ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

Τμήμα : Εφαρμογών Πληροφορικής στην Διοίκηση και στην Οικονομία

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Τίτλος: ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΕΙΣΗΓΗΤΡΙΑ: ΑΝΤΩΝΙΑ ΣΤΕΦΑΝΗ

ΣΠΟΥΔΑΣΤΗΣ: ΚΑΠΕΛΛΑΚΗΣ ΓΕΩΡΓΙΟΣ

ΜΕΣΟΛΟΓΓΙ 2004

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΚΕΦΑΛΑΙΟ 2

ΚΕΦΑΛΑΙΟ 3

ΚΕΦΑΛΑΙΟ 4

ΚΕΦΑΛΑΙΟ 5

Κεφάλαιο 1ο:

Ηλεκτρονικό Εμπόριο B2C

1.1 Εισαγωγή

Με την είσοδο της ανθρωπότητας στον 21ο αιώνα, παρατηρούμε εκτός των άλλων, την τεχνολογία να εξελίσσεται με ραγδαίους ρυθμούς σε όλους τους τομείς της ζωής μας, από την υγεία μέχρι την αγορά και την πώληση υπηρεσιών και αγαθών. Έτσι, τα τελευταία χρόνια έχει αρχίσει να αναπτύσσεται ένας κλάδος, γνωστός ως «ηλεκτρονικό εμπόριο», το οποίο με την εξέλιξη της τεχνολογίας θα αλλάξει και την ζωή μας. Το ηλεκτρονικό εμπόριο δεν διαφέρει σε τίποτα από το κανονικό εμπόριο εκτός του ότι τα πάντα είναι ψηφιακά, από τις υπογραφές και τα πιστοποιητικά μέχρι τα χρήματα και τις τραπεζικές επιταγές. Η ψηφιοποίηση, όμως, τέτοιων δεδομένων, απαιτεί και κάποια μέτρα ασφάλειας τόσο από την μεριά των εμπόρων, όσο και από την μεριά των καταναλωτών. Πριν συνεχίσουμε σε αυτό το φλέγον και ενδιαφέρον ζήτημα, θα πρέπει να δώσουμε έναν ορισμό για το ηλεκτρονικό εμπόριο, θα αναφέρουμε ποιες κατηγορίες υπάρχουν και θα δούμε το πόσο απαραίτητο είναι στην ζωή μας.

Ένας απλός ορισμός για το ηλεκτρονικό εμπόριο είναι ο εξής:

"***Ένα on-line σύστημα καταστημάτων καθορίζει την διεπαφή αγοραστή/πωλητη που χρησιμοποιεί την τεχνολογία του Διαδικτύου. Υποστηρίζει κυρίως το επιχείρηση – προς - καταναλωτή (B2C) επιχειρησιακό πρότυπο***".

1.2 *Κατηγορίες – Υποκατηγορίες ηλεκτρονικού εμπορίου*

Το ηλεκτρονικό εμπόριο χωρίζεται σε 2 βασικές κατηγορίες:
1. Η επιχείρηση – προς – επιχείρηση (B2B)
2. Η επιχείρηση – προς – καταναλωτή (B2C)

και σε 6 υποκατηγορίες:
1. C2B (πελάτης - προς – επιχείρηση): σε αυτή την κατηγορία ο πελάτης πουλάει αγαθά κυρίως, στις επιχειρήσεις οι οποίες θα τα χρησιμοποιήσουν για να παράγουν άλλα αγαθά.
2. C2C (πελάτης – προς – πελάτη): σε αυτή την κατηγορία η αγορά και η πώληση αγαθών γίνεται ΜΟΝΟ μεταξύ των πελατών. Η διακίνηση "ψηφιακού χρήματος" δεν είναι ασφαλής στο μέγιστο βαθμό, γιατί κανείς δεν μπορεί να δώσει εγγύηση για την ακεραιότητα των δύο συμβαλλόμενων μερών.
3. G2C (κυβέρνηση – προς – πελάτη)
4. C2G (πελάτης – προς – κυβέρνηση)
5. G2B (κυβέρνηση – προς – επιχείρηση)
6. B2G (επιχείρηση – προς – κυβέρνηση)

1.2.1 B2B:

Η πρώτη κατηγορία αναφέρεται στην αγορά και πώληση υπηρεσιών και αγαθών μεταξύ

των επιχειρήσεων. Σε αυτή την κατηγορία τα μέλη διακινούν "ψηφιακό χρήμα", υπηρεσίες, αγαθά, τα οποία δεν αφορούν τον απλό καταναλωτή και γι΄αυτό το λόγο δεν έχει πρόσβαση σε αυτού του είδους τις συναλλαγές.

1.2.2 B2C:
Η δεύτερη κατηγορία ,με την οποία θα ασχοληθούμε, είναι αγορά και πώληση υπηρεσιών και αγαθών από τις επιχειρήσεις – προς – τους πελάτες. Σε αυτή την κατηγορία ο πελάτης μπορεί να διαλέξει με ποια επιχείρηση θα συνδιαλλαγεί. Για να μπορέσει να πραγματοποιηθεί η συναλλαγή μεταξύ του πελάτη και της επιχείρησης, τα ηλεκτρονικά καταστήματα ακολουθούν ένα πρότυπο ως προς την δομή τους, και την διασφάλιση των προσωπικών δεδομένων του πελάτη. Η διασφάλιση των προσωπικών δεδομένων του πελάτη μπορεί να διαφέρει μεταξύ των ηλεκτρονικών καταστημάτων.

1.3 *Δομή της κατηγορίας B2C*

Τα ηλεκτρονικά καταστήματα που ανήκουν στην κατηγορία B2C πρέπει να έχουν την εξής δομή για να μπορεί ο πελάτης να βρει και να αγοράσει τα προϊόντα που επιθυμεί. Η δομή τους αποτελείται απο τα εξής:

- Μηχανή Αναζήτησης (Search Machine)
- Μενού Πλοήγησης (Navigation Bar)
- Ηλεκτρονικούς Καταλόγους (e-Catalog)
- Ηλεκτρονικές Φόρμες Παραγγελίας (Order e-Form)
- Ηλεκτρονικές Φόρμες Πληρωμών (Payment e-Form)
- Ηλεκτρονική Διεύθυνση αλληλογραφίας (e-mail)

Προαιρετικά μπορούν να συμπεριλαμβάνουν τα εξής:

- Φόρμες για την δημιουργία μελών
- Επίδειξη "ψηφιακού πιστοποιητικού" του καταστήματος
- Πιστοποίηση χρήστη

1.3.1 Μηχανές Αναζήτησης (Search Machine)

Οι μηχανές αναζήτησης είναι ένα από τα πιο βασικά σημεία ενός ηλεκτρονικού καταστήματος, γιατί βοηθά τον χρηστή να βρει τα προϊόντα που θέλει χωρίς να ψάχνει ώρες μέχρι να το βρει. είναι πιο εύκολο να γράψει ο πελάτης "Μουσική Παπακωσταντίνου" και να του βγάλει η ιστοσελίδα την δισκογραφία που σχετίζεται με τον συγκεκριμένο καλλιτέχνη , από το να μπει στην σελίδα της μουσικής και από εκεί να επιλέξει να μεταβεί στην σελίδα τις rock μουσικής, από εκεί στο γράμμα "Π" και να ψάχνει όλους τους καλλιτέχνες που το επώνυμο τους ξεκινάει από "Π".

Ο πελάτης μπορεί να κάνει και μια γενικότερη αναζήτηση στην ιστοσελίδα του καταστήματος όταν δεν γνωρίζει την κατηγορία που ανήκει το προϊόν που θέλει.

