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δύο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άλλο άτομο. Κατά συνέπεια, η μη αποποίηση της ευθύνης (non-repudation) για την αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με την κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση.

Διαδικασία συμμετρικής κρυπτογράφησης



5.2 Ασύμμετρη κρυπτογράφηση (Asymmetric key encryption)

Η κρυπτογράφηση δημοσίου κλειδιού βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό ενώ το άλλο είναι ιδιωτικό. Στην κρυπτογράφηση δημοσίου κλειδιού οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί.

Τα δύο αυτά κλειδιά μπορούν να χρησιμοποιηθούν με δύο διαφορετικούς τρόπους: για να εξασφαλίσουν την εμπιστευτικότητα του μηνύματος και να αποδείξουν την αυθεντικότητα του δημιουργού του.

Στην πρώτη περίπτωση, για την παραγωγή ενός εμπιστευτικού μηνύματος, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα, έτσι ώστε να παραμείνει απόρρητο έως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη.

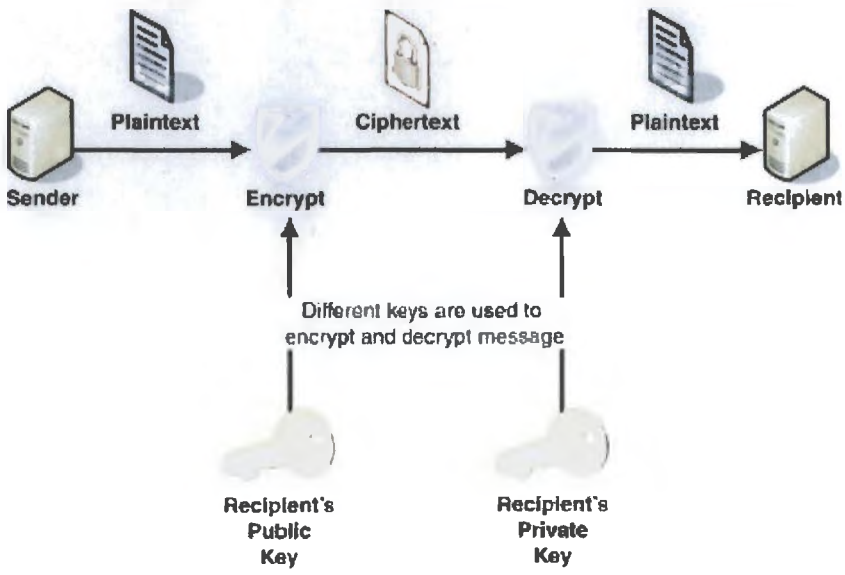
Στην δεύτερη περίπτωση, ο αποστολέας κωδικοποιεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Το ιδιωτικό κλειδί αποδεικνύει την ταυτότητα του χρήστη (αυθεντικοποίηση). Δηλαδή, η χρήση ιδιωτικού κλειδιού για την κρυπτογράφηση ενός μηνύματος είναι αντίστοιχη με την προσθήκη της υπογραφής του αποστολέα σε κάποιο έγγραφο. Έτσι λοιπόν οποιοσδήποτε χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει το μήνυμα θα είναι σίγουρος για την ταυτότητα του πρώτου.

Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημοσίου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει.

Η κρυπτογράφηση δημοσίου κλειδιού θεωρείται κατάλληλη για το ηλεκτρονικό εμπόριο για τους εξής λόγους :

- Εξασφαλίζει την εμπιστευτικότητα του μηνύματος.
- Παρέχει πιο ευέλικτα μέσα αυθεντικοποίησης των χρηστών.
- Υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος).

Διαδικασία ασύμμετρης κρυπτογράφησης



5.2.1 Εφαρμογές Κρυπτογραφίας Δημοσίου Κλειδιού

Η ασύμμετρη κρυπτογραφία αποτελεί τεχνολογικά τον ακρογωνιαίο λίθο σε πολλές εφαρμογές και μηχανισμούς ασφάλειας στο Διαδίκτυο, όπως:

- Υποδομές Πιστοποίησης, οι οποίες διαχειρίζονται ψηφιακά πιστοποιητικά έμπιστων τρίτων φορέων, με σκοπό την αναγνώριση και πιστοποίηση της ταυτότητας των χρηστών (πιστοποιητικά ταυτότητας), αλλά και τον έλεγχο των εξουσιοδοτήσεών τους (πιστοποιητικά χαρακτηριστικών).

- Ασφαλής παρουσίαση ιστοσελίδων αλλά και δικτυακών αγορών, βάσει του πρωτοκόλλου SSL (Secure Sockets Layer) της Netscape αλλά και του πρωτοκόλλου TLS (Transport Layer Security) της IETF (Internet Engineering Task Force).

- Ασφαλείς συναλλαγές μέσω πιστωτικών καρτών, βάσει του πρωτοκόλλου SET (Secure Electronic Transactions) των VISA και Mastercard.

- Ασφαλής ηλεκτρονική αλληλογραφία, βάσει του πρωτοκόλλου S/MIME (Secure Multipurpose Internet Mail Extensions) της IETF.

5.3 Γνωστοί Αλγόριθμοι κρυπτογράφησης

Μερικοί από τους πιο γνωστούς και χρησιμοποιήσιμους αλγόριθμους κρυπτογράφησης είναι οι παρακάτω:

- DES - Data Encryption Standard

Είναι ένα σώμα κρυπτογραφικών εντολών που δημιουργήθηκε από την IBM και πήρε έγκριση από την Αμερικάνικη κυβέρνηση το 1977. Χρησιμοποιεί ένα 56-bit κλειδί και χρησιμοποιεί μια ομάδα από 64 bits. Είναι σχετικά γρήγορος αλγόριθμος και χρησιμοποιείται για την κρυπτογράφηση μεγάλου όγκου δεδομένων, ταυτόχρονα.

- Triple DES

Βασίζεται στον DES αλγόριθμο. Κρυπτογραφεί μια ομάδα δεδομένων τρεις φορές, με τρία διαφορετικά κλειδιά. Έχει προταθεί σαν εναλλακτική λύση αντί του DES, γιατί υποστηρίζεται ότι τον τελευταίο καιρό έχει γίνει πιο εύκολο και πιο γρήγορο το "σπάσιμο" του DES αλγόριθμου.

- RC2 και RC4

Σχεδιάστηκαν από τον Ron Rivest (από εκεί προέρχεται το R στην RSA Data Security Inc.) . Παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού κρυπτογράφησης, για πολύ γρήγορη και μεγάλου όγκου κρυπτογράφηση. Οι δύο αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DES και μπορούν να γίνουν ακόμα πιο ασφαλείς αν επιλέξουμε μεγαλύτερο μήκος κλειδιού. Ο αλγόριθμος RC2 αποτελεί μια ομάδα (block) κρυπτογράφησης και μπορεί να χρησιμοποιηθεί στην θέση του DES. Ο RC4 είναι ένα "ρεύμα" (stream) ψηφίων κρυπτογράφησης και θεωρείται περίπου 10 φορές πιο γρήγορος από τον DES.

- IDEA

Ο International Data Encryption Algorithm δημιουργήθηκε το 1991 και σχεδιάστηκε για να είναι ικανός για πραγματοποίηση υπολογισμών στο λογισμικό. Προσφέρει πολύ δυνατή κρυπτογράφηση, χρησιμοποιώντας ένα 128-bit κλειδί.

- RSA

Ονομάστηκε έτσι από τους σχεδιαστές του, Rivest, Shamir και Adelman. Είναι ένας αλγόριθμος "δημόσιου κλειδιού" (public-key) ο οποίος υποστηρίζει μια ποικιλία μήκους κλειδιών, καθώς επίσης ποικιλία όσον αφορά το μέγεθος του σώματος του κειμένου προς κρυπτογράφηση. Το απλό block κειμένου πρέπει να είναι μικρότερο από το μήκος του κλειδιού. Το συνηθισμένο μήκος κλειδιού είναι 512 bits.

- Diffie-Hellman

Αποτελεί το παλιότερο "δημόσιου κλειδιού" σύστημα κρυπτογραφίας, που ακόμα χρησιμοποιείται. Δεν υποστηρίζει κρυπτογράφηση ή ψηφιακές υπογραφές. Το σύστημα έχει σχεδιαστεί για να επιτρέπει στις δύο πλευρές να συμφωνούν με την χρήση ενός κατανεμημένου κλειδιού (shared key) , ακόμα και αν το μόνο που κάνουν είναι να ανταλλάσσουν μηνύματα δημοσίως.

- DSA

Ο Digital Signature Algorithm σχεδιάστηκε από την NIST και στηρίχθηκε πάνω σε αυτό που αποκαλείται El Gamal αλγόριθμος. Το σχήμα των υπογραφών χρησιμοποιεί το ίδιο είδος κλειδιών που χρησιμοποιεί και ο Diffie - Hellman αλγόριθμος και μπορεί να δημιουργήσει υπογραφές πιο γρήγορα από τον RSA. Έχοντας προωθηθεί από την NIST ως ένα DSS σύστημα, το Digital Signature Standard, παρόλη την αποδοχή του, απέχει ακόμα πολύ από το να παρέχει σιγουριά.

5.4 Κρυπτογραφική δύναμη των συμμετρικών αλγορίθμων

Οι διαφορετικοί αλγόριθμοι κρυπτογράφησης δεν είναι ίσοι. Μερικά συστήματα δεν είναι πολύ καλά στην προστασία των στοιχείων, επιτρέποντας στις κρυπτογραφημένες πληροφορίες να αποκρυπτογραφηθούν χωρίς τη γνώση του απαραίτητου κλειδιού. Άλλοι είναι αρκετά ανθεκτικοί ακόμη και στην πιο απλή επίθεση. Η δυνατότητα ενός κρυπτογραφικού συστήματος να προστατεύσει τις πληροφορίες από μια επίθεση καλείται ως η δύναμή του. Η δύναμη αυτή εξαρτάται από πολλούς παράγοντες, που περιλαμβάνουν:

- την μυστικότητα του κλειδιού
- την δυσκολία να μαντέψει κάποιος το κλειδί ή όλα τα πιθανά κλειδιά. Τα μεγαλύτερα σε μήκος κλειδιά είναι γενικά δυσκολότερο να βρεθούν ή να τα μαντέψει
- την δυσκολία αποκάλυψης του αλγόριθμου κρυπτογράφησης χωρίς γνώση του κλειδιού κρυπτογράφησης (το "σπάσιμο" του αλγόριθμου κρυπτογράφησης)
- την ύπαρξη (ή έλλειψη) πίσω πορτών (backdoors), ή πρόσθετοι τρόποι από την οποία ένα κρυπτογραφημένο αρχείο μπορεί να αποκρυπτογραφηθεί ευκολότερα χωρίς γνώση του κλειδιού.
- την δυνατότητα να αποκρυπτογραφηθεί ένα ολόκληρο κρυπτογραφημένο μήνυμα εάν ξέρετε τον τρόπο με τον οποίο αποκρυπτογραφείται (η μέθοδος είναι γνωστή ως επίθεση "plaintext")
- τις ιδιότητες του plaintext (απλού κειμένου) και της γνώσης εκείνων των ιδιοτήτων από έναν επιτιθέμενο. Παραδείγματος χάριν, ένα κρυπτογραφικό σύστημα μπορεί να είναι τρωτό στην επίθεση εάν όλα τα μηνύματα που κρυπτογραφούνται αρχίζουν ή τελειώνουν με ένα γνωστό κομμάτι του plaintext. Αυτά τα είδη τακτικών χρησιμοποιήθηκαν από τους συμμάχους για να "σπάσουν" το γερμανικό Enigma κατά τη διάρκεια του παγκόσμιου πολέμου II.

Γενικά, η κρυπτογραφική δύναμη δεν αποδεικνύεται. Όταν ένας νέος αλγόριθμος κρυπτογράφησης προτείνεται, ο συντάκτης του αλγορίθμου σχεδόν πάντα θεωρεί ότι ο αλγόριθμος προσφέρει τη "τέλεια" ασφάλεια, δηλαδή ο συντάκτης θεωρεί ότι δεν υπάρχει κανένας τρόπος να αποκρυπτογραφηθεί ένα κρυπτογραφημένο μήνυμα χωρίς κατοχή του αντίστοιχου κλειδιού. Τελικά, εάν ο αλγόριθμος περιείχε μια γνωστή ρωγμή, κατόπιν ο συντάκτης δεν θα πρότεινε τον αλγόριθμο αρχικά (ή τουλάχιστον δεν θα τον πρότεινε με καλή συνείδηση).

Ως τμήμα της παρουσίασης αποδείξεων της δύναμης ενός αλγορίθμου, ένας μαθηματικός μπορεί να δείξει ότι ο αλγόριθμος είναι ανθεκτικός στα συγκεκριμένα είδη επιθέσεων που έχουν αποδειχθεί προηγουμένως για να παραβιάσουν άλλους αλγορίθμους. Δυστυχώς, ούτε ένας αλγόριθμος που είναι ανθεκτικός σε κάθε γνωστή επίθεση δεν είναι απαραιτήτως ασφαλής, επειδή οι νέες επιθέσεις αναπτύσσονται συνεχώς.

Κατά διαστήματα, μερικά άτομα ή εταιρίες υποστηρίζουν ότι έχουν εφεύρει τους νέους συμμετρικούς αλγορίθμους κρυπτογράφησης που είναι εντυπωσιακά ασφαλέστεροι από τους υπάρχοντες αλγορίθμους. Γενικά, αυτοί οι αλγόριθμοι πρέπει να αποφευχθούν. Δεδομένου ότι δεν υπάρχει καμία γνωστή επίθεση ενάντια στους αλγορίθμους κρυπτογράφησης που είναι σε ευρεία χρήση σήμερα, δεν υπάρχει κανένας λόγος να χρησιμοποιηθούν οι νέοι, μη αποδεδειγμένοι αλγόριθμοι κρυπτογράφησης που μπορεί να έχουν ρωγμές.

5.5 Επιθέσεις στους συμμετρικούς αλγορίθμους κρυπτογράφησης

Εάν πρόκειται να χρησιμοποιήσετε το σύστημα της κρυπτογραφίας για να προστατεύσετε τις πληροφορίες, κατόπιν πρέπει να υποθέσετε ότι οι άνθρωποι που δεν επιθυμείτε να έχουν πρόσβαση στις πληροφορίες σας θα καταγράφουν τα κρυπτογραφημένα στοιχεία και θα προσπαθούν να τα αποκρυπτογραφήσουν βίαια. Για να είναι χρήσιμο, το κρυπτογραφικό σύστημά σας πρέπει να είναι ανθεκτικό σε αυτό το είδος άμεσης επίθεσης.

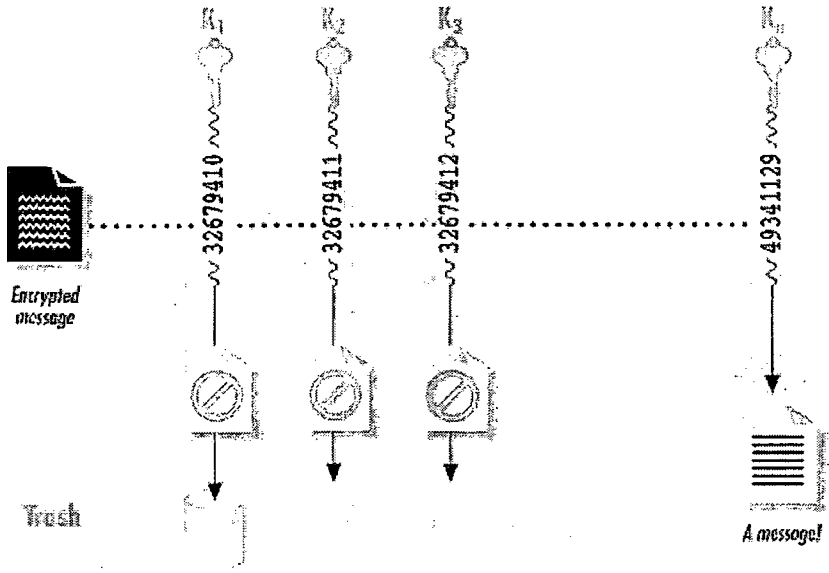
Επιθέσεις ενάντια στην κρυπτογραφημένη πληροφορία χωρίζονται στις ακόλουθες κατηγορίες:

- Brute force attacks επιθέσεις (βασικής αναζήτησης)
- Cryptanalysis επιθέσεις (κρυπτολογική ανάλυση)

5.5.1 Brute force attacks επιθέσεις (βασικής αναζήτησης)

Ο απλούστερος τρόπος να επιτεθεί κάποιος σε ένα κρυπτογραφημένο μήνυμα είναι απλά να προσπαθήσει να αποκρυπτογραφήσει το μήνυμα με κάθε πιθανό κλειδί. Οι περισσότερες προσπάθειες θα αποτύχουν, αλλά τελικά μια από τις δοκιμές θα πετύχει και είτε θα επιτρέψει στον εισβολέα την είσοδο στο σύστημα είτε θα επιτρέψει την αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος. Δεν υπάρχει κανένας τρόπος για την προστασία από αυτού του είδους τις επιθέσεις επειδή δεν υπάρχει τρόπος για την εμπόδιση κάποιου από το να δοκιμάσει να αποκρυπτογραφήσει ένα μήνυμα με κάθε πιθανό κλειδί.

Απεικόνιση της λειτουργίας επίθεσης brute force



Οι brute force attacks (βασικές επιθέσεις αναζήτησης) δεν είναι πολύ αποδοτικές, διότι, εάν το επιλεγμένο κλειδί είναι αρκετά μεγάλο, μια τέτοιου είδους επίθεση δεν μπορεί να είναι εφικτή. Για παράδειγμα με ένα κλειδί των 128-bit και οποιαδήποτε κατανοητή τεχνολογία υπολογισμού, η ζωή στη γη θα πάψει να υπάρχει πολύ πριν ακόμη ένα κλειδί να είναι πιθανό να σπάσει.

Κατ' εκτίμηση επιτυχία των επιθέσεων αναζήτησης
(για τους διαφορετικούς αριθμούς bits στο κλειδί και τον αριθμό κλειδιών που μπορούν να δοκιμαστούν ανά δευτερόλεπτο)

Length of key	Keys searched per second	Postulated key searching technology[8]	Approximate time to search all possible keys
40 bits[9]	10	10-year-old desktop computer	3,484 years
40 bits	1,000	Typical desktop computer today	35 years
40 bits	1 million	Small network of desktops	13 days
40 bits	1 billion	Medium-sized corporate network	18 minutes
56 bits	1 million	Desktop computer a few years from-now	2,283 years
56 bits	1 billion	Medium-sized corporate network	2.3 years
56 bits[10]	100 billion	DES-cracking machine	8 days
64 bits	1 billion	Medium-sized corporate network	585 years
80 bits	1 million	Small network of desktops	38 billion years
80 bits	1 billion	Medium-sized corporate network	38 million years
128 bits	1 billion	Medium-sized corporate network	10^{22} years
128 bits	1 billion billion (1×10^{18})	Large-scale Internet project in the year 2005	10,783 billion years
128 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	108 million years
192 bits	1 billion	Medium-sized corporate network	2×10^{41} years
192 bits	1 billion billion	Large-scale Internet project in the year 2005	2×10^{32} years
192 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	2×10^{27} years
256 bits	1×10^{23}	Special-purpose quantum computer, year 2015?	3.7×10^{46} years
256 bits	1×10^{32}	Special-purpose quantum computer, year 2040?	3.7×10^{37} years

5.5.2 Κρυπτολογική ανάλυση (Cryptanalysis)

Εάν το βασικό μήκος ήταν ο μόνος παράγοντας που καθορίζει την ασφάλεια , ο καθένας ενδιαφερόμενος στην ανταλλαγή των μυστικών μηνυμάτων θα χρησιμοποιούσε απλά τους κώδικες με τα 128-bit κλειδιά, και όλοι οι κρυπταναλυτές (άνθρωποι που σπάζουν τους κώδικες) θα έπρεπε να βρούν άλλους τρόπους απασχόλησης.

Αυτό που κρατά το σύστημα της κρυπτογραφίας σε ενδιαφέρον είναι το γεγονός ότι οι περισσότεροι αλγόριθμοι κρυπτογράφησης δεν αντέχουν μέχρι εκεί που επιθυμούμε.. Οι βασικές επιθέσεις αναζήτησης απαιτούνται σπάνια για να αποκαλύψουν το περιεχόμενο ενός κρυπτογραφημένου μηνύματος. Αντί αυτού, οι περισσότεροι αλγόριθμοι κρυπτογράφησης μπορούν να νικηθούν με τη χρησιμοποίηση ενός συνδυασμού περίπλοκης δύναμης μαθηματικών και υπολογισμού. Το αποτέλεσμα είναι ότι πολλά κρυπτογραφημένα μηνύματα μπορούν να αποκρυπτογραφηθούν χωρίς γνώση του κλειδιού. Ένα επιδέξιος κρυπταναλυτής cryptanalyst μπορεί μερικές φορές να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο χωρίς ακόμη και να ξέρει τον αλγόριθμο κρυπτογράφησης.

Μια επίθεση αυτής της κατηγορίας μπορεί να έχει δύο πιθανούς στόχους. Ο κρυπταναλυτής να έχει το κρυπτογράφημα και να θελήσει να ανακαλύψει το plaintext, ή να έχει το κρυπτογράφημα και να θελήσει να ανακαλύψει το κλειδί κρυπτογράφησης που χρησιμοποιήθηκε για να το κρυπτογραφήσει. Οι ακόλουθες επιθέσεις χρησιμοποιούνται συνήθως όταν είναι γνωστός ο αλγόριθμος κρυπτογράφησης, και μπορούν να εφαρμοστούν στην κυκλοφορία του διαδικτύου:

5.5.3 Γνωστή plaintext επίθεση (Known plaintext attack)

Σε αυτόν τον τύπο επίθεσης, ο κρυπταναλυτής έχει ένα κομμάτι του plaintext και ένα αντίστοιχο κομμάτι του κρυπτογραφήματος. Αν και αυτό μπορεί να φανεί ένα απίθανο περιστατικό, είναι πραγματικά αρκετά κοινό όταν χρησιμοποιείται το σύστημα κρυπτογραφίας για να προστατεύσει το ηλεκτρονικό ταχυδρομείο (με τις τυποποιημένες επιγραφές στην αρχή κάθε μηνύματος), τα τυποποιημένα έντυπα, ή τους σκληρούς δίσκους (με τις γνωστές δομές στις προκαθορισμένες θέσεις σε δίσκο). Ο στόχος μιας γνωστής plaintext επίθεσης είναι να καθοριστεί το κρυπτογραφικό κλειδί (και ενδεχομένως ο αλγόριθμος), το οποίο μπορεί έπειτα να χρησιμοποιηθεί για την αποκρυπτογράφηση άλλων μηνυμάτων.

