1/1/2012

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ | ΚΑΡΒΟΥΝΗΣ ΣΠΥΡΙΔΩΝ

Περιεχόμενα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της διπλωματικής μου εργασίας θα ήθελα να ευχαριστώ όλους όσους αποτέλεσαν αρωγό για την ολοκλήρωση της διπλωματικής μου εργασίας

Ιδιαίτερα καταλυτικό ρόλο διαδραμάτισε η επιβλέπουσα καθηγήτρια Σινανιώτη Αριστέα. Στηριζόμενη στην επιστημονική της κατάρτιση και στην ερευνητική της εμπειρία, ήταν σε θέση να μου μεταλαμπαδεύσει με βέλτιστο τρόπο τις απαραίτητες γνώσεις, προκειμένου να πορευθώ ορθά αλλά ταυτόχρονα και ελεύθερα προς την ολοκλήρωση της διπλωματικής μου εργασίας. Διακατεχόμενη από πνεύμα επαγγελματισμού, συνεργασίας και πλήρους κατανόησης ήταν σε θέση ανά πάσα στιγμή να διευθετήσει προκύπτοντα εμπόδια και δυσκολίες καθ' όλη τη διάρκεια συγγραφής της εργασίας αυτής. Η αμεσότητα, η εμπιστοσύνη και οι γνώσεις της είναι στοιχεία που συνέβαλλαν στην ολοκλήρωση της διπλωματικής.

Σημαντική ήταν και η συμμετοχή του Ιωάννη Φαρσαρώτα. Με την υπομονή, την προθυμία και τις γνώσεις του γύρω από το διαπραγματευόμενο αντικείμενο της διπλωματικής, μου έδωσε χρήσιμες και άκρως καθοριστικές καθοδηγήσεις.

Τέλος, ευχαριστώ την οικογένεια μου και τον φιλικό μου περίγυρο, για τη συναισθηματική κυρίως βοήθεια που μου προσέφερε κατά τη διάρκεια εκπόνησης της διπλωματικής.

ΠΕΡΙΛΗΨΗ

Στην παρούσα διπλωματική εργασία παρουσιάζονται αναλυτικά οι τρόποι ασφαλείας για την εξασφάλιση της διασυνοριακής και εθνικής διακίνησης χρημάτων, υπηρεσιών και προϊόντων. Το Διαδίκτυο συνιστά τον πιο διαδεδομένο τρόπο «ανταλλαγής» των ανωτέρω και λόγω της ευρύτητας και μη οριοθέτησής του, χαρακτηρίζεται και από ένα βαθμό επικινδυνότητας. Οι ικανοί και δολοπλόκοι χρήστες μπορούν ανά πάσα στιγμή να υποκλέψουν στοιχεία, να τα τροποποιήσουν, να «ξεγελάσουν» τους χρήστες και να διαστρευλώσουν το λειτουργικό έργο του Διαδικτύου είτε για προσωπικό τους όφελος είτε για ευχαρίστηση. Με τις μεθόδους της κρυπτογράφησης, τη βοήθεια των Firewalls, των Συστημάτων Ανίχνευσης Εισβολών, του IPSec και του SSL, των ψηφιακών υπογραφών και πιστοποιητικών, αλλά και με την εκπαίδευση και πολύπλευρη ενημέρωση των χρηστών εξασφαλίζεται η προστασία στο Διαδίκτυο και επομένως, επιτυγχάνεται η προστασία των ηλεκτρονικών πληρωμών.

Αναλύοντας τη δομή των ακόλουθων κεφαλαίων στο πρώτο μέρος (Ά) παρουσιάζεται και αναλύεται ο όρος και η συμβολή της ασφάλειας (κεφάλαιο 1). Στη συνέχεια, προσδιορίζεται η έννοια της ηλεκτρονικής πληρωμής, η οποία εντάσσεται εντός των ορίων της έννοιας του ηλεκτρονικού εμπορίου (κεφάλαιο 2). Τέλος, παρατίθενται ποικίλοι τρόποι συστημάτων πραγματοποίησης ηλεκτρονικών πληρωμών (κεφάλαιο 3).

Στο δεύτερο μέρος (΄Β) εξετάζεται η ασφάλεια στις ηλεκτρονικές πληρωμές (κεφάλαιο 4), προτείνονται και αναλύονται τρόποι επίτευξής της (κεφάλαιο 5) και τέλος εξετάζεται σε διασυνοριακό επίπεδο (κεφάλαιο 6) ενώ παράλληλα δίδεται έμφαση στο ισχύον νομοθετικό ευρωπαϊκό πλαίσιο (κεφάλαιο 7).

Η εργασία ολοκληρώνεται με τη διατύπωση συμπερασμάτων που προκύπτουν από το σύνολο της παραπάνω ανάλυσης.

ABSTRACT

In this dissertation are analytically presented the ways of safety in order to guarantee the cross-border and national transactions, and distribution of services and products. Internet is the reason for the widespread way of “exchange” and because of its broadness, is also characterized by dangerouosity. Hackers are able any moment to break into personal information and elements, modify them, and destroy the functional work of Internet. They do that as for their personal profit or for their pleasure.

With the methods of encryption, the help of Firewalls, Intruction Detection System, IPSec, and SSL, digital signatures and certificates, but also with the education and multifaced briefing of users, is ensured the protection in the Internet and consequently, is achieved the protection of electronic payments.

Analyzing the structure of following chapters in the first part (‘A) is presented and analyzed the contribution of the term “safety” (chapter 1). In addition, is determined the significance of electronic payment, which is included under the “umbrella” of electronic trade (chapter 2). Finally, are mentioned various ways of systems, suitable for execution an electronic payment (chapter 3).

Moreover, in the second part (‘B) is examined the safety especially in electronic payments (chapter 4). Then, it is analyzed the most common, widespread known ways which ensure safe transactions (chapter 5). Finally it is examined in international level the same term (chapter 6), while at the same time is given attention in the European legislative framework (chapter 7). The completion of this dissertation is happening with the most important conclusions that extracts from all the previous analysis.

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη των Τεχνολογιών Πληροφορίας αποτελεί το βασικό χαρακτηριστικό της σημερινής εποχής. Αυτό απαιτεί παράλληλα την εγρήγορση των ατόμων της κοινωνίας προκειμένου να προσαρμοστούν άμεσα και αποτελεσματικά στις νέες επιταγές που επιτάσσει η τεχνολογία. Ένα από τα βασικότερα επιτεύγματά της αποτελεί το Διαδίκτυο.

Η σημερινή κοινωνία συλλέγει περισσότερες γνώσεις, οι οποίες ολοένα και πληθαίνουν καθώς είναι όλο και μεγαλύτερος ο διαθέσιμος όγκος τους στο Διαδίκτυο. Το τελευταίο αποτελεί τη θεμέλια βάση για την παγκοσμίου επιπέδου επικοινωνία και πρόσβαση απομακρυσμένων πόρων ή ανταλλαγής δεδομένων, πληροφοριών και προϊόντων. Η τεχνολογία και κυρίως το Διαδίκτυο, ως επίτευγμα αυτής, ανοίγει το δρόμο σε πολλές επιχειρήσεις και χρηματοπιστωτικά ιδρύματα καθώς βρίσκουν οικονομικότερο, πιο άμεσο και με παγκόσμια εμβέλεια τρόπο επικοινωνίας, διαφήμισης και συναλλαγών.

Ευκολία, εκμηδενισμός του χρόνου, άμεσα πρόσβαση από οποιοδήποτε μέρος ανά πάσα στιγμή, από οποιονδήποτε χωρίς οποιουδήποτε είδους διακρίσεις, είναι μερικά από τα θετικά χαρακτηριστικά του Διαδικτύου. Στη σημερινή κοινωνία, οι πτυχές του Διαδικτύου ολοένα και εξαπλώνονται. Μία από τις πιο διαδεδομένες χρήσεις του (λόγω χρησιμότητας) αποτελεί η πραγματοποίηση πάσις φύσεως ηλεκτρονικών πληρωμών-συναλλαγών.

Παρόλο που η τεχνολογίες πληροφορικής διαρκώς εξελίσσονται, παρατηρείται πως οι Ευρωπαίοι δεν την υιοθετούν άμεσα. Έτσι, σημειώνονται τα παρακάτω: οι καταγεγραμμένες επιτυχείς προσπάθειες να «κατεβάσουν» (downloads) οι πολίτες της Αμερικής, μουσική μέσω του διαδικτύου είναι *τέσσερις* φορές περισσότερες από ότι των Ευρωπαίων. Επιπλέον, το 30% των ευρωπαίων δεν χρησιμοποιεί το διαδίκτυο. Η Ευρώπη έχει 1% διείσδυση σε δίκτυα οπτικών ινών υψηλής ταχύτητας, όταν η Ιαπωνία έχει 12% και η Νότια Κορέα 15%. Οι διαφορές αυτές οφείλονται σε επτά βασικά εμπόδια σύμφωνα με την Ευρωπαϊκή Επιτροπή:

1. Κατακερματισμένες ψηφιακές αγορές
2. Έλλειψη διαλειτουργικότητας
3. Αύξηση του ψηφιακού εγκλήματος και κίνδυνος λόγω ελάχιστης εμπιστοσύνης στα δίκτυα
4. Έλλειψη επενδύσεων σε δίκτυα
5. Αναποτελεσματικές έρευνες και προσπάθειες καινοτομίας
6. Έλλειψη ψηφιακών γνώσεων και ικανοτήτων
7. Χαμένες ευκαιρίες για την αντιμετώπιση κοινωνικών προκλήσεων

Αξίζει να σημειωθεί, ωστόσο, πως κάθε ενέργεια ακολουθείται και από τα αρνητικά της αποτελέσματα. Έτσι, και η χρήση του Κυβερνοχώρου κρύβει κάποιους κινδύνους, γεγονός που απαιτεί την ύπαρξη απαραίτητων μέτρων ασφαλείας, κυρίως αν αφορά εγχρήματες συναλλαγές. Θα πρέπει επομένως, να προστατεύονται ευαίσθητα δεδομένα των ηλεκτρονικών συναλλαγών είτε αυτά προέρχονται από επικοινωνία είτε από εμπορικές συναλλαγές. Σε έρευνα παρατηρήθηκε πως το 2009 μόνο το 38% των πολιτών της Ευρωπαϊκής Ένωσης χρησιμοποιούσε το διαδίκτυο για χρήση ηλεκτρονικών συναλλαγών, σε αντίθεση με το 72% των ευρωπαϊκών επιχειρήσεων. Αυτό οφείλεται σε ποικίλους παράγοντες όπως, η έλλειψη εμπιστοσύνης στο διαδίκτυο,

στο ίδιο το κράτος, η απουσία κανονιστικού πλαισίου, η άγνοια χρήσης διαδικτυακών εφαρμογών κλπ. Η Ευρωπαϊκή Ένωση προσπαθεί να εξαλείψει τα προκύπτοντα εμπόδια, δίδοντας στους πολίτες εφόδια και κίνητρα ώστε να ενστερνιστούν τη χρήση του διαδικτύου αρχικά και τις υπηρεσίες των ηλεκτρονικών πληρωμών μετέπειτα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΜΕΡΟΣ Ά

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Καθώς οι επιθέσεις και οι απειλές στο διαδίκτυο ολοένα και αυξάνονται, είναι γεγονός πλέον ότι αποτελεί επιτακτική ανάγκη, οι χρήστες του διαδικτύου να έχουν βασικές γνώσεις ασφάλειας και κρυπτογραφίας, καθώς επίσης και οι υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο να προστατεύονται με χρήση κατάλληλου λογισμικού ασφάλειας. Πρώτα από όλα όμως κάποιος πρέπει να κατανοήσει τόσο τις έννοιες των πιθανών επιθέσεων όσο και της ασφάλειάς του από αυτές.

1.1 Έννοια ασφάλειας

Η έννοια της ασφάλειας ενός δικτύου υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης να προστατεύει τις πληροφορίες της από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται, επίσης, με την ικανότητά της να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια πληροφοριακών συστημάτων έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών ενός πληροφοριακού συστήματος, καθώς και τη λήψη μέτρων. Πιο συγκεκριμένα η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- Πρόληψη (prevention): την πρόληψη, δηλαδή μέτρων για να προληφθούν “φθορές” των συστατικών ενός πληροφοριακού συστήματος.
- Ανίχνευση (detection): την λήψη μέτρων για την ανίχνευση του πότε, πως και από ποιον προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
- Αντίδραση (reaction): τη λήψη μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί, καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

1.2 Θεμελιώδεις έννοιες ασφάλειας

Σήμερα η έννοια της ασφάλειας συνδέεται στενά με τρείς βασικές έννοιες:

1. Εμπιστευτικότητα
2. Ακεραιότητα
3. Διαθεσιμότητα

1. Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Άλλες εκφάνσεις της εμπιστευτικότητας είναι:
    - Η ιδιωτικότητα: προστασία δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
    - Η μυστικότητα: προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.
2. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.
3. Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Για τους σκοπούς ασφαλείας μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών (denial of service attacks). Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης και λειτουργιών που είναι κρίσιμες στο χρόνο (time – critical). Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη παρά τυχαία απώλεια της διαθεσιμότητας. Παράδειγμα αποτελούν οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

1.3 Αναγκαιότητα ασφάλειας

Ένα δικτυωμένο σύστημα είναι επιρρεπές σε ένα αριθμό απειλών που προέρχονται και από νόμιμους χρήστες του συστήματος, αλλά και κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφάλειας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας μέσω ενός πολύ εκτεθειμένου μέσου και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη – έμπιστων υπολογιστικών συστημάτων. Τα τελευταία χρόνια παρατηρείται τεράστια αύξηση των επιθέσεων από εισβολείς σε συστήματα πληροφορικής επιχειρήσεων, τραπεζών και οργανισμών με σκοπό την υποκλοπή σημαντικών πληροφοριών, προσωπικών δεδομένων και την παρεμπόδιση παροχής υπηρεσιών. Οι επιθέσεις αυτές πραγματοποιούνται από ανθρώπους που διαθέτουν υψηλή γνώση όσον αφορά στην τοπολογία των δικτύων, τη λειτουργία τους και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Επιπλέον, διαθέτουν την τεχνογνωσία

για να εξετάζουν τον κώδικα επικοινωνίας προκειμένου να ανακαλύψουν ατέλειες σε συγκεκριμένα προγράμματα.

Στη συνέχεια παρουσιάζονται οι κύριες μορφές επιθέσεων.

- Υποκλοπή επικοινωνιών*:* Οι ηλεκτρονικές επικοινωνίες μπορούν να υποκλαπούν και τα δεδομένα να αντιγραφούν ή να τροποποιηθούν. Η υποκλοπή μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Η παράνομη υποκλοπή μπορεί να προξενήσει βλάβη, τόσο ως παραβίαση της ιδιωτικής ζωής των ατόμων, όσο και μέσω της εκμετάλλευσης των δεδομένων που έχουν υποκλαπεί
- Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών: Η μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή ή σε ένα δίκτυο υπολογιστών πραγματοποιείται συνήθως κακόβουλα με την πρόθεση αντιγραφής, τροποποίησης ή καταστροφής δεδομένων. Αυτό τεχνικά αποκαλείται παρείσφρηση και μπορεί να γίνει με διάφορους τρόπους. Η μη εξουσιοδοτημένη παρείσφρηση έχει ενίοτε ως κίνητρο διανοητική πρόκληση και όχι κερδοσκοπία.
- Διατάραξη δικτύων, δηλαδή πρόκληση κατάρρευσης ενός δικτύου λόγω υπερφόρτωσης: Ο πλέον κοινός λόγος διατάραξης δικτύου υπήρξε η βλάβη στο σύστημα υπολογιστή που ελέγχει το δίκτυο, ενώ οι επιθέσεις εναντίον δικτύου κατευθύνονταν κυρίως προς τους εν λόγω υπολογιστές. Οι διακοπές είναι επιζήμιες για ορισμένες ιστοσελίδες, καθώς οι επιχειρήσεις βασίζονται ολοένα περισσότερο στην ανεμπόδιστη διάθεση των δικτυακών τους τόπων για τις εμπορικές τους συναλλαγές.
- Εκτέλεση κακόβουλου λογισμικού που τροποποιεί ή καταστρέφει δεδομένα: Ο ιός είναι μια μορφή κακόβουλου λογισμικού. Πρόκειται για ένα πρόγραμμα που αναπαράγει τον κώδικά του προσκολλώμενο σε άλλα προγράμματα, με τρόπο ώστε ο κώδικας του ιού να εκτελείται κατά την εκτέλεση προγράμματος του υπολογιστή που έχει προσβληθεί. Υπάρχουν πολλοί άλλοι τύποι κακόβουλου λογισμικού. Ορισμένοι βλάπτουν μόνο τον υπολογιστή όπου έχουν αντιγραφεί, ενώ άλλοι μεταδίδονται σε άλλα δικτυωμένα προγράμματα.
- Παραπλάνηση/ ψευδής δήλωση*:* Η παραπλάνηση ατόμων ή φορέων είναι επιζήμια κατά διαφορετικούς τρόπους. Οι πελάτες ενδέχεται να τηλεφορτώσουν κακόβουλο λογισμικό από δικτυακό τόπο που αντιποιείται έμπιστη πηγή. Ενδέχεται να δοθούν εμπιστευτικές πληροφορίες σε λάθος άτομα. Η μεγαλύτερη ίσως ζημία είναι το γεγονός ότι η έλλειψη επαλήθευσης ταυτότητας αποτρέπει δυνητική πελατεία.

Εκτός από τις κακόβουλες επιθέσεις κατά των δικτύων, η ασφάλειά τους μπορεί να πληγεί και από απρόβλεπτα και ακούσια γεγονότα, που μπορούν να οφείλονται σε φυσικές καταστροφές, τρίτα μέρη που δεν έχουν συμβατική σχέση με το φορέα εκμετάλλευσης ή το χρήστη, τρίτα μέρη που έχουν συμβατική σχέση με το φορέα εκμετάλλευσης ή το χρήστη, ανθρώπινο σφάλμα ή κακή διαχείριση εκ μέρους του φορέα εκμετάλλευσης ή του χρήστη.

Μπορεί εύκολα να θεωρηθεί ότι η σχέση ασφάλειας και αποδοτικότητας του πληροφοριακού συστήματος είναι αντιστρόφως ανάλογη. Αυτό διότι, η εγκατάσταση μηχανισμών ασφάλειας επιφέρει κόστος χρόνου και χρήματος. Κάτι τέτοιο δεν είναι σωστό καθώς η ασφάλεια είναι αναγκαίο κόστος για την ομαλή και εύρυθμη λειτουργία του ΠΣ. Το συγκεκριμένο κόστος εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφαλείας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από τη μια και από την άλλη το κόστος ζημιών από πιθανολογούμενο κίνδυνο.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από τη φύση της ως δυναμική παράμετρος και όχι ως στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των «επιτιθέμενων», απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφαλείας. Συνεπώς, η ακολουθούμενη πολιτική ασφάλειας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

1.4 Συνήθεις επιθέσεις

Υπάρχουν πολλοί τρόποι που μπορεί να χρησιμοποιήσει κάποιος για να προκαλέσει ζημιά σε μη προστατευμένους υπολογιστές, όπως:

- *Απομακρυσμένη Πρόσβαση (Remote Login)*. Συμβαίνει όταν κάποιος έχει τη δυνατότητα να συνδεθεί σε έναν υπολογιστή και να τον ελέγξει κατά κάποιον τρόπο. Αυτό μπορεί να κυμαίνεται από το να μπορεί να δει απλά ή να έχει πρόσβαση σε αρχεία έως το να μπορεί να τρέχει προγράμματα στον υπολογιστή .
- *Κερκόπορτες Εφαρμογής (Application Backdoors)*. Μερικά προγράμματα έχουν ιδιαίτερα χαρακτηριστικά που επιτρέπουν την απομακρυσμένη πρόσβαση (remote access), ενώ άλλα περιέχουν σφάλματα (bugs) τα οποία δίνουν τη δυνατότητα για την ύπαρξη κερκόπορτας ή πίσω πόρτας (backdoor), δηλαδή μιας κρυφής πρόσβασης, με την οποία μπορεί να έχει κάποιος κάποιο επίπεδο ελέγχου του προγράμματος.
- *SMTP Session Hijacking*. Το SMTP αποτελεί την πιο κοινή μέθοδο αποστολής ηλεκτρονικού ταχυδρομείου (e-mail) στο Internet και αποκτώντας πρόσβαση σε μια λίστα από διευθύνσεις e-mail, κάποιος μπορεί να στείλει αυτόκλητα e-mail (spam) σε χιλιάδες χρήστες.
- *Σφάλματα στο Λειτουργικό Σύστημα*. Όπως και οι εφαρμογές, μερικά λειτουργικά συστήματα έχουν backdoors, ενώ άλλα παρέχουν απομακρυσμένη πρόσβαση με ανεπαρκείς ελέγχους ασφαλείας ή έχουν ελαττώματα (bugs) που μπορεί να εκμεταλλευθεί ένας έμπειρος hacker.
- *Άρνηση Υπηρεσίας (Denial of Service)*. Αυτό το είδος επίθεσης είναι σχεδόν αδύνατο να αντιμετωπισθεί. Αυτό που συμβαίνει είναι ότι ο hacker στέλνει μια αίτηση (request) στον server για να συνδεθεί σ' αυτόν. Όταν ο server απαντήσει με μια αναγνώριση (acknowledgement) και προσπαθήσει να κάνει μια σύνοδο (session), δεν θα μπορεί να βρει το σύστημα που έκανε την αίτηση (request). Κατακλύζοντας έναν server με τέτοιες αναπάντητες αιτήσεις session, ένας hacker αναγκάζει τον server να δουλεύει πολύ αργά έως ότου καταρρεύσει.
- *Βόμβες e-mail (e-mail Bombs)*. Μια βόμβα e-mail είναι συνήθως μια προσωπική επίθεση όπου κάποιος μάς στέλνει το ίδιο e-mail εκατοντάδες ή

και χιλιάδες φορές μέχρις ότου το σύστημά μας να μην μπορεί να δεχθεί άλλα μηνύματα.