1.3.5 Ηλεκτρονικές Φόρμες Πληρωμών

Όταν έχει φτάσει σε αυτό το σημείο ,σημαίνει ότι γνωρίζει τί μέτρα ασφάλειας έχει λάβει το κατάστημα, τους τρόπους πληρωμής, και φυσικά γνωρίζει ότι η συγκεκριμένη σελίδα από την οποία θα στείλει τα προσωπικά του στοιχεία είναι ασφαλής. Αυτό μπορεί να το διαπιστώσει από μόνος του κοιτώντας κάτω και δεξιά στην μπάρα του φυλλομετρητή, όπου θα πρέπει να δει ένα λουκέτο κλειστό και αν μετακινήσει το ποντίκι πάνω από το λουκέτο θα δει ποιον αλγόριθμο κρυπτογράφησης χρησιμοποιείται (SSL 128 bit) ή από ποια εταιρεία ασφάλειας είναι πιστοποιημένη η σελίδα αυτή (Veri Sign).

Εικόνα 1: Πριν τοποθετηθεί το ποντίκι πάνω στο λουκέτο

Εικόνα 2: Το ποντίκι έχει τοποθετηθεί πάνω στο λουκέτο

1.3.6 Ηλεκτρονική Διεύθυνση αλληλογραφίας (e-mail)

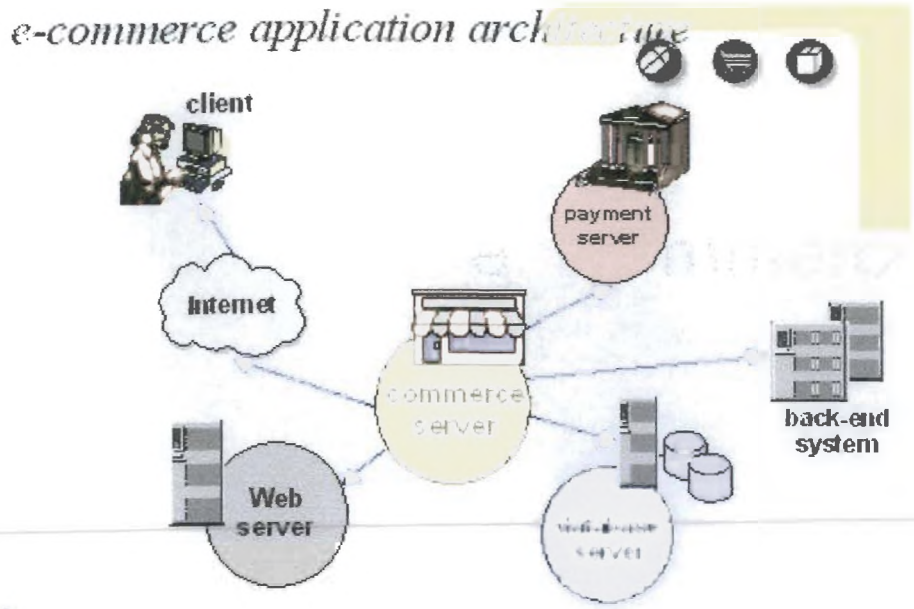
Το e-mail είναι απαραίτητο να υπάρχει για να μπορεί ο πελάτης να επικοινωνήσει με κάποιον από τους υπεύθυνους του ηλεκτρονικού καταστήματος για να τον ρωτήσει απορίες που πιθανόν να έχει όσον αφορά στον τρόπο μετάδοσης προσωπικών στοιχείων καθώς και στα μέτρα ασφάλειας. Το e-mail έχει συνήθως την μορφή **username@domainname.extension**
username= κάποιο όνομα χρήστη π.χ *webmaster, administrator, info*
domainname= το όνομα του ηλεκτρονικού καταστήματος π.χ *amazon, papasotiriou*
extension= ακολουθεί μετα το domainname π.χ *.com, .gr, .de, .org, .net, .be*

Η διαδικασία που γίνεται από τον πελάτη για την αγορά ενός ή και περισσότερων προϊόντων ονομάζεται ***κύκλος ζωής του ηλεκτρονικού εμπορίου.***

Η διαδικασία που ακολουθείται είναι η εξής:

- ο πελάτης μπαίνει στο ηλεκτρονικό κατάστημα,
- βρίσκει το προϊόν ή τα προϊόντα που θέλει να αγοράσει,
- συμπληρώνει την φόρμα με τα προσωπικά του στοιχεία και την στέλνει στο ηλεκτρονικό κατάστημα,
- το ηλεκτρονικό κατάστημα επιβεβαιώνει την αγορά,
- και στέλνει στον πελάτη ευχαριστήριο e-mail και τα προϊόντα.

Σε οποιαδήποτε σημείο ο πελάτης μπορεί να ακυρώσει την αγορά ακόμη και αν έχει στείλει τα προσωπικά στοιχεία. Για κάθε σημείο του κύκλου ζωής έχει δημιουργηθεί ένα διαφορετικό λογισμικό, ώστε να επιτυγχάνεται η μέγιστη ασφάλεια. Για την διασφάλιση των χρηματοοικονομικών συναλλαγών χρησιμοποιείται το EDI για την κατηγόρια B2B και το FEDI για την κατηγόρια B2C.



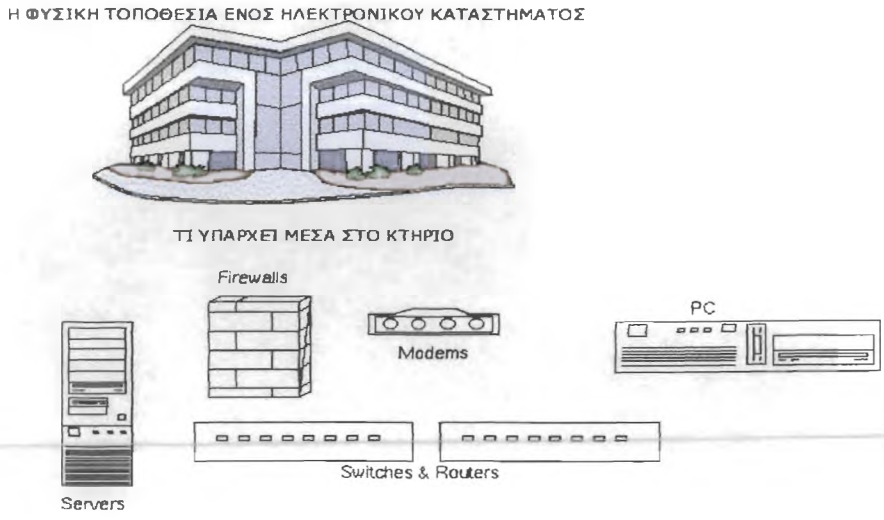
Ο κύκλος ζωής του ηλεκτρονικού εμπορίου σχηματικά

1.4 Φυσική Δομή ενός Ηλεκτρονικού Καταστήματος

Μέχρι στιγμής έχουμε αναφέρει πώς πρέπει να είναι δομημένο το ηλεκτρονικό κατάστημα ,από την ηλεκτρονική μεριά, ώστε να μπορεί ο πελάτης να βρίσκει εύκολα και γρήγορα το προϊόν που θέλει να αγοράσει. Για να μπορέσει να υπάρξει ένα ηλεκτρονικό κατάστημα θα πρέπει πρώτα να υπάρχει σαν φυσική τοποθεσία.

Με τον όρο φυσική τοποθεσία εννοούμε ότι 1) στεγάζεται σε κάποιο κτίριο, και 2) έχει κάποια ιθαγένεια, δηλαδή είναι ελληνικό κατάστημα, αγγλικό, αμερικάνικο, ιταλικο, κλπ.
Μέσα στο κτίριο θα πρέπει να υπάρχει ένας χώρος με τα προϊόντα που πουλάει, ούτως ώστε να μπορεί ο πελάτης να έρθει σε φυσική επαφή με τα προϊόντα, και ένας χώρος στον οποίο θα υπάρχουν τα μηχανήματα τα οποία θα δείχνουν σε πελάτες άλλων χωρών τα προϊόντα του καταστήματος σε ψηφιακή μορφή.