5.5.4 Επιλεγμένη plaintext επίθεση (Chosen plaintext attack)

Οι επιλεγμένες plaintext επιθέσεις είναι απλούστερες να πραγματοποιηθούν από το να εμφανιστούν. (Παραδείγματος χάριν, το θέμα της επίθεσης να είναι μια ράδιο-σύνδεση που κρυπτογραφεί και αναμεταδίδει τα μηνύματα που παραλαμβάνονται τηλεφωνικώς.) Ο στόχος μιας επιλεγμένης plaintext επίθεσης είναι να καθοριστεί το κρυπτογραφικό κλειδί, το οποίο μπορεί έπειτα να χρησιμοποιηθεί για να αποκρυπτογραφήσει άλλα μηνύματα.

5.5.5 Διαφορική κρυπτολογική ανάλυση (Differential cryptanalysis)

Αυτή η επίθεση, που είναι μια μορφή επιλεγμένης plaintext επίθεσης, περιλαμβάνει την κρυπτογράφηση πολλών κειμένων που είναι μόνο ελαφρώς διαφορετικά μεταξύ τους και γίνεται σύγκριση των αποτελεσμάτων.

5.5.6 Διαφορική ανάλυση ελαττωμάτων (Differential fault analysis)

Αυτή η επίθεση λειτουργεί ενάντια στα κρυπτογραφικά συστήματα που χτίζονται στο υλικό. Η συσκευή υποβάλλεται στους περιβαλλοντικούς παράγοντες (θερμότητα, πίεση, ακτινοβολία) με σκοπό να πείσουν τη συσκευή στην παραγωγή των λαθών κατά τη διάρκεια της κρυπτογράφησης ή της λειτουργίας αποκρυπτογράφησης. Αυτά τα ελαττώματα μπορούν να αναλυθούν και από αυτά το εσωτερικό καθεστώς της συσκευής, συμπεριλαμβανομένου του κλειδιού κρυπτογράφησης ή του αλγόριθμος, πού μπορεί ενδεχομένως να μαθευτεί.

5.5.7 Διαφορική ανάλυση δύναμης (Differential power analysis)

Αυτή είναι μια άλλη επίθεση ενάντια σε κρυπτογραφικό υλικό και στις έξυπνες κάρτες. Με την παρατήρηση της δύναμης που μια έξυπνη κάρτα χρησιμοποιεί για να κρυπτογραφήσει έναν επιλεγμένο κομμάτι των δεδομένων, είναι δυνατό να μαθευτούν λίγες πληροφορίες για τη δομή του μυστικού κλειδιού.

5.5.8 Διαφορική ανάλυση συγχρονισμού (Differential timing analysis)

Αυτή η επίθεση είναι παρόμοια με τη διαφορική ανάλυση δύναμης, εκτός από το ότι ο επιτιθέμενος ελέγχει προσεκτικά το χρόνο που η έξυπνη κάρτα παίρνει για να εκτελέσει τις ζητούμενες διαδικασίες κρυπτογράφησης.

5.6 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. Στο ανοικτό περιβάλλον του διαδικτύου, 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. Επιπλέον, η ηλεκτρονική υπογραφή πρέπει να δημιουργείται και να αναγνωρίζεται εύκολα, ενώ δύσκολα να πλαστογραφείται. Οι ηλεκτρονικές υπογραφές που βασίζονται στη κρυπτογραφία δημοσίου κλειδιού, ονομάζονται ψηφιακές υπογραφές (digital signatures).

Δημιουργία και επαλήθευση ψηφιακών υπογραφών

Ένα ασφαλές σύστημα παροχής ψηφιακών υπογραφών αποτελείται από δύο μέρη. Στον μεν αποστολέα πραγματοποιείται η μέθοδος υπογραφής ενός κειμένου με "ορθό" τρόπο, στον δε παραλήπτη πραγματοποιείται η μέθοδος επαλήθευσης αν η ψηφιακή υπογραφή παράχθηκε από αυτόν που πραγματικά αντιπροσωπεύει. Η ψηφιακή υπογραφή δημιουργείται από ένα ιδιωτικό κλειδί. Ένα δημόσιο κλειδί χρησιμοποιείται για να επαληθευθεί ότι η υπογραφή δημιουργήθηκε χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί. Η ψηφιακή υπογραφή δημιουργείται κατά τέτοιο τρόπο ώστε να είναι αδύνατο να παραχθεί και πάλι η ίδια ψηφιακή υπογραφή χωρίς τη γνώση του ιδιωτικού κλειδιού.

Το παρακάτω σχήμα είναι αναπαράσταση της δημιουργίας ψηφιακής υπογραφής. Ο υπογράφων παράγει μια αφομοίωση μηνυμάτων των στοιχείων και χρησιμοποιεί έπειτα ένα ιδιωτικό κλειδί για να κρυπτογραφήσει την αφομοίωση. Η υπογραφή περιλαμβάνει την κρυπτογραφημένη αφομοίωση και τις πληροφορίες για το ψηφιακό πιστοποιητικό του υπογράφοντος. Το πιστοποιητικό χρησιμοποιείται για να ελέγξει την υπογραφή, περιλαμβάνει το δημόσιο κλειδί που απαιτείται για να αποκρυπτογραφήσει την αφομοίωση και τον αλγόριθμο που χρησιμοποιούνται για να την δημιουργήσει. Για να ελέγξει ότι το υπογεγραμμένο έγγραφο δεν έχει αλλάξει, ο παραλήπτης χρησιμοποιεί τον αλγόριθμο για να δημιουργήσει το δικό του αφομοιωμένο μήνυμα και χρησιμοποιεί το δημόσιο κλειδί για να αποκρυπτογραφήσει την αφομοίωση στην υπογραφή. Εάν οι δύο αφομοιώσεις είναι ίδιες, σημαίνει ότι το μήνυμα δεν έχει δεχτεί τροποποίηση και πρέπει να έχει σταλεί από τον ιδιοκτήτη του δημόσιου κλειδιού.

Digest: αφομοίωση
Hash: αλγόριθμος κρυπτογράφησης
Encrypted Digest: κρυπτογραφημένη αφομοίωση
Signed Document: υπογεγραμμένο έγγραφο
Certificate: πιστοποιητικό
Public Key: δημόσιο κλειδί
Pricate Key: ιδιωτικό κλειδί
ο κόκκινο χρώμα δείχνει την ιδιοκτησία

5.7 Ψηφιακά Πιστοποιητικά

Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί μια διαδεδομένη τεχνολογία εφαρμογής της αυθεντικοποίησης που βασίζεται σε κάτι που ο χρήστης κατέχει. Τα ψηφιακά πιστοποιητικά έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στη κρυπτογραφία δημόσιου κλειδιού.
Μπορούν να χρησιμοποιηθούν για τον περιορισμό της αποκάλυψης της ταυτότητας του χρήστη ενσωματώνοντας ψευδώνυμα αντί της πραγματικής ταυτότητάς του.

Υπάρχουν διάφορα πρότυπα ψηφιακών πιστοποιητικών όπως:

- PKIX (Internet PKI based on X.509): Το PKIX είναι μια σειρά από προσχέδια για το διαδίκτυο που περιγράφουν διάφορα θέματα σχετικά με την ανάπτυξη μια ιεραρχικής Υποδομής Δημοσίου Κλειδιού (ΥΔΚ), Τα προσχέδια του PKIX αναπτύχθηκαν εξαιτίας του γεγονότος ότι το X.509 είναι ένα γενικό πρότυπο, το οποίο αφήνει πολλά κενά που σχετίζονται με τη πραγματική λειτουργία και διαχείριση μιας Έμπιστης Τρίης Οντότητας (ΕΤΟ).

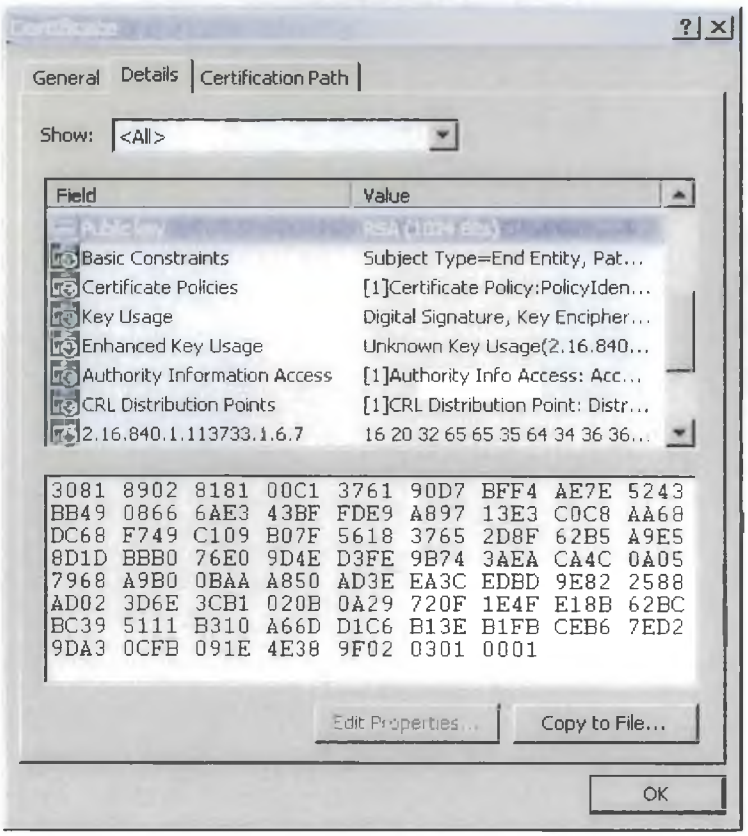
- SPKI (Simple Public Key Infrastructure): Περιγράφει τα πιστοποιητικά, τις απαιτήσεις, τις λειτουργίες και τα παραδείγματα χρήσης για μια υποδομή δημόσιου κλειδιού μη καθολικού χαρακτήρα, για χρήση σε περιορισμένα πεδία εφαρμογής. Ενώ το X.509 αντιστοιχίζει δημόσια κλειδιά με ονόματα, το SPKI χρησιμοποιεί πιστοποιητικά που έχουν ως κωδικό αναφοράς το δημόσιο κλειδί αντί για το όνομα και αντιστοιχούν σε ρόλους και όχι σε πρόσωπα. Επιπλέον κατά το πρότυπο αυτό τα διακριτικά ονόματα έχουν τοπικό χαρακτήρα και όχι οικουμενικό όπως αυτά που βασίζονται στις υπηρεσίες ευρετηρίου του X.500.

- PGP (Pretty Good Privacy): Το PGP θαμπορούσε να ονομαστεί πρότυπο αλλάς την πραγματικότητα είναι μια ευρέως αποδεκτή εφαρμογή που προσδίδει χαρακτηριστικά ασφάλειας στην ηλεκτρονική αλληλογραφία. Σύμφωνα με το PGP, κάθε χρήστης δημιουργεί το προσωπικό οτυ πιστοποιητικό και το καταχωρεί σε ένα κεντρικό ευρετήριο. Δεν υπάρχει έμπιστη τρίη οντότητα ενώ η εμπιστοσύνη προς την ακρίβεια του περιεχομένου του πιστοποιητικού εδραιώνεται μεταξύ των χρηστών, εφόσον ένας χρήστης υπογράψει το πιστοποιητικό ενός άλλου. Συνεπώς δημιουργούνται Ν προς Ν σχέσεις εμπιστοσύνης, σχηματίζοντας ένα πλέγμα εμπιστοσύνης (web of trust). Το ρόλο του διακριτικού ονόματος παίζει εδώ το όνομα της ηλεκτρονικής αλληλογραφίας, η οποία είναι μεν οικουμενικά μοναδική αλλά έχει το μειονέκτημα ότι αλλάζει συχνά.

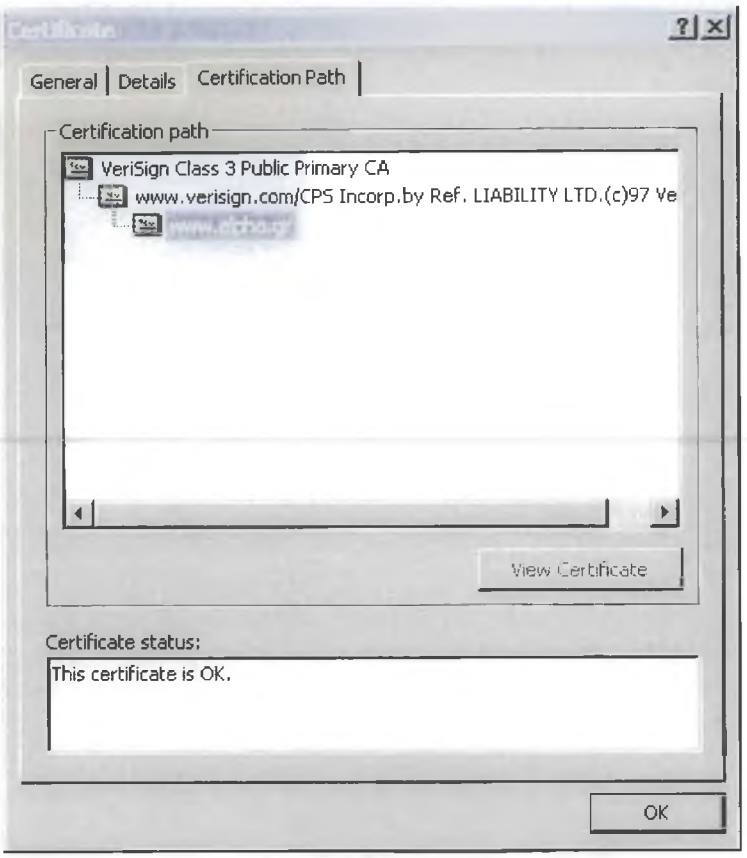
Όταν βρισκόμαστε σε μία ιστοσελίδα μπορούμε να λάβουμε πληροφορίες για το αν γίνεται χρήση κάποιου πιστοποιητικού ασφάλειας ή όχι.

Στον Internet Explorer αλλά και στον Netscape Navigator κάνουμε τα παρακάτω: επιλέγουμε File-Properties και στο παράθυρο που μας εμφανίζεται επιλέγουμε το Certificates. Στην περίπτωση που χρησιμοποείται πιστοποιητικό ασφάλειας θα εμφανιστεί ένα παράθυρο με πληροφορίες για το πιστοποιητικό όπως είναι το ακόλουθο.

Επιλέγοντας το details μας δίνονται λεπτομερειακά στοιχεία για το δημόσιο κλειδί και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται.



Τέλος επιλέγοντας το certification path μας δίνονται στοιχεία για την διαδρομή πιστοποίησης και μια αναφορά κατάστασης η οποία λέει αν το πιστοποιητικό είναι έγκυρο ή όχι.



6 Πρωτόκολλα ασφαλής επικοινωνίας στο Internet

Σήμερα υπάρχουν πολλά πρωτόκολλα που υπόσχονται ασφαλή μετακίνηση των δεδομένων μεταξύ δικτύων. Η επιλογή μπορεί να γίνει μεταξύ των:

- Secure HyperText Transport Protocol (S-HTTP)
- Secure Sockets layer (SSL)
- Private Communication Technology (PCT).
- Secure Electronic Transaction (SET)

Για μια εταιρία που ασχολείται με online εφαρμογές στο διαδίκτυο, υπάρχουν δύο επιλογές: το S-HTTP και το SSL. Για περισσότερη ασφάλεια σε ένα περιβάλλον διαδικτύου υπάρχει το πρωτόκολλο SSL, το οποίο είναι ενσωματωμένο στην στους περισσότερους web browsers.. Το SSL θεωρείται πιο ασφαλές από το S-HTTP διότι δεν ασφαλίζει τις συνδέσεις στο HTTP επίπεδο, αλλά στο IP-sockets επίπεδο. Αυτό σημαίνει ότι το SSL μπορεί να κρυπτογραφήσει, να αυθεντικοποιήσει και να πιστοποιήσει όλα τα πρωτόκολλα που υποστηρίζονται από έναν web browser με SSL δυνατότητες, (ftp, telnet, e-mail)

Για συναλλαγές που παρέχουν ρουτίνες αυθεντικοποίησης και κρυπτογράφησης υλοποιώντας online εμπόριο με πιστωτικές κάρτες, το πρωτόκολλο PCT της Microsoft είναι μια αρκετά ασφαλής λύση.

Τέλος λιγότερο διαδεδομένο, αλλά όχι λιγότερο αποτελεσματικό είναι το πρωτόκολλο SET, που αναπτύχθηκε από τις Visa International και MasterCard International Inc. Το SET παρέχει στους online τραπεζικούς πελάτες ένα ασφαλές περιβάλλον για οικονομικές συναλλαγές.

6.1 Το πρωτόκολλο S-HTTP

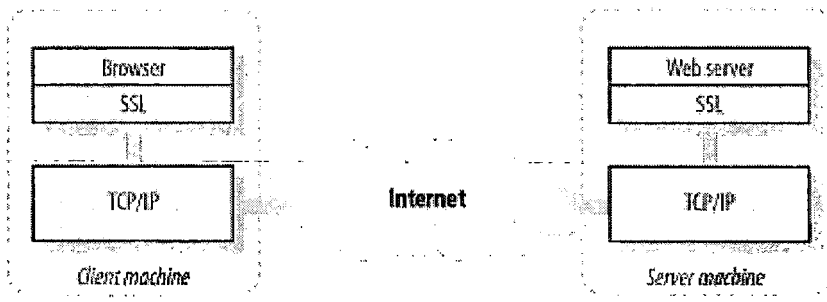
Το πρωτόκολλο S-HTTP ενεργεί στο επίπεδο εφαρμογής, εκτελείται ουσιαστικά σαν μια ξεχωριστή εφαρμογή στο επίπεδο του HTTP και παρέχει κρυπτογράφηση, αυθεντικοποίηση και υπογραφή καθώς και οποιονδήποτε συνδυασμό εξ'αυτών. Ένα από τα πλεονεκτήματα του S-HTTP είναι ότι μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση συγκεκριμένων δεδομένων σε μια Web σελίδα. Έτσι, για παράδειγμα, τα δεδομένα ενός field μιας HTML φόρμας που θα αποτελέσουν input σε ένα cgi script και τα οποία κρίνονται εμπιστευτικά, μπορούν να κρυπτογραφηθούν (ή/και υπογραφούν), ενώ τα υπόλοιπα δεδομένα της HTML φόρμας θα μεταφερθούν στον server μη κρυπτογραφημένα. Έτσι, η ταχύτητα της όλης διαδικασίας είναι ικανοποιητική.

Παράλληλα, το S-HTTP παρέχει έναν απλό μηχανισμό πρόκλησης-απάντησης (challenge-response), επιτρέποντας στα δύο συμβαλλόμενα μέρη να βεβαιωθούν για την επικαιρότητα των μηνυμάτων. Έτσι, εάν ένα S-HTTP μήνυμα περιέχει ένα timestamp, ο αποδέκτης του πρέπει να το συμπεριλάβει στην απάντησή του. Για μεγαλύτερη ταχύτητα και απόδοση, τα documents μπορούν να προ-υπογραφούν και προ-κρυπτογραφηθούν.

6.2 Το πρωτόκολλο SSL

Το πρωτόκολλο SSL καθιερώθηκε ως de facto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων και βασίζεται σε κρυπτογραφικές τεχνικές δημόσιου κλειδιού. Σκοπός του είναι η προστασία πρωτοκόλλων υψηλότερου επιπέδου. Στην ιεραρχία των πρωτοκόλλων, το πρωτόκολλο SSl βρίσκεται ακριβώς επάνω από το επίπεδο δικτύου και κάτω από το επίπεδο εφαρμογής. Χρησιμοποιείται ευρέως σε ενδοδίκτυα (intranets) αλλά και στο internet, κυρίως σε συναλλαγές ηλεκτρονικού εμπορίου.

Το σχήμα δείχνει την αρχιτεκτονική τοποθέτηση του SSL



Συνοπτικά μπορεί να αναφερθεί ότι το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού
- Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων, αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων , καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς

Για να χρησιμοποιηθεί το SSL θα πρέπει τόσο ο εξυπηρετούμενος όσο και ο εξυπηρέτης να γνωρίζουν ότι η άλλη πλευρά επίσης χρησιμοποιεί SSL. Γενικά υπάρχουν τρεις δυνατές λύσεις για την αντιμετώπιση αυτού του ζητήματος:

- Η πρώτη είναι να χρησιμοποιηθούν αφιερωμένοι αριθμοί θυρών (ports). Θα πρέπει να ανατίθεται ένας ξεχωριστός αριθμός θύρας για κάθε πρωτόκολλο εφαρμογής που υποστηρίζει SSL
- Η δεύτερη είναι να χρησιμοποιείται κανονικός αριθμός θύρας για κάθε πρωτόκολλο εφαρμογής και να συμφωνούνται επιλογές ασφάλειας ως μέρος του πρωτοκόλλου εφαρμογής και

Η τρίτη δυνατότητα είναι να χρησιμοποιείται μια επιλογή TCP για τη χρήση ενός πρωτοκόλλου ασφάλειας, όπως το SSL, κατά τη διάρκεια της φάσης καθιέρωσης της κανονικής TCP/IP σύνδεσης

Το SSL αποτελείται από δύο υπο-πρωτόκολλα, το SSL Record Protocol και το SSL Handshake Protocol. Το SSL Record Protocol ορίζει το βασικό format των δεδομένων που ανταλλάσσονται σε κάθε session. Επίσης είναι αυτό που κάνει τη συμπίεση των δεδομένων, κάνει τον έλεγχο ακεραιότητας και κρυπτογραφεί τα δεδομένα. Προκειμένου το SSL Record Protocol να κάνει την κρυπτογράφηση, να υπολογίσει την τιμή του ελέγχου ακεραιότητας, πρέπει και ο client και ο server να γνωρίζουν τα κρυπτογραφικά κλειδιά. Το πρωτόκολλο υποστηρίζει την αλλαγή των αλγορίθμων κρυπτογράφησης και των κλειδιών οποιαδήποτε στιγμή.

Το SSL Handshake Protocol χρησιμοποιείται για τη διαπραγμάτευση του αλγορίθμου κρυπτογράφησης που θα χρησιμοποιηθεί, την ανταλλαγή των πιστοποιητικών και την ανταλλαγή των κλειδιών που θα χρησιμοποιηθούν στο session.