- *Μακροεντολές (Macros)*. Για να απλοποιήσουν περίπλοκες διαδικασίες ή εργασίες, πολλές εφαρμογές (applications) μας δίνουν τη δυνατότητα να δημιουργήσουμε ένα μικρό πρόγραμμα (σενάριο εντολών, script) από εντολές που η εφαρμογή μπορεί να εκτελέσει. Αυτό το script είναι γνωστό ως μακροεντολή (macro). Οι hackers μπορούν να εκμεταλλευθούν αυτή τη δυνατότητα και να δημιουργήσουν τα δικά τους macros, τα οποία, ανάλογα με την εφαρμογή, μπορούν να καταστρέψουν τα δεδομένα ή και να προκαλέσουν την κατάρρευση του υπολογιστή μας.
- *Ιοί (Viruses)*. Πιθανώς η πιο γνωστή απειλή είναι οι ιοί των υπολογιστών (computer viruses). Ένας ιός (virus) είναι ένα μικρό πρόγραμμα που μπορεί να αντιγράψει τον εαυτό του σ' άλλους υπολογιστές. Μ' αυτόν τον τρόπο μπορεί να διαδοθεί ταχύτατα από το ένα σύστημα στο άλλο. Το αποτέλεσμα ενός ιού μπορεί να κυμαίνεται από την εμφάνιση ενός αβλαβούς μηνύματος έως και τη διαγραφή όλων των αρχείων του υπολογιστή μας.
- *Spam e-mail*. Μπορεί να μην κάνει ζημιά αλλά είναι πάντα ενοχλητική, η μη ζητηθείσα ή αυτόκλητη εμπορική αλληλογραφία (spam e-mail), που αποτελεί το ηλεκτρονικό ισοδύναμο της άχρηστης διαφημιστικής αλληλογραφίας (junk mail). Το spam e-mail μπορεί να είναι και επικίνδυνο καθώς αρκετά συχνά περιέχει συνδέσμους (links) σε Web sites, τα οποία ενδέχεται να στέλνουν cookies για να ανοίξουν έτσι μια κερκόπορτα (backdoor) στον υπολογιστή μας.
- *Βόμβες Ανακατεύθυνσης (Redirect Bombs)*. Οι hackers μπορούν να χρησιμοποιήσουν το πρωτόκολλο ICMP για να αλλάξουν (ανακατευθύνουν) τη διαδρομή που ακολουθούν οι πληροφορίες, στέλνοντάς τες σ' έναν διαφορετικό δρομολογητή (router). Αυτός είναι κι ένας από τους τρόπους που γίνεται μια επίθεση άρνησης υπηρεσίας (denial of service attack).
- *Source routing*. Στις περισσότερες περιπτώσεις, η διαδρομή που ακολουθεί ένα πακέτο στο Internet (ή σ' ένα άλλο δίκτυο) καθορίζεται από τους δρομολογητές (routers) που υπάρχουν κατά μήκος της διαδρομής. Αλλά η πηγή (source), δηλαδή ο αρχικός υπολογιστής, που παρέχει το πακέτο μπορεί αυθαίρετα να καθορίσει τη διαδρομή (route) που θα πρέπει να ακολουθήσει το πακέτο. Οι hackers το εκμεταλλεύονται αυτό μερικές φορές για να κάνουν τις πληροφορίες να φαίνονται ότι προέρχονται από μια έγκυρη πηγή ή ακόμη και μέσα από το ίδιο το δίκτυο. Τα περισσότερα firewalls μπορούν και εξουδετερώνουν το source routing.

1.5 Τρόποι αντιμετώπισης

Παρουσιάζουμε παρακάτω ορισμένους από τους συνηθέστερους τρόπους αντιμετώπισης:

- Η πλέον κοινή μέθοδος προστασίας έναντι μη εξουσιοδοτημένης πρόσβασης είναι οι έλεγχοι συνθηματικού και η εγκατάσταση firewall. Ωστόσο, με αυτά παρέχεται περιορισμένη μόνο προστασία και πρέπει να συμπληρώνεται και από άλλους ελέγχους ασφαλείας, όπως η αναγνώριση

επιθέσεων, η ανίχνευση παρείσφρησης και οι έλεγχοι στο επίπεδο εφαρμογής.

- Άμυνα έναντι της υποκλοπής μπορεί να προέλθει με την κρυπτογράφηση των δεδομένων που μεταδίδονται μέσω του δικτύου.
- Οι επιθέσεις σε εξυπηρετητές DNS αντιμετωπίζονται καταρχάς εύκολα με την επέκταση των πρωτοκόλλων DNS. Πολύ δυσκολότερη είναι η άμυνα εναντίον επιθέσεων κατά του συστήματος δρομολόγησης. Δεν υπάρχουν αποτελεσματικά μέσα για ασφαλή πρωτόκολλα δρομολόγησης, ιδίως σε δρομολογητές κορμού. Ο όγκος των μεταδιδόμενων δεδομένων δεν επιτρέπει λεπτομερές φιλτράρισμα, καθώς η εν λόγω επαλήθευση θα προκαλούσε ακινητοποίηση των δικτύων.
- Ο κύριος τρόπος άμυνας είναι το λογισμικό κατά των ιών που διατίθεται σε διάφορες μορφές, για παράδειγμα σαρωτές ιών που εντοπίζουν και αχρηστεύουν γνωστούς ιούς. Το κύριο ελάττωμά τους είναι ότι δεν εντοπίζουν εύκολα νέους ιούς, ακόμα και με τακτική ενημέρωση. Άλλο παράδειγμα άμυνας κατά των ιών είναι ο ελεγκτής ακεραιότητας. Για να μπορέσει ένας ιός να προσβάλει έναν υπολογιστή, θα πρέπει να αλλάξει κάτι στο σύστημα αυτό. Ο έλεγχος ακεραιότητας θα μπορούσε να εντοπίζει τις εν λόγω αλλαγές, ακόμα και αν έχουν προκληθεί από άγνωστους ιούς.
- Οι απόπειρες εισαγωγής της επαλήθευσης ταυτότητας στα δίκτυα, σε συνδυασμό με την εισαγωγή του πρωτοκόλλου SSL, αποτελεί ήδη χρήσιμο βήμα για τη διασφάλιση ορισμένου επιπέδου τήρησης του απορρήτου. Τα Ιδεατά Ιδιωτικά Δίκτυα (VPN) χρησιμοποιούν SSL και IPsec για επικοινωνίες μέσω επισφαλών ανοιχτών καναλιών, διαφυλάσσοντας δεδομένο επίπεδο ασφάλειας. Οι λύσεις αυτές είναι ωστόσο περιορισμένης χρησιμότητας, δεδομένου ότι βασίζονται σε ηλεκτρονικά πιστοποιητικά, χωρίς να υπάρχει εγγύηση ότι τα πιστοποιητικά αυτά δεν έχουν παραχαραχθεί.

1.6 Προστασία προσωπικών δεδομένων – νόμος 2472/97

Ένας από τους βασικούς λόγους ανάδειξης της σημαντικότητας της ασφάλειας ΠΣ είναι η διαφύλαξη του προσωπικού απορρήτου (privacy) των ατόμων των οποίων οι εγγραφές διατηρούνται σε υπολογιστικά συστήματα διαφόρων οργανισμών. Αυτή είναι μια δικαιολογημένη και γενικότερα αποδεκτή αρχή, με ελάχιστες αντίθετες απόψεις. Έτσι, «…για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν αρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση. Στην Ελλάδα, για τον σκοπό αυτό ιδρύθηκε με τον Νόμο 2472/97 ως ανεξάρτητη διοικητικός φορέας η «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» που λειτουργεί από τον Νοέμβριο του 1997…».Ο εν λόγο Νόμος με τις τροποποιήσεις του το 2006 και το 2011 βρίσκονται στο διαδικτυακό τόπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, δηλαδή

http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORT

ενώ αναλύονται και παρακάτω.

2 ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

2.1 Ηλεκτρονικό εμπόριο

2.1.1 Ορισμός

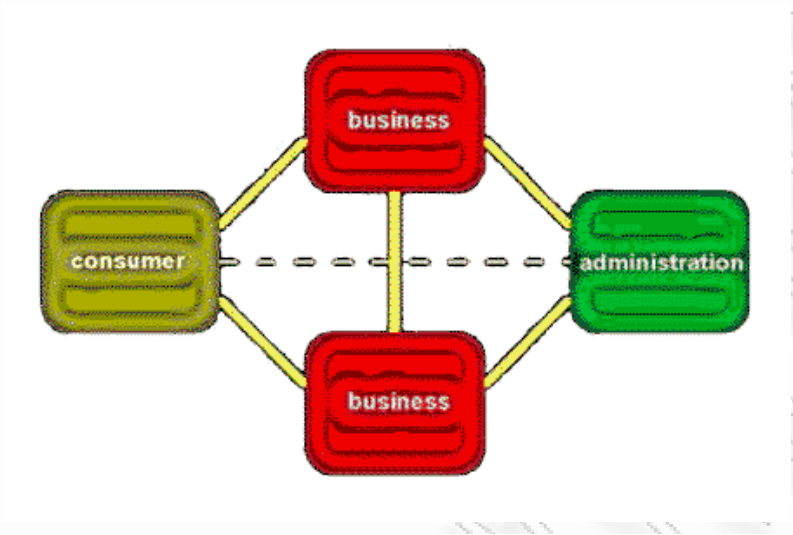
Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα, αποτελεί δηλαδή μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω διαδικτύου – internet χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών (δηλαδή του πωλητή και του αγοραστή).

Εικόνα 1: Το εμπόριο στο Διαδίκτυο

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

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

2.1.2 Είδη Ηλεκτρονικού Εμπορίου



Εικόνα 2: Είδη ηλεκτρονικού εμπορίου

Εσωτερικό εμπόριο:

Στόχος είναι η αποτελεσματικότερη λειτουργία των δραστηριοτήτων μιας επιχείρησης, ώστε να μπορεί να προσφέρει καλύτερα προϊόντα και υπηρεσίες στους πελάτες της. Οι εφαρμογές του συνήθως εντάσσονται στη λειτουργία ενός τοπικού δικτύου (Intranet) και μπορούν να είναι: επικοινωνία μεταξύ ομάδων εργασίας, ηλεκτρονική δημοσίευση (άμεση διανομή πληροφοριών) κτλ.

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

Το ηλεκτρονικό εμπόριο επιτρέπει σε επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες και το κόστος των προμηθειών, την ταχύτερη αποστολή των προμηθειών και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επιπλέον, καθιστά ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και ποιοτικότερη την εξυπηρέτηση πελατών. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς, καθώς και η πραγματοποίηση ηλεκτρονικών πληρωμών βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές περιορίζουν το ανθρώπινο σφάλμα, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών. Το ηλεκτρονικό εμπόριο προσφέρει τη δυνατότητα αυξημένης πληροφόρησης σχετικά με τα προσφερόμενα προϊόντα - είτε από τους προμηθευτές είτε από ενδιάμεσους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου.

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

Πρόκειται για την πιο διαδεδομένη μορφή ηλεκτρονικού εμπορίου. Ο καταναλωτής έχει πρόσβαση σε μια τεράστια ποικιλία προϊόντων σε δικτυακούς κόμβους-καταστήματα, βλέπει, επιλέγει, αν επιθυμεί να αγοράσει είδη ένδυσης μπορεί ενίοτε και να τα

δοκιμάζει (μέσω ειδικών προγραμμάτων), ανακαλύπτει προϊόντα τα οποία δεν θα μπορούσε να βρει εύκολα στη χώρα του, συγκρίνει τιμές και, τέλος, αγοράζει. Κι όλα αυτά χωρίς να βγει από το σπίτι του, κερδίζοντας πολύτιμο χρόνο και κόπο.

Συναλλαγές μεταξύ Καταναλωτών (Consumer-to-Consumer - C2C):

Σε αυτή την κατηγορία ο καταναλωτής πουλά απευθείας σε άλλους καταναλωτές. Παράδειγμα αποτελούν τα άτομα που κάνουν πωλήσεις μέσω καταχωρημένων αγγελιών, δικτυακοί τόποι δημοπρασιών, όπου ο οποιοσδήποτε μπορεί να πουλήσει οτιδήποτε. Τέλος, πολλά άτομα κάνουν χρήση intranets και άλλων ενδοεταιρικών δικτύων για να διαφημίσουν αντικείμενα, προϊόντα ή υπηρεσίες.

2.1.3 Τεχνολογίες για την υποστήριξη του ηλεκτρονικού εμπορίου

Οι τεχνολογίες του ηλεκτρονικού εμπορίου δεν είναι όλες νέες. Οι περισσότερες από αυτές χρησιμοποιούνται εδώ και αρκετά χρόνια από συγκεκριμένες επιχειρήσεις ή κλάδους. Αυτό που τους έδωσε την απαιτούμενη ώθηση και έκανε την αντιμετώπισή τους ενιαία – κάτω από τη μορφή του ηλεκτρονικού εμπορίου – ήταν η αποδοχή διεθνών προτύπων και η ανάγκη για νέες μορφές οργάνωσης και λειτουργικής διαχείρισης. Έτσι, οι επιχειρήσεις θα μπορούσαν στο εξής να αντεπεξέλθουν στις συνθήκες που επιβάλλονται από τη διεθνοποίηση των αγορών, τις νέες καταναλωτικές αντιλήψεις και κοινωνικές συνθήκες.

Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI – Electronic Data Interchange)

Δημιουργήθηκε στις αρχές της δεκαετίας του ’70. Η EDI είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέψει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα. Πρόκειται για την ηλεκτρονική ανταλλαγή εμπορικών και διοικητικών δεδομένων από υπολογιστή σε υπολογιστή, με την ελάχιστη παρέμβαση χειρόγραφων διαδικασιών. Τα δεδομένα αυτά είναι οργανωμένα σε αυτοτελή μηνύματα (τιμολόγια, παραγγελίες, τιμοκατάλογοι, φορτωτικές κλπ.), το περιεχόμενο και η δομή των οποίων καθορίζονται από κάποιο κοινώς αποδεκτό πρότυπο. Τα πρότυπα που χρησιμοποιούνται σε παγκόσμιο επίπεδο προέρχονται από τον Οργανισμό Ηνωμένων Εθνών και καλύπτουν ένα ευρύ φάσμα επικοινωνιακών αναγκών των εμπορικών εταιρειών. Το πρότυπο αυτό είναι το EDIFACT (EDI For Administration, Commerce and Transportation).

Επίπεδο Ασφαλών Συνδέσεων (SSL – Secure Sockets Layer)

Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Το SSL χρησιμοποιεί «κλειδί» δημόσιας κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα, καθώς «ταξιδεύουν» μέσα στο Internet.

Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET – Secure Electronic Transactions)

Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, τυγχάνει μεγάλης αποδοχής από την τραπεζική κοινότητα.

Γραμμωτός κώδικας (Barcode)

Η τεχνολογία του γραμμωτού κώδικα αποτελεί τμήμα του γενικότερου τομέα των τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Είναι ένα σύγχρονο εργαλείο, το οποίο βοηθά καταλυτικά στην ομαλή διακίνηση και διαχείριση (logistics) προϊόντων και υπηρεσιών. Η ανάπτυξη της τεχνολογίας του γραμμωτού κώδικα ξεκίνησε στις αρχές της δεκαετίας του 1960, με σκοπό να εξυπηρετήσει την πληρωμή προϊόντων στα καταστήματα τροφίμων. Οι πρώτες εφαρμογές σε βιομηχανικό περιβάλλον εμφανίστηκαν στα τέλη της ίδιας δεκαετίας σε μεγάλες αυτοκινητοβιομηχανίες, για τον περιορισμό του κόστους εργασίας που σχετιζόταν με την παραγωγή. Εκτεταμένη χρήση παρουσιάστηκε μετά την ανάπτυξη των πρώτων προτύπων (λόγω των πιέσεων των -αρκετών πλέον- χρηστών / προμηθευτών και υποκατασκευαστών των μεγάλων βιομηχανιών) στα τέλη της δεκαετίας του 1970. Κατά τη δεκαετία του 1980 υπήρξε αλματώδης ανάπτυξη του εξοπλισμού, κατ' επέκταση και των τρόπων χρήσης της τεχνολογίας γραμμωτού κώδικα.

2.2 Η έννοια της ηλεκτρονικής τραπεζικής (electronic-banking)

Η ραγδαία ανάπτυξη των τεχνολογιών της πληροφορικής σε συνδυασμό με την διαρκώς αυξανόμενη υιοθέτηση του διαδικτύου παγκοσμίως αποτέλεσαν αρωγό για τη δημιουργία της λεγόμενης «νέας οικονομίας». Η τελευταία είναι άμεσα συνυφασμένη με τους ηλεκτρονικούς υπολογιστές. Σε αυτή την αλλαγή από την «παραδοσιακή» στη «νέα» οικονομία δεν θα μπορούσαν να μείνουν αμέτοχες οι επιχειρήσεις και ειδικότερα τα χρηματοπιστωτικά ιδρύματα (τράπεζες) που κατά κύριο λόγο τη διαμορφώνουν.

Οι τράπεζες ξεκίνησαν να χρησιμοποιούν το διαδίκτυο όχι μόνο σαν ένα καινοτόμο τρόπο παροχής υπηρεσιών και για να αυξήσουν την ικανοποίηση των πελατών τους, αλλά επίσης και σαν έναν τρόπο για να μειώσουν το κόστος και να αυξήσουν τα κέρδη τους. Ο έντονος ανταγωνισμός μεταξύ των τραπεζών, τις έχει οδηγήσει στο να βρούνε νέες και προσοδοφόρες περιοχές για να αναπτυχθούν. Παράλληλα όμως η ηλεκτρονική τραπεζική αποτελεί μια βιώσιμη στρατηγική ακόμα και για νεοεισερχομένους παίκτες στον τραπεζικό χώρο.

2.2.1 Ορισμός

Με τον όρο ηλεκτρονική τραπεζική (e-banking) εννοούμε:

«οποιαδήποτε εμπορική συναλλαγή που διεξάγεται μεταξύ της τράπεζας και των πελατών της διαμέσου ηλεκτρονικών δικτύων και βοηθάει ή οδηγεί στην πώληση τραπεζικών υπηρεσιών/προϊόντων». (*Ένωση Ελληνικών Τραπεζών, 2000)*

Ο όρος του e-banking αναφέρεται σε εφαρμογές τραπεζικής που διεκπεραιώνονται μέσω του διαδικτύου (Internet Banking), μέσω σταθερού τηλεφώνου (Phone Banking) μέσω κινητού τηλεφώνου (Mobile Banking) και μέσω των Αυτόματων Ταμειολογιστικών Μηχανών (ATMς). Πιο συγκεκριμένα:

- Μέσω του Internet Banking δίδεται στους χρήστες η δυνατότητα πραγματοποίησης μεγάλου εύρους συναλλαγών και πληροφόρησής τους άμεσα, ανά πάσα στιγμή και από οποιοδήποτε μέρος του κόσμου.