Τα μηχανήματα είναι: 1) Servers (Εξυπηρετητές), 2) Switches και Routers, 3) Modems, 4) Firewalls (Πυρότειχα Ασφαλείας), 5) PCs. Συνδέοντας τα μηχανήματα και γράφοντας κώδικα σε γλώσσες προγραμματισμού ειδικές για το διαδίκτυο το κατάστημα μπορεί και παρουσιάζει τα προϊόντα του σε μελλοντικούς πελάτες άλλων χωρών.



Σχήμα 1. Φυσική Δομή

Ας δούμε σε τι χρησιμεύει το κάθε ένα χωριστά και κατά πόσο είναι χρήσιμο για το ηλεκτρονικό κατάστημα.

1.4.1 *Servers (Εξυπηρετητές)*

Οι εξυπηρετητές είναι τα μηχανήματα στα οποία έχουν τοποθετήσει τον κώδικα του ηλεκτρονικού καταστήματος και είναι υπεύθυνα για την σωστή εμφάνιση του κώδικα στον πελάτη. Οι εξυπηρετητές μπορούν να είναι παραπάνω του ενός και ανάλογα τι ζητάει εκείνη την στιγμή ο πελάτης , το ερώτημα του πηγαίνει στον αντίστοιχο εξυπηρετητή και αυτός με την σειρά του επεξεργάζεται το ερώτημα και εμφανίζει τα αποτελέσματα στον πελάτη. Τα περισσότερα καταστήματα έχουν εξυπηρετητές άνω του ενός για να επεξεργάζονται καλύτερα τα ερωτήματα και να δίνουν αξιόπιστες απαντήσεις.

1.4.2 *Switches & Routers*

Είναι τα μηχανήματα τα οποία επιτρέπουν την πρόσβαση στο διαδίκτυο, αλλά και την σωστή μεταφορά των δεδομένων από τον ένα υπολογιστή στον άλλο, χρησιμοποιώντας είτε το διαδικτυο, είτε το τοπικό δίκτυο. Αν για κάποιο λόγο δεν δουλεύουν, τότε χρηστές από άλλες χώρες δεν μπορούν να χρησιμοποιήσουν τις υπηρεσίες του ηλεκτρονικού καταστήματος, αλλά ούτε να δουν τα προϊόντα του.

1.4.3 *Modems*

Τα modems χρησιμοποιούνται για την σύνδεση με το διαδίκτυο και για την διατήρηση της σύνδεσης ολόκληρο το 24ωρο.

1.4.4 *Firewalls (Πυρότειχα Προστασίας)*

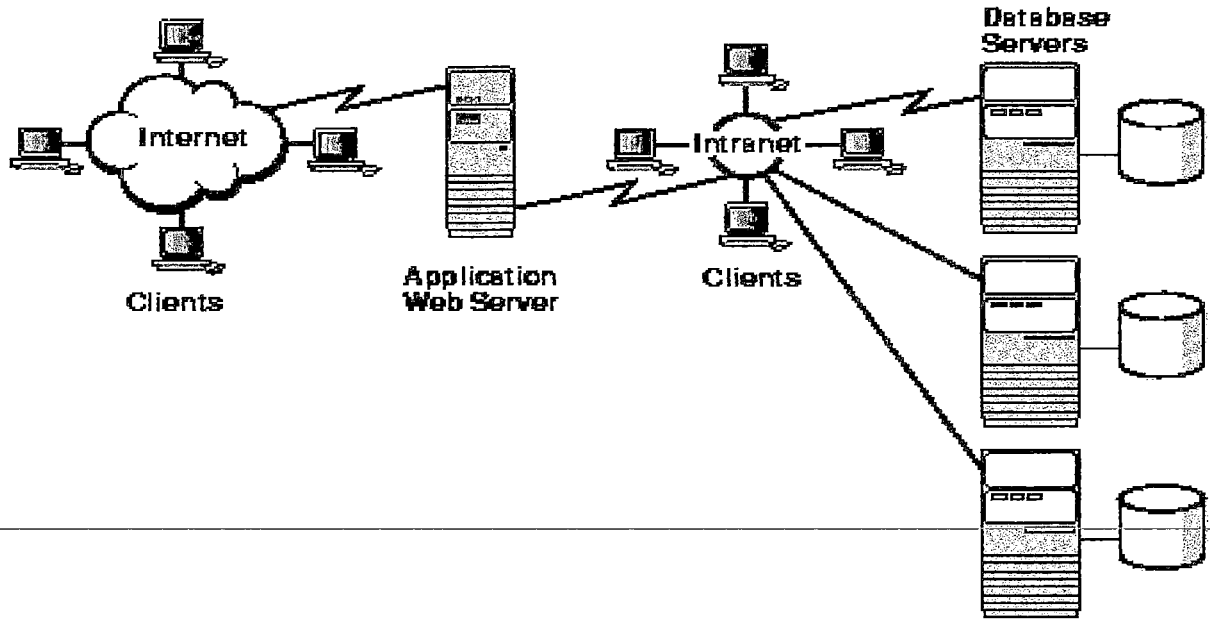
Τα firewalls είναι υπεύθυνα για την προστασία του ηλεκτρονικού καταστήματος από μη εξουσιοδοτημένους χρήστες (Χακερς), και παράνομων προγραμμάτων τα οποία έχουν σκοπό την συλλογή πληροφοριών από το ηλεκτρονικό κατάστημα ή την συλλογή των προσωπικών στοιχείων που έχει εμπιστευτεί ο πελάτης. Τα firewalls μπορούμε να τα βρούμε σε 2 μορφές:

1. Σε υλικό, δηλαδή ενώνονται με τα άλλα μηχανήματα και φιλτράρουν την εισαγωγή και εξαγωγή των δεδομένων. Αυτά είναι πιο αξιόπιστα και προσφέρουν καλύτερη προστασία, αλλά είναι πιο ακριβά.
2. Σε λογισμικό, δηλαδή υπάρχουν εγκατεστημένα σε ένα ή και περισσότερα μηχανήματα και φιλτράρουν την εισαγωγή και εξαγωγή των δεδομένων.

1.4.5 *PCs*

Είναι ηλεκτρονικοί υπολογιστές (Η/Υ) οι οποίοι έχουν ένα λειτουργικό σύστημα (windows, linux, ...) και ίσως κάποιες εφαρμογές που θέλει το κατάστημα και τα χειρίζονται οι υπεύθυνοι του καταστήματος για να παίρνουν τα χρήματα ή να επικυρώνουν τις παραγγελίες.

Το παρακάτω σχήμα μας δείχνει πως μπορούν να συνδυαστούν τα παραπάνω μηχανήματα για έχουμε ένα ηλεκτρονικό κατάστημα. Δεν είναι απαραίτητο να χρησιμοποιηθούν όλα τα παραπάνω που αναφέραμε, αν και το σωστό θα ήταν να χρησιμοποιηθούν.



Ένα ηλεκτρονικό κατάστημα σχηματικά

Έχοντας καταλάβει πως είναι δομημένο ένα ηλεκτρονικό κατάστημα από την φυσική μεριά, με ποια μηχανήματα μπορούμε να χρησιμοποιήσουμε, το μόνο που μένει είναι να γράψουμε κώδικα για το περιβάλλον διεπαφής, και για την διασφάλιση των συναλλαγών. Στο κεφάλαιο που ακολουθεί θα δούμε πως είναι δομημένο από την ψηφιακή μεριά και πως μπορούμε να ελέγξουμε την δομή και την ποιότητα του κώδικα μας.