Στο SSL Handshake Protocol μπορούν να χρησιμοποιηθούν διάφοροι αλγόριθμοι κρυπτογράφησης όπως ο RSA, ο DES, ο Diffie-Hellman. Το πρωτόκολλο SSL είναι σχεδιασμένο ώστε να μπορεί να χρησιμοποιείται και στις Η.Π.Α. και σε άλλες χώρες. Και οι δύο υλοποιήσεις χρησιμοποιούν τον ίδιο αλγόριθμο κρυπτογράφησης με μήκος κλειδιού 128 bits. Η διαφορά στις δύο υλοποιήσεις βρίσκεται στο SSL Handshake Protocol. Το μήκος κλειδιού στις εκδόσεις που προορίζονται για χρήση στις Η.Π.Α. είναι 128 bits, διαφορετικά το μήκος του κλειδιού είναι 40 bits

6.2.1 Χρησιμοποιώντας το SSL για την ασφαλή αποστολή των αριθμών της πιστωτικής μας κάρτας

Ο σκοπός στην χρησιμοποίηση του SSL είναι να κρύψουμε από τον χρήστη και από τους υπεύθυνους για την ανάπτυξη. Εάν οι χρήστες χρησιμοποιούν έναν ενημερωμένο SSL web browser όπως ο Netscape ή ο Explorer της Microsoft, μπορούν να καθοδηγήσουν τη μηχανή αναζήτησης για να δημιουργήσουν μια κρυπτογραφημένη σύνδεση στον κεντρικό υπολογιστή απλά με την αντικατάσταση του HTTP στο URL με HTTPS.

Έστω ότι έχουμε στην παρακάτω τοποθεσία ένα κείμενο

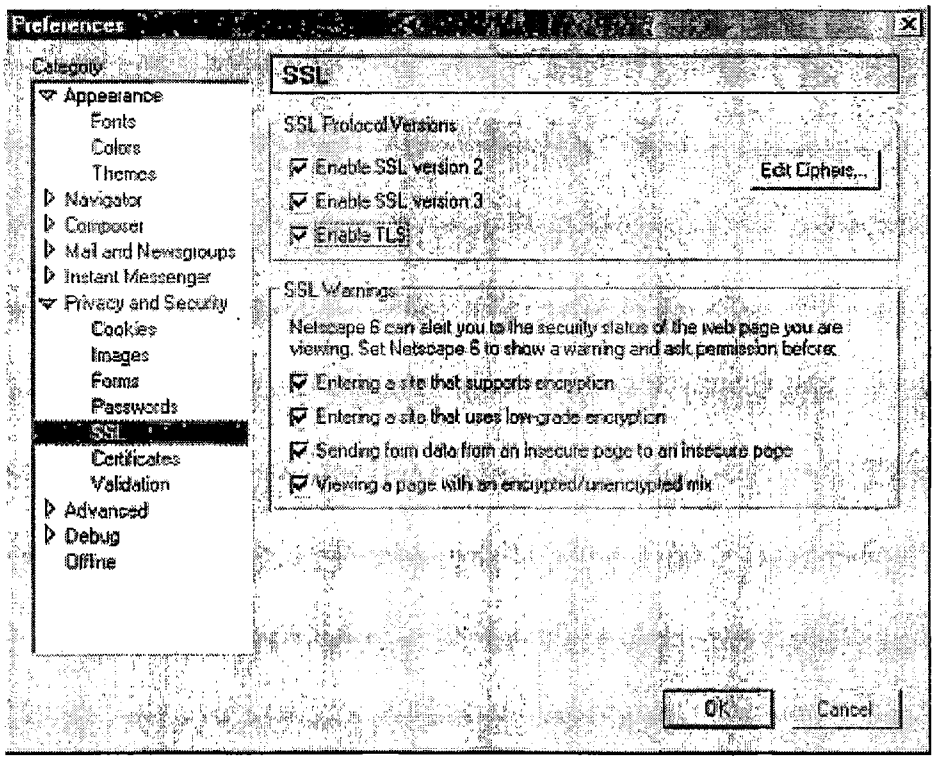
http://www.company.com/document.html

Οι χρήστες μπορούν να ζητήσουν το έγγραφο πληκτρολογώντας την διεύθυνση

https://www.company.com/document.html

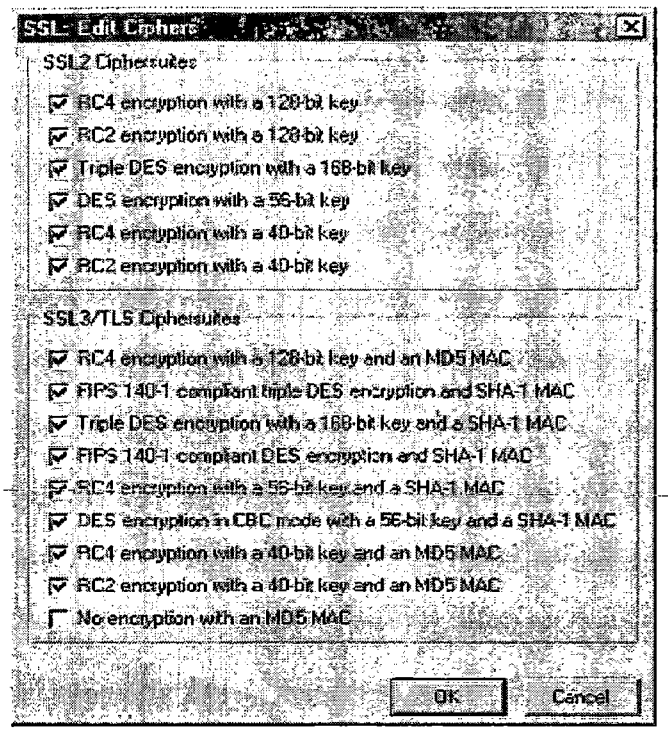
Ο Netscape Navigator και Internet Explorer ελέγχουν την συμπεριφορά του SSL με τη χρήση του πίνακα ελέγχου (control panel). Στην περίπτωση του Netscape Navigator αυτό γίνεται από το Security Preferences ενώ στον Internet Explorer μέσο του Advanced Options πίνακα ο οποίος βρίσκεται στο Internet Options.

Ο πίνακας Security Preferences του Netscape Navigator

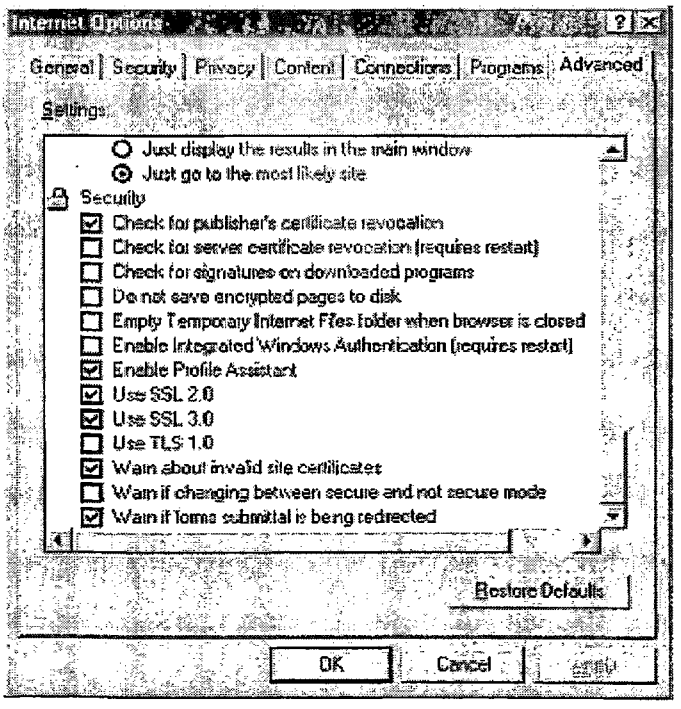


Ο Netscape Navigator μπορεί να ρυθμιστεί έτσι ώστε να ειδοποιεί τον χρήστη όταν κάνει την είσοδό του σε ένα site το οποίο υποστηρίζει το SSL, όταν το site υποστηρίζει μικρού βαθμού κρυπτογράφηση, όταν μία φόρμα συμπληρώνεται χωρίς να κρυπτογραφείται και όταν ένα έγγραφο συνδυάζει στοιχεία κρυπτογράφησης και μη.

Πατώντας το κουμπί "Edit Ciphers . . . " μπορούμε να ορίσουμε την κωδικοποίηση που θέλουμε να χρησιμοποιεί ο browser μας.



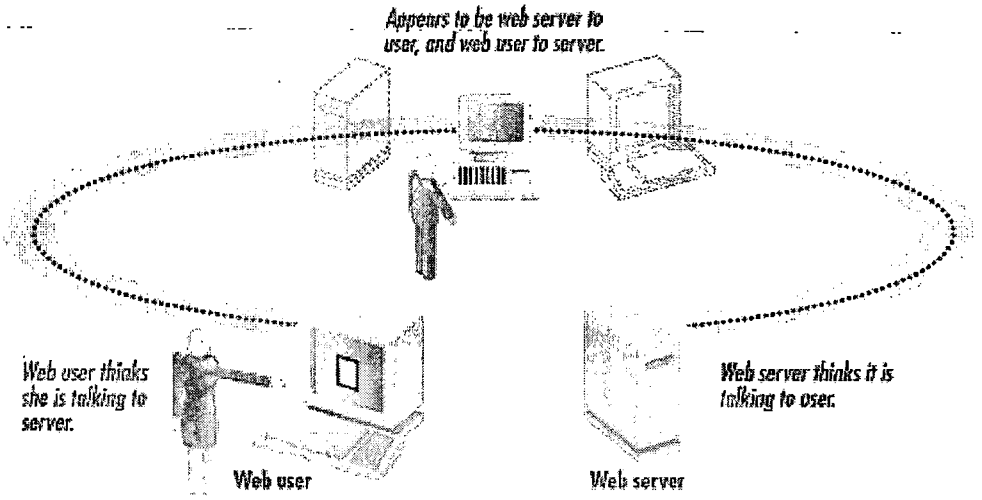
Αντίστοιχα ο πίνακας Security Preferences του Internet Explorer



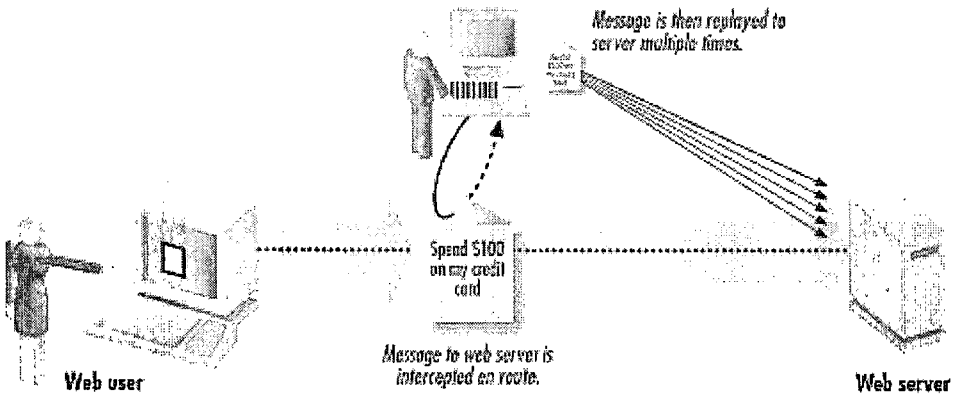
6.2.2 Προστασία από τις επιθέσεις "man-in-the-middle" και "επανάληψης"

Στις επιθέσεις man-in-the-middle ένας επιτιθέμενος παρεμποδίζει όλες τις επικοινωνίες μεταξύ δύο συμβαλλόμενων μερών, κάνοντας κάθε ένα να σκεφτεί ότι επικοινωνεί με το άλλο.

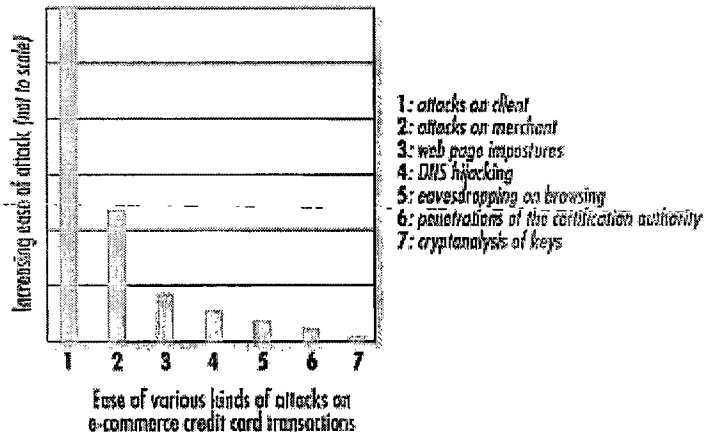
Το SSL/TLS προστατεύει από τις man-in-the-middle επιθέσεις με τη χρησιμοποίηση των ψηφιακών πιστοποιητικών για να επιτρέψει στο χρήστη να μάθει το επικυρωμένο όνομα του ιστοχώρου που επιθυμεί να εισέλθει. Δυστυχώς, κάθε μηχανή αναζήτησης ιστού χρησιμοποιούμενη σήμερα κρύβει αυτές τις πληροφορίες και τις καθιστούν προσιτές μόνο στους χρήστες που χρησιμοποιούν τις πρόσθετες, απόκρυφες εντολές. Επειδή οι πληροφορίες πιστοποιητικών είναι κανονικά κρυμμένες, το SSL κάνει μια εργασία που προστατεύει τους χρήστες από τις man-in-the-middle επιθέσεις.



Σε μια επίθεση επανάληψης, ένας επιτιθέμενος συλλαμβάνει τις επικοινωνίες μεταξύ δύο συμβαλλόμενων μερών και επαναλαμβάνει τα μηνύματα. Για παράδειγμα ο επιτιθέμενος συλλαμβάνει ένα μήνυμα μεταξύ ενός χρήστη και ενός οικονομικού ινστιτούτου που καθοδηγεί μια ηλεκτρονική πληρωμή. Με την επανάληψη αυτής της επίθεσης, ο επιτιθέμενος θα μπορούσε να αναγκάσει την πραγματοποίηση διάφορων ηλεκτρονικών πληρωμών.



Το SSL κάνει πραγματικά λίγα στη προστασία από τις πραγματικές επιθέσεις που οι καταναλωτές και οι έμποροι έχουν αντιμετωπίσει στο διαδίκτυο και αυτό γιατι το SSL και κατ'επέκταση ο Netscape Navigator και Internet Explorer δεν προσπάθησαν να λύσουν τα σοβαρά προβλήματα ασφάλειας του ηλεκτρονικού εμπορίου αλλά αντ' αυτού εστίασαν στα προβλήματα που ήταν εύκολο να λυθούν. Το παρακάτω σχήμα παρουσιάζει εκτιμήσεις ευκολίας των διάφορων τύπων επιθέσεων στις συναλλαγές πιστωτικών καρτών ηλεκτρονικού εμπορίου.



6.2.3 Τα TCP/IP ports που χρησιμοποιούνται από τα SSL-προστατευμένα πρωτόκολλα

Ο παρακάτω πίνακας δείχνει τις θύρες επικοινωνίας οι οποίες χρησιμοποιούνται από το πρωτόκολλο SSL.

https	443/tcp	SSL/TLS-protected HTTP
ssmtp	465/tcp	SSL/TLS-protected SMTP (mail sending)
snews	563/tcp	SSL/TLS-protected Usenet news
ssl-ldap	636/tcp	SSL/TLS-protected LDAP
spop3	995/tcp	SSL-/TLS-protected POP3 (mail retrieving)

6.3 Το πρωτόκολλο PCT

Το πρωτόκολλο PCT (Private Communication Technology) αναπτύχθηκε από τη Microsoft Corporation με σκοπό να αποτρέψει την παρεμβολή τρίτων σε συνδέσεις client/server εφαρμογών. Σύμφωνα με το πρωτόκολλο, τουλάχιστον ένας από τους server ή client αυθεντικοποιείται, ενώ κάθε ένας έχει το δικαίωμα να απαιτήσει την αυθεντικοποίηση του άλλου. Το PCT είναι παρόμοιο με το SSL στη φιλοσοφία του καθώς αποτελεί μια βελτιωμένη έκδοσή του. Είναι ανεξάρτητο από το πρωτόκολλο εφαρμογής που χρησιμοποιείται σε μία σύνδεση. Επάνω από το PCT (στην ιεραρχία των πρωτοκόλλων), μπορεί να βρίσκεται οποιοδήποτε από τα πρωτόκολλα υψηλού επιπέδου (HTTP, FTP, TELNET, κ.λ.π).

Το PCT διαιρείται σε δυο υπο-πρωτόκολλα που ονομάζονται PCT record protocol και PCT handshake protocol. Το PCT record protocol χρησιμοποιείται για την ενθυλάκωση δεδομένων χειραψιών και εφαρμογών μέσα σε PCT εγγραφές, ενώ το PCT handshake protocol στρωματοποιείται στην κορυφή του PCT record protocol και χρησιμοποιείται για να αυθεντικοποίησει τον εξυπηρέτη στον εξυπηρετούμενο.

Οι ανταλλαγές των records μεταξύ ενός client και του server, ομαδοποιούνται σε συνδέσεις, οι οποίες με τη σειρά τους ομαδοποιούνται σε συνόδους (sessions). Κάθε PCT σύνδεση ανήκει σε μια συγκεκριμένη σύνοδο. Κάθε σύνδεση, στα πλαίσια του πρωτοκόλλου, αρχίζει με ένα handshake (χειραψία). Στη φάση αυτή, ανταλλάσσεται μια σειρά από handshake μηνύματα, τα οποία διαπραγματεύονται ένα (συμμετρικό) κλειδί επικοινωνίας για τη σύνδεση, όπως επίσης και επιτελούν τις απαραίτητες αυθεντικοποιήσεις με βάση πιστοποιημένα μη συμμετρικά (δημόσια) κλειδιά. Μόλις τελειώσει η μετάδοση των δεδομένων που προέρχονται από το πρωτόκολλο εφαρμογής, όλα τα δεδομένα (ακόμα και τα μηνύματα λάθους ή/και τα μηνύματα διαχείρισης κλειδιού) κρυπτογραφούνται με τη χρήση κλειδιών κρυπτογράφησης που συμφωνήθηκαν στη φάση του handshake.

6.4 Το πρωτόκολλο SET

Η τεχνολογία SET (Secure Electronic Transaction) αναπτύχθηκε για τη μέγιστη online ασφάλεια που κάνει ικανούς τους καταναλωτές και τους εμπόρους να εξακριβώνουν τη γνησιότητα του άλλου πριν από μια συναλλαγή. Το SET είναι μια ανοικτή προδιαγραφή κρυπτογράφησης και ασφάλειας που σχεδιάστηκε για να προστατέψει τις συναλλαγές με πιστωτικές κάρτες στο Internet.
Το SET αναφέρεται στις αλληλεπιδράσεις ανάμεσα στους κατόχους πιστωτικών καρτών, στους εμπόρους και τις τράπεζες εγγύησης. Όλα τα μέρη του κατέχουν ένα ζεύγος ιδιωτικού-δημόσιου κλειδιού και ένα αντίστοιχο πιστοποιητικό δημόσιου κλειδιού. Επιπλέον κατέχουν επιπλέον δύο ζεύγη κλειδιών, ένα για την ανταλλαγή κλειδιών και ένα για ψηφιακές υπογραφές. Ο κάτοχος της πιστωτικής κάρτας και ο έμπορος πρέπει να αποκτήσουν τα πιστοποιητικά των δημόσιων κλειδιών τους όταν εγγράφονται, προτού συμμετάσχουν σε οποιαδήποτε συναλλαγή. Συνεπώς η χρήση του SET απαιτεί την ύπαρξη μιας ικανοποιητικά λειτουργούσας υποδομής.

Το SET προσφέρει τρεις υπηρεσίες:

- Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ όλων των συμμέτοχων στη συναλλαγή.
- Παρέχει εμπιστοσύνη με τη χρήση των ηλεκτρονικών πιστοποιητικών (digital certificates) X.509v3 για να επιβεβαιώσει ότι οι καταναλωτές και οι έμποροι εξουσιοδοτούνται να χρησιμοποιούν και να δέχονται αντίστοιχα πιστωτικές κάρτες. Αυτό είναι το ηλεκτρονικό ισοδύναμο ενός καταναλωτή που ψάχνει την επιγραφή της πιστωτικής του εταιρείας στη βιτρίνα ενός καταστήματος, και του εμπόρου που ελέγχει την υπογραφή του καταναλωτή στο πίσω μέρος της πιστωτικής του κάρτας.
- Εγγυάται την μυστικότητα επειδή η πληροφορία είναι διαθέσιμη στους ενδιαφερομένους μόνο όταν και όπου αυτό είναι αναγκαίο. Έτσι η πληροφορία της κάρτας πληρωμής του καταναλωτή προστατεύεται έως ότου φτάσει στον οικονομικό οργανισμό. Ο έμπορος δεν μπορεί να διαβάσει αυτή την πληροφορία στη συναλλαγή πληρωμής.

6.4.1 Συμμετέχοντες στο SET

- Κάτοχος της κάρτας (Cardholder): Το άτομο που έχει στην κατοχή του την πιστωτική κάρτα και το ψηφιακό πιστοποιητικό.

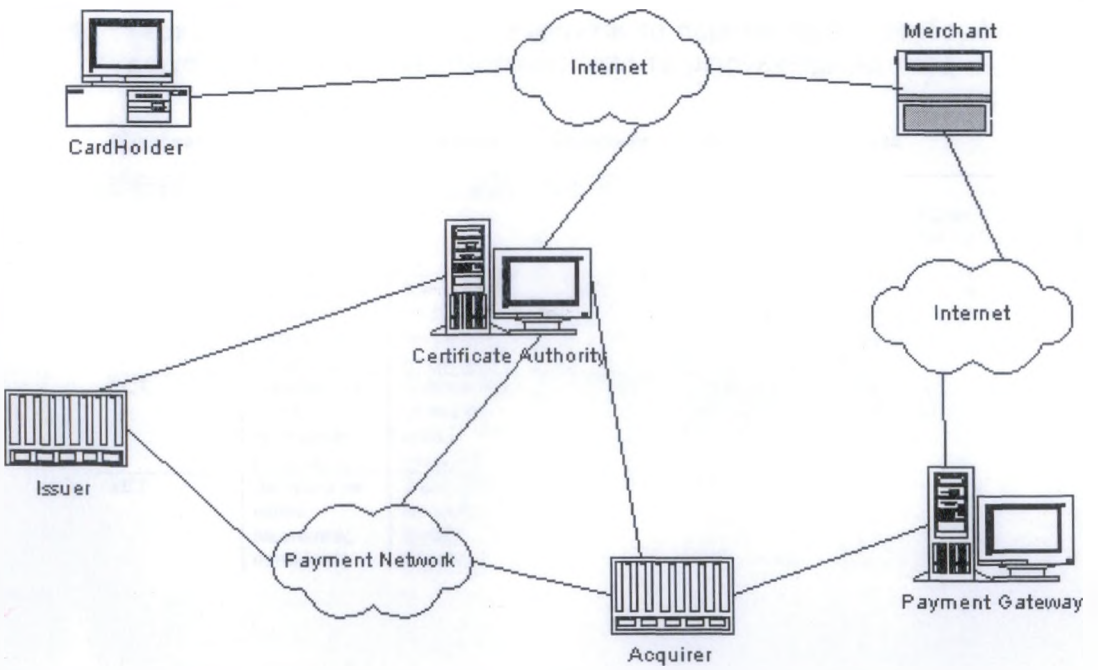
- Πάροχος (Issuer): Είναι οικονομικός οργανισμός, όπως μια τράπεζα, που παρέχει την πιστωτική κάρτα στον κάτοχο αυτής. Ο πάροχος παρέχει ένα ψηφιακό πιστοποιητικό στον κάτοχο της κάρτας που του επιτρέπει να αναγνωριστεί σε αυτόν.