- Το Phone Banking με τη χρήση της τεχνολογίας αναγνώρισης φωνητικών εντολών (IUR) επιτρέπει στους πελάτες της τράπεζας να διεκπεραιώνουν της συναλλαγές τους μέσω του σταθερού τους τηλεφώνου.

- Το Mobile Banking εξασφαλίζει στους χρήστες την ευκολία να συναλλάσσονται και να ενημερώνονται για τους λογαριασμούς τους επί 24 ώρου βάσεως μέσω του κινητού τους τηλεφώνου, απλά εγκαθιστώντας την εκάστοτε κατάλληλα εφαρμογή (application)

- Τα ATM$_S$ ως μηχανές ανάληψης και κατάθεσης διευκολύνουν τους πελάτες απ΄το να περιμένουν σε ταμεία των τραπεζών, εξυπηρετώντας τους άμεσα.

Εικόνα 3: Η έννοια της ηλεκτρονικής τραπεζικής στην Ελλάδα

2.2.2 Ιστορική αναδρομή

Στο ολοένα εξελισσόμενο περιβάλλον του παγκόσμιου ιστού, η σταδιακή εξάπλωση του Διαδικτύου και η ραγδαία ανάπτυξη των τεχνολογιών πληροφορικής αποτελούν αρωγό για την εδραίωση του ηλεκτρονικού επιχειρείν. Στα πλαίσια της πραγματοποίησης εμπορικών συναλλαγών διασυνοριακά, μέσω τηλεπικοινωνιών μέσων, εντάσσεται και η λειτουργία της ηλεκτρονικής τραπεζικής.

Από τα τέλη της δεκαετίας του ’80 οι τράπεζες αρχίζουν να προσθέσουν στα διάφορα κανάλια διανομής τους και το ηλεκτρονικό. Έτσι, απευθύνονται σε ένα

ευρύτερο κοινό, ενώ παράλληλα προσφέρουν άμεση εξυπηρέτηση από οποιοδήποτε σημείο και αν βρίσκεται ο χρήστης. Οι πρώτες εφαρμογές της ηλεκτρονικής τραπεζικής ανά τον κόσμο είναι ως ακολούθως:

- Νέα Υόρκη: 1981 (videotext system) / από τις τράπεζες Citibank, Chase Manhattan, Chemical, Manufacturers Hanover
- Μεγάλη Βρετανία: 1983 (Prestel) / από την Bank of Scotland
- Γαλλία: 1982 (Minitel)
- Ελλάδα:
  1997/ τράπεζα ΕΓΝΑΝΤΙΑ (χρηματοοικονομικές συναλλαγές σε πρωταρχικό στάδιο ως και το 2000)
  2000/ τράπεζα Πειραιώς (εισαγωγή πρώτης ολοκληρωμένης πλατφόρμας ηλεκτρονικών υπηρεσιών “WINBANK”)

2.3 Ηλεκτρονικές πληρωμές

Οι πληρωμές μέσω internet banking ή Ηλεκτρονικές Πληρωμές (Electronic Payments) περιλαμβάνουν κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες επιχειρήσεις από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με τη μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Σύμφωνα με τη Σύσταση 97/489/ΕΚ, Ηλεκτρονική Πληρωμή είναι η πληρωμή που γίνεται είτε με ηλεκτρονική μεταφορά κεφαλαίων (e- banking) είτε με πιστωτική κάρτα είτε με ηλεκτρονικό χρήμα (Οδηγία 2000/46/ΕΚ). Η χρήση ηλεκτρονικών μέσων για την πληρωμή σε μία συναλλαγή έχει σαν συνέπεια την πίστωση του ποσού αυτού και την εμφάνιση επιτοκίου που βαρύνει τον καταναλωτή. Συνεπώς, ο όρος ηλεκτρονική πληρωμή ενέχει τις εξής προϋποθέσεις :

- Οι πληρωμές πραγματοποιούνται απευθείας από τον ίδιο τον πληρωτή (πολίτης ή επιχείρηση), χωρίς την παρέμβαση κάποιου άλλου φυσικού προσώπου
- Οι πληρωμές πραγματοποιούνται εξ αποστάσεως, δηλαδή χωρίς τη φυσική παρουσία του πληρωτή (πολίτης ή επιχείρηση)
- Οι πληρωμές πραγματοποιούνται χωρίς μετρητά
- Οι πληρωμές πραγματοποιούνται με την αξιοποίηση ενός ηλεκτρονικού δικτύου (π.χ. Internet, GPRS κ.λπ.) ή/και μέσου (PC, κινητό τηλέφωνο κ.λπ.).

Ο πληρωτής έχει στη διάθεση του όλα τα προϊόντα που του προσφέρει η τράπεζα του μέσω του συγκεκριμένου δικτύου. Μπορεί να χρεώσει όποιο προϊόν θέλει, υπό την προϋπόθεση ότι αυτό μπορεί να δεχτεί τη χρέωση. Τα κυριότερα προϊόντα προς χρέωση είναι οι λογαριασμοί καταθέσεων (ταμιευτήριο και τρεχούμενος/όψεως), που ενδέχεται να έχουν και όριο χορήγησης (overdraft).

Ο δικαιούχος, με τη σειρά του, πιστώνεται σε λογαριασμό που κι αυτός τηρεί στην ίδια τράπεζα. Η πίστωση μπορεί να γίνεται σε πραγματικό χρόνο (τη στιγμή που διεκπεραιώνεται η πληρωμή) ή μεταγενέστερα για το σύνολο των πληρωμών, ανάλογα με τη συμφωνία που έχει κάνει με την τράπεζα και ανάλογα με το είδος πληρωμής.

2.3.1 Πλεονεκτήματα

Οι ηλεκτρονικές τραπεζικές υπηρεσίες προσφέρουν πληθώρα από οφέλη σε όσους τις χρησιμοποιούν, όπως :

- Ευκολία χρήσης και διαθεσιμότητας των υπηρεσιών σε εικοσιτετράωρη βάση, επτά ημέρες την εβδομάδα, όλο το χρόνο.
- Δυνατότητα πρόσβασης στις ηλεκτρονικές υπηρεσίες της τράπεζας, ανεξάρτητα από την τοποθεσία την όποια βρίσκεται ο χρήστης (σπίτι, γραφείο, εξωτερικό, σε μη σταθερό σημείο), αρκεί να υπάρχει πρόσβαση στο διαδίκτυο.
- Ταχύτητα στη διενέργεια και ολοκλήρωση των συναλλαγών σε σχέση με τα λοιπά παραδοσιακά εναλλακτικά κανάλια πραγματοποίησης των συναλλαγών.
- Υψηλό επίπεδο ασφάλειας συναλλαγών.
- Αποδοτικότερη διαχείριση όλων των συναλλαγών, με δυνατότητα ύπαρξης συνολικής εικόνας των λογαριασμών και των συναλλαγών μέσω ενός ηλεκτρονικού υπολογιστή.
- Πρόσβαση σε μεγάλο φάσμα πληροφοριών, που καλύπτει σχεδόν το σύνολο των αναγκών των ιδιωτών και των επιχειρήσεων.
- Μη υποχρέωση συνεχούς φυσικής παρουσίας στα υποκαταστήματα των τραπεζών και κατά συνέπεια μείωση του κόστους συναλλαγών και εξοικονόμηση χρόνου.
- Επέκταση των δικτύων εξυπηρέτησης των τραπεζών με άμεσο αποτέλεσμα την αύξηση της πελατειακής τους βάσης.
- Μείωση των λειτουργικών τους δαπανών
- Ενίσχυση της τράπεζας στον κλάδο δραστηριοποίησής της λόγω ενίσχυσης του ονόματός της (brand name).

2.3.2 Μειονεκτήματα

Εκτός από τα πολυποίκιλα θετικά αποτελέσματα που προσφέρει η ηλεκτρονική τραπεζική τόσο στον πελάτη όσο και στην ίδια την τράπεζα χαρακτηρίζεται και από μερικά αρνητικά στοιχεία, ως ακολούθως:

- Δυσπιστία του χρήστη, καθώς δεν είναι μεγάλο το ποσοστό των χρηστών που εμπιστεύεται και εν τέλει πραγματοποιεί τις συναλλαγές του μέσω του Διαδικτύου.
- Δυσκολία στο χειρισμό από άτομα μη εξοικειωμένα με τη χρήση ηλεκτρονικών υπολογιστών
- Πιθανότητα ηλεκτρονικής «επίθεσης» μέσω διαφόρων κακόβουλων προγραμμάτων (ιοί, δούρειοι ίπποι, phishing κλπ) με κύριο στόχο την παραπλάνηση των χρηστών και την τελική υποκλοπή των κωδικών τους προκειμένου να αποκτήσουν πρόσβαση στο διαδικτυακό λογαριασμό τους.

3 ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Σήμερα παρατηρείται επανάσταση στα μέσα πληρωμών. Κάρτες και ηλεκτρονικές πληρωμές παίρνουν τη θέση των μετρητών και των φυσικών επιταγών. Το 2003 η συνδυασμένη χρήση πιστωτικών και χρεωστικών καρτών για πληρωμές μέσω καταστημάτων υπερβαίνει για πρώτη φορά τη συνδυασμένη χρήση μετρητών και επιταγών (Gerdes et al. 2005). Μέχρι το 2005 οι χρεωστικές και οι πιστωτικές κάρτες αποτελούσαν το 55% των πληρωμών σε καταστήματα και τα μετρητά και οι επιταγές κάλυπταν το υπόλοιπο ποσοστό. Η αύξηση της χρήσης του πλαστικού χρήματος οδήγησε στην αύξηση της χρήσης πιστωτικών και χρεωστικών καρτών και στη μείωση χρήσης μετρητών.

3.1 Χρήση καρτών στις ηλεκτρονικές πληρωμές

Οι κάρτες πληρωμής είναι ηλεκτρονικές κάρτες που περιέχουν πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν για πληρωμές. Υπάρχουν τρία είδη πληρωμής:

- *Πιστωτικές κάρτες (credit card):* μια πιστωτική κάρτα παρέχει στον κάτοχο πίστωση ώστε να πραγματοποιεί αγορές μέχρι ένα όριο, που καθορίζεται από τον εκδότη της κάρτας.
- *Χρεωστικές κάρτες (debit card)*: το υπόλοιπο της χρεωστικής κάρτας πληρώνεται ολόκληρο μόλις γίνει η λήψη μηνιαίας δήλωσης. Συνήθως, ο κάτοχος μιας χρεωστικής κάρτας λαμβάνει ένα δάνειο για 30 ως 45 μέρες, το οποίο είναι ίσο με το υπόλοιπο της δήλωσής του.
- *Χρεωστική κάρτα άμεσης πληρωμής*: με μια χρεωστική άμεσης πληρωμής τα χρήματα για ένα αγοραζόμενο είδος αφαιρούνται αμέσως από τον τραπεζικό λογαριασμό του κατόχου. Η μεταφορά των χρημάτων από το λογαριασμό του κατόχου στο λογαριασμό του εμπόρου γίνεται σε 1 με 2 μέρες.

3.2 Έξυπνες κάρτες

Οι έξυπνες κάρτες (smart cards) χρησιμοποιούνται συχνά αντί των παραδοσιακών χρεωστικών και πιστωτικών καρτών. Χρησιμοποιούνται ευρέως για υποστήριξη εφαρμογών που δεν έχουν σχέση με το λιανικό εμπόριο και με χρηματοοικονομικά θέματα. Μια έξυπνη κάρτα διακρίνεται από την παρουσία ενός ενσωματωμένου μικροτσίπ. Μπορεί να είναι συνδυασμός ενός είδους μικροεπεξεργαστή με ένα τσιπ μνήμης ή απλώς ένα τσιπ μνήμης με μη προγραμματιζόμενη λογική.

Εικόνα 4: Όψη "έξυπνης κάρτας"

3.3 Κάρτες Αποθηκευμένης Αξίας

Η χρηματική αξία μιας κάρτας αποθηκευμένης αξίας (stored value card) φορτώνεται εκ των προτέρων στην κάρτα. Από φυσική και τεχνική πλευρά, μία τέτοιου είδους κάρτα δεν διαφέρει από μία πιστωτική ή χρεωστική. Φέρει μια μαγνητική ταινία στην οποία αποθηκεύεται η χρηματική της αξία. Αυτό το χαρακτηριστικό τη διακρίνει από μία έξυπνη κάρτα, η οποία φέρει ένα τσιπ. Οι καταναλωτές μπορούν να χρησιμοποιούν μια κάρτα αποθηκευμένης αξίας για να πραγματοποιούν τις αγορές τους παραδοσιακά ή ηλεκτρονικά. Στηρίζονται στα ίδια δίκτυα, κρυπτογραφημένες επικοινωνίες και πρωτόκολλα ηλεκτρονικής τραπεζικής, όπως συμβαίνει και με τις χρεωστικές και πιστωτικές κάρτες. Το διαφορετικό στις κάρτες αποθηκευμένης αξίας είναι ότι μπορούν να τις αγοράσουν όλοι, χωρίς να δώσουν κάποια εγγύηση, ή να έχουν κάποιο τραπεζικό λογαριασμό.

Εικόνα 5: Κάρτες αποθηκευμένης αξίας

3.4 Ηλεκτρονικές επιταγές

Μία ηλεκτρονική επιταγή (e-check) είναι η ηλεκτρονική έκδοση ή απεικόνιση μιας έντυπης επιταγής. Οι ηλεκτρονικές επιταγές περιέχουν τις ίδιες πληροφορίες με τις έντυπες επιταγές, μπορούν να χρησιμοποιηθούν και οι έντυπες επιταγές και βασίζονται στο ίδιο νομικό πλαίσιο. Οι ηλεκτρονικές επιταγές βασίζονται στις τρέχουσες επιχειρηματικές και τραπεζικές πρακτικές και μπορούν να χρησιμοποιηθούν από οποιαδήποτε επιχείρηση διαθέτει έναν τραπεζικό λογαριασμό, περιλαμβανομένων και επιχειρήσεων μικρού και μεσαίου μεγέθους, οι οποίες μπορεί να μην έχουν τη δυνατότητα να χρησιμοποιούν άλλες μορφές ηλεκτρονικών πληρωμών (π.χ. πιστωτικές και χρεωστικές κάρτες).

Εικόνα 6: Ηλεκτρονικές Επιταγές

ΜΕΡΟΣ Ά

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

4 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Η αύξηση σε πωλήσεις ηλεκτρονικού εμπορίου προσελκύουν ολοένα και περισσότερους απατεώνες του κυβερνοχώρου. Οι ηλεκτρονικοί αγοραστές είναι ελκυστικοί στόχοι, επειδή συνήθως έχουν υψηλότερα εισοδήματα. Δυστυχώς, μια σειρά παραγόντων συμβάλλει στη διατήρηση τέτοιων φαινομένων, καθιστώντας τις ηλεκτρονικές πληρωμές επικίνδυνες για το μεγαλύτερο ποσοστό των χρηστών. Πιο συγκεκριμένα, η ισχυρή ασφάλεια προσδίδει εξ ορισμού στις ηλεκτρονικές πληρωμές τα χαρακτηριστικά της άβολης και απαιτητικής μεθόδου πληρωμών. Επιπλεόν, η έλλειψη συνεργασίας από εκδότες πιστωτικών καρτών και από ξένους παρόχους υπηρεσιών Internet (ISP), λόγω του ότι δεν έχουν κίνητρο για κάτι τέτοιο. Αν ο ISP προέλευσης συνεργαστεί και σταματήσει την πρόσβαση του εισβολέα, τότε θα είναι πολύ δύσκολο να κάνουν οι εισβολείς την επιθυμητή τους επίθεση.

Σημαντικό παράγοντα που αποτελεί τροχοπέδη στην αντιμετώπιση προβλημάτων απάτης ηλεκτρονικών πληρωμών, είναι οι ίδιοι οι χρήστες, οι οποίοι δεν λαμβάνουν τα κατάλληλα μέτρα και τις απαραίτητες προφυλάξεις ώστε να μην γίνουν θύματα των επιτείδειων. Θέτουν άθελά τους των εαυτό τους σε κίνδυνο χρησιμοποιώντας προσωπικά στοιχεία, όπως χρεωστικές κάρτες, σε ιστοθέσεις ηλεκτρονικών παιχνιδιών ή ιστοθέσεις κοινωνικής δικτύωσης (πχ. Facebook, MySpace, Skyblog κλπ). Προσωπικές πληροφορίες που δημοσιεύονται σε αυτές τις ιστοσελίδες χρησιμοποιούνται για υποκλοπή ταυτότητας ή για μόλυνση των υπολογιστών των χρηστών με κακόβουλο λογισμικό.

Τέλος, η ίδια η σχεδίαση των πληροφοριακών συστημάτων και ζητήματα της αρχιτεκτονικής ασφαλείας αναστέλλουν τη σωστή παροχή ασφαλείας στις ηλεκτρονικές πληρωμές. Είναι ευρέως γνωστό ότι η αποτροπή της τρωτότητας κατά τη φάση σχεδίασης και πριν από την υλοποίηση της ηλεκτρονικής πληρωμής, είναι λιγότερο ακριβή από την επίλυση των προβλημάτων αργότερα. Η ασφάλεια θα πρέπει να προγραμματίζεται από τη φάση σχεδίασης, καθώς απλά προβλήματα, όπως η μη διασφάλιση ότι όλη η κίνηση που περνά από το δίκτυο περνά μέσα από ένα firewall, συχνά ευθύνεται για το ότι παρέχεται δυνατότητα πρόσβασης σε εισβολείς. Αν η ασφάλεια δεν κτιστεί σε επίπεδο διακομιστή εφαρμογών, τότε θα είναι αδύνατον να μπλοκάρει ορισμένους τύπους επιθέσεων. Ευφυείς εισβολείς δεν χρησιμοποιούν προγράμματα περιήγησης για να εισχωρήσουν σε ιστοσελίδες, αλλά χρησιμοποιούν εργαλειοθήκες για να προσπελάσουν δίκτυα ή εφαρμογές και τελικά να φτάσουν μέσω αυτών σε βάσεις δεδομένων.

4.1 Κύκλος ζωής προγράμματος ασφαλείας

Υπάρχουν τέσσερις (4) φάσεις υψηλού επιπέδου στον κύκλο ζωής ενός προγράμματος ασφαλείας ηλεκτρονικών πληρωμών, οι οποίες είναι:

1. Σχεδιασμός και οργάνωση
2. Υλοποίηση
3. Λειτουργία και συντήρηση
4. Παρακολούθηση και αποτίμηση

Με αυτό τον τρόπο επιτυγχάνεται η μέγιστη δυνατή ασφάλεια, παρέχοντας τη δυνατότητα, βελτίωσης του προγράμματος ώστε να καλύπτει τους σύγχρονους, διαρκώς εξελισσόμενους κινδύνους. Επιπλέον, σήμερα χρησιμοποιείται μια πληθώρα

διαφορετικών προγραμμάτων ασφαλείας, όπως αυτοί αναλύονται στο κεφάλαιο 5 της παρούσας εργασίας.

4.2 Ζητήματα ασφαλείας

Για την πραγματοποίηση ηλεκτρονικών συναλλαγών πρέπει να λαμβάνονται υπόψιν και τα ακόλουθα κύρια ζητήματα:

- Πιστοποίηση αυθεντικότητας: απαιτεί αποδείξεις με τη μορφή διαπιστευτηρίων, που μπορούν να είναι σε διαφορετικές μορφές, που περιλαμβάνουν κάτι γνωστό (πχ. ένα κώδικα πρόσβασης), κάτι που κατέχει το άτομο (πχ. μια έξυπνη κάρτα) ή κάτι μοναδικό (πχ. μια υπογραφή).
- Εξουσιοδότηση: απαιτεί τη σύγκριση πληροφοριών για το άτομο ή το πρόγραμμα με πληροφορίες ελέγχου προσπέλασης που σχετίζονται με τον πόρο που προσπελαύνεται.
- Επιθεώρηση: είναι η διαδικασία κατά την οποία καταγράφεται πότε, ποιος και τι προσπελάστηκε στον κυβερνοχώρο. Με αυτό τον τρόπο παρέχεται η δυνατότητα εντοπισμού του προγράμματος ή του ατόμου που διενήργησε τις ανωτέρω διαδικασίες.
- Εμπιστευτικότητα (διασφάλιση απορρήτου) και ακεραιότητα (πίστη): η πιο συνηθισμένη μέθοδος κρυπτογράφησης.
- Διαθεσιμότητα
- Μη αποκήρυξη: η χρήση μιας ψηφιακής υπογραφής, που δυσκολεύει τους χρήστες να αμφισβητήσουν ότι συμμετείχαν σε μια συναλλαγή.