ΚΕΦΑΛΑΙΟ 2^{ο} :

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΔΟΜΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΚΑΤΑΣΤΗΜΑΤΟΣ

2.1 Εισαγωγή

Στο κεφάλαιο 1 είδαμε πως πρέπει να είναι δομημένο ένα ηλεκτρονικό κατάστημα από την φυσική μεριά (Servers, Switch, Firewalls,...). Στην συνέχεια θα μελετήσουμε την δομή (κώδικας) ενός ηλεκτρονικού καταστήματος και με τι τρόπο πρέπει να είναι δομημένο έτσι ώστε να ελαχιστοποιεί τους κινδύνους του διαδικτύου και να προστατεύει όσο το δυνατόν πιο καλά τα προσωπικά δεδομένα του χρήστη.

Με τον όρο «δομή» ενός ηλεκτρονικού καταστήματος εννοούμε τον κώδικα, ποιες γλώσσες προγραμματισμού χρησιμοποιήθηκαν για την κατασκευή του ηλεκτρονικού καταστήματος. Οι ποιο συνηθισμένες γλώσσες προγραμματισμού για την κατασκευή ενός ηλεκτρονικού καταστήματος είναι: «PHP, JAVA, MYSQL, XML, C, C++, PERL, HTML, CSS». Τα style sheet χρησιμοποιούνται για να δίνουν στυλ και έμφαση στις σελίδες μας. Όμως με την χρήση της XML σε διάφορα σημεία προσφέρει μια μικρή αλλά σημαντική προστασία των δεδομένων μας (Παρακάτω αναλύεται καλύτερα το σημείο αυτό). Πριν συνεχίσουμε σε οποιαδήποτε ανάλυση καλό είναι να αναφέρουμε τους ορισμούς «ποιότητα», «λογισμικό», «ποιότητα λογισμικού». Έχοντας κατανοήσει τους παραπάνω ορισμούς θα μπορέσουμε να καταλάβουμε πως μπορούν και αλλάζουν τις ιστοσελίδες ο επιτιθέμενος ώστε να έχει τα επιθυμητά αποτελέσματα. (κλοπή προσωπικών δεδομένων, κλοπή αριθμών πιστωτικών καρτών, conflict μεταξύ πελάτη και εξυπηρετητή,...)

2.2 Ποιότητα

Όμως για να μπορέσουμε να βεβαιώσουμε για την ασφάλεια που παρέχει ο δικτυακός τόπος που θα κινηθεί ο πελάτης πρέπει να τηρούν ,τα ηλεκτρονικά καταστήματα, κάποιες συγκεκριμένες προδιαγραφές (ISO). Την ποιότητα μπορούμε να την ορίσουμε ως εξής: «**Η ποιότητα τόσο στα αγαθά, όσο και στις υπηρεσίες επιτυγχάνεται στο μέγιστο βαθμό όταν τηρούνται οι προδιαγραφές που έχουν οριστεί από αρμόδιες υπηρεσίες.**» Ο ορισμός αυτός είναι απλός και κατανοητός από τον απλό χρήστη. Για τα ηλεκτρονικά καταστήματα έχουν οριστεί προδιαγραφές (ISO 9001:2000 είναι κάποια από τα πρότυπα που υπάρχουν στον τομέα του ηλεκτρονικού εμπορίου) με σκοπό την ασφαλέστερη προστασία των προσωπικών δεδομένων του πελάτη. Τα ISO εφαρμόζονται τόσο στο υλικό μέρος, όσο και στο λογισμικό μέρος.

Τα ISO είναι κάποια standards (πρότυπα) τα οποία ορίζουν πως πρέπει να είναι δομημένα κάποια μέρη της επιχείρησης ή και ολόκληρη η επιχείρηση. Αυτό εξαρτάται από το τι υπηρεσίες ή προϊόντα προσφέρει. Σε περίπτωση που δεν ακολουθήσει τα ISO το κατάστημα τότε είναι εκτεθειμένο σε όλους τους κινδύνους

που το απειλούν. Υπάρχει και η περίπτωση να τροποποιηθεί κάποιος κανόνας του ISO προκειμένου το ηλεκτρονικό κατάστημα να μπορέσει να ανταποκριθεί στις ελάχιστες απαιτήσεις που έχει θέσει, αλλά και να έχει ένα κύρος όσο αφορά την ασφάλεια των συναλλαγών.

Κάποια πρότυπα όσο αφορά την πληρωμή μέσο των ηλεκτρονικών καταστημάτων είναι τα εξής:

- ISO TC68
- CEN/ISSS WS/EC electronic wallet project
- ETSI Project SCP

,ενώ για την ασφάλεια των προσωπικών δεδομένων είναι τα εξής:

- ISO/COPOLCO proposals
- Canadian Standards Association
- IPSE

2.3 Λογισμικό

Ο Η/Υ από μόνος του δεν μπορεί να λειτουργήσει αν κάποιος δεν του πει τι πρέπει να κάνει. Για να μπορεί ο Η/Υ να στέλνει μηνύματα και να δέχεται εντολές αναπτύχθηκε ένα περιβάλλον διεπαφής μεταξύ του Η/Υ και του χρήστη και το οποίο ονομάστηκε **λογισμικό.**

Ένας άλλος πιο απλός ορισμός για το τι είναι λογισμικό μπορούμε να ορίσουμε το παρακάτω: **"όλα τα προγράμματα που χρησιμοποιεί ο Η/Υ, τα οποία μπορεί να είναι πολύ σύνθετα (Λειτουργικά Συστήματα) μέχρι πολύ απλά (Σημειωματάριο)"**.

2.4 Ασφάλεια στο Λογισμικό

Για να φτιαχτεί ένα ηλεκτρονικό κατάστημα υπάρχουν πολλοί τρόποι και προγράμματα τα οποία φτιάχνουν αμέσως ένα ηλεκτρονικό κατάστημα. Το μόνο που έχει να κάνει ο χρήστης είναι να δώσει το κείμενο και τις φωτογραφίες που θέλει να έχει η κάθε σελίδα. Τα υπόλοιπα αναλαμβάνει να τα κάνει το πρόγραμμα.
Ένας άλλος τρόπος είναι να φτιαχτεί ένα ηλεκτρονικό κατάστημα από προγραμματιστή, όπου σε αυτή την περίπτωση θα δημιουργήσουν αυτοί τον κώδικα από την αρχή μέχρι το τέλος.

Σε περίπτωση που κάποιος αποφασίσει να φτιάξει ένα ηλεκτρονικό κατάστημα και χρησιμοποιήσει κάποια από τα ειδικά προγράμματα που κυκλοφορούν στην αγορά , όταν θελήσει να του κάνει κάποια συντήρηση ή να το αναβαθμίσει ή να διορθώσει κάποια λάθη που είδε είναι αρκετά δύσκολο. Η δυσκολία βρίσκεται στο σημείο που δημιουργείται ο κώδικας αφού το πρόγραμμα το φτιάχνει με ένα τρόπο δυσνόητο και όχι τόσο κατανοητό ακόμη και σε έμπειρους προγραμματιστές. Ένα άλλο μειονέκτημα είναι ότι εκτός δεν μπορεί να αναβαθμιστεί εύκολα ο ιδιοκτήτης του ηλεκτρονικού καταστήματος πρέπει να πληρώσει για μπορέσει να υποστηρίζει το ηλεκτρονικό κατάστημα :

1. πιστωτικές κάρτες,
2. έξυπνες κάρτες,
3. κάρτες προπληρωμένου χρόνου ομιλίας,
4. βάσεις δεδομένων,

και άλλα βασικά στοιχεία που χρειάζονται για δουλέψει σωστά το ηλεκτρονικό κατάστημα και φυσικά να μπορεί να ικανοποιεί όλες τις απαιτήσεις του πελάτη.