- Acquirer: Είναι οικονομικός οργανισμός που ανοίγει ένα λογαριασμό με ένα έμπορο και επεξεργάζεται τις πληρωμές και τις εξουσιοδοτήσεις πληρωμής των καρτών.

- Πύλη πληρωμών (payment gateway): Είναι μια λειτουργία που επιτελείται από τον acquirer ή κάποιο τρίτο, και επεξεργάζεται τα μηνύματα πληρωμής του εμπόρου.

- Υπηρεσία πιστοποίησης (Certificate Authority): Είναι μια οντότητα που εκδίδει X.509v3 πιστοποιητικά δημοσίου-κλειδιού σε κατόχους κάρτας, εμπόρους, και payment gateways.

Το σχήμα απεικονίζει τους συμμετέχοντες στο πρωτόκολλο SET



7 Cookies

Στο πρωτόκολλο HTTP που αποτελεί τη βάση για τον ιστό, δεν υπάρχει προφύλαξη από τη διάθεση μιας πληροφορίας σε διάφορες οντότητες. Αυτή η σχεδιαστική επιλογή παρουσιάζει κάποια πλεονεκτήματα όπως η απλότητα και η μείωση πρόσθετων ανταλλασσόμενων πληροφοριών κατά την αποστολή των μηνυμάτων. Ωστόσο υπάρχουν σημαντικά μειονεκτήματα όπως το ότι κάθε επικοινωνία μεταξύ ενός φυλλομετρητή και ενός εξυπηρετητή στα πλαίσια εφαρμογών ηλεκτρονικού εμπορίου απαιτεί ολοκληρωμένες και σταθερές HTTP αιτήσεις και απαντήσεις για τη διασφάλιση της δυνατότητας χειρισμού σχετικών μηνυμάτων δοσολοψιών.

Τα cookies αποτελούν συνήθως αρχεία με αποθηκευμένη σε αυτά μικρή ποσότητα πληροφοριών. Σχεδιαστικός σκοπός των cookies είναι η απλοποίηση των διαδικασιών κατά την επικοινωνία εξυπηρετούμενου-εξυπηρέτη, επιτρέποντας στο φυλλομετρητή να καταχωρίσει συγκεκριμένες πληροφορίες τις οποίες αποστέλλει στον εξυπηρέτη αυτές τις πληροφορίες κάθε φορά που επικοινωνεί με αυτόν. Αρχικά τα cookies χρησιμοποιούνταν για την υλοποίηση καρτών αγορών. Σήμερα πολλοί χρήστες θεωρούν ότι με την ανίχνευση και καταγραφή των κινήσεών τους στο internet θίγεται η προσωπική τους ζωή και οι φόβοι αυτοί σε πολλές περιπτώσεις έχουν αποδειχθεί βάσιμοι.

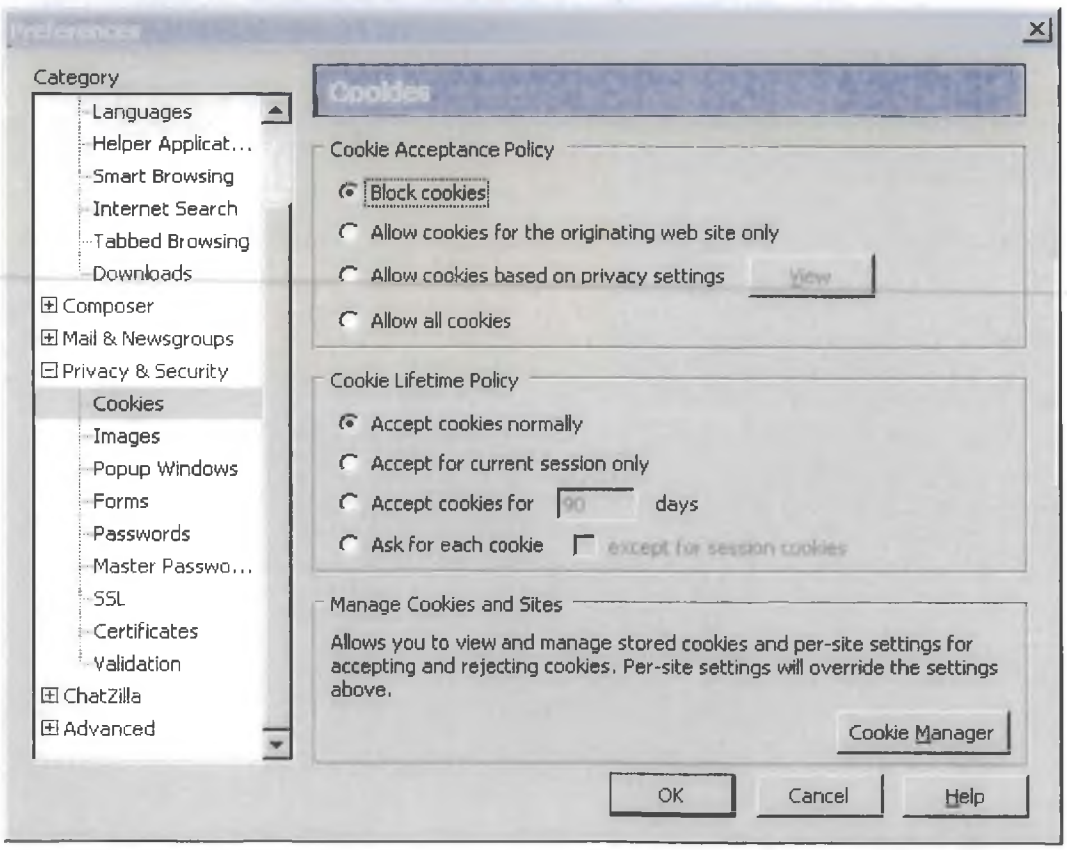
Στο cookie περιλαμβάνεται το domain name του εξυπηρέτη, το μονοπάτι στο οποίο βρίσκεται το έγγραφο της ιστοσελίδας που ζήτησε ο χρήστης, η διάρκεια ζωής του και μια τιμή μεταβλητής την οποί θέτει η ιστοσελίδα. Επίσης είναι χρήσιμα για την καταγραφή των δραστηριοτήτων των χρηστών είναι πιθανό μια ιστοσελίδα να αναγνώσει το cookie που κάποια άλλη ιστοσελίδα έθεσε στο μηχάνημα του χρήστη και να το εκμεταλλευτεί, παρουσιάζοντας στο χρήστη κάποια πληροφορία που ίσως του προκαλέσει ενδιαφέρον. Βέβαια υπάρχει πάντα η δυνατότητα από την πλευρά των χρηστών να απενεργοποιήσουν τα cookies από τους φυλλομετητές.

Χαρακτηριστικά της επικεφαλίδας των cookies

- comment: αποθηκεύει ευανάγνωστο κείμενο που περιλαμβάνει χρήσιμες πληροφορίες για το cookie
- domain: καθορίζει τη δικαιοδοσία για την οποία το cookie είναι έγκυρο
- expires: καθορίζει το χρόνο ζωής του cookie
- path: καθορίζει το μονοπάτι των ιστοσελίδων που θα χρησιμοποιήσει το cookie
- secure: υποδεικνύει συμβουλευτικά στον φυλλομετρητή να χρησιμοποιήσεις ασφαλείς διαύλους όταν θα επιστρέψει στον εξυπηρέτη όπου προήλθε

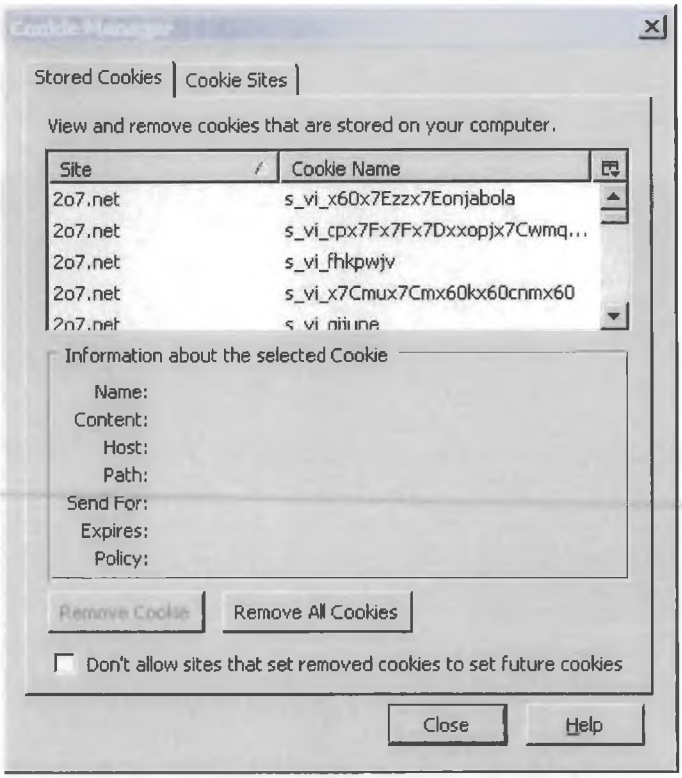
Ο Netscape Navigator και ο Internet Explorer ελέγχουν την συμπεριφορά των cookies με τη χρήση του πίνακα ελέγχου (control panel). Στην περίπτωση του Netscape Navigator αυτό γίνεται από το Preferences και επιλέγοντας το Privacy & Security, ενώ στον Internet Explorer μέσω του Privacy πίνακα ο οποίος βρίσκεται στο Internet Options.

Ο πίνακας Privacy & Security Preferences του Netscape Navigator



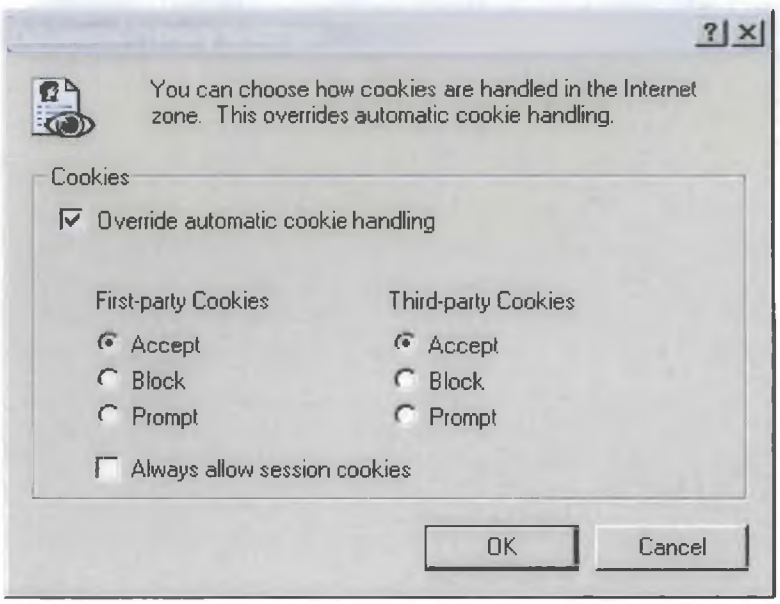
Ο Netscape Navigator μπορεί να ρυθμιστεί έτσι ώστε να δίνει την δυνατότητα στον χρήστη να μπορει να απαγορεύσει τα cookies (μέσο της επιλογης block cookies) ή να τα αποδεχτεί για μια συγκεκριμένη σύνοδο ή για προκαθορισμένο αριθμό ημερών, ενώ με τον διαχειριστή των cookies (cookie manager) μπορούμε να δουμε και διαγράψουμε τα υπάρχοντα cookies που βρίσκονται στον υπολογιστή μας.

Ο πίνακας Cookie Manager στον Netscape Navigator

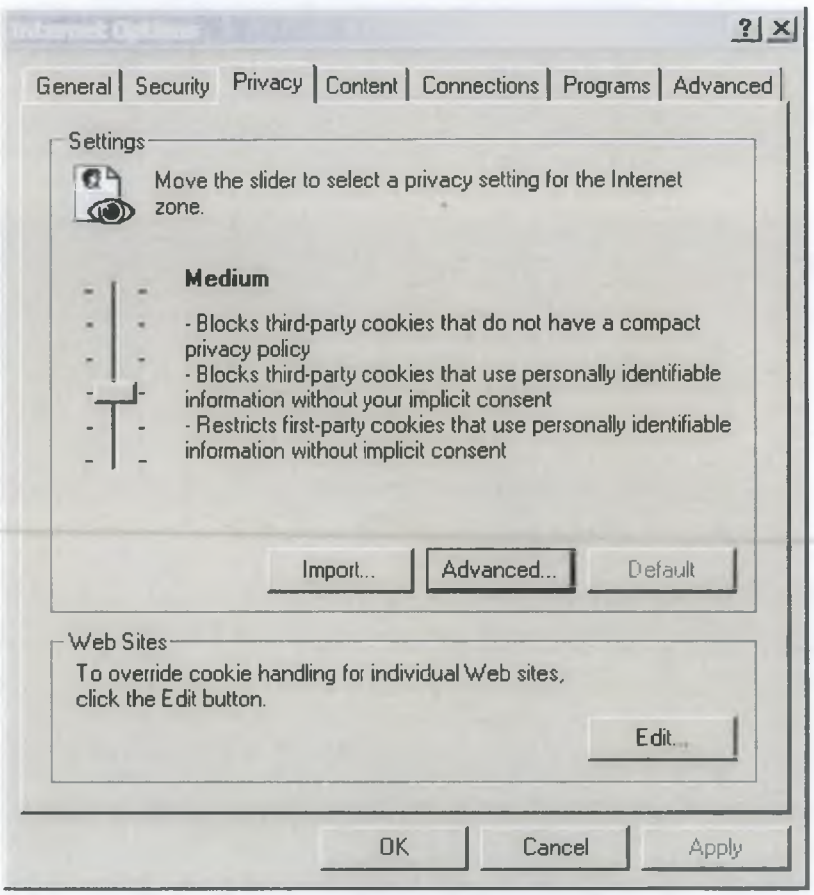


Ο Internet Explorer μπορεί να ρυθμιστεί και αυτός έτσι ώστε να επιτρέπει την αποδοχή ή όχη των cookies από τους χρήστες με την επιλογή της αποδοχής, απόρριψης ή τη δυνατότητα κάθε φορά που κάνει την είσοδο του σε μια ιστοσελίδα που χρησιμοποιεί cookies να του τίθεται το ερώτημα σχετικά με την αποδοχή ή όχι του cookie.

Ο πίνακας Privacy Stettings του Internet Explorer



Ο πίνακας Privacy του Internet Explorer



Από τον πίνακα Privacy του Internet Explorer επιλέγουμε το advanced το ποίο περιλαμβάνει τις επιλογές σχετικά με την διαχείριση των cookies.

7.1 Προσωρινά και μόνιμα cookies

Τα προσωρινά (ή session) cookies είναι αρχεία που διαγράφονται μμόλις ο χρήστης αποσυνδεθεί από το δικτυακό τόπο ή απλά κλείσει το παράθυρο του προγράμματος πλοήγησης. Χρησιμοποιούνται από τον δικτυακό τόπο με σκοπό τη βελτίωση της πλοήγησης του χρήστη (π.χ. κατά την πλοήγηση σε συνδρομητικό περιεχόμενο, ώστε να μη ζητείται από το χρήστη να υποβάλει κωδικό πρόσβασης κάθε φορά που επισκέπτεται μια διαφορετική σελίδα του ίδιου τόπου), ή απλά για τη συλλογή στατιστικών στοιχείων. Τα μόνιμα (persistent) cookies είναι δεδομένα που αποθηκεύονται «μόνιμα» (ή, για μεγάλο χρονικό διάστημα) στο σκληρό δίσκο του χρήστη. Όταν επισκεφτεί ξανά ο χρήστης το δικτυακό τόπο, το πρόγραμμα πλοήγησης αποστέλλει το αρχείο cookie στον web server για περαιτέρω επεξεργασία.

7.2 Ζητήματα κατά τη χρήση cookies

Τα βασικά ζητήματα που προκύπτουν σχετίζονται με την ιδιωτικότητα του χρήστη. Τα cookies επιτρέπουν στις ιστοθέσεις να καταγράψουν και να παρακολουθήσουν συνήθειες των χρηστών. Αυτά τα δεδομένα είναι ιδιαίτερα χρήσιμα και παρέχουν εκτενείς δυνατότητες αξιοποίησης, αφού οι προσωπικές πληροφορίες των χρηστών μπορούν δυνητικά να διαδίδονται σε ευρύτερη κοινότητα αποδεκτών και όχι μόνο στον προορισμό που αναφέρονται.

Ακόμα τα cookies χρησιμοποιούνται για να καταγράψουν την συμπεριφορά των χρηστών και να δημιουργήσουν διαφημίσεις που θα έχουν μεγάλο βαθμό προσπελασιμότητας. Γενικότερα η αποδοχή των αρχείων cookies μπορεί να προκαλέσει, υπό προϋποθέσεις, την παραβίαση της ανωνυμίας των χρηστών κατά την πλοήγηση τους στο Web. Ορισμένες επιχειρήσεις που δραστηριοποιούνται στο Web, καταγράφουν τη συμπεριφορά των χρηστών, τις επισκέψεις τους σε δικτυακούς τόπους και την επιλογή-αναζήτηση προϊόντων στις οποίες εκείνοι προβαίνουν, με σκοπό τα έσοδα από διαφήμιση. Παράδειγμα αποτελεί η εταιρεία DoubleClick συγκεντρώνοντας τη δρατηριότητα των χρηστών διαμέσου άλλων ιστοθέσεων πελατών. Έτσι ένας χρήστης όταν επισκεπτόταν μια αθλητική ιστοσελίδα και δεχόταν μια διαφήμιση από την DoubleClick θα μπορούσε αργότερα να βρεθεί προ εκπλήξεως αφού υπήρχε η δυνατότητα να του παρουσιάζονται τέτοιου είδους διαφημίσεις κατά την εισαγωγή του σε οποιαδήποτε άλλη ιστοσελίδα σχετικού περιεχομένου. Τέλος άλλες αμφιλεγόμενες πρακτικές εμπλέκουν τη χρήση cookies με μαζικά ηλεκτρονικά μηνύματα, τα οποία περιλαμβάνουν συνημμένα HTML αρχεία. Οι εικόνες σε αυτά τα HTML αρχεία αρχικοποιούν αιτήσεις, οι οποίες μπορούν να καταλήξουν σε τοποθέτηση και αργότερα ανάκτηση των cookies.

8 Firewalls

Ένα firewall, δηλαδή μια διάταξη εξειδικευμένων μηχανισμών ασφάλειας που ελέγχει την πρόσβαση και τη μετακίνηση της πληροφορίας μεταξύ ενός δικτύου που εμπιστευόμαστε και ενός δικτύου που δεν εμπιστευόμαστε απαραίτητα αποτελεί την τεχνική έκφραση μια συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού.

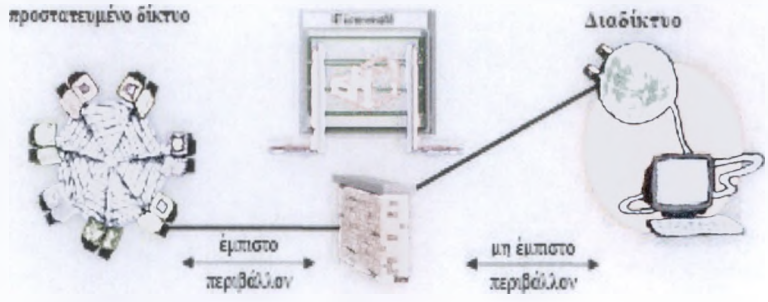
Το firewall μπορεί να οριστεί ως μια συλλογή από συστήματα τοποθετημένα στο σημείο σύνδεσης της υπο προστασία δικτυακής περιοχής με τα υπόλοιπα δίκτυα, που επιβάλλει μια προκαθορισμένη πολιτική ασφάλειας (security policy). Η εγκατάσταση ενός firewall στον οργανισμό γίνεται με σκοπό να βελτιωθεί το επίπεδο προστασίας των δεδομένων και των υπολογιστικών πόρων του οργανισμού από εισβολείς.

Με τον όρο firewall (ανάχωμα ασφάλειας) εννοούμε συστήματα ή ομάδες συστημάτων τα οποία υλοποιούν τους κανόνες μια πολιτικής ασφάλειας μεταξύ δυο δικτύων. Τις περισσότερες φορές, το ένα από τα δυο δκτυα είναι το internet, αλλά ένα firewall σε γενική περίπτωση, μπορεί να τοποθετηθεί και μεταξύ δυο τυχαίων δικτύων υπολογιστών.

Ο ρόλος του firewall μπορεί να είναι τόσο η αποτροπή μη εξουσιοδοτημένων προσβάσεων σε μία ασφαλή περιοχή, όσο και η αποτροπή μη εξουσιοδοτημένης εξόδου πληροφορίας από μια περιοχή. Μπορεί δηλαδή να λειτουργήσει ως θύρα ελέγχου της κίνησης και προς τις δυο κατευθύνσεις.

Κρίσιμο σημείο το οποίο πρέπει να τονιστεί είναι ότι ένα firewall δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως από το πώς έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφαλείας. Είναι δυνατόν ένα firewall, το οποίο έχει εγκατασταθεί, διαμορφωθεί και λειτουργεί για να εξυπηρετήσει λανθασμένους σκοπούς μπορεί να δημιουργήσει σημαντικά προβλήματα. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφαλείας που έχει καθοριστεί και που πρέπει να είναι συγκεκριμένη και σαφής.