4.3 Διάκριση επιθέσεων

Είναι χρήσιμο να αναφερθεί πως οι επιθέσεις διακρίνονται σε δύο τύπους: α) τις μη τεχνικές και β) τις τεχνικές επιθέσεις. Οι μη τεχνικές επιθέσεις αφορούν εκείνες που ένας εισβολέας χρησιμοποιεί απάτη ή άλλες μορφές πειθούς για να παραπλανήσει τους χρήστες ώστε να αποκαλύψουν ευαίσθητες προσωπικές πληροφορίες ή να εκτελέσουν ενέργειες που θα μπορούσαν να θέσουν σε κίνδυνο το δίκτυο. Αντίθετα, οι γνώσεις λογισμικού και συστημάτων χρησιμοποιούνται για διάπραξη τεχνικών επιθέσεων. Οι περισσότερες επιθέσεις περιλαμβάνουν συνδυασμό και των δύο τύπων. Για παράδειγμα ένας εισβολέας μπορεί να χρησιμοποιήσει ένα αυτοματοποιημένο εργαλείο για να δημοσιεύσει ένα μήνυμα σε μια υπηρεσία ανταλλαγής άμεσων μηνυμάτων που ενδιαφέρει τον αναγνώστη, πχ ένα βίντεο. Μόλις, όμως ο χρήστης επιλέξει την αναπαραγωγή του εκτελείται αυτόματα κακοβουλο λογισμικό που μετατρέπει τον υπολογιστή σε υποχείριο του εισβολέα.

5 ΤΡΟΠΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

5.1 Εισαγωγή στους τρόπους ασφάλειας

Λόγοι ανασφάλειας στο διαδίκτυο

Το Διαδίκτυο, όπως είναι γνωστό αποτελεί το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων, όχι κατά ανάγκη ιδίας τεχνολογίας, που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε όλη τη Γή .Είναι λοιπόν αντιληπτό, ότι είναι πολύ δύσκολο να αντιμετωπιστεί ολικά από άποψη ασφάλειας, εξαιτίας της ετερογένειας που το χαρακτηρίζει. Βέβαια πολύ σημαντικό είναι το γεγονός ότι οι μηχανισμοί που στηρίζουν την λειτουργικότητα του σχεδιάστηκαν με σκοπό την βελτιστοποίηση των δυνατοτήτων διασύνδεσης ετερογενών δικτύων και εκμετάλλευσης πόρων-πληροφοριών και όχι για να παρέχουν ασφάλεια. Συμπερασματικά η ασφάλεια επιτυγχάνεται ως πρόσθετο χαρακτηριστικό του δικτυακού σχεδίου και όχι ως κομμάτι του. Οι λόγοι που τρέπουν το Διαδίκτυο ανασφαλές είναι (Ahuja, 1997):

- Η ετερογένεια των δικτύων που διασυνδέει, με δεδομένο το απέραντο μέγεθος του, έχει σαν συνέπεια : Οι διαδικασίες που διασφαλίζουν ένα σύστημα σε ένα τέτοιο περιβάλλον, να απαιτούν ένα μεγάλο αριθμό περίπλοκων ρυθμίσεων και διαμορφώσεων.
- Η εύκολη και απεριόριστη πρόσβαση που παρέχει σε εκατομμύρια χρηστές, το τρέπει πιο ευάλωτο από άλλο δίκτυο. Είναι στόχος πολλών επιθέσεων από επίδοξους εισβολείς. Αυτοί ποικίλουν από έφηβους, βάνδαλους , ηλεκτρονικούς εγκληματίες και άλλους με σκοπό να διεισδύσουν στα συστήματα.
- Η μη ύπαρξη συνολικής πολιτικής ελέγχου προσπέλασης. Δεν υπάρχει κατάλληλη υποδομή στους υπάρχοντες κόμβους , εξαιτίας άγνοιας, κόστους και άλλων λόγων, με αποτέλεσμα να υπάρχει μεγάλος κίνδυνος από την ευρέως ανοικτή σύνδεση τους στο Διαδίκτυο.
- Η φύση των πρωτοκόλλων TCP/IP και των περισσότερων υπηρεσιών που υποστηρίζουν, δεν μπορούν να εκμηδενίσουν τους κινδύνους ασφάλειας (HCFA , 1998). Το γεγονός ότι δεν επιτρέπονται τα πακέτα των δεδομένων , να περνούν από μια σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και επιμέρους δικτύων μέχρι να φθάσουν στον τελικό προορισμό τους , δίνει την δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διάφορους τρόπους στην επικοινωνία των δυο νόμιμων μερών. Επιδέξιοι εισβολείς μπορούν σχετικά εύκολα να παραβιάσουν την ασφάλεια των TCP/IP υπηρεσιών , με δεδομένο και ότι η πλειοψηφία των δεδομένων που διακινούνται είναι σε μη κρυπτογραφημένη μορφή.
- Η αυξημένη πολυπλοκότητα διαδικασιών , περιορίζει το αίσθημα εμπιστοσύνης, μιας και όσο πιο δυσνόητο είναι κάτι τόσο μεγαλύτερη είναι η δυσπιστία που επικρατεί γι' αυτό.

Η αύξηση στον αριθμό δίαυλων επικοινωνίας, σημαίνει ταυτόχρονα αύξηση των πιθανών σημείων επίθεσης, οπότε υπάρχει αναγκαιότητα για μεγαλύτερη και κατάλληλη οχύρωση τους.

- Η ασάφεια όσον αφόρα τα όρια των δικτύων που δεν υπάρχουν στο Διαδίκτυο, καθώς και οι διακρίσεις των τμημάτων ενός οργανισμού. Κάθε κόμβος πρέπει να είναι ικανός να αντιδράσει σωστά στην παρουσία ενός νέου και μη έμπιστου κόμβου (Fleeter, 1997). Βεβαίως είναι πολύ πιθανό ένας κόμβος να ανήκει σε περισσότερα από ένα δίκτυα , οπότε να μην έχουμε σαφή εικόνα των νόμιμων χρηστών του.
- Η δυνατότητα ανωνυμίας ενός χρήστη , απαιτεί πολύ ισχυρούς μηχανισμούς πιστοποίησης , διαφορετικούς από αυτούς που πιστοποιούν ανθρώπους στα υπολογιστικά συστήματα.
- Η ύπαρξη αδυναμίας ελέγχου δρομολόγησης των δεδομένων , που διακινούνται σε κάθε δίκτυο και κατ' επέκταση στο Διαδίκτυο.

Ένα σύστημα ασφάλειας χρησιμεύει στην παρεμπόδιση απόσπασης η καταστροφής δεδομένων που υπάρχουν σε ένα δίκτυο. Για επιχείρηση (ή ένα χρηματοπιστωτικό ίδρυμα) η ασφάλεια είναι διττής σημασίας:

α) εμπιστευτικές πληροφορίες
β) ακεραιότητα.

Υπάρχουν διάφοροι τρόποι προστασίας , οι σημαντικότεροι απ΄αυτούς είναι: κρυπτογραφία , ψηφιακές υπόγραφες , ψηφιακά πιστοποιητικά , antivirus , SSL και IPSec , Firewalls.

Οι τεχνολογίες ασφάλειας προσφέρονται σε διάφορα επίπεδα του μοντέλου OSI-ISO. Αυτές είναι οι ακόλουθες:

- Επίπεδο εφαρμογής: Συμμετρική και Μη-συμμετρική κρυπτογραφία, Ψηφιακές Υπογραφές, Ψηφιακά Πιστοποιητικά και Αρχές Πιστοποίησης, Διαχείριση κλειδιών, Αλγόριθμοι Κρυπτογράφησης

- Επίπεδο μεταφοράς: S-HTTP, SSL, S/MIME, PGP, Firewalls

5.2 Κρυπτογραφία

5.2.1 Ορισμός

Αρχικά , η Κρυπτογραφία αποτέλεσε την τεχνική της απόκρυψης του περιεχομένου ενός μηνύματος , από μη εξουσιοδοτημένες οντότητες. Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές τις διαρκώς να πληθαίνουν.

Οι σύγχρονες επιχειρηματικές ανάγκες απαιτούν συχνά τη μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου. Η νέα ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου επαγγελματικού απορρήτου. Βασική τεχνολογία στον τομέα της ασφάλειας στο internet είναι η κρυπτογράφηση.

Σε νομικό και κοινωνικό επίπεδο , τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και

ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του internet. Από την στιγμή, που άρχισαν να μεταφέρονται πληροφορίες , ξεκίνησε η ιδέα της κρυπτογράφησης του κώδικα για να ασφαλιστούν τα μηνύματα. Αν το μήνυμα είναι γραμμένο σε κώδικα, είναι ασφαλές ακόμα και αν υποκλαπεί. Με άλλα λόγια, η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων.

Οι **μέθοδοι κρυπτογράφησης** καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext) , ενώ τα ακάλυπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση (decryption , deciphering) ονομάζεται η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η μετατροπή του κρυπτογραφήματος σε αρχικό κείμενο. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική , όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

Ο **Αλγόριθμος κρυπτογράφησης** είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγόριθμου , τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key) , για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Γενικά στην σύγχρονη κρυπτογραφία , ακολουθείται ο κανόνας του kerckhoffs. Ο kerckhoffs το 1883 έθεσε ένα πολύ βασικό και απλό κανόνα για τους αλγόριθμους κρυπτογράφησης , η ασφάλεια τους θα πρέπει να βασίζεται μόνο στο κλειδί τους. θεωρητικά κάποιος οποίος θέλει να επιτεθεί στον αλγόριθμο, μπορεί να τον γνωρίζει. Έτσι αν η δομή ου αλγόριθμου δεν είναι ασφαλής και ελεγμένη, η απόκρυψη της δεν την κάνει περισσότερο ασφαλή, μάλιστα η μυστικότητα , μπορεί να δώσει την ψευδή αίσθηση της ασφάλειας. Στη σύγχρονη κρυπτογραφία, όλο και περισσότερο οι αλγόριθμοι παρουσιάζονται δημόσια , προκειμένου η επιστημονική κοινότητα να εκτιμήσει την προσφερόμενη ασφάλεια, αφήνοντας την ασφάλεια να βασίζεται μόνο στην απόκρυψη των κλειδιών αποκρυπτογράφησης. Ένας αλγόριθμος θεωρείται ασφαλής αν κανείς άλλος, εκτός των εξουσιοδοτημένων , δεν μπορεί να υπολογίσει οποιαδήποτε συνάρτηση του αρχικού κειμένου, δεδομένων οποιοδήποτε άλλων ζευγών αρχικού και κρυπτογραφημένου κείμενο η μόνο κρυπτογραφημένου κειμένου, σε γόνιμο για οποιοδήποτε εξουσιοδοτημένο χρήστη χρονικό διάστημα.

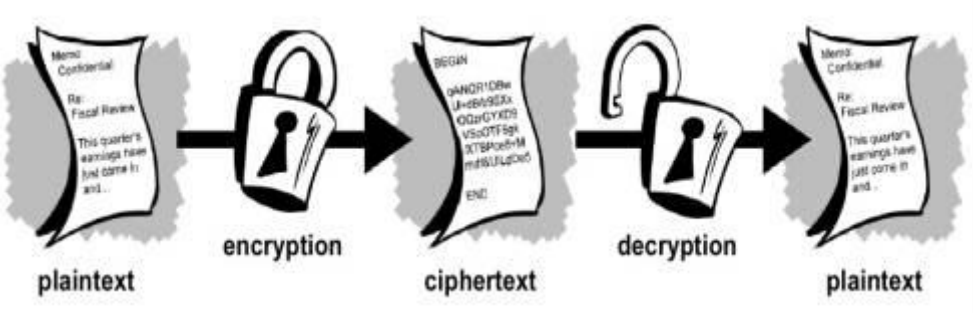
Όλα τα συστήματα κρυπτογράφησης όσο περίπλοκα και αν είναι βασίζονται σε τέσσερα βασικά μέρη:

Απλό κείμενο (plaintext). Ονομάζεται το αρχικό μήνυμα που θέλουμε να κρυπτογραφήσουμε, το οποίο μπορεί να μην είναι μόνο κείμενο αλλά οποιοδήποτε τύπος αρχείου (όπως κείμενο, video). Πολύ συχνά το ονομάζουμε και απλό η καθαρό.

Κρυπτογραφημένο κείμενο (ciphertext). Ονομάζεται η μυστική-κρυπτογραφημενη μορφή του κειμένου, τροποποιημένο με τέτοιο τρόπο έτσι ώστε να μην μπορεί να διαβαστεί από τρίτους.

Αλγόριθμος κρυπτογράφησης (encryption algorithm) . Ονομάζεται η μέθοδος που ακολουθείται για τη μετατροπή του αρχικού κειμένου σε μυστική μορφή.

Κλειδί (key). Ένα μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα. Κάθε κλειδί μετασχηματίζει το ίδιο απλό κείμενο σε διαφορετικό κρυπτογραφημένο κείμενο και μόνο οι κάτοχοι των κλειδιών μπορούν να διαβάσουν το κρυπτογραφημένο κείμενο.



Εικόνα 7: Διαδικασία Κρυπτογράφησης και Αποκρυπτογράφησης

5.2.2 Συμβολή κρυπτογραφίας

Η κρυπτογραφία αποτελεί τον κυριότερο μηχανισμό που προστατεύει τόσο τα στοιχεία όσο και την ομαλή και ασφαλή διεξαγωγή μίας συναλλαγής. Χρησιμοποιείται για να διασφαλίσει την ιδιωτικότητα (privacy), την ακεραιότητα (integrity) και την εμπιστευτικότητα (confidentiality) των επιχειρηματικών συναλλαγών και μηνυμάτων και αποτελεί τη βάση για αρκετά από τα on-line συστήματα πληρωμών, όπως πχ το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές.

Στη βιβλιογραφία απαντώνται δύο είδη κρυπτογραφίας: α) Συμμετρική Κρυπτογράφηση (Symmetric key encryption) ή Κρυπτογράφηση Ιδιωτικού Κλειδιού (Secret key encryption) και β) Ασύμμετρη Κρυπτογράφηση (Asymmetric key encryption) ή Κρυπτογράφηση Δημοσίου Κλειδιού (Public key encryption).

5.2.3 Υποδομή Δημόσιου Κλειδιού

Η αιχμή της τεχνολογίας για πιστοποίηση της αυθεντικότητας αποτελεί η υποδομή δημοσίου κλειδιού (PKI). Αναφέρεται στα τεχνικά συστατικά, στην υποδομή και τις πρακτικές που χρειάζονται για να μπορεί να γίνει χρήση κρυπτογράφησης δημοσίου κλειδιού, ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών με μια εφαρμογή δικτύου. Η PKI βασίζεται στην κρυπτογράφηση. (βλ. εικόνα)

Εικόνα 8: Υποδομή Δημόσιου Κλειδιού

Κρυπτογράφηση Ιδιωτικού Κλειδιού (Secret key encryption)

Με αυτό το είδος κρυπτογράφησης και τα δύο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί και να εξασφαλισθεί η ασφαλής μετάδοσή του. Κάθε χρήστης θα πρέπει να έχει τόσα μυστικά κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται. Επομένως, δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μερών. Από τη 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 για την αποστολή ενός μηνύματος, καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με την κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση.

Κρυπτογράφηση Δημοσίου Κλειδιού (Public 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. 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 ελέγχου της ταυτότητας των χρηστών (authentication).
- Υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος)

Ο αλγόριθμος DES

Ο αλγόριθμος DES (Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων), από το 1973 που δημιουργήθηκε μέχρι το 1997 που αντικαταστάθηκε από τον AES, αποτελούσε πρότυπο αλγορίθμου ισχυρής κρυπτογράφησης. Από αυτόν προέκυψαν πολλοί άλλοι αλγόριθμοι κρυπτογράφησης ενώ η μελέτη που οδήγησε στη δημιουργία πολλών τεχνικών κρυπτανάλυσης, όπως η διαφορική και η γραμμική κρυπτανάλυση.

Ο DES, Data Encryption Standard, αποτελεί το πιο γνωστό πρότυπο κρυπτογράφησης δεδομένων. Από το 1973 που δημιουργήθηκε μέχρι πρόσφατα το 1997 , που αντικαταστάθηκε από τον AES, ο DES αποτελούσε διεθνώς πρότυπο αλγόριθμο ισχυρής κρυπτογράφησης. Η μελέτη του αποτελούσε πηγή δημιουργίας πολλών άλλων αλγορίθμων κρυπτογράφησης και γέννησε πολλές τεχνικές κρυπταναλυσης, όπως τη διαφορικη και την γραμμική κρυπταναλυση. Το 1972 , το NBS (National Bureau of Standard), σήμερα γνωστό ως NIST (National Institute of Standards and Technology) ξεκίνησε ένα πρόγραμμα για την προστασία των δεδομένων επικοινωνίας του υπολογιστή. Σκοπός αυτού του προγράμματος ήταν να δημιουργηθεί ένας απλός αλγόριθμος κρυπτογράφησης, ο οποίος να υλοποιείται με χαμηλό κόστος και να μπορεί να τρέξει σε πολλές διαφορετικές αρχιτεκτονικές. Το 1973 το NBS, προκήρυξε έναν δημόσιο διαγωνισμό για τη δημιουργία ενός κρυπτογραφικού αλγορίθμου.

Η γνωστή εταιρεία IBM, η οποία διέθετε μια ομάδα η οποία ασχολείτο με την κρυπτογραφία, πρότεινε έναν αλγόριθμο που είχε κατασκευάσει, τον Lucifer. Ο Lucifer χρησιμοποιούσε απλές λογικές πράξεις σε μικρές ομάδες από bits και μπορούσε να υλοποιηθεί αποδοτικά σε υπολογιστικά συστήματα. Ο αλγόριθμος αυτός είναι και αυτός ο οποίος τελικά έγινε αποδεκτός σε αυτόν τον διαγωνισμό. Η αναγνώριση και υιοθέτηση του γίνεται γύρω στο 1975. Από τότε χρησιμοποιείται διαρκώς με διάφορες μορφές σχεδόν σε όλους τους τομείς που έχει χρησιμοποιηθεί η κρυπτογραφία.

επιθέσεις (brute-force attacks). Έχουν κατασκευαστεί ειδικά μηχανήματα για τον DES τα οποία μπορούν σε διάστημα μερικών ωρών να βρουν το κλειδί που έχει χρησιμοποιηθεί για την κρυπτογράφηση, γεγονός που οφείλεται στο μήκος των 52 bits για το κλειδί του, που επιτρέπει τη δημιουργία 2^{56} δυνατών κλειδιών. Τα μηχανήματα αυτά βεβαία έχουν κόστος κατασκευής πολύ υψηλό. Αν και έχουν γίνει απόπειρες στο

παρελθόν αλγεβρικής μοντελοποίησης του DES, παρόλα με πιο επιτυχές ως προς την κρυπταναλυση του.

Ο DES είναι ένας συμμετρικός αλγόριθμος τμημάτων ο οποίος κρυπτογραφεί τμήματα των 64 bits. Τόσο η είσοδος του αλγορίθμου όσο και η έξοδος του αλγορίθμου είναι και η δυο τμήματα των 64 bits. Το μήκος του κλειδιού που χρησιμοποιεί ο αλγόριθμος είναι 54 bits. Ο αλγόριθμος αποτελεί ένα δίκτυο SPN με δομή feistel. Αποτελείται από 16 όμοιες επαναλήψεις, στις οποίες χρησιμοποιεί μόνο αριθμητικούς και λογικούς τελεστές σε δυαδικούς αριθμούς το πολύ της τάξης των 64 bits. Έτσι λοιπόν ο αλγόριθμος είναι εύκολα εφαρμόσιμος και υλοποιήσιμος σε επίπεδο λογισμικού και υλικού. Ο DES λειτούργει πάνω σε ένα τμήμα μηνύματος των 64 bits. Η Διαδικασία είναι η ακόλουθη, στο αρχικό μήνυμα γίνεται μια μετάθεση των δυαδικών ψηφίων, η IP, και στη συνεχεία το τμήμα που χωρίζεται σε αριστερό και δεξιό μισό, μήκους 32 bits το καθένα. Ακολούθου μετά 16 επαναλήψεις της ίδιας ακριβώς λειτουργιάς. Σε κάθε επανάληψη η αλλιώς γύρο, μια συνάρτηση f, η οποία συνδυάζει σε κάθε επανάληψη το απλό κείμενο με το κλειδί, εναλλάσσει διαρκώς το δεξιό με το αριστερό μισό. Τέλος μετά την 16 επανάληψη, το δεξιό και το αριστερό μισό ενώνονται και γίνεται μια τελική μετάθεση των bits(η αντίστροφη της αρχικής μετάθεσης).