Σε περίπτωση που δημιουργηθεί από προγραμματιστή τότε κάποια πράματα είναι πιο εύκολα όπως η συντήρηση του, η αναβάθμιση, κλπ. Το μόνο αρνητικό είναι ότι έχει μεγάλο κόστος προκειμένου να γίνει όπως το θέλει ο πελάτης και σωστά.

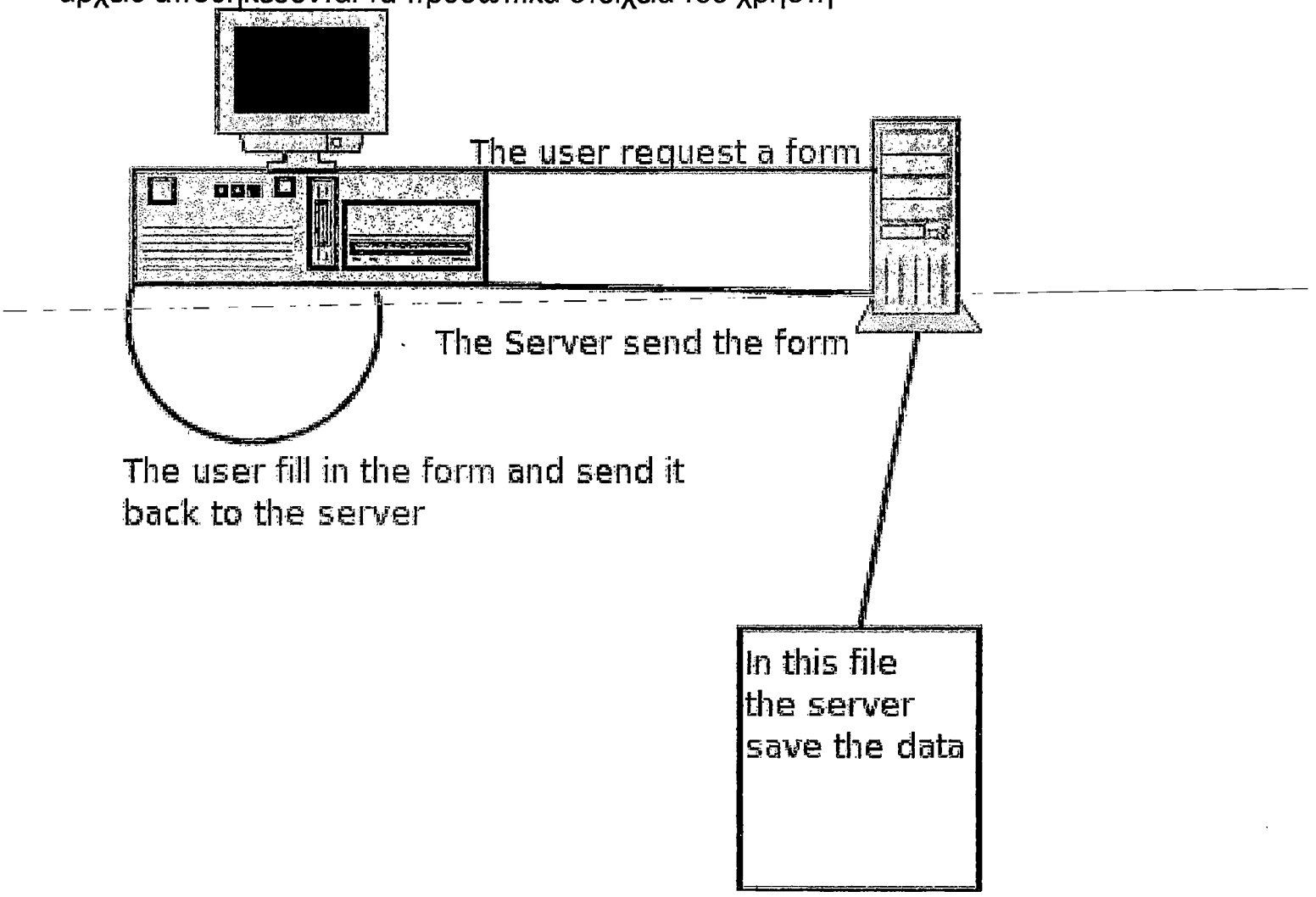
2.4.1 *Επιθέσεις στις σελίδες των ηλεκτρονικών καταστημάτων*

Όλες οι σελίδες των ηλεκτρονικών καταστημάτων βρίσκονται σε ένα Η/Υ που έχει κάποιο λειτουργικό Windows ή Unix, ένα web server IIS, Apache αντίστοιχα, αλλά μπορεί να είναι εγκατεστημένος ο Apache στα Windows. Για να μπορέσει να δει το ηλεκτρονικό κατάστημα κάποιο πελάτης θα πρέπει να έχουν αφήσει το port 8080 ανοιχτό και κάποιες φορές το port 33016 για την MySQL.

Όταν ένας hacker αποφασίσει να κλέψει τα προσωπικά δεδομένα ενός χρήστη πρώτα θα δοκιμάσει να επιτεθεί στην ιστοσελίδα που επισκέπτεται ο χρήστης και συνήθως συνδέεται με μια βάση δεδομένων. Πριν όμως κάνει οποιαδήποτε κίνηση θα πρέπει να κάνει μια μικρή έρευνα για να μπορέσει να βρει τι λειτουργικό σύστημα χρησιμοποιεί ποιες πόρτες είναι ανοιχτές, και αν μπορεί να χρησιμοποιήσει κάποια exploits ή worms, ή virus, ή Trojans. Τα προγράμματα αυτά είναι απαραίτητα για μπορέσει να συνδεθεί στον server ώστε να μπορέσει να «κατεβάσει» τις σελίδες που στέλνουν τα προσωπικά στοιχεία για να τις συναλλαγές. Έτσι τροποποιώντας την σελίδα αυτή μπορεί να κάνει redirect (ανακατεύθυνση) των δεδομένων από το κανονικό αρχείο σε κάποιο άλλο αρχείο που βρίσκεται μέσα στο σύστημα και είναι εύκολα προσβάσιμο.