Απεικόνιση ενός συστήματος Firewall



8.1 Δυνατότητες ενός firewall

Η λειτουργικότητα των firewalls εκτείνεται στα ακόλουθα:

- Το firewall αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφάλειας

Επιτρέπει στο διαχειριστή του δικτύου να ορίσει ένα κεντρικό σημείο ελέγχου, το οποίο αποτρέπει την προσπέλαση μη εξουσιοδοτημένων χρηστών στο προστατευμένο δίκτυο. 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.

- Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο, υλοποιώντας και υποστηρίζοντας την πολιτική ασφάλειας του οργανισμού

Πρόκειται για την έκφραση του βασικού σκοπού ύπαρξης ενός firewall, ο οποίος επιτυγχάνεται συγκεντρώνοντας όσο το δυνατό περισσότερη πληροφόρηση για την ταυτότητα τόσο των πακέτων (packets) όσο και των συνόδων (sessions) που διέρχονται από το firewall. Με βάση αυτή τη πληροφόρηση και μια ήδη καθορισμένη πολιτική ασφάλειας η οποία περιγράφει σε ποιά πακέτα και σε ποιες συνόδους επιτρέπεται η είσοδος ή η έξοδος, το firewall αποφασίζει εάν θα επιτρέψει την είσοδο ή έξοδο ενός πακέτου ή την έναρξη μιας συνόδου. Η μία από τις δυνατές πολιτικές ενός firewall βασίζεται στην άρνηση σε οποιαδήποτε πρόσβαση η οποία δεν έχει σαφώς επιτραπεί. Χωρίς το firewall κάθε υπολογιστής στο εσωτερικό δίκτυο του οργανισμού είναι εκτεθειμένος σε προσβολές από άλλους υπολογιστές στο internet.

- Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο

Ένα αξιόπιστο firewall καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου. Μερικά firewalls προσφέρουν και μηχανισμούς συναγερμού ώστε να βοηθήσουν στον έγκαιρο εντοπισμό μια ύποπτης δραστηριότητας τη στιγμή που αυτή λαμβάνει χώρα και στην άμεση πληροφόρηση του διαχειριστή.

- Το firewall προσφέρει διευρυμένη ιδιωτικότητα (enhanced privacy)

Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί εισβολείς (intruders) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν» από τα όρια χρήσης του δικτύου που εμείς ορίσαμε. Γενικότερα, υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς, περιέχουν σημαντικά στοιχεία για έναν επιδέξιο χρήστη που θέλει να επιχειρήσει επίθεση. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν υπηρεσίες όπως η Finger και η DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου, όπως το πότε συνδέθηκαν για τελευταία φορά, αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο κλπ. Έτσι όμως διαρρέουν πληροφορίες στους εισβολείς σχετικές με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίησή τους στο Διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται.

- Προσφέρει διευρυμένη ιδιωτικότητα (enhanced privacy).

Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί εισβολείς (intruders) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν» από τα όρια χρήσης του δικτύου που εμείς τους ορίσαμε. Γενικότερα, υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς, περιέχουν σημαντικά στοιχεία για έναν επιδέξιο χρήστη που θέλει να επιχειρήσει επίθεση. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν υπηρεσίες όπως η Finger και η DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου, όπως το πότε συνδέθηκαν για τελευταία φορά, αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο κλπ. Έτσι όμως διαρρέουν πληροφορίες στους εισβολείς σχετικές με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίησή τους στο διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται.

- Τα firewall προσφέρουν ως μια επιπλέον λειτουργία και τις υπηρεσίες τους ως πύλες κρυπτογράφησης (encrypting gateways)

Αρκετά σύγχρονα συστήματα firewall έχουν ταυτόχρονα δυνατότητες κρυπτογράφησης στις επικοινωνίες μεταξύ των διακομιστών που προστατεύουν. Ακόμη και εξωτερικά συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή, αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Ένας τέτοιος λογικός διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα εικονικά ιδιωτικά δίκτυα (VPN, Virtual Private Networks). Η κρυπτογράφηση μπορεί να είναι επιλεκτική, ανάλογα με την αιτούμενη από το διαδίκτυο υπηρεσία και η διαχείρισή της είναι ενσωματωμένη με τα υπόλοιπα χαρακτηριστικά του firewall, έτσι ώστε να είναι δυνατή η εκμετάλλευση όλων των βοηθημάτων που υποστηρίζονται για τη κατασκευή των κανόνων ελέγχου προσπέλασης, τη καταγραφή-παρακολούθηση των ενεργειών κλπ.

8.2 Περιορισμοί ενός firewall

Οι αδυναμίες που παρουσιάζουν γενικά τα firewalls είναι:

- Το firewall δε μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό

Ένα firewall παρέχει προστασία σε ένα περιβάλλον μόνο αν ελέγχει ολόκληρη την περίμετρο του περιβάλλοντος. Συνδέσεις που δε διέρχονται από το σημείο που βρίσκεται το firewall προφανώς δεν μπορούν να διασφαλισθούν από αυτό.

- Το firewall δεν μπορεί να προστατέψει από απειλές άγνωστου τύπου

Δεν υπάρχει η δυνατότητα το firewall να αμυνθεί αυτόματα σε νέες απειλές οι οποίες προκύπτουν κατά καιρούς. Μπορεί να προστατέψει το δίκτυο μόνο από γνωστές απειλές που έχουν αντιμετωπισθεί στο παρελθόν.

- 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, των πολλαπλών επιπέδων ασφάλειας και κατά συνέπεια της συνολικής ελαττωμένης φιλικότητας και μειωμένης ευχρηστίας που εισάγει.

- Δεν είναι εντελώς άτρωτα, μπορούν να διαπεραστούν

Οι κατασκευαστές των συστημάτων firewalls τα κρατούν μικρά και απλά έτσι ώστε ο πιθανός εισβολέας να μην αποκτήσει στη συνέχεια τον έλεγχο επικίνδυνων εργαλείων όπως τα προγράμματα μεταγλώττισης (compilers), τα προγράμματα σύνδεσης (linkers) κλπ. Όμως σε καμιά περίπτωση δεν πρέπει να θεωρείται ότι είναι ικανά μόνα τους να εξασφαλίσουν την απόκρουση όλων των εξωτερικών επιθέσεων. Πρέπει να θεωρούνται απλώς σαν μια ισχυρή πρώτη γραμμή άμυνας.

- Δεν προστατεύουν από τους εσωτερικούς χρήστες (πχ. από τους υπάλληλους του οργανισμού)

Εφόσον ένα εσωτερικό μηχάνημα μπορεί να επικοινωνήσει με ένα άλλο, κάνοντας χρήση πρωτοκόλλου Internet, χωρίς να «περάσει» μέσα από το firewall, οποιαδήποτε ζημιά μπορεί να προκληθεί χωρίς να γίνει αντιληπτό από αυτό. Απαιτούνται επιπλέον μηχανισμοί πιστοποίησης και ελέγχου προσπέλασης για τους χρήστες και τις δραστηριότητες των συστημάτων τους. Φυσικά, τα intranet firewalls ελαχιστοποιούν ανάλογους κινδύνους, παρακολουθώντας την κυκλοφορία ανάμεσα στα διάφορα τμήματα ενός οργανισμού.

8.3 Αποδεκτή λειτουργικότητα στα συστήματα firewalls

Ένα σύστημα firewall θα πρέπει να ικανοποιεί τις ακόλουθες προϋποθέσεις:

- Να απορρίπτει κάθε πακέτο που ρητά κάποιος κανόνας δεν το επιτρέπει. Είναι η εξ' ορισμού (default) άλλωστε ρύθμιση για τα περισσότερα firewalls, και επιβάλλει στο διαχειριστή τους να διευκρινίσει ποιες ακριβώς επικοινωνίες είναι αποδεκτές.

- Να κρατάει τους εξωτερικούς χρήστες έξω από το προστατευμένο δίκτυο. Αν για παράδειγμα πρέπει κάποια αρχεία να γίνουν προσιτά μέσω διαδικτύου, τότε το πιο σίγουρο – αλλά όχι και απαραίτητο – είναι αυτά να τοποθετηθούν έξω από το firewall. Εναλλακτικά απαιτούνται ισχυροί μηχανισμοί πιστοποίησης (authentication) σε επίπεδο εφαρμογών πια, για την παρεμπόδιση των μη-εξουσιοδοτημένων χρηστών.

- Να διαθέτει προηγμένα εργαλεία καταγραφής, επίβλεψης και πρόκλησης συναγερμού (alarm generation), ικανά να δημιουργούν και να αναλύουν τις πραγματοποιημένες συναλλαγές με σκοπό την εξαγωγή συμπερασμάτων σχετικά με το είδος και τη φύση των επιθέσεων και τη συνακόλουθη προσαρμογή της υφιστάμενης πολιτικής ασφάλειας.

8.4 Αρχιτεκτονική των firewalls

8.4.1 Firewalls επιπέδου δικτύου

Πραγματοποιούν ελέγχους στα IP πακέτα (Internet Protocol packets). Ένα πακέτο είναι μια μικρή μονάδα επικοινωνίας, συνήθως μερικές εκατοντάδες bytes, και ένας δρομολογητής (router) μπορεί να διοχετεύσει χιλιάδες πακέτα σε ένα δευτερόλεπτο. Τα περισσότερα firewalls επιπέδου δικτύου είναι απλοί δρομολογητές. Οι δρομολογητές αυτοί γενικά αναφέρονται ως δρομολογητές φιλτραρίσματος (filtering routers) ή firewalls επιπέδου δικτύου (network level ή packet filter firewalls).

Ένα πακέτο IP αποτελείται από μία επικεφαλίδα και από δεδομένα. Η επικεφαλίδα περιέχει συγκεκριμένη πληροφορία όπως:

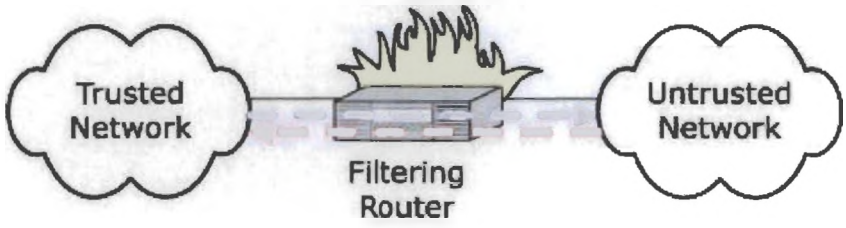
IP Διεύθυνση προέλευσης
IP Διεύθυνση προορισμού
Πρωτόκολλο (TCP ή UDP πακέτο)
TCP ή UDP θύρα προέλευσης
TCP ή UDP προορισμού
Τύπος μηνύματος ICMP

Ένας απλός δρομολογητής βασισμένος σε αυτή την πληροφορία και στην διεπαφή από την οποία έλαβε ένα πακέτο καθώς και τη διεπαφή στην οποία θα μεταδώσει ένα πακέτο, δέχεται το πακέτο, εξετάζει τη διεύθυνση προορισμού του κοιτάζοντας την επικεφαλίδα του και επιλέγει τον καλύτερο τρόπο για να το προωθήσει προς τον τελικό προορισμό του.

Η διαφορά με το firewall είναι ότι το firewall δεν καθόριζει μόνο εάν το πακέτο μπορεί να δρομολογηθεί προς τον προορισμό του αλλά και το αν πρέπει να δρομολογηθεί, εφαρμόζοντας την πολιτική ασφάλειας η οποία έχει καθορισθεί.

Συνολικά ένα firewall επιπέδου δικτύου εξετάζει την επικεφαλίδα του IP πακέτου και βασιζόμενο στις διευθύνσεις πηγής και προορισμού καθορίζει εάν θα επιτραπεί η είσοδος στο πακέτο χωρίς να εξετάζει καθόλου τα δεδομένα του.

Firewall επιπέδου δικτύου



Μερικά παραδείγματα ελέγχων που μπορεί να πραγματοποιήσει ένα firewall επιπέδου δικτύου είναι τα ακόλουθα:

- Εμπόδισε όλες τις εισερχόμενες συνδέσεις από και προς συγκεκριμένα συστήματα τα οποία δεν είναι έμπιστα
- Επέτρεψε την πρόσβαση στον εξυπηρετητή παγκόσμιου ιστού
- Επέτρεψε τις υπηρεσίες e-mai, ftp (file transfer protocol), αλλά εμπόδισε υπηρεσίες όπως rlogin (remote login), rcp (remote copy) και (tftp (trivial file transfer protocol)

Ορισμένα πλεονεκτήματα των firewalls επιπέδου δικτύου είναι:

- Η εύκολη εγκατάστασή τους
- Η διαφάνεια τους προς τους χρήστες
- Η μεγάλη ταχύτητα εκτέλεσης
- Το χαμηλό κόστος

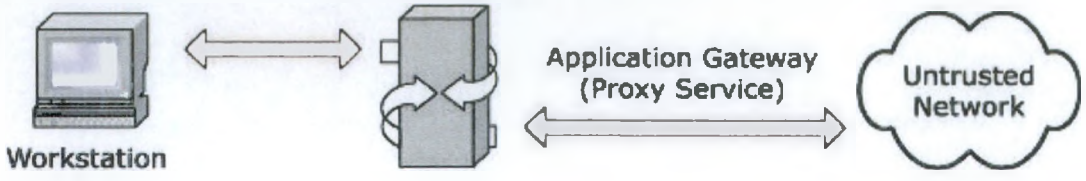
Ενώ στα μειονεκτήματα εντάσσονται στα παρακάτω:

- Η απλοϊκή καταγραφή των συμβάντων
- Δεν προσφέρουν μηχανισμούς συναγερμών
- Δε διαθέτουν μηχανισμούς αυθεντικοποίησης σε επίπεδο χρήστη

8.4.2 Firewalls επιπέδου εφαρμογής

Ένα firewall επιπέδου εφαρμογής υλοποιείται ως ένα πρόγραμμα λογισμικού σε μια συγκεκριμένη πλατφόρμα υπολογιστή. Στην περίπτωση αυτή δηλαδή κάνουμε λόγο για firewalls βασισμένα σε ξενίστη-υπολογιστή (host-based firewalls). Ένα firewall αυτής της κατηγορίας δεν επιτρέπει σε κανένα πακέτο να περάσει κατευθείαν από το ένα δίκτυο στο άλλο. Εκείνο το οποίο συμβαίνει στην πράξη είναι ότι η πραγματική σύνδεση πραγματοποιείται σε μια εφαρμογή ειδικού σκοπού που εκτελείται στο firewall, η οποία ονομάζεται πληρεξούσια εφαρμογή ή πληρεξούσια υπηρεσία (proxy applixation). Η πληρεξούσια υπηρεσία αποτελεί μια εξειδικευμένη εφαρμογή, ή ένα πρόγραμμα εξυπηρετητή, το οποίο εκτελείται στον υπολογιστή- firewall ασφαλείας και δέχεται αιτήσεις των χρηστών.

Firewall επιπέδου εφαρμογής

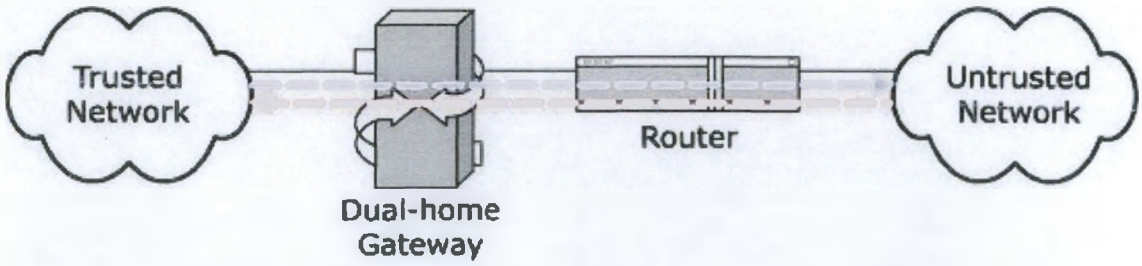


Τα πλεονεκτήματα των firewall αυτής της κατηγορίας είναι ότι παρέχουν μεγαλύτερη ασφάλεια και καλύτερο έλεγχο προσπέλασης αφού κατανοούν σε βάθος το πρωτόκολλο το οποίο εξυπηρετεί η πληρεξούσια υπηρεσία. Ακόμα παρέχουν καλύτερη καταγραφή συμβάντων καθώς επιτρέπουν την παρακολούθηση μιας δραστηριότητας και την καταγραφή συγκεκριμένων γεγονότων.

8.4.3 Υβριδικά firewalls

Ο όρος υβριδικές ή σύνθετες πύλες (hybrid or complex gateways) χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών-τύπων, προχωρούν ακόμη ένα βήμα παραπέρα. Παρατηρείται μια τάση υιοθέτησης της σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστήματος firewall για περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας (medium-to-high risk environments).

Υβριδικό Firewall



8.5 Παράδειγμα κανόνων λειτουργίας ενός Firewall

Ο παρακάτω ψευδοκώδικας αποτελεί ένα πολύ βασικό κανόνα που έχει καθοριστεί για τις ανάγκες ενός δικτύου που υποστηρίζει το ηλεκτρονικό εμπόριο.

#Pseudo-Code Ruleset for E-Commerce Network Firewall

#Format is as below:

#Allow or Deny, Src Address, Src Port, Dest Address, Dest Port

#Signs (#) indicate comments

#Network is 10.1.0.0/24

#Database Network is 10.2.0.0/24

#Financial Processing Network is 10.3.0.0/24

#Internal Company Network (Protected Network) is 10.4.0.0/24

#Allow Internal Network Traffic To All Except Dbase and Financial Nets

deny 10.4.0.0/24 all 10.2.0.0/24 all

deny 10.4.0.0/24 all 10.3.0.0/24 all

allow 10.4.0.0/24 all all all

#Allow the world to talk to the web servers on ports 80 (http) and 443 (https)

#You should also lock this down to specific hosts if possible.

allow any any 10.1.0.0/24 80

allow any any 10.1.0.0/24 443

#Allow the master web server to talk to the Dbase server via a defined port

allow 10.1.0.100/32 10092 10.2.0.10/32 10092

#Allow SMTP and Pop3

allow any any 10.1.0.15/32 25

allow any any 10.1.0.15/32 110

#Deny all else "Clean Up Rule"

deny any any any any

8.6 Firewalls στο εμπόριο

Μερικά από τα πιο γνωστά firewalls που κυκλοφορούν στο εμπόριο είναι:

CheckPoint FW-1

(www.checkpoint.com/products/firewall-1)

Cisco Pix Firewall

(www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html)

Gauntlet Firewall

(www.pgp.com/products/gauntlet/)

Symantec Raptor Firewall

(enterprisesecurity.symantec.com/products/products.cfm?ProductID=47&PID=3505192)

Secure Computing's Sidewinder Firewall

(www.securecomputing.com/index.cfm?skey=1111)

WatchGuard Appliance Firewalls

(www.watchguard.com/)

9 Η έννοια των προσωπικών δεδομένων

9.1 Πληροφορία και δεδομένα

Τόσο σε νομοθετικά κείμενα όσο και στη βιβλιογραφία παρατηρείται συχνά η ταυτόχρονη χρήση και εναλλαγή των όρων "δεδομένο" και "πληροφορία". Το ερώτημα που γεννιέται είναι ποια η σχέση μεταξύ δεδομένου και πληροφορίας. Ως εισαγωγική παρατήρηση αξίζει να σημειωθεί ότι τα δεδομένα αναδείχθηκαν, σημασιοδοτήθηκαν και καθιερώθηκαν ως "ξεχωριστός" όρος σε συνάρτηση με την επεξεργασία δεδομένων και κυρίως με την ανάπτυξη και διάδοση της αυτοματοποιημένης επεξεργασίας δεδομένων. Η συσχέτιση αυτή αναπόφευκτα τονίζει το "δεδομένο" ως τεχνικό όρο και μέρος ενός συστήματος επεξεργασίας και οδηγεί στον προσδιορισμό των "δεδομένων" ως στοιχείων μιας "επεξεργασμένης" πληροφορίας ως στοιχεία της πληροφορίας που έγινε αντικείμενο αυτοματοποιημένης επεξεργασίας.

Σύμφωνα με μια άποψη το δεδομένο διακρίνεται από την πληροφορία καταρχήν και κυρίως από ποσοτική άποψη: το δεδομένο συνιστά τη μικρότερη μονάδα πληροφορίας, ενώ σύμφωνα με άλλη διατύπωση το δεδομένο συνιστά "πληροφοριακό άτομο". Αυτό δε σημαίνει ωστόσο ότι η πληροφορία συνιστά μια "πολλαπλότητα δεδομένων". Συναφής είναι η θεώρηση δεδομένων ως ένα είδος "πρώτης ύλης" από την οποία προκύπτει η πληροφορία ως "ολοκληρωμένο προϊόν".

Περαιτέρω η έννοια "πληροφορία" παραπέμπει αυτόματα στην πληροφοριακή αξία της ενώ δεν συμβαίνει το ίδιο με τον όρο "δεδομένο". Στην έννοια του δεδομένου προσδίδεται μια ουδετερότητα όσον αφορά το σκοπό ενώ η έννοια της πληροφορίας συσχετίζεται με την χρησιμότητά της. Ανεξάρτητα από τις εννοιολογικές διαφορές πρέπει να παρατηρήσουμε ότι οι δύο όροι στη χρήση της γλώσσας έχουν καταλήξει να είναι συνώνυμοι.

9.2 Το περιεχόμενο μια πληροφορίας και η διάκριση σε "απλές" και "ευαίσθητες" πληροφορίες

Το "περιεχόμενο" φαίνοταν να υπήρξε το καθοριστικό σημείο για την διατύπωση του αιτήματος και την παραδοχη της ρύθμισης και κατ'επέκταση της προστασίας μιας πληροφορίας προσωπικού χαρακτήρα, υπό την έννοια ότι το (ιδιαίτερο) περιεχόμενο μιας πληροφορίας είναι εκείνο που δημιουργούσε την αναμονή ότι αυτή θα θεωρηθεί ως αυστηρά προσωπική ή ευαίσθητη και για το λόγο αυτό θα έπρεπε να παρεμποδιστεί η τουλάχιστον να περιοριστεί η συλλογή, η χρήση ή η κυκλοφορία της.