Η συνάρτηση f , η οποία αναφέρθηκε προηγουμένως, παίρνει το δεξιό μισό των δεδομένων κάθε γύρου και αρχικά από 32 bits και το επεκτείνεται στα 48 bits μέσω μιας συνάρτησης Ε η οποία εφαρμόζει μετάθεση των bits και επανάληψη τους. Στη συνεχεία, εφαρμόζει αποκλειστική διάζευξη με το υποκλειδιά του α γυρου. Το αποτέλεσμα χωρίζεται σε εξάδες και ανάλογα με τον αύξοντα αριθμό της κάθε εξάδας στέλνεται αντίστοιχα στα 8s-boxes, παράγοντας 32 νέα bits τα οποία συνενώνονται και μετατίθενται ξανά ξανά μέσω τις μετάθεσης P.

Ο γύρος ολοκληρώνεται παίρνοντας το αποτέλεσμα τις συνάρτησης f και εφαρμόζοντας αποκλειστική διάζευξη με το αριστερό μισό του τρέχοντος γύρου. Το αποτέλεσμα αυτό αποτελεί το νέο δεξιό μισό, ενώ το παλιό δεξιό μισό αποτελεί το νέο αριστερό μισό. Αυτές οι λειτουργιές επαναλαμβάνονται 16 φορές αποτελώντας τις 16 επαναλήψεις του DES.

Η αρχική μετάθεση IP των δυαδικών ψηφίων λαμβάνει χώρα πριν την πρώτη επανάληψη. Μετατοπίζει το εισερχόμενο τμήμα προς κρυπτογράφηση. Τέλος, αξίζει να σημειωθεί πως τόσο η αρχική όσο και η αντίστοιχη τελική μετάθεση δεν επιδρούν στην ασφάλεια του DES καθώς ως πράξεις είναι γραμμικές και αποσκοπούν περισσότερο στη διάχυση των δεδομένων.

Ο αλγόριθμος AES

Ο αλγόριθμος AES (Advanced Encryption Standard) δημιουργήθηκε όταν το 1997 το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ θέλησε να αντικταστήσει τον DES , ο οποίος δεν κάλυπτε πλέον τις ανάγκες τόσο σε ασφάλεια όσο και σε επιδόσεις. Ο αλγόριθμος αποτελεί σήμερα τον πλέον γωνστό και διαδεδομένο συμμετρικό αλγόριθμο κρυπτογράφησης. Σε σχέση με τον προκάτοχό του είναι ταχύτερος, ευκολότερος στην εφαρμογή και έχει μικρότερες απαιτήσεις μνήμης.

Λόγω των πολλών επιθέσεων που είχε δεχθεί ο DES και σε συνδυασμό με το γεγονός πως κάλυπτε τεχνολογικές απαιτήσεις του 1973, το 1997 το Εθνικό Ινστιτούτο Πρότύπων και Τεχνολογίας των ΗΠΑ αποφάσισε την αντικατάσταση του DES και ανακοίνωσε την ανάγκη ανάπτυξης ενός νέου κρυπτοσυστήματος, του AES. Στις προδιαγραφές κατασκευής του εντασσόταν η αναγκαιότητα χρησιμοποίησης τμημάτων

εισόδου τουλάχιστον 128 bits και η υποστήριξη τουλάχιστον τριών μεγεθών κλειδιών μήκους, 128, 192, και 256 bits. Η αλγεβρική δομή του Sbox, διαφοροποιεί τον AES από τον DES, καθώς δίνει ξεκάθαρα και προφανή θεμέλια στην ασφάλεια του νέου αλγορίθμου.

Ο AES ανάλογα με το μέγεθος των τμημάτων και το μέγεθος του κλειδιού αποτελείται από 10, 12 ή 14 επαναλήψεις. Τα διάφορα μέρη που τον απαρτίζουν δρούν σε ενδιάμεσα αποτελέσματα, τα οποία ονομάζονται καταστάσεις (states). Μια κατάσταση είναι ένας ορθογώνιος πίνακας από bytes, με τέσσερις γραμμές και Nb (το μήκος του τμήματος) στήλες. Αντίστοιχα το κλειδί είναι ένας ορθογώνιος πίνακας από bytes, με τέσσερις γραμμές και Nκ (μήκος κλειδιού) στήλες. Το κλειδί, τέλος, επεκτείνεται και τοποθετείται σε ένα πίνακα με W[Nb (Nr+1)] λέξεις, όπου Nr το πλήθος επαναλήψεων. Σε κάθε επανάληψη γίνονται τέσσερις μετασχηματισμοί.

5.3 Firewalls

Η λύση για την αντιμετώπιση των ζητημάτων ασφάλειας που προκύπτουν είναι η χρήση αναχωμάτων ασφάλειας (firewalls). Σε ένα δίκτυο υπολογιστών, όταν η κίνηση που εισέρχεται και εξέρχεται από ένα δίκτυο ελέγχεται, καταγράφεται, απορρίπτεται και/ή προωθείται, αυτός ο έλεγχος γίνεται στο firewall.

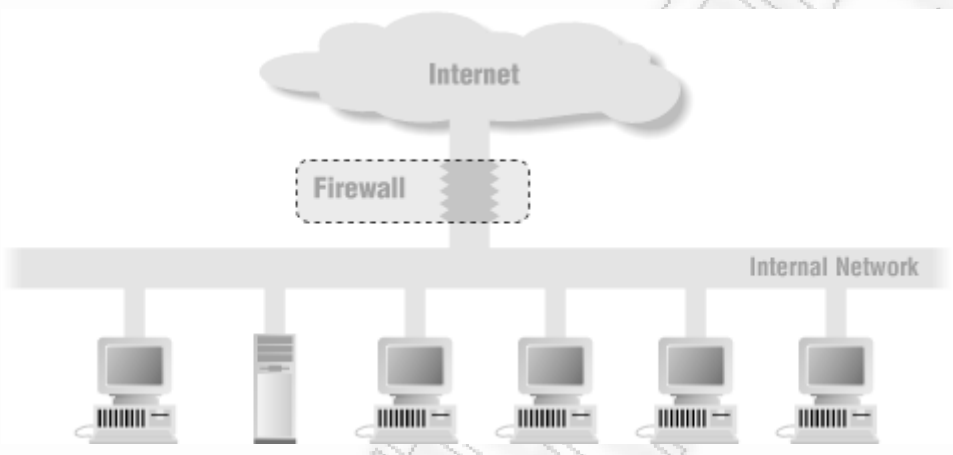
Ως firewall ορίζεται ένα στοιχείο ή σύνολο στοιχείων που περιορίζει την πρόσβαση ανάμεσα σε ένα προστατευόμενο δίκτυο και το Internet, ή μεταξύ άλλων δικτύων.

Η τεχνολογία των firewalls πρωτοεμφανίστηκε στα τέλη της δεκαετίας του 1980, όταν το Internet ήταν μία αρκετά νέα τεχνολογία. Η ανάπτυξή τους προήλθε από μία σειρά μεγάλων διαδικτυακών παραβιάσεων στα τέλη της δεκαετίας του 1980. Το 1988 ο ιός Morris Worm διαδόθηκε μέσω e-mail και αποτέλεσε την πρώτη μεγάλη επίθεση στην ασφάλεια του Internet, την οποία η διαδικτυακή κοινότητα δεν περίμενε, και για την οποία δεν ήταν έτοιμη. Η κοινότητα του διαδικτύου έθεσε άμεση προτεραιότητα να αντιμετωπίσει την παρουσία κάθε μελλοντικής επίθεσης, οπότε και άρχισε να δουλεύει πάνω σε νέες ιδέες, συστήματα και λογισμικό έτσι ώστε να αποκαταστήσει την ασφάλεια του Internet.

Ο όρος firewall προέρχεται από το γεγονός ότι με την κατάτμηση ενός δικτύου στα διαφορετικά φυσικά υποδίκτυα, περιορίζεται η ζημιά που θα μπορούσε να διαδοθεί από ένα υποδίκτυο στο άλλο, λειτουργώντας ακριβώς όπως οι αντιπυρικές πόρτες ή αντιπυρικές ζώνες (firewalls). Αντί να προστατεύουν από την εξάπλωση μίας φωτιάς, τα firewalls προστατεύουν πόρους εναντίον επιδρομών που προκαλούν απώλειες σημαντικών πληροφοριών.

Ένα firewall είναι ένας συνδυασμός υλικού και λογισμικού που απομονώνει το εσωτερικό δίκτυο ενός υπολογιστή από το υπόλοιπο Διαδίκτυο, επιτρέποντας σε ορισμένα πακέτα να περνούν και μπλοκάροντας άλλα πακέτα. Ένα firewall επιτρέπει σε ένα διαχειριστή δικτύου να ελέγχει την προσπέλαση ανάμεσα στον έξω κόσμο και στους πόρους μέσα στο διαχειριζόμενο δίκτυο, διαχειριζόμενο την κίνηση ροής προς και από αυτούς τους πόρους. Το ανάχωμα τοποθετείται μεταξύ του εσωτερικού δικτύου και του Διαδικτύου (Εικόνα 1), αποτελεί έναν ελεγχόμενο κρίκο επικοινωνίας και ορθώνει μία εξωτερική περίμετρο ασφάλειας ή τοίχο γύρω από το εσωτερικό δίκτυο. Ο σκοπός της περιμέτρου αυτής είναι να προστατεύσει το εσωτερικό δίκτυο από επιθέσεις που εξαπολύονται μέσω του Internet και να παρέχει ένα μοναδικό σημείο ελέγχου όπου μπορούν να εφαρμοστούν ισχυροί μηχανισμοί ασφάλειας και ελέγχου.

Ο κύριος στόχος της ύπαρξης ενός firewall είναι η προστασία ενός δικτύου από ένα άλλο δίκτυο. Το δίκτυο που προστατεύεται είναι υπό την ευθύνη ενός ή περισσοτέρων ατόμων, ενώ το δίκτυο από το οποίο προστατεύεται είναι ένα εξωτερικό δίκτυο το οποίο δε θεωρείται έμπιστο. Οι δικτυωμένοι υπολογιστές προστατεύονται από εισβολές οι οποίες θα μπορούσαν να έχουν ως αποτέλεσμα συμβιβασμούς στην εμπιστευτικότητα ή καταστροφή δεδομένων ή άρνηση της υπηρεσίας. Το firewall μπορεί να είναι μία συσκευή υλικού ή ένα πρόγραμμα λογισμικού που τρέχει σε έναν ασφαλή υπολογιστή. Ενδέχεται να είναι ένα μοναδικό υπολογιστικό σύστημα ή να αποτελείται από δύο ή περισσότερα συστήματα που συνεργάζονται προκειμένου να επιτελέσουν την επιθυμητή λειτουργία. Επίσης, επιβάλλει μία πολιτική ασφάλειας. Με τον όρο firewall εννοείται το σύνολο του υλικού (hardware), του λογισμικού (software), της πολιτικής και των διαδικασιών που χρησιμοποιούνται για να εφαρμόσουν την πολιτική στο firewall.



Εικόνα 9: Λειτουργία Firewalls

Στο Firewall είναι όπου αποφασίζεται αν θα επιτραπεί ή όχι η διέλευση των δεδομένων σύμφωνα με την πολιτική ασφάλειας που εφαρμόζει ο οργανισμός του συστήματος. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα δεδομένων επιτρέπεται να περάσουν εντός του ιδιόκτητου δικτύου και ποια όχι. Έτσι, ένα firewall δεν μπορεί να λειτουργήσει σωστά εάν δεν έχει καθορισθεί μία σαφής πολιτική ασφάλειας, ανεξάρτητα του σχεδιασμού ή της υλοποίησής του. Αυτή η πολιτική πρέπει να είναι συγκεκριμένη και σαφής.

Πρέπει να ληφθεί υπόψη ότι η χρήση ενός firewall δε λύνει όλα τα θέματα ασφάλειας ενός δικτύου. Κάποιος εισβολέας ενδέχεται να παραβιάσει το σύστημα. Όπως με κάθε προστασία, υπάρχουν ανταλλαγές μεταξύ της ευκολίας και της ασφάλειας. Ένα firewall είναι διάφανο στους χρήστες εάν δεν παρατηρούν ή δεν σταματούν στο firewall προκειμένου να εισέλθουν σε ένα δίκτυο. Τα firewalls διαμορφώνονται συνήθως κατά τέτοιο τρόπο ώστε να είναι διαφανή στους χρήστες των εσωτερικών δικτύων και αδιαφανή για το εξωτερικό δίκτυο που έρχεται μέσω του firewall. Έτσι, παρέχεται υψηλό επίπεδο ασφάλειας χωρίς την τοποθέτηση περιττού φορτίου στους εσωτερικούς χρήστες.

Τα firewalls μπορούν να διαρθρωθούν ποικιλοτρόπως, σχηματίζοντας διάφορες αρχιτεκτονικές και παρέχοντας διαφορετικά επίπεδα ασφάλειας, με διαφορετικό κόστος εγκατάστασης και λειτουργίας. Η αρχιτεκτονική ενός firewall πρέπει να επιλεχτεί ανάλογα με τους εκάστοτε κινδύνους που χρήζουν αντιμετώπισης.

Η επιλογή του κατάλληλου firewall που θα πλαισιώσει τους μηχανισμούς ασφάλειας του δικτύου, αποτελεί ίσως τη σημαντικότερη απόφαση που πρέπει να λάβει ένας οργανισμός ο οποίος επιδιώκει να εγκαταστήσει ένα ασφαλές δίκτυο στο Internet.

Υπάρχουν τρεις κατηγορίες firewalls:

- Firewalls επιπέδου δικτύου
- Firewalls επιπέδου εφαρμογής
- Υβριδικά firewalls

5.4 Συστήματα Ανίχνευσης Εισβολής

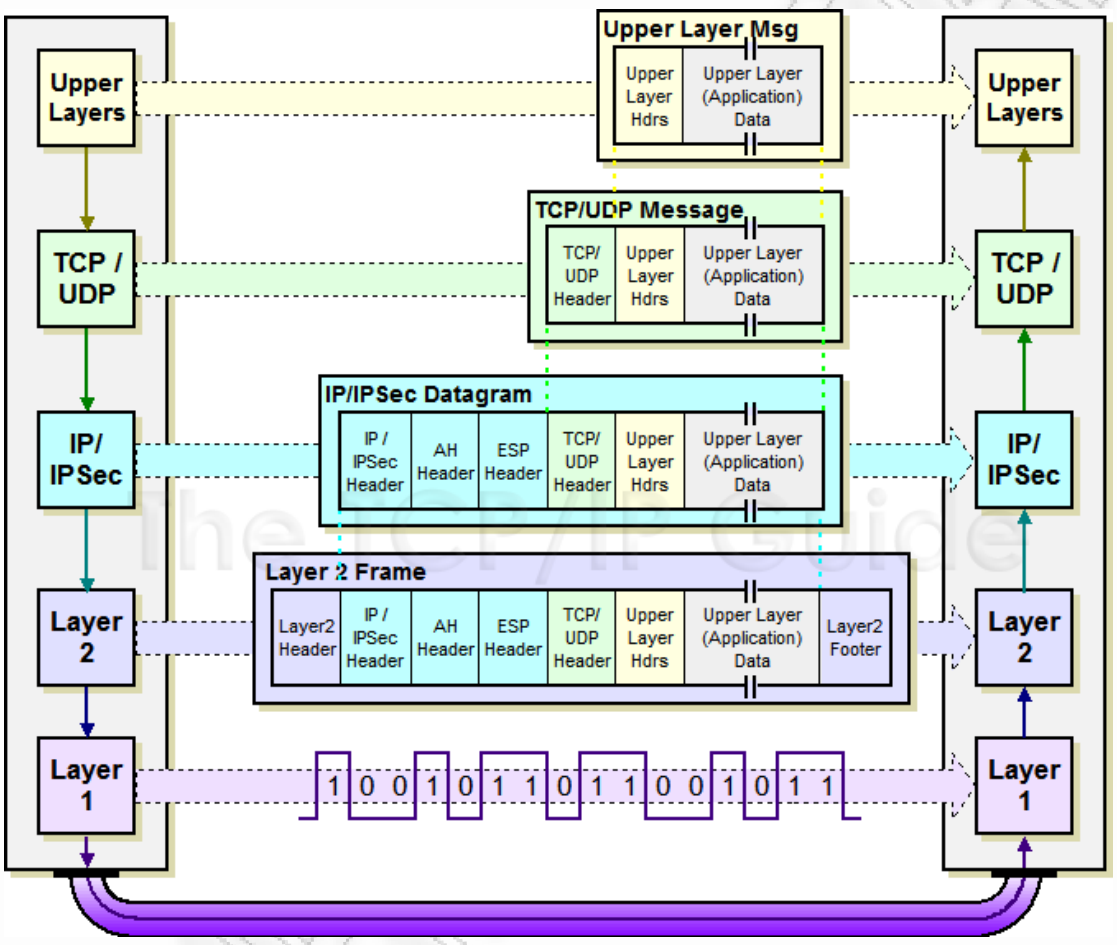
Σήμερα υπάρχουν τα συστήματα ανίχνευσης εισβολής (IDS), τα οποία είναι εγκατεστημένα ή στον ξενιστή ή στο δίκτυο. Ένα IDS εγκατεστημένο στον ξενιστή μπορεί να ανιχνεύσει αν ένα κρίσιμο αρχείο ή ένα αρχείο που σχετίζεται με την ασφάλεια έχει παραβιαστεί ή αν ένας χρήστης έχει προσπαθήσει να προσπελάσει αρχεία, τα οποία δεν είναι εξουσιοδοτημένος να χρησιμοποιεί. Αυτό πραγματοποιείται υπολογίζοντας το IDS μια ειδική υπογραφή ή μέσω αθροίσματος ελέγχου ενός αρχείου. Επιπλέον, ελέγχει αρχεία σε τακτά χρονικά διαστήματα για να δει αν οι τρέχουσες υπογραφές ταιριάζουν με προηγούμενες υπογραφές. Αν δεν ταιριάζουν, τότε ειδοποιείται άμεσα το προσωπικό ασφαλείας. Παραδείγματα εμπορικών συστημάτων IDS εγκατεστημένων στον ξενιστή αποτελούν τα Intruder Alert της Symantec, Tripwire της Tripwire Security, Entercept Desktop και Server Agant της McAfee.

Ένα IDS εγκατεστημένο στο δίκτυο χρησιμοποιεί για να αναλύσει ύποπτη δραστηριότητα στην περίμετρο του δικτύου ή σε θέσεις κλειδιά μέσα στο δίκτυο. Συνήθως, αποτελείται από ένα σύστημα παρακολούθησης-ένα πακέτο λογισμικού που σαρώνει το δίκτυο-και πράκτορες λογισμικού, που βρίσκονται σε διάφορους υπολογιστές ξενιστές και τροφοδοτούν με πληροφορίες το σύστημα παρακολούθησης. Αυτός ο τύπος IDS εξετάζει την κίνηση του δικτύου για γνωστά πρότυπα επιθέσεων και ειδοποιεί αυτόματα το προσωπικό ασφαλείας, όταν εμφανίζονται συγκεκριμένα συμβάντα ή ξεπερνιούνται τιμές κατωφλίου συμβάντων. Επίσης, μπορεί να κάνει ορισμένες ενέργειες όταν εντοπιστεί κάποια επίθες, όπως το να τερματίσει τις συνδέσεις του δικτύου ή να αναδιαμορφώσει τις συσκευές του δικτύου (firewalls, δρομολογητές), με βάση τις πολιτικές ασφαλείας. Παραδείγματα αποτελούν τα εξής: NetRanger της Cisco και eTrust Intrusion Detection της Computer Associates.