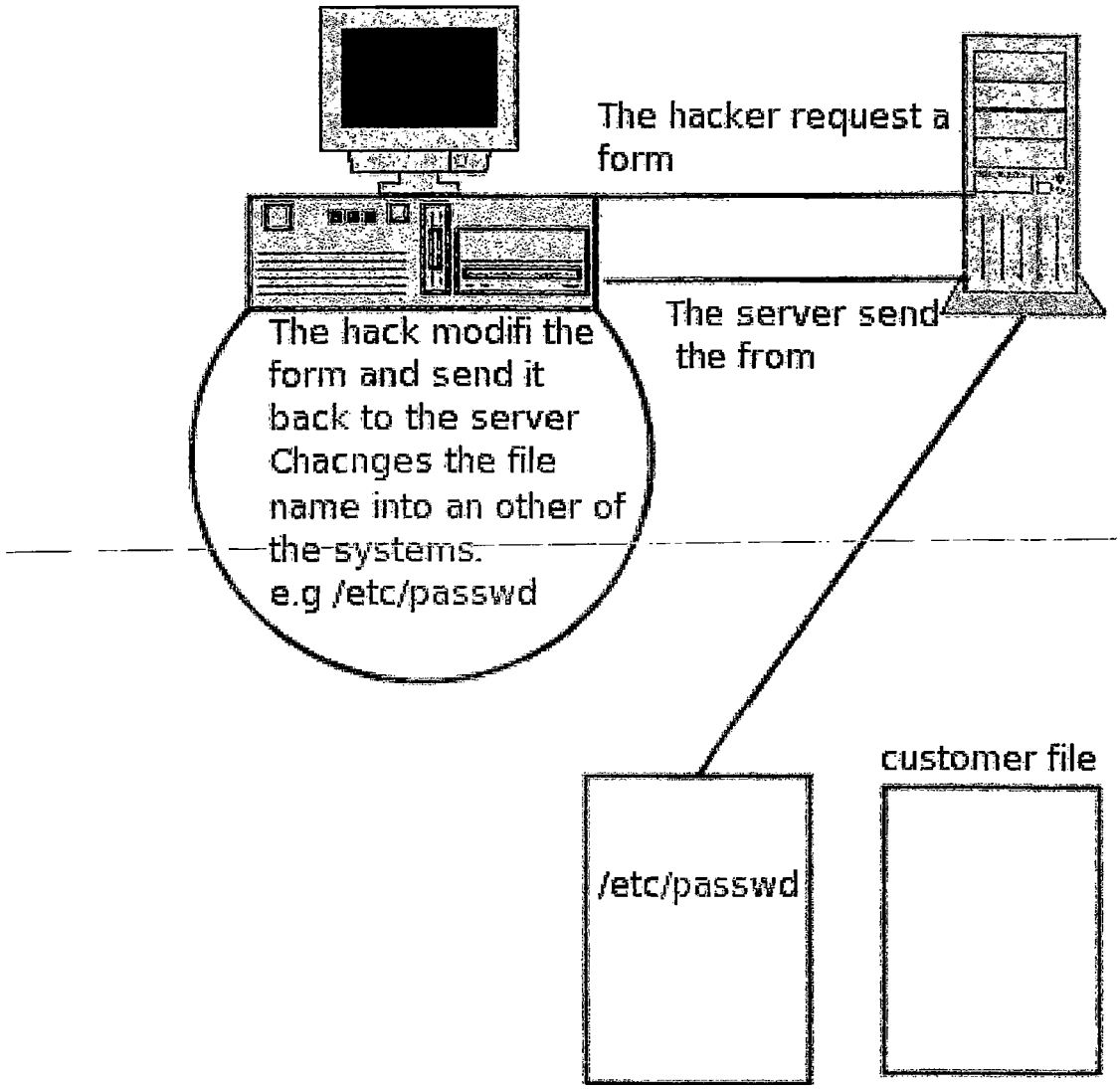
Έτσι όταν συνδεθεί ο χρήστης και πληκτρολογήσει το ***όνομα χρήστη*** και *τον* ***κωδικό πρόσβασης*** αυτόματα θα δημιουργηθεί ένα αντίγραφο σε ένα άλλο αρχείο το οποίο θα σταλθεί στον hacker. Αυτό επιτυγχάνεται με την εντολή: *telnet ip ή address 80.* Ο hacker κάνει απομακρυσμένη σύνδεση μέσο **telnet** στην **ip** ή

στην **address** που έχει ορίσει στην **port 80** με αποτέλεσμα να εμφανίσει στην οθόνη τον κώδικα της κεντρικής ή της εισαγωγικής ιστοσελίδας. Εφ΄ όσον έχει τον κώδικα στην διάθεση του τον τροποποιεί ανάλογα με τον τρόπο που θέλει να κλέψει τις προσωπικές πληροφορίες του χρήστη. Στο παρακάτω σχήμα βλέπουμε σε ποιο αρχείο αποθηκεύονται τα προσωπικά στοιχεία του χρήστη



Σχήμα 1: Η διαδικασία που ακολουθείτε για να σταλθούν τα στοιχεία από μια φόρμα που έχει συμπληρώσει ο χρήστης πριν από την επίθεση ενός hacker.

Ενώ στο επόμενο σχήμα βλέπουμε σε ποιο αρχείο στέλνονται τα στοιχεία του χρήστη ύστερα από την παρέμβαση ενός hacker στον κώδικα της ιστοσελίδας.



Σχήμα 2: Ο επιτιθέμενος έχει τροποποιήσει την φόρμα έτσι ώστε τα δεδομένα τις φόρμας να αποθηκεύονται σε αρχείο του συστήματος (το οποίο είναι γνωστό σε όλους) που έχει ορίσει και μπορεί να το πάρει εύκολα.

Σε καμία περίπτωση ένας hacker δεν προσπαθεί να «σπάσει» κωδικούς πρόσβασης που βρίσκονται στο αρχείο /etc/passwd, γιατί σε κάθε αποτυχημένη προσπάθεια καταγράφεται σε log αρχείο και στέλνεται ένα e-mail στον διαχειριστή του συστήματος. Αυτό που μπορεί να κάνει είναι να αντιγράψει το αρχείο αυτό σε ένα άλλο με διαφορετικό όνομα π.χ. passwd.1 ή mitsos.rd και να σπάσει τους κωδικούς με την ησυχία του χωρίς να γίνει αντιληπτό από κανένα.

Επομένως είναι πολύ σημαντικό να υπάρχει ασφάλεια και στον κώδικα με τον οποίο έχει φτιαχτεί ένα ηλεκτρονικό κατάστημα για μην μπορέσει να βρει και να καταλάβει εύκολα τον κώδικα για να τον τροποποιήσει.

2.5 Γλώσσες Προγραμματισμού για το ηλεκτρονικό εμπόριο

2.5.1 XML για το ηλεκτρονικό εμπόριο

Τα τελευταία χρόνια η γλώσσα που χρησιμοποιείται για την ανάκτηση πληροφοριών και η ανταλλαγή δεδομένων στα ηλεκτρονικά καταστήματα είναι η Extensible Markup Language (XML). Η XML χρησιμοποιείται πολύ τα τελευταία χρόνια για εφαρμογές web, αλλά και για τα ηλεκτρονικά καταστήματα.

Η XML διαφέρει από την HTML. Η διαφορά τους είναι στην χρήση των tags που χρησιμοποιεί η κάθε γλώσσα. Στην HTML τα tags χρησιμεύουν για να δίνουν οδηγίες για το πώς θα εμφανίζεται η ιστοσελίδα από τον φυλλομετρητή (browser) ,αντίθετα με την XML η οποία προσδιορίζει τα tags και τον τύπο των δεδομένων που περιέχει ο κώδικας. Έτσι λοιπόν θα μπορούσαμε να πούμε ότι η XML είναι περισσότερο μια γλώσσα **προγραμματισμού, παρά μια γλώσσα περιγραφής σελίδων του διαδικτύου**.
Για παράδειγμα το tag <postcode> θα μπορούσε να προσδιορίζει ότι ο αριθμός που ακολουθεί είναι ο ταχυδρομικός κώδικας και όχι ένας απλός αριθμός, ενώ το tag <surname> ότι η επόμενη λέξη που ακολουθεί είναι το επίθετο κάποιου πελάτη κ.α. Τα tags στην XML δεν είναι standard με αποτέλεσμα η κάθε εταιρεία να μπορεί να τα αλλάζει και να ορίζει τα δικά της tags.

Η ανταλλαγή δεδομένων μέχρι τώρα απαιτούσε αρκετές ώρες εργασίας και διάφορες εφαρμογές προκειμένου να γίνει σωστά η ανταλλαγή των δεδομένων. Η XML έρχεται να κάνει την διαδικασία αυτή ζήτημα λεπτών και εγγυάται για την ασφαλή μεταφορά των δεδομένων ανεξάρτητα από τον αριθμό των χρηστών.
Η XML έχει προεκταθεί και έχει δημιουργηθεί η ebXML (electronic business XML) η οποία χρησιμοποιείται για την δημιουργία και μόνο ηλεκτρονικών καταστημάτων. Για την συγκεκριμένη γλώσσα έχουν εγκριθεί 4 διαφορετικά ISO

- ISO 15000-1: ebXML Collaborative Partner Profile Agreement
- ISO 15000-2: ebXML Messaging Service Specification
- ISO 15000-3: ebXML Registry Information Model
- ISO 15000-4: ebXML Registry Services Specification

2.5.2 ebXML

Η δημιουργία αυτής της γλώσσας έγινε για γρηγορότερη και καλύτερη ανταλλαγή δεδομένων και στόχος είναι να αντικαταστήσει το EDI το οποίο χρησιμοποιείται

μέχρι σήμερα. «Πολλές από τις επιχειρήσεις, εξηγεί ο οργανισμός OASIS που ενέκρινε τα ISO, βρίσκουν το EDI πολύ ακριβό και δύσκολο όσο αφορά την διαχείριση.» Η ebXML προτείνει μια standard μέθοδο για την ανταλλαγή μηνυμάτων μεταξύ των επιχειρήσεων, να συνάπτουν επιχειρηματικές σχέσεις, η επικοινωνία και η ανταλλαγή δεδομένων να γίνεται από κοινά τερματικά, και να γίνεται προσδιορισμός και κατοχύρωση των επιχειρηματικών διαδικασιών.