Σε αυτή την αντίληψη ανάγεται η άποψη ότι υπάρχουν "αβλαβή δεδομένα" και δεδομένα "ευαίσθητα" που χρήζουν προστασίας. Η αντίληψη αυτή προέρχεται από τη "θεωρία των σφαιρών προσωπικότητας" σύμφωνα με την οποία η ανθρώπινη ύπαρξη κατανέμεται σε τρεις σφαίρες:

- την ατομική στην οποία προσδιορίζονται τα χαρακτηριστικά γνωρίσματα της προσωπικότητας ενός ανθρώπου σε σχέση με τον κοινωνικό του περίγυρο,
- την ιδιωτική η οποία προσδιορίζει το πεδίο της δραστηριότητας ενός ανθρώπου, το οποίο είναι προσιτό μόνο σε στενό κύκλο προσώπων και σε τρίτους υπο προϋποθεσεις, και
- την απόρρητη ή μυστική σφαίρα που ορίζεται ως το πεδίο της ανθρώπινης προσωπικότητας, στο οποίο ένας άνθρωπος επιτρέπει την πρόσβαση μόνο από υπό εξαιρετικές περιστάσεις σε ιδιαίτερα στενό κύκλο προσώπων.

Η ταξινόμηση αυτή είχε το επιχείρημα ότι οι "κανονικές" πληροφορίες είναι "αβλαβείς" συνεπώς ελεύθερα προσιτές ενώ αντίθετα ιδιαίτερη μεταχείριση και ρύθμιση χρειάζονται οι ευαίσθητες πληροφοριες.

Μια τέτοια ταξινόμηση των πληροφοριών, ανταποκρίνεται μεν στην κλασική θεωρία των ζωνών της ανθρωπινης ύπαρξης και προσωπικότητας και ίσως σε διαδεδομένες κοινωνικές αντιλήψεις σχτικά με το τι είναι ιδιωτικό, απόκρυφο, απόρρητο, δεν λαμβάνει όμως υπόψη τις δυνατότητες και τις επιπτώσεις της αυτοματοποιημένης επεξεργασίας: τα δεδομένα προσωπικού χαρακτήρα δεν είναι εκ των προτέρων ασήμαντα ή "ευαίσθητα". Αποκτούν ή υποβάλλουν αυτούς τους προσδιορισμούς ανάλογα με το σκοπό και τη συγκυρία, στην οποία χρησιμοποιούνται. Έτσι οι πληροφορίες που φαίνονται συνηθισμένες σε ένα πλαίσιο σε μια άλλη συγκυρία μπορούν να αποβούν "υπερευαίσθητες".

9.3 Ο νομοθετικός προσδιορισμός της "προσωπικής πληροφορίας" ή "δεδομένου προσωπικού χαρακτήρα"

Ενδεικτική της τάσης επιλογής μιας ευρείας έννοιας της "προσωπικής πληροφορίας" ή των "δεδομένων προσωπικού χαρακτήρα" είναι η ρύθμιση της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών". Ο ορισμός των δεδομένων προσωπικού χαρακτήρα στην οδηγία (άρθρο 2 α) επιλέγει ως στοιχείο του προσωπικού χαρακτήρα τη "σύνδεση" με ένα φυσικό πρόσωπο, προσδιορισμένο ή προσδιορίσιμο. Δεν υπάρχει αναφορά στην πληροφορία καθ' αυτή, δηλαδή στο περιεχόμενό της, την ποιότητά της ως προσωπικής , στο είδος της σύνδεσης της με το πρόσωπο, στο αν το άτομο την προσδιορίζει ως προσωπική.

Ο ορισμός των δεδομένων προσωπικού χαρακτήρα της οδηγίας περιλαμβάνει ταυτόχρονα τον ορισμό του προσώπου το οποίο αφορούν τα δεδομένα. Συγκεκριμένα ως "δεδομένα προσωπικού χαρακτήρα" προσδιορίζονται όλες οι πληροφορίες που αφορούν ένα φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να προδιοριστεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά τα οποία χρησιμοποιούνται συνήθως για τον προσδιορισμό της ταυτότητας του προσώπου. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός του δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (π.χ κωδικός πρόσβασης).

Οι προσωπικές πληροφορίες μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις προς πράγματα. Σε αυτές τις σχέσεις αντιστοιχούν πληροφορίες τόσο για τα εξωτερικά στοιχεία όσο και για ψυχικές καταστάσεις (κίνητρα, επιθυμίες,απόψεις), ενέργειες, αντιδράσεις, τρόπους συμπεριφοράς ανεξάρτητα από το αν αφορούν το παρόν ή το παρελθόν και πόσο αντρέχουν σε αυτό. Είναι αναμφισβήτητο ότι στις πληροφορίες προσωπικού χαρακτήρα εντάσσονται και οι σχέσεις προς το περιβάλλον, όπως στοιχεία για την περιουσιακή και οικογενιακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις καθώς και για τις σχέσεις και καταστάσεις ιδιωτικού και δημόσιου δικαίου (ιδιοκτησία, διοικητικές άδειες, συμβατικές σχέσεις κλπ).

Δεδομένα προσωπικού χαρακτήρα θεωρούνται και οι αξιολογικού χαρακτήρα κρίσεις στο βαθμό που δηλώνουν σχέσεις προς πρόσωπα ή πράγματα και αποσκοπούν σε μια πληροφορική δήλωση για το πρόσωπο το οποίο αφορά η πληροφορία. Μια αξιολογική κρίση όπως π.χ "καλός πελάτης" ακόμα και αν δεν περιέχει τα στοιχεία επί των οποίων βασίζεται η "αξιολόγηση" δηλώνει κάτι για τις σχέσεις του προσώπου στο οποίο αναφέρονται.

9.4 Το αίτημα της προστασίας των προσωπικών δεδομένων

Η δημιουργία μιας "αγοράς προσωπικών πληροφοριών" έχει συνέπειες για τα δικαιώματα και τις ελευθερίες των ατόμων. Η αυξανόμενη χρήση και εμπορευματοποίηση των προσωπικών δεδομένων έχει οδηγήσει στην περιαγωγή των προσωπικών δεδομένων και εν τέλει των προσώπων που αυτά αφορούν σε "αντικείμενο των συναλλαγών", καθώς αυτά αντιμετωπίζονται ως το σύνολο μιας ποικιλίας δεδομένων που μπορούν να αποχωριστούν και να χρησιμοποιηθούν κατά βούληση, ακόμη και για οικονομικούς και εμπορικούς σκοπούς. Το άτομο περιπίπτει στη θέση ενός "πληροφοριακού αντικειμένου".

Το αίτημα της "προστασίας" διατυπώθηκε "αυθόρμητα" με την αφηρημένη επίκληση της προστασίας του ιδιωτικού βίου, των "ευαίσθητων πληροφοριών", της "απόρρητης σφαίρας". Οι προσεγγίσεις και οι απόψεις για το θεμέλιο της "προστασίας προσωπικών δεδομένων" που εκφράστηκαν δεν ήταν και δεν είναι ενιαίες. Διακρίνονται σε δύο βασικές κατηγορίες:

- αυτές που αναδεικνύουν την περιουσιακή διάσταση των προσωπικών δεδομένων και των αντίστοιχων δικαιωμάτων και αντιμετωπίζουν το δικαίωμα προστασίας των προσωπικών δεδομένων ως ιδιοκτησιακό ή περιουσιακό δικαίωμα

- αυτές που επικεντρώνουν την ανάλυσή τους στις ατομικές ελευθερίες και τις επικοινωνιακές σχέσεις που σχετίζονται με την επεξεργασία και την προστασία των προσωπικών δεδομένων και αντιμετωπίζουν την προστασία προσωπικών δεδομένων ως δικαίωμα της ελευθερίας και της προσωπικότητας κάθε προσώπου.

9.5 Νομοθετική προστασία των προσωπικών δεδομένων: Η διεθνής διάσταση

Η ανάγκη προστασίας της ιδιωτικότητας διατυπώνεται ήδη στη σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστσία των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών. Στο άρθρο 8 ρυθμίζεται το δικαίωμα κάθε προσώπου να γίνεται σεβαστή η ιδιωτική και οικογενειακή του ζωή, η κατοικία του και η αλληλογραφία του.

Στα πρώτα σχετιά κείμενα κατατάσσεται επίσης η απόφαση 2450/19.12.1968 της γεβικής συνέλευσης των Ηνωμένων Εθνών, η οποία αφορά τα προβλήματα που ανακύπτουν σχετικά με τα ναθρώπινα δικαιώματα από την ανάπτυξη της επιστήμης και της τεχνολογίας και ειδικότερα από τη χρήση των ηλεκτρονικών μέσων.

Ο οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) υπήρξε ο δεύτερος διεθνής οργανισμός που ασχολήθηκε με την προστσία προσωπικών δεδομένων, εκδίδοντας τις λεγόμενες "κατευθυντήριες αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων". Οι αρχές αυτές περιλαμβάνουν την αρχή της περιορισμένης συγκέντρωσης και συλλογής των δεδομένων, την αρχή της ποιότητας των δεδομένων, την αρχή του προσδιορισμένου σκοπού, την αρχής της περιορισμένης χρήσης των προσωπικών δεδομένων, την αρχή μέτρων ασφαλείας των προσωπικών δεδομένων, την αρχή της διαφάνειας και τέλος την αρχή της ευθύνης.

Η πρώτη ουσιαστική κωδικοποίηση των αρχών που αποτελούν τον "σκληρό πυρήνα" της προστασίας δεδομένων προσωπικού χαρακτήρα συντελείται με τη σύμβαση 108/28.1.1981 "για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα" του Συμβουλίου της Ευρώπης. Η σύμβαση αυτή αποτέλεσε την αφετηρία μιας δεύτερης περιόδου για την προστασία από την επεξεργασία προσωπικών δεδομένων και αρκετές χώρες ψήφισαν ειδικούς νόμους ενώ άλλες τροποποίησαν τις νομοθεσίες τους.

Σταθμός όμως για την προστασία δεδομένων προσωπικού χαρακτήρα θεωρείται η κοινοτική οδηγία 95/46/ΕΚ "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών".

Το κοινοτικό κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων συμπληρώθηκε από την οδηγία 97/66/ΕΚ για την προστσία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Η Ευρωπαϊκή Ένωση έκδωσε επίσης την οδηγία 2000/31/ΕΚ «για ορισμένες πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά». Η οδηγία αυτή σκοπό έχει την ομαλή διεξαγωγή του ηλεκτρονικού εμπορίου, μέσα από τη θεσμοθέτηση ενός ενιαίου και σταθερού νομοθετικού πλαισίου σε όλες τις χώρες-μέλη της ΕΕ. Τα άρθρα τα οποία έχουν άμεσο αντίκτυπο στη διεξαγωγή του ηλεκτρονικού εμπορίου και έχουν ισχύ από την 17η Ιανουαρίου 2002 είναι τα παρακάτω:

- Άρθρο 4: Αρχή της μη αναγκαίας προηγούμενης άδειας. Η Ευρωπαϊκή ένωση ορίζει ότι η άσκηση επαγγέλματος παροχής υπηρεσιών της κοινωνίας της πληροφορίας δεν απαιτεί και κατά κανέναν τρόπο δεν θα έπρεπε να απαιτεί έκδοση άδειας. Εξαίρεση αποτελούν οι περιπτώσεις που δεν αφορούν αποκλειστικά και μόνο υπηρεσίες της κοινωνίας της πληροφορίας.

- Άρθρο 5: Γενικές πληροφορίες που πρέπει να παρέχονται. Η Ευρωπαϊκή Ένωση ορίζει ότι ο φορέας υπηρεσιών της κοινωνίας της πληροφορίας οφείλει να παρέχει άμεση και συνεχή πρόσβαση σε πληροφορίες όπως:

- επωνυμία του φορέα,

- γεωγραφική διεύθυνση όπου είναι εγκατεστημένος,

- στοιχεία που επιτρέπουν την άμεση επικοινωνία με το φορέα, συμπεριλαμβανομένης της ηλεκτρονικής του διεύθυνσης,

- το εμπορικό ή άλλο δημόσιο μητρώο του φορέα, εφόσον αυτός είναι εγγεγραμμένος σε τέτοιο,

- τα στοιχεία της εποπτικής αρχής, εάν η δραστηριότητα υπόκειται σε τέτοιου είδους έλεγχο,

όσον αφορά τα νομικώς κατοχυρωμένα επαγγέλματα:

- επαγγελματική ένωση ή παρόμοιο όργανο όπου είναι εγγεγραμμένος ο φορέας,

- επαγγελματικό τίτλο και τι κράτος μέλος όπου έχει χορηγηθεί,

- μνεία των επαγγελματικών κανόνων που ισχύουν στο κράτος μέλος εγκατάστασης, καθώς και του τρόπου πρόσβασης σε αυτούς,

- Εάν η δραστηριότητα υπόκειται σε ΦΠΑ, τον αριθμό αναγνώρισης.

Θα πρέπει επίσης να εξασφαλίζεται ότι εάν η υπηρεσία της κοινωνίας της πληροφορίας αναφέρεται σε τιμές, αυτές θα πρέπει να αναγράφονται σαφώς και επακριβώς και να αναφέρεται επίσης εάν περιλαμβάνουν φόρο και έξοδα αποστολής.

- Άρθρο 9: Μεταχείριση ηλεκτρονικών συμβάσεων. Τα κράτη μέλη πρέπει να έχουν μεριμνήσει ώστε οι συμβάσεις που συνάπτονται με ηλεκτρονικά μέσα να μην θεωρούνται νομικά υποδεέστερες από τις συμβάσεις που συνάπτονται με τον παραδοσιακό τρόπο. Ωστόσο, εξαίρεση προβλέπεται για ειδικές περιπτώσεις συμβάσεων, όπως η μεταβίβαση ακίνητης περιουσίας, οι συμβάσεις που απαιτούν εκ νόμου προσφυγή σε δημόσιες αρχές ή δικαστήρια, συμβάσεις εγγυοδοσίας και συναφούς ασφάλειας και συμβάσεις που εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο. Τα κράτη μέλη οφείλουν να ανακοινώνουν τις κατηγορίες συμβάσεων που δεν θεωρούνται έγκυρες ηλεκτρονικά.

- Άρθρο 11: Παραγγελία. Όταν ένας αποδέκτης υπηρεσίας αναθέτει παραγγελία με ηλεκτρονικά μέσα και εφόσον δεν έχει συμφωνηθεί από τα συμβαλλόμενα μέρη διαφορετικά, ισχύουν οι ακόλουθες αρχές:

- ο φορέας παροχής των υπηρεσιών οφείλει να αποστέλλει αποδεικτικό της παραλαβής της παραγγελίας του αποδέκτη άμεσα και με ηλεκτρονικά μέσα,

- η παραγγελία και το αποδεικτικό παραλαβής θεωρείται ότι έχουν παραληφθεί όταν τα μέρη στα οποία απευθύνονται έχουν πρόσβαση σε αυτά.

Στην συνέχεια ακολούθησε η οδηγία 2002/58/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα στο τομέα των ηλεκτρονικών επικοινωνιών η οποία αποτελούσε αντικατάσταση της οδηγίας 97/66/ΕΚ.

9.6 Ελληνικό νομοθετικό πλαίσιο

Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική οδηγία στο εσωτερικό δίκαιο, παρά το γεγονός ότι ήδη από το 1985, είχαν εκπονηθεί σχετικά προσχέδια νόμου και μάλιστα είχαν κατατεθεί στο Κοινοβούλιο σχέδια και προτάσεις νόμου. Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται κυρίως:

- από την οικεία συνταγματική ρύθμιση
- τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις από τους Ν.2819/2000 (ΦΕΚ Α' 84) και Ν.2915/2001 (ΦΕΚ Α' 109). Ο Ν.2472/97 μεταφέρει τις ρυθμίσεις της κοινοτικής οδηγίας για την προστασία δεδομένων (95/46/ΕΚ) στην εσωτερική έννομη τάξη

Υπάρχουν ωστόσο και άλλες προγενέστερες ή μεταγενέστερες ρυθμίσεις που είτε άπτονται (άμεσα ή έμμεσα) της προστασίας προσωπικών δεδομένων, όπως τα άρθρα 57-59 του Αστικού Κώδικα για την προστασία της προσωπικότητας ή τα άρθρα για την προστασία της σφαίρας του απορρήτου (όπως π.χ τα άρθρα 248 και 370Α του Ποινικού Κώδικα) είτε παραπέμπουν στον Ν.2472/97 για την παροχή εγγυήσεων στην περίπτωση της προστασίας προσωπικών δεδομένων.

Γενικότερα το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) με τον οποίο η Αρχή Προστασίας Δεδομένων και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχουν αντίστοιχες αρμοδιότητες όπως ο νόμος αυτός ορίζει. Κάθε συλλογή και επεξεργασία στοιχείων των χρηστών του διαδικτύου (π.χ. ηλεκτρονική διεύθυνση αλληλογραφίας, διεύθυνση διαδικτύου κ.λ.π) εμπίπτουν στις διατάξεις των παραπάνω νόμων. Οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών όπως ορίζονται στο νόμο 2774/99 προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/94 όπως ισχύει.

Αναλυτικότερα ο νόμος 2472/1997 του ελληνικού δικαίου για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα οριοθετεί τη λήψη και επεξεργασία προσωπικών δεδομένων. Επίσης, ορίζει τη συγκρότηση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που επιφορτίζεται με το ρόλο του ελέγχου και της επιβολής κυρώσεων πάνω σε τέτοια θέματα. Ο νόμος έχει συνταχθεί σε συμφωνία με τις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ του Ευρωπαϊκού κοινοβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων.

Ο νόμος ορίζει ότι, για να τύχουν νόμιμης επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα πρέπει:

- Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών
- Να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας

- Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση

- Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής [...]. Η τήρηση των διατάξεων της παραγράφου αυτής βαρύνει τον υπεύθυνο επεξεργασίας.

Όσον αφορά τις προϋποθέσεις επεξεργασίας τέτοιων δεδομένων, ο νόμος ορίζει ρητά ότι επιτρέπεται όταν το υποκείμενο των δεδομένων έχει δώσει την συγκατάθεσή του. Εξαίρεση αποτελούν ορισμένες ειδικές περιπτώσεις, όπως για παράδειγμα αν ο υποκείμενος τελεί σε φυσική αδυναμία να δώσει τη συγκατάθεση του και η τελευταία είναι απολύτως απαραίτητη.

Πρέπει επίσης να σημειωθεί ότι σύμφωνα με τον ίδιο νόμο ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας, γνωστοποιώντας τα στοιχεία της επιχείρησης.

Η συλλογή και η επεξεργασία ευαίσθητων δεδομένων απαγορεύεται από το νόμο. Επιτρέπεται μόνο κατ' εξαίρεση και ύστερα από ειδική άδεια της Αρχής, για ορισμένες ειδικές περιπτώσεις. Για να γίνει αυτό πρέπει να εκδοθεί ειδική άδεια από την Αρχή, ορισμένου χρόνου.

Η διασύνδεση αρχείων προσωπικών δεδομένων μπορεί να γίνει επιτροπή από την Αρχή έπειτα από δήλωση που καταθέτουν από κοινού οι υπεύθυνοι επεξεργασίας των αρχείων που διασυνδέονται. Η άδεια που εκδίδεται είναι περιορισμένου χρόνου και μπορεί να ανανεωθεί ύστερα από αίτηση των υπεύθυνων επεξεργασίας. Η διαβίβαση δεδομένων προς χώρα της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Το ίδιο ισχύει, έπειτα από έκδοση άδειας, και για χώρες για τις οποίες θεωρείται ότι διατηρείται ένα υψηλό επίπεδο ασφαλείας. Για τις υπόλοιπες χώρες δεν επιτρέπεται η εξαγωγή προσωπικών δεδομένων, εκτός και αν συντρέχουν ιδιαίτεροι λόγοι, όπως η συγκατάθεση του υποκειμένου.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη και διεξάγεται αποκλειστικά από τον υπεύθυνο επεξεργασίας και από κατάλληλα καταρτισμένα πρόσωπα που τελούν υπό τις εντολές του. Ο υπεύθυνος επεξεργασίας πρέπει να διαφυλάσσει τα δεδομένα από τυχόν απώλεια, κλοπή ή καταστροφή. Αν η επεξεργασία διεξάγεται από πρόσωπο διορισμένο από τον υπεύθυνο επεξεργασίας, πρέπει η ανάθεση να έχει γίνει εγγράφως.

Τέλος, άξια αναφοράς είναι τα άρθρα 370Β, 370Γ και 386^{Α} του ποινικού κώδικα που αναφέρονται στο ηλεκτρονικό έγκλημα.

- Το άρθρο 370Β ορίζει ότι όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

- Το άρθρο 370Γ αναφέρεται στα εξής:

- Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και χρηματικό πρόστιμο 300 έως 6.000 ευρώ

- Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με σήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 3.000 ευρώ

Το άρθρο 386Α αφορά την απάτη με υπολογιστή και αναφέρεται ότι όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή, είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλειπών στοιχείων, είτε με οποιονδήποτε άλλον τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα άτομα.

9.7 Ηλεκτρονικό εμπόριο και προσωπικά δεδομένα

Οι έμποροι θέλοντας να διαπιστώσουν τις καταναλωτικές προτιμήσεις του κοινού με σκοπό να ορίσουν τη βάση πάνω στην οποία θα βασιστεί η παραγωγή τους και να προωθήσουν τις πωλήσεις τους μέσω του διαδικτύου, δημιουργούν νέους τρόπους συλλογής, επεξεργασίας και διασύνδεσης των προσωπικών δεδομένων.

Τα προσωπικά δεδομένα τις περισσότερες φορές συλλέγονται κατά την διαδικασία σύνδεσης του πελάτη (client) με τον δικτυακό τόπο του πωλητή (server) και εισάγωνται σε βάσεις δεδομένων όπου με τη χρήση τεχνικών ανάλυσης πληροφοριών γίνεται καταχώρηση σύμφωνα με καταναλωτικό προφίλ των πελατών.

Οι οντότητες οι οποίες τυπικά εμπλέκονται στην εγκατάσταση μιας ηλεκτρονικής σύνδεσης, με σκοπό την πραγματοποίηση ηλεκτρονικών συναλλαγών είναι οι ακόλουθες:

- Χρήστης: Ο ενδιαφερόμενος για την απόκτηση μιας υπηρεσίας του διαδικτύου, την απόκτηση ενός προϊόντος με χρήση τεχνολογιών που βοηθούν στην ανάπτυξη του ηλεκτρονικού εμπορίου κ.λ.π.

- Παροχέας Υπηρεσιών Διαδικτύου, ΠΥΔ, (Internet Service Provider, ISP): Η οντότητα που παρέχει, τυπικά σε χρήστες, το υλικό (hardware) και πιθανώς λογισμικό (software), για την απόκτηση πρόσβασης στις βασικές υπηρεσίες του διαδικτύου.