5.5 IPSec

Το IPsec είναι ένα σύνολο πρωτοκόλλων που παρέχουν ασφαλείς συνδέσεις. Είναι η βάση για την ασφάλεια των ηλεκτρονικών συναλλαγών. Τα χαρακτηριστικά του ορίζονται από αρκετά επιστημονικά άρθρα που προσδιορίζουν τις λεπτομέρειες για τα διαφορετικά τμήματα του πρωτοκόλλου, ενώ όλα ορίζουν πως αυτά αλληλεπιδρούν μεταξύ τους. Σκοπός του IPsec είναι να παρέχει ασφάλεια σε επίπεδο πακέτων IP. Αυτό το επιτυγχάνει παρέχοντας υπηρεσίες ακεραιότητας δεδομένων με πιστοποίηση

αυθεντικότητας χωρίς σύνδεση (connectionless data integrity authentication), προαιρετική προστασία anti-replay, ταυτοποίηση προέλευσης δεδομένων (data origin authentication) και εμπιστευτικότητα ροής δεδομένων (data flow confidentiality). Το IPsec λειτουργεί σε επίπεδο Δικτύου και αυτό του επιτρέπει να παρέχει τις παραπάνω υπηρεσίες ανεξάρτητα από τα πρωτόκολλα που χρησιμοποιούνται σε παραπάνω επίπεδα.



Εικόνα 10: IPSec

Το IPsec αποτελείται από τρείς διαφορετικούς μηχανισμούς ασφαλείας: α) την επικεφαλίδα ελέγχου ταυτότητας, β) το ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας και γ) το κλειδί διαχείρισης. Αυτές οι επιπλέον κεφαλίδες, υποστηρίζουν και υλοποιούν τρία πρωτόκολλα, το AH (Authentication Header) και το ESP (Encapsulating Security Payload) και το Internet Key Management Protocol.

- Το AH παρέχει data integrity, data origin authentication και προστασία anti-replay. Με λίγα λόγια, πραγματοποιεί έλεγχο ταυτότητας των ατόμων που στέλνουν πληροφορίες και βεβαιώνει πως οι πληροφορίες δεν έχουν αλλοιωθεί.

Μπαίνει μετά την IP επικεφαλίδα και πριν από τις πηροφορίες που θα πιστοποιηθούν.

- Το ESP παρέχει τα ίδια χαρακτηριστικά με το AH και επιπλέον data confidentiality, δηλαδή υποστιρίζει την κρυπτογράφιση δεδομένων. Τα AH και ESP δεν ορίζουν ποιοι ακριβώς αλγόριθμοι θα παρέχουν αυτές τις υπηρεσίες, αλλά τον τρόπο που θα το κάνουν. Οι κρυπτογραφικοί αλγόριθμοι που συνήθως χρησιμοποιούνται για το AH είναι οι MD5 και SHA1 και για το ESP οι DES, 3DES και AES. Αυτοί οι αλγόριθμοι λειτουργούν με τρόπο που απαιτεί την ύπαρξη μυστικών κλειδιών τα οποία μπορούν είτε να δημιουργούνται δυναμικά κατά τη διαπραγμάτευση (negotiation) μιας σύνδεσης ή να είναι προμοιρασμένα (preshared). Η τελευταία λύση δεν είναι κατάλληλη για ευρεία εφαρμογή και γι αυτό συνήθως χρησιμοποιείται η δυναμική ανάθεση χρησιμοποιώντας λύσεις που ορίζει το πρωτόκολλο IKE (Internet Key Exchange).

- Το Πρωτόκολλο Διαχείρισης Κλειδιού Internet (Internet Key Management Protocol) αποτελεί τον πυρήνα του IPSec. Επιτρέπει να ανταλλάσσουν δύο μέρη τα δημόσια κλειδιά τους και να διαμορφώνουν μια ασφαλή σύνοδο. Υπάρχουν δύο διαφορετικοί τρόποι που μπορούν να ανταλλαγούν τα κλειδιά μεταξύ δύο διαφορετικών μερών: η μη αυτόματη ανταλλαγή και η μέθοδος ISAKMP.

5.6 Secure Sockets Layer (SSL)

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Από την εμφάνισή του το 1994 από την εταιρία Netscape, το **πρωτόκολλο SSL** (**S**ecure **S**ocket **L**ayer) έχει εδραιωθεί στο χώρο του ηλεκτρονικού εμπορίου (e-commerce) προσφέροντας ασφαλείς συναλλαγές και προστασία προσωπικών δεδομένων στο Διαδίκτυο. Το 1996, το SSL μετονομάστηκε σε Transport Layer Security (TLS), αλλά πολλοί συνεχίζουν να χρησιμοποιούν τον όρο SSL. Είναι το κύριο πρότυπο που χρησιμοποιείται για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών. Στις περιπτώσεις που χρησιμοποιείται το SSL, δημιουργείται μία ασφαλής σύνδεση μεταξύ του πελάτη (client) και του διακομιστή (server) με αποτέλεσμα την αξιόπιστη μετάδοση και μεταφορά των δεδομένων. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server.

Η μετάδοση πληροφοριών μέσω του δικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το (προβολή ιστοσελίδων), το FTP (μεταφορά

αρχείων) και το IMAP (email). Επομένως, αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο δίκτυο προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.

4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

5.6.1 A simple single-threaded proxy server

```
import java.io.IOException;
import java.io.InputStream;
```

```
import java.io.OutputStream;
import java.io.PrintWriter;
import java.net.ServerSocket;
import java.net.Socket;

/**
 * This class implements a simple single-threaded proxy server.
 */
public class SimpleProxyServer {
  /** The main method parses arguments and passes them to runServer */
  public static void main(String[] args) throws IOException {
    try {
      // Check the number of arguments
      if (args.length != 3)
        throw new IllegalArgumentException("Wrong number of args.");

      // Get the command-line arguments: the host and port we are proxy
      // for and the local port that we listen for connections on.
      String host = args[0];
      int remoteport = Integer.parseInt(args[1]);
      int localport = Integer.parseInt(args[2]);
      // Print a start-up message
      System.out.println("Starting proxy for " + host + ":" + remoteport + " on port " + local
port);
      // And start running the server
      runServer(host, remoteport, localport); // never returns
    } catch (Exception e) {
      System.err.println(e);
      System.err.println("Usage: java SimpleProxyServer " + "<host> <remoteport> <loca
lport>");
    }
  }

  /**
   * This method runs a single-threaded proxy server for host:remoteport on the
   * specified local port. It never returns.
   */
  public static void runServer(String host, int remoteport, int localport) throws IOExc
eption {
    // Create a ServerSocket to listen for connections with
    ServerSocket ss = new ServerSocket(localport);

    // Create buffers for client-to-server and server-to-client transfer.
    // We make one final so it can be used in an anonymous class below.
    // Note the assumptions about the volume of traffic in each direction.
    final byte[] request = new byte[1024];
    byte[] reply = new byte[4096];

    // This is a server that never returns, so enter an infinite loop.
    while (true) {
      // Variables to hold the sockets to the client and to the server.
      Socket client = null, server = null;
```

```
    try {
      // Wait for a connection on the local port
      client = ss.accept();

      // Get client streams. Make them final so they can
      // be used in the anonymous thread below.
      final InputStream from_client = client.getInputStream();
      final OutputStream to_client = client.getOutputStream();

      // Make a connection to the real server.
      // If we cannot connect to the server, send an error to the
      // client, disconnect, and continue waiting for connections.
      try {
        server = new Socket(host, remoteport);
      } catch (IOException e) {
        PrintWriter out = new PrintWriter(to_client);
        out.print("Proxy server cannot connect to " + host + ":" + remoteport + ":\n" + e +
"\n");
        out.flush();
        client.close();
        continue;
      }

      // Get server streams.
      final InputStream from_server = server.getInputStream();
      final OutputStream to_server = server.getOutputStream();

      // Make a thread to read the client's requests and pass them
      // to the server. We have to use a separate thread because
      // requests and responses may be asynchronous.
      Thread t = new Thread() {
        public void run() {
          int bytes_read;
          try {
            while ((bytes_read = from_client.read(request)) != -1) {
              to_server.write(request, 0, bytes_read);
              to_server.flush();
            }
          } catch (IOException e) {
          }

          // the client closed the connection to us, so close our
          // connection to the server. This will also cause the
          // server-to-client loop in the main thread exit.
          try {
            to_server.close();
          } catch (IOException e) {
          }
        }
      };

      // Start the client-to-server request thread running
```

```
      t.start();

      // Meanwhile, in the main thread, read the server's responses
      // and pass them back to the client. This will be done in
      // parallel with the client-to-server request thread above.
      int bytes_read;
      try {
        while ((bytes_read = from_server.read(reply)) != -1) {
          to_client.write(reply, 0, bytes_read);
          to_client.flush();
        }
      } catch (IOException e) {
      }

      // The server closed its connection to us, so we close our
      // connection to our client.
      // This will make the other thread exit.
      to  client.close();
    } catch (IOException e) {
      System.err.println(e);
    } finally { // Close the sockets no matter what happens.
      try {
        if (server != null)
          server.close();
        if (client != null)
          client.close();
      } catch (IOException e) {
      }
    }
  }
 }
}
```

5.7 SET

Το **SET – Secure Electronic Transactions**, σχεδιάστηκε και αναπτύχθηκε αρχικά από τη Visa και τη MasterCard τον Φεβρουάριο του 1996 και έκτοτε αναπτύσσεται. Στο κονσόρτσιουμ του SET συμμετέχουν οι εταιρείες Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems και VeriSign. Το SET, το οποίο είναι σχεδιασμένο πάνω στο πρωτόκολλο SSL, αποτελεί ένα ειδικά σχεδιασμένο πρωτόκολλο για την διενέργεια κρυπτογραφημένων πληρωμών με χρήση πιστωτικών καρτών μέσω Internet και άλλων ανοικτών δικτύων. Το SET βασίζεται στη χρήση κρυπτογράφησης δημοσίου κλειδιού και χρησιμοποιεί τα λεγόμενα “ψηφιακά πιστοποιητικά” για την πιστοποίηση της ταυτότητας των συμμετεχόντων σε μία συναλλαγή. Τα πιστοποιητικά αυτά αποτελούν τεχνολογία της RSA Data Security.

Το πρωτόκολλο αυτό ικανοποιεί όλες τις απαιτήσεις ασφάλειας για την διεξαγωγή του ηλεκτρονικού εμπορίου όπως και το SSL, δηλαδή τον έλεγχο της αυθεντικότητας του πελάτη και του εμπόρου, με τη χρήση ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών που εκδίδουν οι Αρχές Πιστοποίησης, την εμπιστευτικότητα των

δεδομένων με την κρυπτογράφηση των μηνυμάτων, την ακεραιότητα των δεδομένων με τη χρήση των ψηφιακών υπογραφών, την μη- αποποίηση ευθύνης εκ μέρους των συμμετεχόντων στη συναλλαγή, καθώς και την εξασφάλιση της δια-λειτουργικότητας μεταξύ των λογισμικών που υποστηρίζουν αυτό το πρωτόκολλο.

Επιπρόσθετα το SET προσδιορίζει τη μορφή του μηνύματος, του ψηφιακού πιστοποιητικού καθώς και την διαδικασία της ανταλλαγής των μηνυμάτων Το SET αποτελεί θεωρητικά ένα τέλειο πρωτόκολλο.

5.8 Ψηφιακές Υπογραφές [EETT]

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα.

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα

προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

Αποστολέας

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

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

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

Παραλήπτης

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

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

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

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

5.9 Ψηφιακά πιστοποιητικά

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση).

Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

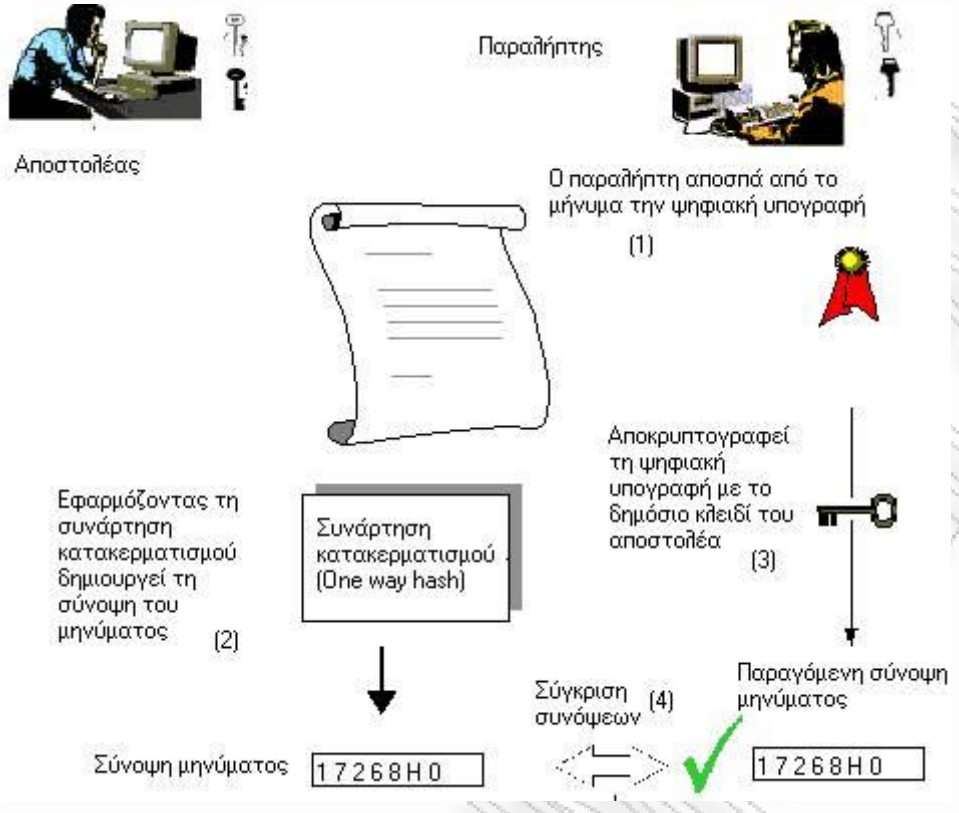
Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του κ.λπ), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.



Εικόνα 11: Ψηφιακό Πιστοποιητικό

5.10 3-D Secure

Σε κάποιες διαδικτυακές πληρωμές μέσω κάρτας, δίδεται η δυνατότητα (βάσει αρχιτεκτονικής) στον ηλεκτρονικό έμπορο (e-merchant) να ζητάει από το χρήστη την επιβεβαίωση του κατόχου της κάρτας. Χαρακτηριστικό παράδειγμα αυτής της εφαρμογής αποτελεί το 3-D Secure. Αποτελεί πρωτόκολλο επικοινωνίας που συνδέει τον ηλεκτρονικό έμπορο, το PSP αποδέκτη και το PSP εκδότη. Ύστερα από εντολή του server του εμπόρου ζητείται η αυθεντικοποίηση του κατόχου της κάρτας, αφού πρώτα έχει αποδεχτεί τους όρους συναλλαγής και έχει ορίσει το ποσό πληρωμής. Αυτό το σύστημα πιστοποίησης παρέχει επιπρόσθετη ασφάλεια καθώς μπορούν να χρησιμοποιηθούν τα αποτελέσματα της υπηρεσίας προκειμένου να αποφευχθεί μια ηλεκτρονική απάτη. Πράγματι αν ο έμπορος είναι το θύμα μιας ηλεκτρονικής απάτης και η συναλλαγή έχει πραγματοποιηθεί υπό καθεστώς 3-D Secure, τότε εκτείθεται ο χρήστης και όχι ο έμπορος.

Τα βήματα που χαρακτηρίζουν την 3-D Secure διαδικασία είναι τα ακόλουθα:

1. Ο έμπορος λαμβάνει μέσω της ιστοσελίδας το αίτημα του καταναλωτή για αγορά. Αφού ο χρήστης επιλέξει να πληρώσει με κάρτα, το σύστημα του ζητάει να εισάγει τα στοιχεία της κάρτας του.

2. Αφού υπάρχει το σύστημα ασφαλείας e-D Secure, ζητείται πιστοποίηση του καταναλωτή και ο τελευταίος οδηγείται στο κέντρο πιστοποίησης του εκδότη. Σημειώνεται ότι αυτή τη διαδικασία-βήμα ο καταναλωτής-χρήστης θα πρέπει ήδη να το γνωρίζει από την εκδότρια τράπεζα πριν την πραγματοποίηση της πρώτης του ηλεκτρονικής συναλλαγής με χρήση κάρτας

3. Θα αναδυθεί ένα καινούριο παράθυρο στο οποίο θα ζητείται η καταχώρηση του κωδικού από μέρους του χρήστη. Το επίπεδο ασφαλείας που προσφέρεται εξαρτάται από τη φύση του κωδικού (στατικό ή δυναμικό). Ένας στατικός κωδικός προσφέρει μικρότερη ασφάλεια.

4. Μόλις πιστοποιηθεί η ταυτότητα του καταναλωτή ειδοποιείται ο αποδέκτης. Έπειτα ο έμπορος επιστρέφει στον εκδότη ένα αίτημα εξουσιοδότησης, το οποίο περιλαμβάνει και την ψηφιακή απόδειξη της επιτυχούς πιστοποίησης του κατόχου της κάρτας. Ακόλουθα ο εκδότης δίνει την έγκρισή του για την εκτέλεση της συναλλαγής. Μόλις παραλάβει και την τελική έγκριση ο έμπορος από τον εκδότη μπορεί να προβεί στην ολοκλήρωση της συναλλαγής.

Εικόνα 12: 3-D Secure

5.11 Ενημέρωση και εκπαίδευση χρηστών

Οι ίδιοι οι χρήστες θα πρέπει να διασφαλίζουν την προστασία τους. Θα πρέπει να ενημερώνονται πλήρως γύρω από τον τρόπο λειτουργίας των ιστοσελίδων μέσω των οποίων πρόκειται να πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές. Αρχικά, θα πρέπει να είναι σίγουροι ότι βρίσκονται στο «αυθεντικό» ιστότοπο που επιθυμούν. Αν τους ζητείται η δημιουργία και εισαγωγή κωδικού, να δημιουργούν κωδικούς δυναμικούς και να μην πληροφορούν κανέναν σχετικά. Σε περιπτώσεις όπου απαιτείται η εισαγωγή ειδικών επιπρόσθετων αριθμών ασφαλείας (κλειδαρίθμων) για την ολοκλήρωση μιας συναλλαγής, όπως στην περίπτωση συναλλαγών μέσω Internet Banking, θα πρέπει να φυλάσσονται με προσοχή οι συσκευές παροχής κλειδαρίθμων

(tokens), και σε περίπτωση απώλειάς τους θα πρέπει να ειδοποιείται άμεσα η εκδούσα υπηρεσία αυτών. Τέλος, θα πρέπει να ενημερώνονται για τυχόν αλλαγές ασφαλείας που έχουν πραγματοποιηθεί στις επιθυμητές ιστοθέσεις.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

6 Η ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΑΣΥΝΟΡΙΑΚΟ ΕΠΙΠΕΔΟ

6.1 Άποψη ευρωπαϊκής ένωσης

Τον Απρίλιο του 2012, η Ευρωπαϊκή Κεντρική Τράπεζα, δημοσίευσε ένα άρθρο σχετικά με τις προτάσεις γύρω από το θέμα της ασφάλειας των ηλεκτρονικών πληρωμών. Η έρευνα πραγματοποιήθηκε από το Ευρωπαϊκό Φόρουμ της Ασφάλειας στις Λιανικές Πληρωμές [SecuRe Pay (the "Forum")], που ιδρύθηκε το 2011 ως μια εθελοντική, συνεργατική πρωτοβουλία μεταξύ των αρχών. Συμμετείχαν κεντρικές τράπεζες ευρωπαϊκών χωρών, όπως φαίνονται παρακάτω:

- BE Nationale Bank van België/Banque Nationale de Belgique
- BG Българска народна банка (Bulgarian National Bank)
- CZ Česká národní banka
- DK Danmarks National bank Finanstilsynet
- DE Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht
- EE Eesti Pank Finantsinspektsioon
- IE Central Bank of Ireland
- GR Bank of Greece
- ES Banco de España
- FR Banque de France Banque de France, Autorité de Contrôle Prudentiel
- IT Banca d'Italia
- CY Central Bank of Cyprus
- LV Latvijas Banka Finanšu un kapitāla tirgus komisija
- LT Lietuvos bankas
- LU Banque centrale du Luxembourg Commission de Surveillance du Secteur Financier
- HU Magyar Nemzeti Bank Pénzügyi Szervezetek Állami Felügyelete
- MT Central Bank of Malta
- NL De Nederlandsche Bank
- AT Oesterreichische Nationalbank
- Österreichische Finanzmarktaufsicht
- PL Narodowy Bank Polski Komisja Nadzoru Finansowego
- PT Banco de Portugal
- RO Banca Națăionalã a României
- SI Banka Slovenije
- SK Národná banka Slovenska

- FI Suomen Pankki – Finlands Bank Finanssivalvonta
- SE Sveriges Riksbank Finansinspektionen
- UK Bank of England Financial Services Authority-European Banking Authority European Central Bank

Επιπλέον συμμετείχαν ως παρατηρητές οι εξής:

- IS Central Bank of Iceland
- Fjármálaeftirlitið
- LI Liechtensteinische Landesbank 1861
- Finanzmarktaufsicht Liechtenstein
- NO Norges Bank
- Finanstilsynet – The Financial Supervisory Authority of Norway
- European Commission
- Europol

Σκοπός της έρευνας ήταν η καταπολέμηση της διαδικτυακής απάτης, η ενίσχυση της εμπιστοσύνης των καταναλωτών στις διαδικτυακές πληρωμές και η ενθάρρυνση υιοθέτησης από τους παρόχους υπηρεσιών πληρωμής-Payment Service Providers, PSPs-βέλτιστων εφαρμογών (best practices).