Σκοπεύει να φτιάξει ένα εύκολο περιβάλλον διεπαφής για τους οργανισμούς ώστε να είναι δυνατό το άνοιγμα καινούριων αγορών με το μικρότερο δυνατό κόστος. Εφαρμόζοντας τα ISO αυτά ένα ηλεκτρονικό κατάστημα B2C μπορεί να κερδίσει την εμπιστοσύνη του πελάτη μια που οι συναλλαγές του θα είναι διασφαλισμένες από ένα έμπιστο οργανισμό (OASIS). Άλλωστε εφαρμόζοντας μια καινούρια μέθοδο οι γνωστές επιθέσεις από τους hackers δεν θα έχουν το ίδιο αποτέλεσμα, και δίνεται η δυνατότητα να δοκιμαστούν οι μέθοδοι αυτοί.

Η XML και η ebXML δεν είναι η μόνες γλώσσες στις οποίες μπορεί να φτιαχτεί ένα ηλεκτρονικό κατάστημα, αλλά μπορούν να χρησιμοποιηθούν και άλλες όπως η JAVA, PHP, C/C++, κλπ. και σε συνδιασμό με τις XML και ebXML να δώσουν καλύτερα αποτελέσματα. Ποια γλώσσα προγραμματισμού θα χρησιμοποιηθεί εξαρτάται από τον υπεύθυνο του ηλεκτρονικού καταστήματος.

2.6 *Ανίχνευση κρίσιμων σημείων στο λειτουργικό σύστημα*

2.6.1 Εισαγωγή

Για να μπορέσει να εισβάλει ένας hacker σε ένα ηλεκτρονικό κατάστημα θα πρέπει να γνωρίζει το λειτουργικό σύστημα που χρησιμοποιεί το ηλεκτρονικό κατάστημα, γνωρίζοντας τις ανοιχτές πόρτες που έχει φτιάχνει το κατάλληλο exploit και αυτόματα έχει root access στο σύστημα ή στην βάση δεδομένων του συστήματος. Ποιες πόρτες είναι ανοιχτές και τι λειτουργικό χρησιμοποιεί μπορεί να το μάθει χρησιμοποιώντας το Nmap το οποίο κάνει τις παραπάνω λειτουργίες και πολλές άλλες ακόμη. [Για περισσότερες πληροφορίες πηγαίνετε στο manual του Linux]. Αυτά τα κρίσιμα σημεία μπορεί να τα μάθει και να τα διορθώσει ο διαχειριστής του ηλεκτρονικού καταστήματος αν του τα πει κάποιος ή κάνει ο ίδιος μια προσομοίωση των γνωστότερων επιθέσεων, η οποία θα του αποκαλύψει τα αδύναμα σημεία.

2.6.2 *Nessus*

Το nessus είναι πρόγραμμα το οποίο κάνει αυτή την δουλεία, δηλαδή βρίσκει τα αδύνατα σημεία ενός λειτουργικού συστήματος, βάσεων δεδομένων, και ενημερώνει τον διαχειριστή για τα αποτελέσματα. Σε αυτό το σημείο πρέπει να θυμίσω ότι αδύνατα σημεία δεν έχουν ΜΟΝΟ τα Windows, αλλά έχουν και το Linux και το Unix.

Αφού γίνει σωστή εγκατάσταση του nessus στο λειτουργικό σύστημα που επιθυμούμε, πρέπει να του πούμε που να κοιτάξει για να εντοπίσει αδυναμίες ή τρύπες, που θα έδιναν πρόσβαση σε μη εξουσιοδοτημένα άτομα. Μπορεί ο

διαχειριστής αν το θέλει να χρησιμοποιήσει και το nmap για να έχει καλύτερα αποτελέσματα, καθώς και άλλες επιλογές όπως RPC Scanning, null connection, κλπ. Ας το δούμε αυτό όμως καλύτερα με ένα παράδειγμα.

Γνωρίζοντας ότι όλα τα λειτουργικά συστήματα έχουν αδυναμίες αποφάσισα να δω αν και το δικό μου λειτουργικό σύστημα έχει αδυναμίες και αν έχει πόσο σοβαρές είναι και πού ώστε να τις αντιμετωπίσω. Λαμβάνοντας υπ' όψιν ότι χρησιμοποιώ Linux με την τελευταία έκδοση του πυρήνα θεωρώ ότι οι περισσότερες αδυναμίες του Linux θα έχουν βρεθεί και θα έχουν διορθωθεί.

Τεστάροντας το σύστημα

Εκτελώ σαν απλός χρήστης το nessus από την γραμμή εντολών, κάνω login (όπως του είχα πει κατά την εγκατάσταση) και στην συνέχει του δηλώνω που θα κάνει ανίχνευση. Επειδή θέλω να γίνει στον δικό μου υπολογιστή στο πεδίο *host* βάζω *localhost* και ξεκινάω την ανίχνευση.
Στην αρχή το nessus κάνει ένα πέρασμα για να βρει ποιες πόρτες είναι ανοιχτές, και από ποία προγράμματα χρησιμοποιούνται. Στο δεύτερο πέρασμα κάνει μια προσομοίωση επιθέσεων στο σύστημα και παίρνει τα αντίστοιχα αποτελέσματα. Σε καμία περίπτωση δεν κάνει χρησιμοποιεί plug-in τα οποία θα προκαλέσουν πρόβλημα στο σύστημα με αποτέλεσμα την κατάρρευση του.

Αποτελέσματα

Από τα αποτελέσματα βρήκα δυο μόνο κρίσιμα σημεία τα οποία μπορούσαν να δώσουν πρόσβαση σε hackers και τα υπόλοιπα ήταν προειδοποιητικά μηνύματα. Στο port 443/tcp το οποίο χρησιμοποιείται από το https:// (το " **s** " στο τέλος σημαίνει ότι χρησιμοποιεί το πρωτόκολλο ασφαλείας SSL) βρέθηκε ένα *security warning* το οποίο είναι:

Warning found on port https (443/tcp)
It seems that your web server tries to hide its version
or name, which is a good thing.
However, using a special crafted request, Nessus was able
to determine that is running :
Apache/2.0.50 (Fedora)

Risk factor : None
Solution : Fix your configuration.

. Information found on port https (443/tcp)

A SSLv2 server answered on this port

και το δεύτερο στο port 3306/tcp για την βάση δεδομένων MySQL το οποίο αναφέρει:

Vulnerability found on port mysql (3306/tcp) :

Your MySQL database is not password protected.

Anyone can connect to it and do whatever he wants to your data (deleting a database, adding bogus entries, ...)
We could collect the list of databases installed on the remote host :

. mysql
. phones
. rpm_list
. test

Solution : Log into this host, and set a password for the root user through the command 'mysqladmin -u root password <newpassword>'
Read the MySQL manual (available on www.mysql.com) for details.
In addition to this, it is not recommended that you let your MySQL daemon listen to request from anywhere in the world. You should filter incoming connections to this port.