- Παροχέας Φυσικού Μέσου επικοινωνίας, ΠΦΜ, (Carrier Provider): Η οντότητα που παρέχει το φυσικό τεχνολογικό μέσο μετάδοσης και επικοινωνίας δεδομένων π.χ. αναλογικές ή/και ψηφιακές γραμμές, εξοπλισμός αναμετάδοσης σημάτων με χρήση ψηφιακών κέντρων, δορυφόρων κ.λ.π. Οι οντότητες αυτές τυπικά αντιπροσωπεύονται από μεγάλους τηλεπικοινωνιακούς οργανισμούς π.χ. ΟΤΕ.

- Παροχέας Τελικής Υπηρεσίας ΠΤΥ. Η οντότητα που παρέχει με χρήση κάποιου πρωτοκόλλου επικοινωνίας, την ζητούμενη από τον χρήστη υπηρεσία π.χ. αναζήτηση πληροφοριών με χρήση μηχανών αναζήτησης (search machines), αγορά προιόντων με χρήση τεχνολογιών ανάπτυξης ηλεκτρονικού εμπορίου κ.λ.π.

9.7.1 Οι κίνδυνοι

Ο χώρος του ηλεκτρονικού εμπορίου κρύβει πολλούς κινδύνους για τον ανυποψίαστο χρήστη. Οι περιπτώσεις όπου διακριτά καταγράφονται προσωπικά δεδομένα διακρίνονται στις παρακάτω κατηγορίες:

- Όταν με τη συγκατάθεσή του ο χρήστης δίνει τα προσωπικά του στοιχεία, όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν /υπηρεσία ή να κατεβάσει (download) κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου. Προσωπικά δεδομένα, όπως στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης ή και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.

- Όταν χωρίς την συγκατάθεσή του χρήστη, συλλέγονται προσωπικά στοιχεία μέσω των λεγόμενων προγραμμάτων cookies τα οποία καταγράφουν και επεξεργάζονται την συμπεριφορά του χρήστη κατά την πλοήγησή του στο διαδίκτυο (πχ προτιμήσεις).

- Όταν στα πλαίσια του παροχέα υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ' επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων (ιστοσελίδες) τις οποίες επισκέπτεται, τον ακριβή χρόνο και τη διάρκεια της επίσκεψης.

Είναι γεγονός, ότι σε όλες τις παραπάνω περιπτώσεις, η συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να οδηγήσει σε παραβίαση της ιδιωτικής και προσωπικής ζωής του χρήστη όταν αυτή δεν εφαρμόζεται σύμφωνα με τις οικείες διατάξεις. Αποτελέσματα δημοσκοπήσεων, έχουν δείξει ότι η έλλειψη προστασίας της ιδιωτικότητας στις επικοινωνίες είναι ο κύριος λόγος αποχής των δυνητικών χρηστών από την χρήση των υπηρεσιών του διαδικτύου. Οι χρήστες θεωρούν ότι η έλλειψη ιδιωτικότητας στις επικοινωνίες είναι ο σημαντικότερος παράγοντας που εμποδίζει την ανάπτυξη του ηλεκτρονικού εμπορίου και τη θεωρούν σημαντικότερη από άλλους παράγοντες όπως το κόστος πραγματοποίησης ηλεκτρονικών συναλλαγών, οι δυσκολίες χρήσης του τεχνολογικού εξοπλισμού και η παραλαβή ανεπιθύμητων ηλεκτρονικών διαφημιστικών μηνυμάτων.

9.7.2 Τα μέτρα προφύλαξης

Το αντίδοτο στην παραβίαση της προσωπικής ζωής είναι η δημιουργία καναλιών επικοινωνίας που δεν αποκαλύπτουν την ταυτότητα των επικοινωνούντων μερών. Η εξέλιξη στις τεχνολογίες πληροφορικής σήμερα, δίνει τη δυνατότητα σε οργανισμούς να επεξεργάζονται απλά ή/και ευαίσθητα προσωπικά δεδομένα, έτσι όπως αυτά νοούνται στο Ν.2472/97 με μεγάλη ταχύτητα.

Σήμερα έχουν αναπτυχθεί τεχνολογίες οι οποίες βοηθούν τους χρήστες του διαδικτύου να αυξήσουν αφενός την ασφάλεια των συνδέσεων που πραγματοποιούν με χρήση του διαδικτύου και αφετέρου να διατηρήσουν το δικαίωμα της ανωνυμίας των διακινούμενων πληροφοριών που τους αφορούν. Οι μεν πρώτες είναι γνωστές ως τεχνολογίες ασφάλειας πληροφοριών, ΤΑΠ, (Infromation Security Technologies, IST) οι δε δεύτερες ως τεχνολογίες αύξησης ιδιωτικότητας, ΤΑΙ (Privacy Enhancing Technologies, PETs).

Οι χρήστες που χρησιμοποιούν υπηρεσίες ηλεκτρονικού εμπορίου θα πρέπει να:

- Χρησιμοποιούν όλα τα διαθέσιμα μέσα για να προστατεύουν τα δεδομένα που τους αφορούν και τις επικοινωνίες, όπως τα νόμιμα διαθέσιμα τεχνολογικά εργαλεία κρυπτογράφησης δεδομένων, ηλεκτρονικού ταχυδρομείου, κωδικών πρόσβασης κ.λ.π.

- Είναι προσεκτικοί σε σχέση με τις πληροφορίες που μεταβιβάζουν σε κάθε επίσκεψή τους στις ιστοσελίδες ενός δικτυακού τόπου, κατά την πραγματοποίηση μιας ηλεκτρονικής σύνδεσης και γενικότερα μιας επικοινωνίας με χρήση του διαδικτύου. Οι προσωπικές πληροφορίες που μεταβιβάζονται ποικίλλουν και αφορούν σε:

- Πληροφορίες που μεταβιβάζονται εις γνώσιν του χρήστη π.χ. ονοματεπώνυμο, ταχυδρομική διεύθυνση κ.λ.π.

- Πληροφορίες που μεταβιβάζονται εν αγνοία του χρήστη π.χ. IP διεύθυνση, το όνομα του υπολογιστή κ.λ.π. Τις περισσότερες φορές η μεταβίβαση αυτών των πληροφοριών είναι αναγκαία για λόγους επίτευξης της επικοινωνίας και επιβάλλεται από την φύση της σχεδίασης των επικοινωνιακών πρωτοκόλλων

- Αναζητά και να του παρέχονται, στο βέλτιστο βαθμό, τεχνολογίες που του εξασφαλίζουν την ανωνυμία στο βαθμό εκείνο που δεν θίγονται άλλοι νόμοι και αρχές που θεωρούνται ανώτερες από την προσωπική ζωή

- Αποκαλύπτει μόνο τα δεδομένα εκείνα που είναι απαραίτητα για την επίτευξη των σκοπών που επιδιώκονται μέσω της συγκεκριμένης επικοινωνίας ή συναλλαγής. Ιδιαίτερη προσοχή πρέπει να δοθεί στην περίπτωση αποκάλυψης αριθμών πιστωτικών καρτών, στοιχείων τραπεζικών λογαριασμών, ευαίσθητων δεδομένων κ.λ.π. Σε αυτές τις περιπτώσεις συστήνεται η χρήση τεχνολογιών διασφάλισης εμπιστευτικότητας πληροφοριών (SSL)

10 Ηλεκτρονικό εμπόριο και επιχειρήσεις

10.1 Τι πρέπει να προσέξει μια επιχείρηση που επιθυμεί την είσοδό της στο χώρο του ηλεκτρονικού εμπορίου

Η ηλεκτρονική επιχειρηματική δραστηριότητα της επιχείρησης πρέπει να είναι σύμφωνη με την ισχύουσα νομοθεσία σε εθνικό και κοινοτικό επίπεδο. Απαιτείται ενημέρωση για όλες τις ειδικές διατάξεις που αφορούν στο Ηλεκτρονικό Εμπόριο. Σε περίπτωση οποιασδήποτε αμφιβολίας για τα νομικά θέματα η επικοινωνία με τους συλλογικούς φορείς ή με εξειδικευμένους νομικούς συμβούλους θα ωφελήσει στην λήψη των κατάλληλων απαντήσεων. Η προστασία των προσωπικών δεδομένων των καταναλωτών που επισκέπτονται το ηλεκτρονικό κατάστημα αποτελεί βασική υποχρέωση. Τα προσωπικά δεδομένα δεν είναι "ελεύθερο εμπόρευμα". Πρέπει να χρησιμοποιούνται μόνο για το σκοπό για τον οποίο συλλέγονται και να διατηρούνται μόνο όσο είναι αναγκαίο για τη συγκεκριμένη συναλλαγή.

Συλλογή και επεξεργασία προσωπικών δεδομένων που δεν εντάσσονται σε συγκεκριμένη συναλλαγή μπορεί να γίνει μόνο με τη ρητή συγκατάθεση των καταναλωτών, αφού προηγουμένως ενημερωθούν για το σκοπό, τις κατηγορίες των δεδομένων κλπ. Η συγκατάθεσή τους είναι απαραίτητη και στην περίπτωση που το ηλεκτρονικό κατάστημα θέλει να διαβιβάσει τα δεδομένα τους σε τρίτους. Η εμφανής παρουσίαση των τρόπων προστασίας και χρήσης των προσωπικών δεδομένων στο δικτυακό σας τόπο (Privacy Statement) αποτελεί σημαντικό βήμα για την οικοδόμηση κλίματος εμπιστοσύνης μεταξύ του ηλεκτρονικού καταστήματος και του καταναλωτή.

Επιπλέον, οι επισκέψεις των καταναλωτών σε ένα ηλεκτρονικό κατάστημα και οι συναλλαγές τους αφήνουν ψηφιακά ίχνη, τα οποία χρησιμοποιούνται συχνά για τη δημιουργία καταναλωτικού προφίλ. Η συλλογή των δεδομένων αυτών, με τεχνολογίες όπως τα cookies εν αγνοία των καταναλωτών και χωρίς τη συγκατάθεσή τους, συνιστά παράβαση.

Το Ηλεκτρονικό Εμπόριο αφορά και στις πωλήσεις προϊόντων και υπηρεσιών προς καταναλωτές διαφορετικών χωρών, στα πλαίσια των κρατών-μελών της Ευρωπαϊκής Ένωσης, σε περίπτωση διαφωνίας, ο καταναλωτής μπορεί να απευθυνθεί στις δικαστικές αρχές του τόπου κατοικίας του.

Σε μια ηλεκτρονική επικοινωνία, η εμπιστοσύνη μεταξύ των συναλλασσομένων μερών είναι πολύ σημαντική, γι' αυτό χρειάζεται ιδιαίτερη έμφαση στο θέμα της ασφάλειας των συναλλαγών. Σήμερα, η τεχνολογία παρέχει προηγμένες λύσεις στο θέμα αυτό. Ένα ηλεκτρονικό κατάστημα που μεριμνά για την ασφάλεια των πελατών του οφείλει να χρησιμοποιεί και να αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφαλείας (πρωτόκολλο ασφαλείας π.χ. Secure Socket Layer - SSL, ή Secure Electronic Transaction - SET) καθώς και να παρέχει τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του (ψηφιακό πιστοποιητικό ταυτότητας από κάποιο αναγνωρισμένο φορέα πιστοποίησης).

Οι έλεγχοι για την ασφάλεια και την εγκυρότητα του ηλεκτρονικού καταστήματος πρέπει να γίνονται ανεξάρτητα από το αν η πρόσβαση στο διαδίκτυο γίνεται από τον υπολογιστή, από κινητό τηλέφωνο (WAP) ή από τη διαδραστική τηλεόραση (interactive TV).

Όσον αφορά στην "ταυτότητά" του, ένα ηλεκτρονικό κατάστημα θα πρέπει να παρουσιάζει ρητά σε ποιόν ακριβώς έχει κατοχυρωθεί, δηλαδή ποιος είναι ο πραγματικός ιδιοκτήτης. Η ύπαρξη ενός ειδικού σήματος στην ιστοσελίδα που να πιστοποιεί την ταυτότητα (από γνωστούς δημόσιους ή ιδιωτικούς οργανισμούς) αποτελεί πλεονέκτημα. Επιπλέον, θα πρέπει να παρέχεται η δυνατότητα στον καταναλώτή, προτού προβεί σε αγορές, να επικοινωνήσει με τον τηλεφωνικό αριθμό στη φυσική έδρα του καταστήματος (είναι υποχρεωτική η αναγραφή του στην ιστοσελίδα) ώστε να διαπιστώσει ότι όντως πρόκειται για το κατάστημα που έχει επιλέξει.

Συνοπτικά, οι πληροφορίες που πρέπει να αναφέρει κάθε ηλεκτρονικό κατάστημα στους καταναλωτές συνοψίζονται στα παρακάτω:

- Πραγματική ταυτότητα του εμπόρου (όνομα, γεωγραφική διεύθυνση, τηλέφωνο κλπ.)
- Τρόποι επικοινωνίας τόσο με ηλεκτρονικό όσο και με συμβατικό τρόπο (ηλεκτρονικό ταχυδρομείο [email], fax, τηλέφωνο, κλπ.)
- Τελική τιμή του προϊόντος ή της υπηρεσίας συμπεριλαμβανομένων των φόρων, εξόδων αποστολής, κλπ.)
- Εγγύηση του προϊόντος.
- Μέθοδος αποστολής και χρόνος παράδοσης, δυνατότητα υπαναχώρησης, τρόπος πληρωμής και παράδοσης, κλπ.
- Τρόπος ακύρωσης της παραγγελίας σε περίπτωση λάθους ή αλλαγής γνώμης.
- Επιβεβαίωση της παραλαβής της παραγγελίας.
- Πληροφορίες για την προστασία των προσωπικών δεδομένων (Privacy Statement)
- Πού μπορεί να απευθυνθεί ο καταναλωτής για τα παράπονά του εάν κάτι δεν πάει καλά (π.χ. αργοπορημένη παράδοση ή μη παράδοση).
- Πώς θα επιστραφεί το προϊόν, τι πρόσθετες επιβαρύνσεις υπάρχουν για την επιστροφή, κλπ.
- Ποιο δικαστήριο είναι αρμόδιο και ποίο Δίκαιο θα εφαρμοσθεί σε περίπτωση διαφοράς.

Τέλος πολλοί καταναλωτές διστάζουν να δώσουν τον αριθμό της πιστωτικής τους κάρτας σε ένα ηλεκτρονικό κατάστημα ακόμη και αν αυτό είναι γνωστό και καθιερωμένο. Για την αντιμετώπιση της πιθανής επιφυλακτικότητας των πελατών στο να δώσουν τα στοιχεία της πιστωτικής τους κάρτας, απαιτείται η παροχή εναλλακτικών τρόπων πληρωμής, όπως είναι η αντικαταβολή ή η αποστολή του αριθμού της πιστωτικής κάρτας μέσο fax σε αρμόδιο υπάλληλο της επιχείρησης.

10.2 Μελέτη Περίπτωσης: Παπασωτηρίου

Το ηλεκτρονικό κατάστημα Παπασωτηρίου (http://www.papasotiriou.gr) αποτελεί ένα από τα πρώτα καταστήματα που έκαναν της είσοδο τους στο χώρο του ηλεκτρονικού εμπορίου. Τα προϊόντα που εμπορεύεται ποικίλουν και περιλαμβάνουν κυρίως βιβλία ξενόγλωσσα και ελληνικά, παιχνίδια, καθώς και λογισμικό ηλεκτρονικού υπολογιστή.

Πατώστας στην επιλογή "Ασφάλεια Συναλλαγών" η οποία βρίσκεται στο κάτω μέρος της σελίδας μας δίνονται οι ακόλουθες πληροφορίες:

- Προστασία των συναλλαγών

Το Papasotiriou.gr χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128bit (την πιο ισχυρή σήμερα), για ασφαλείς on-line εμπορικές συναλλαγές. Με αυτό τον τρόπο κρυπτογραφούνται όλες οι προσωπικές σας πληροφορίες, συμπεριλαμβανομένων του αριθμού της πιστωτικής κάρτας, του ονόματος και της διεύθυνσής σας, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχτούν κατά τη μεταφορά τους στο Internet. Το πρωτόκολλο SSL (Secure Sockets Layer) είναι σήμερα το παγκόσμιο standard στο Διαδίκτυο για την πιστοποίηση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών (web servers).

Μία κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να

κρυπτογραφούνται από το λογισμικό αποστολής και να αποκρυπτογραφούνται από το λογισμικό αποδοχής, προστατεύοντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατεύονται από ένα μηχανισμό που αυτόματα εξακριβώνει εάν τα δεδομένα έχουν αλλαχτεί κατά τη μεταφορά. Το σύστημα ασφαλούς επικοινωνίας του Papasotiriou.gr είναι πιστοποιημένο από την εταιρεία Verisign.

Πατώστας στην επιλογή "Ιδιωτική Σύμβαση Πελάτη" μας δίνονται οι ακόλουθες πληροφορίες:

- ΓΕΝΙΚΟΙ ΟΡΟΙ

Το Papasotiriou.gr είναι ένα ηλεκτρονικό κατάστημα πώλησης προϊόντων μέσω του Διαδικτύου, της ανώνυμης εταιρείας με την επωνυμία «ΠΑΠΑΣΩΤΗΡΙΟΥ Α.Ε» (ΑΦΜ: 094397477, ΔΟΥ : ΦΑΕΕ ΑΘΗΝΩΝ), που εδρεύει στην Αθήνα (Στουρνάρη 35).

Κύριο και πρωταρχικό μέλημα της εταιρείας μας είναι η γνωστοποίηση των όρων, που διέπουν τα δικαιώματα και τις υποχρεώσεις του Papasotiriou.gr προς όλους εσάς τους επισκέπτες των ιστοσελίδων του και που σκοπό έχει την ενημέρωσή σας για τα δικά σας δικαιώματα και υποχρεώσεις και την καλύτερη εξυπηρέτησή σας στην αναζήτηση και αγορά των προϊόντων από το κατάστημά της.

- ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Απαραίτητη προϋπόθεση για την έναρξη της μεταξύ μας συνδιαλλαγής είναι η εκ μέρους σας γνωστοποίηση κάποιων προσωπικών σας στοιχείων. Κατά τη διάρκεια μιας παραγγελίας, θα σας ζητηθεί το πλήρες ονοματεπώνυμό σας, η διεύθυνση στην οποία θέλετε να αποσταλούν τα πωλούμενα προϊόντα, τον αριθμό του σταθερού σας τηλεφώνου (ή όποιο άλλο τηλέφωνο θέλετε το οποίο θα χρησιμοποιηθεί για την καλύτερη εξυπηρέτηση σας), την ηλεκτρονική σας διεύθυνση (e-mail address) κ.λπ. και στην περίπτωση που επιλέξετε οι πληρωμές σας να γίνονται μέσω πιστωτικής κάρτας και τον αριθμό και την ημερομηνία λήξεως της.

Η εταιρεία και το Papasotiriou.gr, υπακούοντας πιστά στις αρχές της προστασίας των προσωπικών δεδομένων που προβλέπονται από τους σχετικούς νόμους και διεθνείς συμβάσεις δεν πρόκειται να προβούν σε οποιαδήποτε αθέμιτη και χωρίς την προηγούμενη έγκρισή σας χρήση. Το Papasotiriou.gr με κανέναν τρόπο δεν αποκαλύπτει, δημοσιοποιεί, πωλεί, ανταλλάσσει τα προσωπικά στοιχεία και τις πληροφορίες που μας εμπιστεύεστε. Εξαιρετικά μπορεί να δημοσιοποιηθούν προσωπικά σας στοιχεία από την εταιρεία, τηρουμένης πάντα της προβλεπόμενης από το νόμο διαδικασίας όταν τούτο επιβάλλεται από Δημόσια Αρχή, δικαστήριο κλπ.

Το Papasotiriou.gr επιφυλάσσεται του δικαιώματος του να ενημερώνει τους προμηθευτές του με στατιστικές καταστάσεις πωλήσεων, οι οποίες όμως σε καμία περίπτωση δεν θα περιέχουν προσωπικά στοιχεία που μπορεί να οδηγήσουν σε αναγνώριση ατόμων.

Επίσης μπορείτε οποτεδήποτε να προβείτε εφόσον υπάρχει λόγος στην αλλαγή των προσωπικών στοιχείων που μας έχετε γνωστοποιήσει ή και να περιορίσετε ή ακυρώσετε τη χρήση κάποιων από τα στοιχεία αυτά (πχ ο αριθμός της πιστωτικής σας κάρτας) με τη συμπλήρωση της σχετικής ηλεκτρονικής φόρμας.

- ΑΣΦΑΛΕΙΑ

Το Papasotiriou.gr χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128-bit (την πιο ισχυρή σήμερα), για ασφαλείς online εμπορικές συναλλαγές. Με αυτόν τον τρόπο κρυπτογραφούνται όλες οι προσωπικές σας πληροφορίες, συμπεριλαμβάνοντας τον αριθμό της πιστωτικής κάρτας, το όνομα και την διεύθυνσή σας, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχτούν κατά την μεταφορά τους στο Internet.

Το πρωτόκολλο SSL (Secure Sockets Layer), είναι σήμερα το παγκόσμιο standard στο διαδίκτυο για την πιστοποίηση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών (web servers). Μία κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να κρυπτογραφούνται από το λογισμικό αποστολής και να αποκρυπτογραφούνται από το λογισμικό αποδοχής, προστατεύοντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατεύονται από έναν μηχανισμό που αυτόματα εξακριβώνει εάν τα δεδομένα έχουν αλλαχτεί κατά την μεταφορά.

- ΤΡΟΠΟΙ ΠΛΗΡΩΜΗΣ:

Για τη διευκόλυνση και εξυπηρέτηση όλων όσων επιθυμούν να αγοράσουν από το κατάστημά μας, διαθέτουμε τους ακόλουθους εναλλακτικούς τρόπους πληρωμής:

1. Με πιστωτική κάρτα VISA, MAESTRO, AMERICAN EXPRESS, DINERS & MASTERCARD που έχει εκδοθεί σε οποιαδήποτε τράπεζα.

2. Με αντικαταβολή μετρητοίς.

- ΤΡΟΠΟΣ - ΧΡΟΝΟΣ - ΚΟΣΤΟΣ ΑΠΟΣΤΟΛΗΣ:

Τα προϊόντα θα σας αποσταλούν στον τόπο που μας έχετε υποδείξει με υπηρεσία ταχυμεταφορών (courier).

Σε περιοχές στις οποίες δεν είναι δυνατή η αποστολή της παραγγελίας σας μέσω της υπηρεσίας ταχυμεταφορών, ο χρόνος αποστολής είναι αυτός που προβλέπεται από τα Ελληνικά Ταχυδρομεία. Αποστολές θα πραγματοποιούνται καθημερινά, εκτός Κυριακής και αργιών. Τώρα και το Σάββατο από 09:00 έως 14:00, εντός Αττικής και σε όλες τις μεγάλες πόλεις της Ελλάδος.