6.1.1 Προτάσεις

Για τον προσδιορισμό και τη διατύπωση προτάσεων βασίστηκαν σε τέσσερις (4) κατευθυντήριους άξονες:

1. Αξιολόγηση κινδύνων / Διαρκής αναβάθμιση συστημάτων – υπηρεσιών
2. Ύπαρξη μηχανισμών ισχυρούς επικύρωσης της ταυτότητας των καταναλωτών
3. Εφαρμογή αποτελεσματικών διαδικασιών για τον εντοπισμό ‘ύποπτων’ συναλλαγών
4. Εκπαίδευση και πλήρης πληροφόρηση καταναλωτών.

Με γνώμονα τα ανωτέρω διατυπώθηκε ένα σύνολο προτάσεων που ομαδοποιήθηκαν σε τρείς (3) κατηγορίες, που θα αναλυθούν παρακάτω:

1. *Γενικός έλεγχος και περιβάλλον ασφαλείας*
2. *Ειδικός έλεγχος και μέτρα ασφαλείας*
3. *Ενημέρωση καταναλωτών, εκπαίδευση, επικοινωνία*

Γενικός έλεγχος και περιβάλλον ασφαλείας

Πρόταση 1: *«Διακυβέρνηση»*

εφαρμογή επίσημης πολιτικής ασφαλείας και τακτική αναθεώρησή της

Πρόταση 2: «*Προσδιορισμός κινδύνου – αξιολόγηση»*

- προσδιορισμός και αξιολόγηση απειλών και κινδύνων των διαδικτυακών πληρωμών
- προσδιορισμός του πότε και σε ποιά έκταση θα πρέπει να πραγματοποιηθούν οι απαραίτητες αλλαγές
- προστασία και ασφάλεια σπουδαίων δεδομένων και των δύο συμβαλλομένων πλευρών

Πρόταση 3: «*Εποπτεία και αναφορά»*

διαδικασία αναφοράς περιστατικών δυσαρέσκειας καταναλωτών

Πρόταση 4: «*Έλεγχος κινδύνου και περιορισμός»*

- πραγματοποίηση ελέγχων σε επίπεδα (levels), για την καλύτερη ασφάλεια των πληρωμών (“defence in depth”)
- χρήση μέσων όπως firewalls, proxy servers, για την ασφάλεια των δικτύων, των ιστοσελίδων και της επικοινωνίας
- μέθοδοι επικύρωσης αξιοπιστίας ιστοσελίδων

Πρόταση 5: *«Ανιχνευσιμότητα (traceability)»*

- ενσωμάτωση μηχανισμών αναφοράς λεπτομερώς των στοιχείων συναλλαγής π.χ. χρονοσφραγίδα, αύξοντα αριθμό συναλλαγής
- επιβεβαίωση καταχωρημένων αρχείων από άκρως εξουσιοδοτημένα άτομα

Ειδικός έλεγχος και μέτρα ασφαλείας

Πρόταση 6: «*Αρχική αναγνώριση χρήστη-πληροφόρηση»*

- ενημέρωση καταναλωτών των απαραίτητων προϋποθέσεων για τη χρήση των συναλλαγών (λογισμικό, προγράμματα προστασίας του υπολογιστή / βήμα-βήμα περιγραφή της διαδικασίας κλπ)
- επιλογή του χρήστη της εφαρμογής εν τέλει ή όχι της συναλλαγής

- επιθυμητή η υπογραφή συμβολαίου με τον πάροχο των εκάστοτε συναλλαγών (δικαίωμα μη εκτέλεσης συναλλαγών υπό συγκεκριμένες συνθήκες κλπ)

Πρόταση 7: *«Ισχυρή πιστοποίηση»*

- προσωπικά στοιχεία
- συσκευές κλειδαρίθμων (token)
- λογισμικό

Πρόταση 8: «*Είσοδος-Αυτόματη έξοδος-Αποδοχή πιστοποίησης»*

- κωδικός μιας χρήσης (one-time password)
- μέγιστος αριθμός λανθασμένων προσπαθειών εισόδου στο σύστημα συναλλαγών, με το πέρας των οποίων «κλειδώνει» η πρόσβαση
- μέγιστο χρονικό διάστημα παραμονής στο σύστημα χωρίς την πραγματοποίηση «κινήσεων» εντός του συστήματος με αυτόματη έξοδο (log-out) από αυτό

Πρόταση 9: «*Εποπτεία συναλλαγών και πιστοποίηση»*

άμεσο, σε πραγματικό χρόνο (real time) έλεγχο ύποπτων ή υψηλού κινδύνου συναλλαγών (black lists, στοιχεία κλεμμένων καρτών κλπ)

Πρόταση 10: «*Προστασία σημαντικών δεδομένων»*

- αναγνώριση και προστασία αρχείων, δεδομένων και διεπαφών (interfaces)
- παροχή ασφαλούς καναλιού επικοινωνίας (end-to-end) με αναγνωρισμένες τεχνικές κρυπτογράφησης
- αποφυγή αποθήκευσης σημαντικών στοιχείων

Ενημέρωση καταναλωτών, εκπαίδευση, επικοινωνία

Πρόταση 11: *«Εκπαίδευση και επικοινωνία χρηστών»*

- ουσιαστική επικοινωνία που να διαβεβαιώνει την ακεραιότητα και την αυθεντικότητα των μηνυμάτων που λαμβάνουν οι καταναλωτές
- αναφορά των τρόπων επικοινωνίας και των δύο πλευρών π.χ. μέσω mail, μεσω τηλεφώνου κλπ
- προγράμματα ενημέρωσης για διασφάλιση των απαραίτητων στοιχείων (προστασία κωδικών, συσκευών, προσωπικών δεδομένων)
- τμήματα υποστήριξης πελατών για πάσης φύσεως πρόβλημα (παράπονο, τεχνικό πρόβλημα, γενική πληροφόρηση)
- κατανόηση των κινδύνων από μέρους των χρηστών

Πρόταση 12: «*Ενημερώσεις»*

- πάσης φύσεως ενημερώσεις εμφάνισης κινδύνου
- περιορισμένο χρηματικό ποσό πραγματοποίησης συναλλαγών σε συγκεκριμένη χρονική περίοδο

Πρόταση 13: « *Έλεγχος πιστοποίησης συναλλαγών»*

δυνατότητα ελέγχου των συναλλαγών ανά πάσα στιγμή μέσω ειδικής πλατφόρμας

6.2 Διασυνοριακές συναλλαγές και νομοθετικό πλαίσιο

Το μοναδικό ρυθμιστικό όργανο για το διαδικτυακό έγκλημα ιδρύθηκε το 2004 και μέχρι σήμερα μόνο 37 χώρες την έχουν υιοθετήσει. Η διαδικτυακή απάτη αποτελεί παγκόσμια απειλή και καθιστά απαιτητή για τη σταδιακή εξάλειψή της την διασυνοριακή και αρμονική αντιμετώπισή της.

7 ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Η ηλεκτρονική τραπεζική συνεπάγεται την άμεση πλέον επαφή της τράπεζας με το παγκόσμιο κοινό. Δεδομένης της μέχρι σήμερα απουσίας ύπαρξης ενός «διεθνούς δικαίου» που να καλύπτει πλήρως σε όλο τον κόσμο το θέμα του Internet Banking, για πρακτικούς λόγους οι συναλλαγές των ελληνικών τραπεζών θα πρέπει να διέπονται από τρείς κύριους κλάδους του ελληνικού δικαίου. Πιο αναλυτικά:

1) από τη νομοθεσία για τη διεξαγωγή τραπεζικών και χρηματοοικονομικών συναλλαγών και την τραπεζική εποπτεία.
2) τη νομοθεσία για την προστασία του καταναλωτή
3) και τη νομοθεσία για την προστασία των προσωπικών δεδομένων.

7.1 Γενικό Ρυθμιστικό Πλαίσιο

Η αρχική σκέψη ότι οι δραστηριότητες internet banking πρέπει να υπαχθούν, πέραν των γενικών ρυθμίσεων για τη διεξαγωγή τραπεζικών συναλλαγών, και στις ειδικές ρυθμίσεις για τις ηλεκτρονικές πληρωμές δεν οριοθετεί πλήρως το πρόβλημα. Η φύσει παγκόσμια διάσταση του Internet επιβάλλει οποιαδήποτε εμπορική- επιχειρηματική δραστηριότητα σε αυτό, να εξετάζεται υπό το πρίσμα της διεθνούς δραστηριότητας και επομένως στην περίπτωση του internet banking πρέπει να εξετάζεται το ρυθμιστικό πλαίσιο της διασυνοριακής παροχής τραπεζικών και χρηματοοικονομικών υπηρεσιών.

Σε αυτή την περίπτωση τα παραδοσιακά εργαλεία του θετικού δικαίου ίσως δεν είναι επαρκή και ίσως άλλες μέθοδοι, όπως η αυτορρύθμιση (self-regulation), η συρρύθμιση (co-regulation) ή και η βοήθεια από την ίδια την τεχνολογία είναι απαραίτητες.

7.2 Internet banking και τραπεζική νομοθεσία

Οι συναλλαγές μέσω e-banking υπάγονται στην εποπτεία των Κεντρικών Τραπεζών και των σχετικών Οδηγιών της ΕΕ για τα χρηματοπιστωτικά ιδρύματα. Συνεπώς, όπως σε όλες τις τραπεζικές συναλλαγές ισχύουν τα ακόλουθα:

α) εποπτεία της Κεντρικής Τράπεζας, β) οι διατάξεις για τον περιορισμό του σκοπού και των ποσοστών συμμετοχής φυσικών ή νομικών προσώπων σε πιστωτικά ιδρύματα ή της συμμετοχής των πιστωτικών ιδρυμάτων σε άλλες επιχειρήσεις και γ) οι ειδικές διατάξεις για τη δημοσιοποίηση των οικονομικών αποτελεσμάτων.

Σημαντική διαφοροποίηση αποτελεί η τάση για στροφή προς το καθολικό τραπεζικό σύστημα, δηλαδή τη συνδυασμένη παροχή τραπεζικών και χρηματοοικονομικών υπηρεσιών. Σημειώνεται ότι για την παροχή αυτών των υπηρεσιών, τουλάχιστον στο χώρο της ΕΕ και με βάση την αρχή της ελευθερίας παροχής υπηρεσιών, απαιτείται μια μοναδική άδεια σε ένα κράτος μέλος , η οποία αναγνωρίζεται αμοιβαία σε όλα τα κράτη-μέλη.

Οι ηλεκτρονικά παρεχόμενες υπηρεσίες διέπονται από την Οδηγία 2003/31 (Οδηγία για το ηλεκτρονικό εμπόριο), που εισάγει την αρχή του «κράτους προέλευσης», σύμφωνα με την οποία « ο τόπος εγκατάστασης εταιρείας που παρέχει υπηρεσίες μέσω διεύθυνσης (site) Internet, δεν βρίσκεται εκεί που είναι η τεχνολογία που υποστηρίζει την εν λόγω διεύθυνση ούτε εκεί που παρέχεται πρόσβαση στην εν λόγω διεύθυνση, αλλά εκεί που ασκεί την οικονομική της δραστηριότητα». Επομένως

και η διεξαγωγή internet banking, με βάση την ανωτέρω αρχή, από την οποία μόνο κατ' εξαίρεση επιτρέπεται παρέκκλιση, υπάγεται στην τραπεζική νομοθεσία του «κράτους προέλευσης», ενώ υπό την ανωτέρω έννοια της καθολικής τραπεζικής υπηρεσίας υπάγεται και σε κανόνες του χρηματοοικονομικού τομέα, που πιθανώς δεν είχαν αρχικά προβλεφθεί για την απλή διεξαγωγή τραπεζικών εργασιών. Οι υπεύθυνοι για το internet banking πρέπει σε αυτή την περίπτωση να επιδείξουν ιδιαίτερη προσοχή, επειδή η παράβαση των διατάξεων για την παροχή χρηματοοικονομικών υπηρεσιών στις περισσότερες περιπτώσεις συνιστά και ποινικό αδίκημα, είτε για παράνομη δραστηριότητα είτε για απαγορευμένη διαφήμιση.

Συνεπώς, η διεξαγωγή τραπεζικών συναλλαγών στο Internet από τράπεζα εδρεύουσα στην Ελλάδα υπάγεται στην κείμενη ελληνική και κοινοτική τραπεζική και χρηματοπιστωτική νομοθεσία. Δηλαδή ως προς το σκέλος της τραπεζικής νομοθεσία ισχύει ο Ν.2076/92 για τα χρηματοδοτικά και πιστωτικά ιδρύματα, όπως έχει τροποποιηθεί, και συνακολούθως οι κατ' εξουσιοδότηση εκδοθείσες νομοθετικές ρυθμίσεις. Επομένως οι πράξεις του Διοικητή της Τράπεζας της Ελλάδος εφαρμόζονται και στις δραστηριότητες internet banking. Ως προς το σκέλος των χρηματοοικονομικών υπηρεσιών ισχύει ο Ν.2396/96, με τον οποίο ενσωματώθηκαν στην εσωτερική νομοθεσία οι Οδηγίες 93/22/ΕΟΚ, για τις επενδυτικές υπηρεσίες στον τομέα των κινητών αξιών, και 93/6/ΕΟΚ, για την επάρκεια των ιδίων κεφαλαίων των επιχειρήσεων παροχής επενδυτικών υπηρεσιών και των πιστωτικών ιδρυμάτων. Σε περιβάλλον internet banking εφαρμόζονται, και σε αυτή την περίπτωση, οι κατ' εξουσιοδότηση εκδοθείσες ρυθμίσεις της Τράπεζας της Ελλάδος, της Επιτροπής Κεφαλαιαγοράς ή άλλων αρμόδιων αρχών. Επιπλέον, με την Οδηγία 2002/65/ΕΚ ρυθμίστηκε και η εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές.

Σημειώνεται ότι στο πλαίσιο της γενικής τραπεζικής νομοθεσίας, που διέπει και το internet banking, η Τράπεζα της Ελλάδος είναι αρμόδια για την εφαρμογή από τα πιστωτικά ιδρύματα και των διατάξεων του Ν.2331/95, που αφορά την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες.

7.3 Θεσμικό πλαίσιο πληρωμών

Το θεσμικό πλαίσιο πληρωμών, που μπορεί να χρησιμοποιηθεί και στο internet banking, ορίζεται από την Οδηγία 98/26, με την οποία έχει ήδη προσαρμοστεί το ελληνικό δίκαιο με το Ν.2789/2000. Περαιτέρω το θεσμικό πλαίσιο για τις διασυνοριακές μεταφορές πιστώσεων μέχρι 50.000 ευρώ. Σύμφωνα με την Οδηγία 97/5:

α) Για την εκτέλεση της εντολής ευθύνεται η τράπεζα του εντολέα. β) Θεσπίζεται υποχρέωση για αναλυτική πληροφόρηση των πελατών πριν και μετά από την εκτέλεση της εντολής. γ) Η εντολή πρέπει να διεκπεραιωθεί εντός πέντε εργάσιμων ημερών. δ) Προβλέπονται ειδικές δεσμεύσεις για τις προμήθειες και τα έξοδα και ε) προβλέπεται ειδική αποζημίωση σε περίπτωση μη εκπλήρωσης. Το θεσμικό πλαίσιο συμπληρώνεται από τον Κανονισμό 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε ευρώ, που διασφαλίζει τη διαφάνεια των εξόδων που επιβάλλονται και ευθυγραμμίζει το ύψος τους κατά τις συναλλαγές εντός ΕΕ.

Στην Ελλάδα ρητή αναφορά στο internet banking υπάρχει στην Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: «καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών», στην οποία προβλέπεται άσκηση επίβλεψης από την Τράπεζα της Ελλάδος και στους τρόπους πρόσβασης και στα υποστηρικτικά προϊόντα των συστημάτων πληρωμής, ενώ στο σχετικό ερωτηματολόγιο υπάρχει ειδική πρόβλεψη για internet και mobile banking, γεγονός που αναδεικνύει ότι και πρακτικά η

κεντρική τράπεζα επιθυμεί να θέσει υπό την εποπτεία της και το internet banking. Για τη διεξαγωγή ασφαλών συναλλαγών μέσω internet banking η ελληνική νομοθεσία συμπληρώνεται από το ΠΔ 150/01 για τις ηλεκτρονικές υπογραφές, που εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 99/93. Για την περίπτωση διεξαγωγής συναλλαγών με ίδρυμα ηλεκτρονικού χρήματος ισχύει ο Ν.3148/2003.

7.4 Προστασία καταναλωτών στις ηλεκτρονικές συναλλαγές

Η εξασφάλιση της προστασίας των καταναλωτών στην παροχή τραπεζικών υπηρεσιών επιτυγχάνεται μέσω του νόμου 2251/94, όπως αναλύεται στα κάτωθι αναφερόμενα υποκεφάλαια. Ειδικά όμως για την παροχή χρηματοοικονομικών υπηρεσιών ισχύει πλέον η Οδηγία 2002/65 «σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές», η οποία αποδίδει την ιδιότητα του καταναλωτή σε «κάθε πρόσωπο το οποίο, στο πλαίσιο των συμβάσεων εξ αποστάσεως ενεργεί για σκοπούς εκτός του πεδίου της εμπορικής ή επαγγελματικής του δραστηριότητας». Η Οδηγία προβλέπει: α) υποχρέωση για λεπτομερή πληροφόρηση του καταναλωτή πριν και μετά από την κατάρτιση της σύμβασης, για την υπηρεσία, τη σύμβαση και τα μέσα αποκατάστασης, β) υποχρέωση για ανακοίνωση των συμβατικών όρων σε χαρτί ή άλλο σταθερό μέσο, γ) δικαίωμα υπαναχώρησης εντός 14 ημερών εκτός από i) τις υπηρεσίες με διακυμάνσεις τιμών (π.χ. συνάλλαγμα, futures, swaps, options), ii) τις βραχυπρόθεσμες συμβάσεις (π.χ. ασφαλιστήρια για ταξίδια), iii) τις συμβάσεις, η εκτέλεση των οποίων ολοκληρώθηκε και iv) τις συμβάσεις ασφαλίσεων ζωής, για τις οποίες προβλέπεται δικαίωμα υπαναχώρησης εντός 30 ημερών (Οδηγία 90/619), δ) δυνατότητα ακύρωσης των συναλλαγών με πιστωτική κάρτα, ε) πρόβλεψη μέτρων για τις μη αιτηθείσες υπηρεσίες και την αυτόκλητη επικοινωνία (π.χ. με ανεπιθύμητα ηλεκτρονικά μηνύματα). Οι διατάξεις της οδηγίας έχουν αναγκαστικό χαρακτήρα, ώστε να αποκλείεται συμβατική παραίτηση από τα παρεχόμενα δικαιώματα.

7.5 Προστασία προσωπικών δεδομένων

Η προστασία προσωπικών δεδομένων θωρακίζεται με το συνδυασμό τόσο του ελληνικού όσο και του διεθνούς δικαίου. Πιο συγκεκριμένα, μέσω του νόμου 3471/2006 (τροποποίηση ν. 2472/1997) καθώς επίσης και από διεθνής συμβάσεις και οδηγίες.