- ΤΙΜΕΣ ΤΩΝ ΠΩΛΟΥΜΕΝΩΝ ΠΡΟΙΟΝΤΩΝ:

Στις τιμές που αναγράφονται στους σχετικούς καταλόγους δίπλα από κάθε προϊόν περιλαμβάνεται το ΦΠΑ (4,5% για βιβλία και περιοδικά, 19% για τα υπόλοιπα είδη).

Για ορισμένες περιοχές της Ελλάδας για τις οποίες ισχύουν μειωμένοι συντελεστές ΦΠΑ και εφόσον η παραγγελία σας γίνει με τιμολόγιο τότε οι τιμές των προϊόντων είναι χαμηλότερες από τις αναγραφόμενες κατά τον μειωμένο ΦΠΑ.

- ΔΙΑΦΟΡΑ:

1. Ανωτέρα βία: Αν για λόγους ανωτέρας βίας (π.χ. κακές καιρικές συνθήκες, απεργίες κλπ) δεν είναι δυνατό να σας παραδώσουμε τα προϊόντα εντός του προκαθορισμένου χρόνου θα σας ενημερώσουμε μέσω e-mail, προκειμένου να μας δηλώσετε αν επιθυμείτε, υπ' αυτές τις συνθήκες, την ολοκλήρωση της παραγγελίας σας.

2. Ευθύνη Papasotiriou.gr: Το Papasotiriou.gr δεν ευθύνεται για ελαττώματα ή κακή ποιότητα των προϊόντων που διαθέτει στους πελάτες του.

Σε περίπτωση πάντως που στις παραδιδόμενες ποσότητες αποδεδειγμένα ανευρεθεί ελαττωματικό προϊόν διατηρείτε το δικαίωμα επιστροφής του με δυνατότητα αντικατάστασής του με δικά μας έξοδα αποστολής ή επιστροφής των χρημάτων σας.

3. Δόλια χρήση πιστωτικής κάρτας πελάτου: Το Papasotiriou.gr αναλαμβάνει την υποχρέωση να καλύψει την ευθύνη σας προς την Τράπεζα που έχει εκδώσει τις πιστωτικές σας κάρτες (ποσό που προκύπτει από τη σύμβαση για την έκδοση της πιστωτικής σας κάρτας), σε περίπτωση που γίνει χρήση αυτής από μη εξουσιοδοτημένο πρόσωπο (δόλια χρήση πιστωτικής κάρτας). Η ευθύνη αυτή καλύπτει μόνο τις περιπτώσεις που η μη εξουσιοδοτημένη/δόλια χρήση της πιστωτικής σας κάρτας για αγορές στο Papasotiriou.gr δεν οφείλεται σε δικό σας σφάλμα ή αμέλεια. Για το λόγο αυτό έχετε υποχρέωση αμέσως μόλις αντιληφθείτε την απώλεια της πιστωτικής σας κάρτας να προβείτε σε ενημέρωση της εκδούσας Τράπεζας, ώστε να ακυρωθεί αυτή και να αποκλεισθεί η χρήση της από μη εξουσιοδοτημένα πρόσωπα. Σε περίπτωση δόλιας χρήσης της πιστωτικής σας κάρτας, τα χρήματα που έχουν χρεωθεί στον Τραπεζικό λογαριασμό σας, θα επαναπιστωθούν ή θα σας επιστραφούν.

4. Διαφημιστικά μηνύματα: Το Papasotiriou.gr παρέχει τη δυνατότητα στους χρήστες του να επιλέξουν την πληροφόρησή τους για τα νέα προϊόντα που διαθέτει στην αγορά και για άλλες τυχόν προσφορές, διακανονισμούς πληρωμής κλπ με την αποστολή διαφημιστικών - ενημερωτικών μηνυμάτων στην ηλεκτρονική ή ταχυδρομική τους διεύθυνση ή δια του τηλεφώνου. Το Papasotiriou.gr δεν θα χρησιμοποιήσει καταχρηστικά την παραπάνω υπηρεσία του. Δίδεται δε πάντοτε στους χρήστες η δυνατότητα διακοπής της λήψης διαφημιστικών μηνυμάτων.

5. Cookies: Όπως τα περισσότερα sites στο διαδίκτυο έτσι και στο Papasotiriou.gr χρησιμοποιούμε cookies έτσι ώστε να έχουμε πρόσβαση σε ορισμένες πληροφορίες κάθε φορά που περιηγείστε με κάποιον web browser στο κατάστημα μας. Χωρίς την χρησιμοποίηση των cookies θα ήταν αδύνατον να σας προσφέρουμε σημαντικές υπηρεσίες όπως: κατάσταση παραγγελιών, προσωπικές ρυθμίσεις, αποθήκευση αντικειμένων στο καλάθι ή στην λίστα υπενθύμισης σας μεταξύ δύο επισκέψεών σας κ.α. Τα Cookies είναι αλφαριθμητικά αρχεία που μεταβιβάζουμε στον σκληρό δίσκο των υπολογιστών σας διαμέσου του διαδικτύου σας έτσι ώστε να σας προσφέρουμε υπηρεσίες όπως αυτές που αναφέρθηκαν παραπάνω. Στις ρυθμίσεις του browser σας μπορείτε να επιλέξετε να εμποδίσετε τον browser σας από το να δέχεται νέα cookies ή να σας ρωτάει κάθε φορά που ένα νέο cookie πρόκειται να εγκατασταθεί στον σκληρό σας δίσκο. Παρ' όλα αυτά θα πρέπει να γνωρίζετε πως αν επιλέξετε να εμποδίζετε τα cookies από το να αποθηκευτούν στον σκληρό σας δίσκο δεν θα μπορείτε να χρησιμοποιήσετε κάποιες υπηρεσίες του καταστήματος μας.

6. Ισχύον Δίκαιο: Όλες οι συναλλαγές που πραγματοποιείτε μέσω του Papasotiriou.gr διέπονται από το Διεθνές και Ευρωπαϊκό δίκαιο που ρυθμίζει θέματα σχετικά με το ηλεκτρονικό εμπόριο καθώς επίσης και από το Νόμο περί προστασίας των καταναλωτών (Ν. 2251/1994) που ρυθμίζει θέματα σχετικά με τις πωλήσεις από απόσταση.

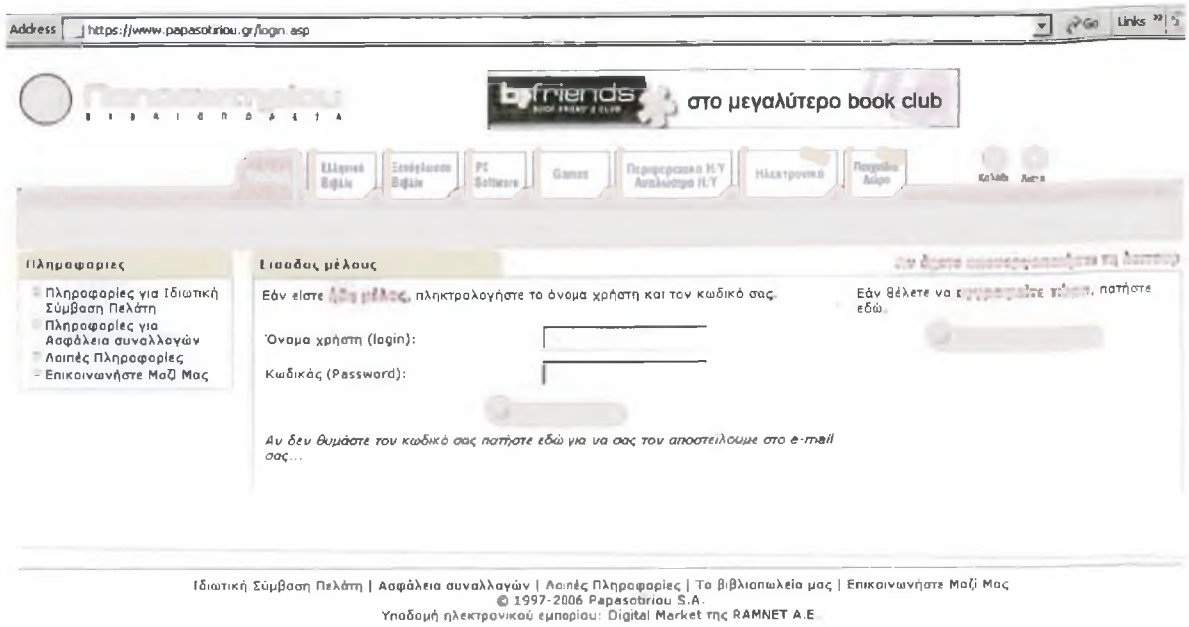
10.2.1 Παρατηρήσεις

Το ηλεκτρονικό κατάστημα [redacted] πληρεί όλες τις προϋποθέσεις λειτουργίας μιας επιχείρησης ηλεκτρονικού εμπορίου και παρέχει ασφαλείς συναλλαγές για τους πελάτες του.

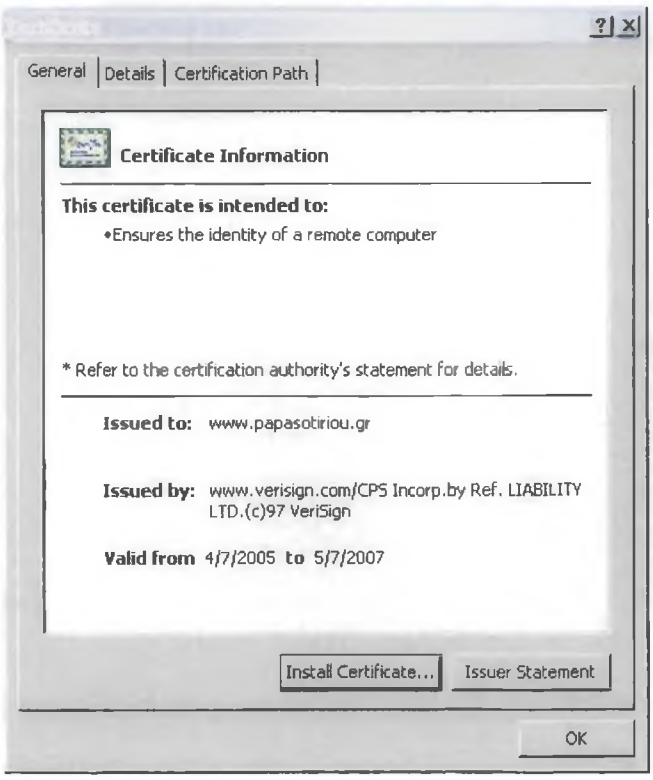
Γενικότερα:

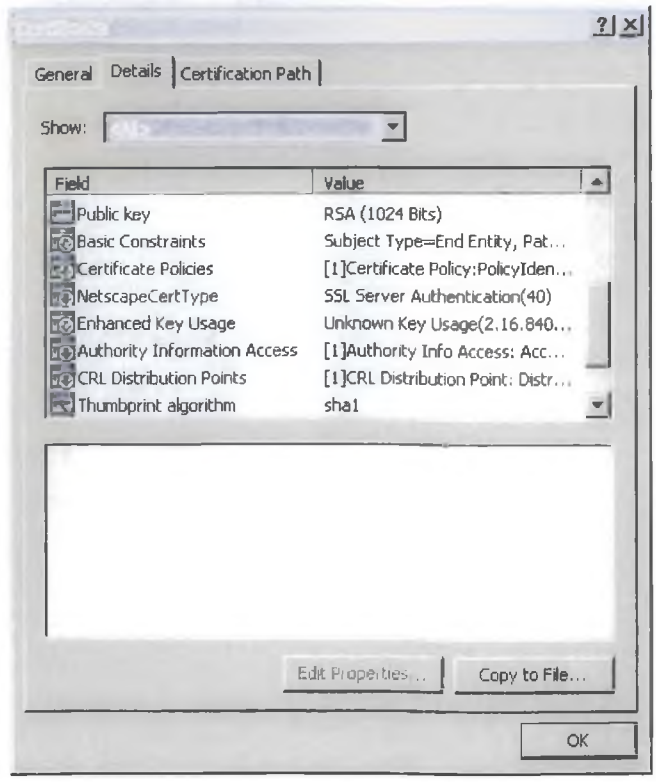
- χρησιμοποιεί το πρωτόκολλο SSL με κρυπτογράφηση 128-bit
- ξεκαθαρίζει ότι η εταιρεία και το papasotiriou.gr δεν πρόκειται να προβούν σε οποιαδήποτε αθέμιτη και χωρίς την προηγούμενη έγκριση των πελατών
- αναφέρει την υπακοή στις αρχές της προστασίας των προσωπικών δεδομένων που προβλέπονται από τους σχετικούς νόμους και διεθνείς συμβάσεις
- δίνει τη δυνατότητα στους πελάτες να κάνουν πληρωμές εκτός της πιστωτικής τους κάρτας και με αντικαταβολή μετρητοίς
- ενημερώνει ότι τα προϊόντα αποστέλλονται στον τόπο που έχει υποδείξει ο πελάτης με υπηρεσία ταχυμεταφορών
- γνωστοποιεί ότι χρησιμοποιεί cookies έτσι ώστε να έχει πρόσβαση σε ορισμένες πληροφορίες κάθε φορά που γίνεται περιήγηση με κάποιον web browser στο ηλεκτρονικό του κατάστημα
- αναλαμβάνει την υποχρέωση να καλύψει την ευθύνη του πελάτη προς την Τράπεζα που έχει εκδώσει την πιστωτική του κάρτα (ποσό που προκύπτει από τη σύμβαση για την έκδοση της πιστωτικής κάρτας), σε περίπτωση που γίνει χρήση αυτής από μη εξουσιοδοτημένο πρόσωπο
- χρησιμοποιεί έγκυρα ψηφιακά πιστοποιητικά και χρησιμοοιεί πολύ δυνατό αλγόριθμο κρυπτογράφησης
- ακολουθεί τους κανόνες ευχρηστίας και φιλικότητας και
- προσφέρει 15% έκπτωση στις ηλεκτρονικές συναλλαγές και δωρεάν αποστολή εντός Ελλάδας

Διαδικασία αυθεντικοποίησης ενός χρήστη του καταστήματος



Το ψηφιακό πιστοποιητικό που χρησιμοποεί το ηλεκτρονικό κατάστημα Παπασωτηρίου παρέχεται από την μεγαλύτερη εταιρεία παροχής πιστοποιητικών (Verisign) ενώ χρησιμοποιεί και πολύ ισχυρό αλγόριθμο κτρυπτογράφησης (RSA 1024bits)





Συμπεράσματα

Παίρνοντας όλα τα προηγούμενα που αναφέρθηκαν σε αυτή την εργασία ως δεδομένα τότε καταλήγουμε στο συμπέρασμα ότι αν και οι κίνδυνοι που αφορούν την ασφάλεια συναλλαγών στο ηλεκτρονικό εμπόριο καθώς και την αποκάλυψη πληροφοριών προσωπικών δεδομένων είναι πιθανοί και πραγματοποιήσιμοι, μπορούμε με βεβαιότητα να πούμε ότι έχουν γίνει τεράστια βήματα για την εξάλειψη των παραπάνω φαινομένων και ουσιαστικά να υπάρχει ένα πολύ καλό επίπεδο ασφάλειας σε αυτού του είδους τις συναλλαγές.

Το διαδίκτυο αποτελεί ένα εκφραστικό μέσο ελευθερίας και επικοινωνίας των ανθρώπων. Αρκετοί κακόβουλοι χρήστες του όμως κάνουν κατάχρηση των υπηρεσιών που αυτό προσφέρει με βασική επιδίωξη να εισβάλλουν στην διαδικασία ηλεκτρονικών δοσοληψιών μεταξύ δύο συναλλασσόμενων και να κλέψουν αριθμούς πιστωτικών καρτών ή προσωπικά δεδομένα έτσι ώστε αν αποκομίσουν οικονομικά οφέλη εις βάρος άλλων. Όμως η τεχνολογία έχει φτάσει σε τέτοιο σημείο που μπορεί να μας εξασφαλίσει ότι οι συναλλαγές μας με τη χρήση του ηλεκτρονικού εμπορίου θα είναι ασφαλείς και δε θα διατρέχουμε κινδύνους αποκάλυψης των προσωπικών μας στοιχείων.

Πλέον έχουμε την δυνατότητα να αγοράζουμε από το διαδίκτυο ότι επιθυμούμε χωρίς να έχουμε την φοβία ότι κάτι δεν θα πάει καλά στην διαδικασία της συναλλαγής μας, ενώ το επίπεδο ασφάλειας μπορεί να παρομοιαστεί ως ίδιο με το επίπεδο ασφάλειας που έχει μια συναλλαγή που θα κάναμε από ένα κανονικό κατάστημα.

Βιβλιογραφία

- Ασφάλεια Πληροφοριακών Συστημάτων

  Εκδόσεις: Νέων Τεχνολογιών
  Επιμέλεια: Σωκράτης Κ. Κάτσικας, Δημήτρης Γρίτζαλης, Στέφανος Γκρίτζαλης

- Ασφάλεια Δικτύων Υπολογιστών

  Εκδόσεις Παπασωτηρίου
  Επιμέλεια: Σωκράτης Κ. Κάτσικας, Δημήτρης Γρίτζαλης, Στέφανος Γκρίτζαλης

- Web Security, Privacy & Commerce, 2nd Edition

  Εκδόσεις O'Reilly
  Επιμέλεια: Simson Garfinkel, Gene Spafford

- Hack Proofing Your E-Commerce Site

  Εκδόσεις: Syngress Publishing, Inc
  Επιμέλεια: Ryan Russell, Teri Bidwell, Oliver Steudler, Robin Walshaw, L. Brent Huston

- E-commerce Basics: Technology Foundations & E-business Applications

  Εκδόσεις: Addison Wesley & Pearson Education
  Επιμέλεια: Davis & Benamati

- Ηλεκτρονικό Εμπόριο: Αρχές, Εξελίξεις και Στρατηγική από τη σκοπιά του Manager

  Εκδόσεις: Γκιούρδας
  Επιμέλεια: Turban E., Lee J., King D., Chung H.M

- Ηλεκτρονικό Εμπόριο

  Εκδόσεις: Νέων Τεχνολογιών
  Επιμέλεια: Δουκίδης.Γ, Θεμιστοκλέους.Μ, Δράκος.Β, Παπαζαφειροπούλου.Ν

- Secure Electronic Commerce

  Εκδόσεις: Prentice Hall PTR
  Επιμέλεια: Warwick Ford, Michael S. Baum

- Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων

  Εκδόσεις: ΑΝΙΚΟΥΛΑ
  Επιμέλεια: Γ. Πάγκαλος, Ι. Μαυρίδης

- Ηλεκτρονικό Εμπόριο

  Εκδόσεις: Κλειδάριθμος
  Επιμέλεια: Πασχόπουλος.Α, Σκαλτσάς.Π

- Δίκτυα Υπολογιστών

  Εκδόσεις: Κλειδάριθμος
  Επιμέλεια: Andrew S. Tannenbaum

- Hacking Exposed

  Εκδόσεις: Osborne
  Επιμέλεια: Joel Scambray, Stuart McClure, George Kurtz

- Maximum Security

  Εκδόσεις: Sams Publishing
  Επιμέλεια: Greg Shipley, Anonymous

- Αλγοριθμικά Θέματα Δικτύων και Τηλεματικής

  Εργασία στο Ηλεκτρονικό εμπόριο
  Εκδόσεις: Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Πατρών
  Επιμέλεια: Βενάκης Περικλής, Καζαντζή Αθανασία, Κουρούπας Γεώργιος

- Ανάλυση Επικινδυνότητας Πληροφοριακών Συστημάτων

  Εκδόσεις: Οικονομικού Πανεπιστημίου Αθηνών
  Επιμέλεια: Σπύρος Κοκκολάκης

- Control and Security of E-Commerce

  Εκδόσεις: John Wiley & Sons
  Επιμέλεια: Gordon E. Smith

- Σημειώσεις από το Μάθημα Ηλεκτρονικό Εμπόριο

  Εκδόσεις: Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Διοικητικής Επιστήμης & Τεχνολογίας
  Επιμέλεια: Δρ. Αδάμ Βρεχόπουλος

- Τεχνολογίες και Πολιτικές Ασφάλειας., Σημειώσεις μαθήματος

  Εκδόσεις: Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς
  Επιμέλεια: Δρ.Π. Κοτζανικολάου

- Προβλήματα Ασφάλειας στο Ηλεκτρονικό Εμπόριο. Σημειώσεις μαθήματος

  Εκδόσεις: Παν. Θεσσαλίας
  Επιμέλεια: Δρ. Χ. Κ. Γεωργιάδης

Ιστοσελίδες

Ηλεκτρονικό Εμπόριο

Ο δεκάλογος του e-Business Forum για το ηλεκτρονικό εμπόριο

Γενική Γραμματεία του Καταναλωτή του Υπουργείου Ανάπτυξης. παρουσιάζει τις κατευθυντήριες Γραμμές για την προστασία του καταναλωτή στα πλαίσια του ηλεκτρονικού εμπορίου που έχουν αποφασισθεί από τον οργανισμό Οικονομικής Ανάπτυξης και Συνεργασίας (ΟΟΣΑ)

Ψωνίζοντας στο διαδίκτυο

Η Σημερινή κατάσταση του Ηλεκτρονικού Εμπορίου Στην Ελλάδα

An Overview of SSL

Νομικά Θέματα Ηλεκτρονικού Εμπορίου

Άρθρο για την προστασία προσωπικών δεδομένων στο διαδίκτυο

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

An Overview of SSL

An Overview of Cryptography

Internet Firewalls: Frequently Asked Questions

The PGP: Frequently Asked Questions

The Emergence of Electronic Commerce on the Internet

Ευρωπαϊκή Ένωση και Ηλεκτρονικό Εμπόριο

Ασφάλεια Συναλλαγών

Πώς να προστατεύετε τα προσωπικά δεδομένα σας όταν χρησιμοποιείτε ηλεκτρονικές υπηρεσίες πληρωμής

Αλγοριθμικά Θέματα Δικτύων και Τηλεματικής

Ασφάλεια Η/Υ και Προστασία Δεδομένων (Σημειώσεις)
Ασφαλή ηλεκτρονικά συστήματα συναλλαγών στο διαδίκτυο (Slides)
Ασφάλεια στο World Wide Web (Πτυχιακή Εργασία)

Σελίδα για το μάθημα Ηλεκτρονικό Εμπόριο, Ιόνιο Πανεπιστήμιο

Σελίδα για το μάθημα Ασφάλεια Η/Υ και Προστασία Δεδομένων, Ιόνιο Πανεπιστήμιο

Ασφάλεια στο World Wide Web

An Introduction to Network Firewalls and the Firewall Selection Process