7.5.1 Προστασία προσωπικών δεδομένων και ΕΕ

Η προστασία προσωπικών δεδομένων καλύπτεται νομικά και από την Ευρωπαϊκή Ένωση. Πιο αναλυτικά προσδιορίζεται από τα ακόλουθα:

Διεθνείς συμβάσεις όπως:

- η “Οικουμενική διακήρυξη των Δικαιωμάτων του ανθρώπου” του ΟΗΕ (1948)
- το “Διεθνές Σύμφωνο Ατομικών και Πολιτικών Δικαιωμάτων»
- η «Σύμβαση Ρώμης»

Κοινοτικές οδηγίες όπως:

- η 95/46/ΕΚ που αποτελεί τη βάση για την προστασία των καταναλωτών και την ελεύθερη κυκλοφορία των δεδομένων αυτών
- η 97/66/ΕΚ που αποσκοπεί στην εναρμόνιση όλων των κρατών μελών, με στόχο να επιτευχθεί ένα ίδιο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων των πολιτών τους και ειδικότερα στον τομέα των τηλεπικοινωνιών (ενσωματώθηκε στο νόμο 2774/1999)
- η 2002/58/ΕΚ που αφορά στην προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Στην ηλεκτρονική τραπεζική όπου υπάρχει διασυνοριακή ροή δεδομένων ισχύει ότι:

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη:

α) προς χώρες - μέλη της Ευρωπαϊκής Ένωσης, β) προς χώρα μη μέλος της Ευρωπαϊκής Ένωσης, μετά από άδεια της Αρχής που παρέχεται εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπόψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων. Δεν απαιτείται άδεια της Αρχής εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφανθεί, με τη διαδικασία του άρθρου 31 παρ. 2 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, ότι η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, κατά την έννοια της παρ. 2 του άρθρου 25 της ανωτέρω Οδηγίας. (Ν. 3471/2006 - τροποποίηση άρθρου 9 Ν. 2472/1997).

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής, εφ' όσον συντρέχει ειδική περίπτωση (όπως παρουσιάζεται στο Ν. 3471/2006, άρθρο 9, παράγραφος 2).

7.5.2 Το συνταγματικό πλαίσιο της προστασίας προσωπικών δεδομένων

Το δίκαιο της προστασίας προσωπικών δεδομένων έχει συνταγματικό υπόβαθρο. Συγκεκριμένα ο ν. 3471/2006 στοχεύει στην προστασία ιδιωτικής ζωής, αλλά και των θεμελιωδών δικαιωμάτων των ατόμων. Η εν λόγω προστασία δεν εξαντλείται στην προστασία του απαραβίαστου της ιδιωτικής ζωής, αλλά αφόρα και αλλά δικαιώματα, ιδίως το δικαίωμα ελεύθερης ανάπτυξης της προσωπικότητας. Το δικαίωμα προστασίας της ιδιωτικής ζωής, ορίζεται ως δικαίωμα που έχει κάθε άνθρωπος να μην ενοχλείται από τους άλλους.

Το δικαίωμα προστασίας της ιδιωτικής ζωής εμπεριέχεται στο σύνταγμα το οποίο ορίζει ότι η ιδιωτική και οικογενειακή ζωή του ανθρώπου είναι απαραβίαστη. Ακόμα η προστασία της ιδιωτικής ζωής δεν αναφέρεται μονό στην κλασική προστασία του άσυλου της κατοικίας αλλά και σε ποιο νέες μορφές προσβολής της όπως π.χ., η οπτικοακουστική παρακολούθηση ή απαίτηση πληροφοριών που αφορούν την ιδιωτική ζωή.

Επιπλέον στην προστασία προσωπικών δεδομένων εμπεριέχεται και του δικαίωμα του πολίτη να αποφασίζει ελευθέρα για τις πράξεις του. Ο πολίτης θα

αποφασίζει αυτός ποιες πληροφορίες που αφορούν τον ίδιο θα γνωστοποιούνται σε τρίτους.

Το άρθρο 9Α του συντάγματος εμπεριέχει σε συνταγματικό δικαίωμα, το ατομικό δικαίωμα προστασίας του άτομου απέναντι στη συλλογή, αποθήκευση και επεξεργασία με συμβατικό η ηλεκτρονικό τρόπο των προσωπικών πληροφοριών και δεδομένων.

Δικαίωμα στο άρθρο 9 Α έχουν όλα τα πρόσωπα της ελληνικής επικράτειας, Έλληνες και αλλοδαποί. Επιπλέον, αποδέκτες του δικαιώματος είναι όλοι οι φορείς δημόσιας εξουσίας.

Σύστημα προστασίας του ν. 3471/2006

Με το νόμο 3471/2006 θεσμοθετείται ένα σαφές πλαίσιο προστασίας προσωπικών δεδομένων, το οποίο περιέχει κανόνες ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς. Χρησιμεύουν στην οριοθέτηση της συνταγματικά ανεκτής επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κατ' αυτόν τον τρόπο αυτό, συμβάλλουν στη ρύθμιση της ροής και της κατανομής των πληροφοριών στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας. Το αντικείμενό του συνίσταται στη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, με στόχο την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και της ιδιωτικής ζωής. Ο εν προκειμένω νόμος εφαρμόζεται στην επεξεργασία δεδομένων1 με αυτοματοποιημένες και συμβατικές μεθόδους, τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα.

7.6 Ενιαίος ευρωπαϊκός χώρος πληρωμών σε ευρώ (SEPA)

Η βελτίωση της ανταγωνιστικότητας της οικονομίας των κρατών-μελών της Ευρωπαϊκής Ένωσης και η εξυπηρέτηση της ελεύθερης διακίνησης προσώπων, αγαθών και υπηρεσιών προϋποθέτουν την ύπαρξη ενός ενιαίου ευρωπαϊκού χώρου πληρωμών, στον οποίο οι πολίτες και οι επιχειρήσεις θα έχουν τη δυνατότητα να πραγματοποιούν και να δέχονται πληρωμές σε ευρώ με την ίδια ευκολία ασφάλεια και κόστος που τις πραγματοποιούν στη χώρα τους. Για την επίτευξη αυτού του στόχου υπάρχει η SEPA- Single Euro Payments Area. Σκοπός της είναι η προώθηση της ευρωπαϊκής ολοκλήρωσης μέσω μιας ανταγωνιστικής και καινοτόμου αγοράς πληρωμών μικρής αξίας στη ζώνη του ευρώ, που θα παρέχει υψηλότερο επίπεδο υπηρεσιών, πιο αποτελεσματικά προϊόντα και φθηνότερες εναλλακτικές λύσεις για τη διενέργεια πληρωμών. Αποτελεί μία ολοκληρωμένη αγορά για τις υπηρεσίες πληρωμών με αποτέλεσμα τη δυνατότητα εκτέλεσης μη εγχρήματων πληρωμών σε ολόκληρη τη ζώνη του ευρώ από ένα μόνο τραπεζικό λογαριασμό, χρησιμοποιώντας ένα μόνο σύνολο μέσων πληρωμής με την ίδια ευκολία, αποδοτικότητα και ασφάλεια. Ίσοι όροι ανταγωνισμού για όλα τα συστήματα πληρωμών ώστε να απολαμβάνει ο ευρωπαίος καταναλωτής αυξημένα προνόμια σε σχέση με τα εθνικά συστήματα, ελεύθερη και ευκολότερη εγκατάσταση χρηματοπιστωτικών οργανισμών σε άλλες χώρες και ανταγωνιστικό περιβάλλον.

7.6.1 Επιδράσεις SEPA

Για τους καταναλωτές

Τα μέσα πληρωμών SEPA θα διατίθενται στις 32 χώρες SEPA και θα διευκολύνουν τις συναλλαγές των καταναλωτών.

- Οι καταναλωτές θα χρειάζονται μόνο έναν λογαριασμό πληρωμών. Από αυτό το λογαριασμό θα μπορούν να διενεργούν μεταφορές πιστώσεων και άμεσες χρεώσεις σε ευρώ οπουδήποτε στις 32 χώρες SEPA με την ίδια ευκολία με την οποία διενεργούν εγχώριες πληρωμές
- Η χρήση καρτών πληρωμής θα είναι πιο ασφαλής και αποτελεσματική, αφού οι καταναλωτές θα μπορούν να χρησιμοποιούν την ίδια κάρτα για όλες τις πληρωμές σε ευρώ. Αυτό θα μειώσει και την ανάγκη των ανθρώπων να μεταφέρουν μετρητά
- Η παροχή καινοτόμων υπηρεσιών δεν θα επηρεάζεται από τα εθνικά σύνορα. Ο μακροπρόθεσμος στόχος του τραπεζικού κλάδου είναι τα μέσα πληρωμών SEPA να χρησιμοποιούνται αποκλειστικά σε ηλεκτρονική μορφή. Οι υπηρεσίες αυτές περιλαμβάνουν την ηλεκτρονική τιμολόγηση, την ενεργοποίηση πληρωμής από κινητό τηλέφωνο ή το διαδίκτυο, τα ηλεκτρονικά αεροπορικά εισιτήρια, την ενημέρωση κινήσεων ή την ηλεκτρονική συμφωνία λογαριασμών. Έτσι, θα μειωθεί ο χρόνος που δαπανούν οι καταναλωτές για την εκτέλεση πληρωμών
- Θα επιτυγχάνεται εγγυημένη χρονικά ολοκλήρωση της μεταφοράς πίστωσης ή της άμεσης χρέωσης

Για τους εμπόρους

Οι καταναλωτές προτιμούν ολοένα και περισσότερο τις πληρωμές με κάρτα, οπότε, η χρήση καρτών αναμένεται να αυξηθεί στο μέλλον. Για την αποδοχή πληρωμών με κάρτα, οι έμποροι πρέπει να έχουν συνάψει συμφωνία με ένα πιστωτικό ίδρυμα που να αποδέχεται συναλλαγές με κάρτα, και την προώθησή τους μέσω της υποδομής εκκαθάρισης στο πιστωτικό ίδρυμα του κατόχου της κάρτας. Από αυτή την άποψη, ο SEPA παρέχει τα ακόλουθα πλεονεκτήματα:

- Οι αποδέκτες συναλλαγών με κάρτα θα είναι σε θέση να επεξεργάζονται όλες τις πληρωμές που είναι συμβατές με τον SEPA, ακόμα και τις διασυνοριακές. Στο περιβάλλον του SEPA, οι έμποροι θα μπορούν να επιλέγουν οποιονδήποτε αποδέκτη συναλλαγών με κάρτα στη ζώνη του ευρώ για την επεξεργασία των πληρωμών τους. Αυτό θα ενισχύσει τον ανταγωνισμό και θα μειώσει το κόστος
- Ο βαθμός τυποποίησης των τερματικών που βρίσκονται σε σημεία πώλησης στις 32 χώρες του SEPA θα αυξάνεται ολοένα και περισσότερο, με αποτέλεσμα να υπάρχει μεγαλύτερο φάσμα παρόχων τερματικών και οι έμποροι να μπορούν να δέχονται μεγαλύτερο αριθμό διαφορετικών καρτών με ένα μόνο τερματικό. Επιπλέον, ο αυξημένος ανταγωνισμός μεταξύ των συστημάτων καρτών αναμένεται να οδηγήσει σταδιακά σε μείωση των προμηθειών

Για τις επιχειρήσεις

Ο SEPA θα βοηθήσει τις επιχειρήσεις να απλουστεύσουν τη διαχείριση των πληρωμών τους, διότι:

- Οι επιχειρήσεις θα είναι σε θέση να διενεργούν όλες τις συναλλαγές τους σε ευρώ κεντρικά, από έναν λογαριασμό πληρωμών, με τα μέσα πληρωμών SEPA. Η διαχείριση των πληρωμών θα απλουστευθεί, καθώς όλες οι εισερχόμενες και εξερχόμενες πληρωμές θα έχουν την ίδια μορφή. Για τις επιχειρήσεις που ασκούν δραστηριότητες στον SEPA, η ενοποίηση της διαχείρισης πληρωμών και ρευστότητας σε ένα σημείο θα οδηγήσει σε μείωση όχι μόνο του λειτουργικού κόστους αλλά και του απαιτούμενου χρόνου
- Οι υπηρεσίες προστιθέμενης αξίας, όπως η ηλεκτρονική τιμολόγηση και η ηλεκτρονική συμφωνία λογαριασμών, θα βοηθήσουν τις επιχειρήσεις να βελτιώσουν ακόμη περισσότερο τη διαχείριση των πληρωμών τους. Επί του παρόντος, οι εν λόγω υπηρεσίες συχνά παρέχονται μόνο σε εγχώριο επίπεδο, καθώς οι διαφορετικές μορφές πληρωμών δυσχεραίνουν τη χρήση τους σε διασυνοριακό επίπεδο

Για τους παρόχους υπηρεσιών πληρωμών

Με την παροχή νέων μέσων πληρωμών και υποδομών στις 32 χώρες του SEPA, ο SEPA θα ωφελήσει τους φορείς υπηρεσιών πληρωμών με τους ακόλουθους τρόπους:

- Οι πάροχοι υπηρεσιών πληρωμών θα είναι σε θέση να επεκτείνουν τις δραστηριότητές τους και να ανταγωνίζονται στον SEPA, καθώς θα μπορούν πιο εύκολα να προσφέρουν τις υπηρεσίες τους στις 32 χώρες του SEPA
- Ο SEPA θα ενισχύσει την ευρωπαϊκή ολοκλήρωση και την αποτελεσματικότητα της αγοράς. Με την ευθυγράμμιση των όρων βάσει των οποίων διενεργούνται οι πληρωμές, ο SEPA θα παράσχει μια ενιαία δέσμη κανόνων, ισότιμη, ανοικτή και πλήρη πρόσβαση, διαφάνεια και διαλειτουργικότητα. Όλοι αυτοί οι παράγοντες θα ενισχύσουν τον ανταγωνισμό και, κατ' επέκταση, θα δώσουν στα πιστωτικά ιδρύματα τη δυνατότητα να διαπραγματεύονται καλύτερους όρους με τους παρόχους υπηρεσιών

8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Ο κόσμος των υπολογιστών είναι πολύ επικίνδυνος για να «κυκλοφορεί» κάποιος χωρίς προστασία. Κάθε χρήστης πρέπει να έχει στην κατοχή του ένα τουλάχιστον antivirus updated, να έχει ρυθμίσει τις επιλογές προστασίας σε ένα firewall, να έχει θέσει όσο πιο ασφαλείς passwords στο σύστημά του και να προσέχει πολύ τα δεδομένα που εισάγονται στον υπολογιστή του κρατώντας συνεχώς back up τα δικά του. Απαιτείται μεγάλη προσοχή για να μην υπάρχουν πιθανές απώλειες. Η εκτεταμένη χρήση τους δείχνει πως στο μέλλον θα αποτελέσουν βασικό και αναπόσπαστο κομμάτι κάθε δικτυακής αρχιτεκτονικής. Η τάση, σήμερα, είναι ο συνδυασμός της χρήσης της ισχύος του υλικού (hardware) και της ευφυΐας του λογισμικού (software).

Η ετερογένεια των δικτύων, η εύκολη και απεριόριστη πρόσβαση, η απουσία συνολικής πολιτικής ελέγχου προσπέλασης, η αυξημένη πολύ πολυπλοκότητα διαδικασιών, η αύξηση αριθμού διαύλων επικοινωνίας, η ασάφεια στα όρια δικτύων, η δυνατότητα ανωνυμίας του χρήστη είναι μερικοί από τους σημαντικότερους λόγους επικινδυνότητας των ηλεκτρονικών πληρωμών. Για το λόγο αυτό παρουσιάστηκαν και αναλύθηκαν διεξοδικά τα βασικότερα μέσα προστασίας του χρήστη από κακόβουλες επιθέσεις και υποκλοπές.

Τέλος, αν τελικά το Διαδίκτυο αποτελεί ένα ασφαλή χώρο διενέργειας συναλλαγών, μπορεί να διατυπωθεί πως δεν υπάρχει απόλυτη ασφάλεια. Η τεχνολογία εξελίσσεται και μαζί με αυτή αναδιαμορφώνονται και οι υφιστάμενες απειλές της. Θα πρέπει μα υπάρχει διαρκής αναβάθμιση των μέσων προστασίας και διαρκής ενημέρωση των χρηστών, ώστε να γνωρίζουν και τι καινούριο ή αναδιαμορφωμένο μπορεί να συναντήσουν, αλλά και το πώς να το διαχειριστούν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Derfler E., (2001). “Secure Your Network”, PC Magazine
2. E. D. Zwicky, S. Cooper, and D. B. Chapman: *Building Internet Firewalls*, 2nd ed., O’Reilly & Associates, 2000, pp. 22, 102 – 105, 122, 224. (Μετάφραση από τους συγγραφείς της παρούσας εργασίας).
3. European Central Bank-Eurosystem (2012). “Recommendations for the Security of Internet Payments”.
4. Fumy W., (1998). “Internet Security Protocols”, COSIC’97 Course
5. J. F. Kurose και K. W. Ross, *Δικτύωση Υπολογιστών: Προσέγγιση από Πάνω προς τα Κάτω με Έμφαση στο Διαδίκτυο*, 2η Έκδοση, Εκδόσεις Μ. Γκιούρδας, σελ. 12 – 14 , 80, 432, 640 – 646.
6. K. C. Laudon και J. P. Laudon, *Πληροφοριακά Συστήματα Διοίκησης*, 6η Αμερικανική έκδοση, Εκδόσεις Κλειδάριθμος, pp. 305 – 306.
7. Klein S.A., and Menendez J.N, (1993). “Information security consideration in open systems archetectures”, IEEE Transactions on Power Systems, Vol.8
8. Lincoln D. Stein, *Ασφάλεια Δικτύων WEB*, Εκδόσεις Ιών, 2000.
9. Mao W., (2003) “Modern Cryptography: Theory and Practice”, Prentice Hall PTR, Vol.1
10. Morten Hertzum, Niels Jorgensen, Mie Norgard, (2004). “Usable Security and e-banking: Ease of use vis-á-vis security”, Roskilde Univerdity, Denmark, pp52-65.
11. Oliver C., (1995). “Privacy, anonymity and accountability”, Computers and Security, Vol.14
12. R. Oppliger, *Internet and Intranet Security*, 2nd edition, Artech House: Computer Security Series, 2001, p. 54. (Μετάφραση από τους συγγραφείς της παρούσας εργασίας).
13. Ruben Hernandez-Murillo, Gerard Liobet, Roberto Fuentes (2006). “Strategic Online-Banking Adoption”, Working Paper 2006-058E, pp 1-33.
14. Αλεξανδρής Ν., Χρυσικόπουλος Β., και Πεππές Δ., (1995). «Ασφάλεια Δικτύων Υπολογιστικών Συστημάτων», Έκδοση: Ελληνική εταιρεία επιστημόνων υπολογιστών και Πληροφορικής, Αθήνα.
15. Γ. Πάγκαλος και Ι. Μαυρίδης, *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*, Εκδόσεις Ανικούλα, 2002.
16. Γεωργόπουλος Ν.Β., Πανταζή Μ.Α., Νικολαράκος Χ.Θ., και Βαγγελάτος Ι.Χ., (2001). «Ηλεκτρονικό Επιχειρείν, Προγραμματισμός και Σχεδίαση», Ά έκδοση, Εκδόσεις Μπένου, Αθήνα.
17. Κ. Αντωνής, *Ασφάλεια Υπολογιστικών Συστημάτων*, 2003.
18. Κάτος Β.Α., και Στεφανίδης Π., (2000). «Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης», Ζυγός.
19. Κομνηνός Θεόδωρος, Σπυράκης Παύλος, *Ασφάλεια Δικτύων και Υπολογιστικά Συστήματα*, Εκδόσεις Ελληνικά Γράμματα, 2002.

20. Πατσάκης Κ. Ε., Φούντας Ε. Χ., «Κρυπτογραφία και Εφαρμογές», Εκδόσεις Βαρβαρήγου, Τόμος Ά, Αθήνα.
21. Σ. Κάτσικας, *Ασφάλεια Δικτύων*, Τόμος Β', Ελληνικό Ανοικτό Πανεπιστήμιο, 2001, σελ. 172, 177 – 179.
22. Σινανιώτη Α., Φαρσαρώτας Ι., «Ηλεκτρονική Τραπεζική», Εκδόσεις Σάκκουλας, Αθήνα, 2005.
23. Φαρσαρώτας Ι., «Κατανοώντας τη Σύγχρονη Τραπεζική», Εκδόσεις Σάκκουλας, Αθήνα, 2009.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