Risk factor : High

. Vulnerability found on port mysql (3306/tcp) :

It is possible to login to your MySQL database using a null-password by crafting a special packet.
In a typical attack scenario where a specific DB user has remote login access, an attacker needs
only to compile a slightly modified version of the MySQL client program in order to automatically
gain that user's access to the database
BID : 10654

Συγκεκριμένα για την βάση δεδομένων μου έβγαλε ποιες βάσεις έχω δημιουργήσει, και πως μπορεί ένας hacker με την χρήση ενός exploit να πάρει null session access, δηλαδή να μπορεί να δει ΟΛΑ τα αποτελέσματα από ΟΛΕΣ τις βάσεις δεδομένων χωρίς να χρειαστεί να πληκτρολογήσει *USERNAME*, *PASSWORD* !!! Η λύση που μου έδινε το nessus και είναι η μόνη αποδεκτή είναι να βάλω root password ώστε να μην μπορεί να κάνει null session και να φιλτράρω την κίνηση στο συγκεκριμένο port και να τρέχω τον δαίμονα μόνο όταν χρειάζεται.

Στην περίπτωση του https πρέπει να φτιάξω το configuration file και να ορίσω ciphers ώστε να μπορεί να αντέξει στην επίθεση *Brute Force Attack.*

Όπως διαπιστώνουμε σε κάθε port βγάζει αναφορές ασφαλείας και όπου βρίσκει τρύπες «bugs» αναφέρει την λύση και πως μπορεί να πάρει πρόσβασή στο μηχάνημα.

Συμπεράσματα

Τα συμπεράσματα από αυτή την μικρή, αλλά διαφωτιστική έρευνα είναι ότι σε περίπτωση που είχα ένα ηλεκτρονικό κατάστημα και δούλευα το μηχάνημα σαν server για να μπορεί να βγαίνει στο internet, τότε θα πρόσφερα απλόχερα στους hackers τα προσωπικά στοιχεία των πελατών μου αφού θα μπορούσαν να μπουν χωρίς να γίνουν αντιληπτοί από κανένα αφού μπορούν να μπουν στην βάση δεδομένων που επιθυμούν, αλλά και να συνδεθούν στον υπολογιστή μου σαν χρήστες του συστήματος χωρίς να υπάρχουν. Το αποτέλεσμα είναι ότι θα μάζευαν περισσότερες πληροφορίες για το πως δουλεύει το ηλεκτρονικό κατάστημα, αλλά θα μπορούσαν να άλλαζαν τον κώδικα για να εξυπηρετήσουν δικούς τους σκοπούς.

Εκτός από τα προσωπικά στοιχεία των πελατών εκτίθεται και το ηλεκτρονικό κατάστημα, και πλέων παύει να είναι αξιόπιστο στους πελάτες, γιατί μπορεί να δουν τον αριθμό της πιστωτικής κάρτας του υπερχρεωμένη από τους hackers. Αν το πρόβλημα αντιμετωπιστεί πριν γίνει οτιδήποτε τότε δεν υπάρχει κανένας φόβος, αλλά αν προσπαθήσουν να το αντιμετωπίσουν αφού έχουν δεχτεί επίθεση τότε τα πράματα είναι πιο σοβαρά αφού θα πρέπει να ελεγχθεί και η ακεραιότητα της ιστοσελίδας του, αν έχουν τοποθετήσει Trojans, worms, γενικά αν έχουν παραμετροποιήση το σύστημα για να μπορούν να έχουν πρόσβαση και αυτοί εκτός από τον διαχειριστή.

2.7 *Ανίχνευση κρίσιμων σημείων στην δομή του κώδικα*

Όταν αναλαμβάνει ένας προγραμματιστής να φτιάξει ένα ηλεκτρονικό κατάστημα θα πρέπει να το παραδώσει τέλειο στον πελάτη του, χωρίς το παραμικρό λάθος το οποίο θα προκαλέσει ζημία στο ηλεκτρονικό κατάστημα. Για την ανίχνευση τέτοιων λαθών χρησιμοποιούνται γλώσσες προγραμματισμού από την μεριά του εξυπηρετητή (Server Side Programming όπως είναι πιο γνωστό) για να μην μπορεί να είναι ορατός ο κώδικας στον οποιοδήποτε.

Η ανίχνευση των ατελειών του κώδικα γίνεται με το debugging. Το debugging προσδιορίζει σε πιο σημείο μπορεί να δημιουργήσει πρόβλημα στην ομαλή λειτουργία του κώδικα. Αυτές οι ατέλειες μπορούν να καλυφθούν με δυο τρόπους:

1. αλλάζοντας το συγκεκριμένο σημείο ξαναγράφοντας περισσότερες ή λιγότερες γραμμές κώδικα, (π.χ. το ***if (expression){ commands } else if (expression) {***

commands } else { commands } να αντικατασταθεί από το ***switch(variable){ case: result_of_variable { commands } break;.....default: "Message"***)

2. γράφοντας κάποιες γραμμές κώδικα σε μια άλλη γλώσσα προγραμματισμού για να καλύψει το συγκεκριμένο αδύνατο σημείο. (π.χ. αν φτιάχνουμε σε **PHP** μια ιστοσελίδα και βρούμε μια ατέλεια, τότε μπορούμε να καλύψουμε την ατέλεια αυτή γράφοντας κώδικα σε **C**, και πάλι compile, debugging μέχρι να καλυφθούν όλα τα κρίσιμα σημεία του κώδικα.)

Ο λόγος που κάνουμε κάτι τέτοιο είναι για να δυσκολέψουμε την παραποίηση του κώδικα από hacker που έχουν μπει στο σύστημα μας, αλλά δεν μπορούν να βρουν και πάρουν τα προσωπικά στοιχεία των πελατών μας. Επίσης μας δίνεται η δυνατότητα με αυτό τον τρόπο να κάνουμε πιο αποτελεσματική και λειτουργική την ιστοσελίδα. Για να μπορέσουμε να πούμε με επιτυχία ότι έγινε σωστά και ο κώδικας δεν θα δημιουργήσει στον χρήστη κάποιο πρόβλημα κατά την περιήγηση του στο ηλεκτρονικό κατάστημα, θα πρέπει να έχουμε μηδενίσει τα κρίσιμα σημεία.

Ένα άλλο εργαλείο πολύ χρήσιμο για την ασφάλεια του λογισμικού τόσο για το λειτουργικό σύστημα όσο και για το ηλεκτρονικό κατάστημα είναι το ***tripwire.***

2.7.1 Tripwire

Το ***tripwire*** δουλεύει σε λειτουργικά συστήματα Unix και ελέγχει τα αρχεία του λειτουργικού συστήματος καθώς και την βάση δεδομένων και αν χρειαστεί βγάζει μια αναφορά για αναβάθμιση ή όχι της βάσης δεδομένων. Το συγκεκριμένο πρόγραμμα μπορεί να το τρέξει μόνο ο διαχειριστής ώστε να μπορεί να έχει μια πλήρη εικόνα για το πώς είναι το σύστημα του, αν έχουν πειραχτεί ή αλλοιωθεί ή αν περιέχουν ιούς. Το μόνο αρχείο που πρέπει να αλλάζει είναι το αρχείο καταγραφείς λαθών (log file) και κανένα άλλο. Στην περίπτωση που κάνοντας τον έλεγχο βρει κάποια αρχεία διαφοροποιημένα τότε σημαίνει ότι κάποιος έχει μπει στο σύστημα και το έχει πειράξεί. Το αποτέλεσμα σε αυτή την περίπτωση είναι να αλλαχθεί το:

1. security policy,
2. να βρεθεί το bug.

Επομένως στην περίπτωση που περιγράφω στην εικόνα 2 ο διαχειριστής του ηλεκτρονικού καταστήματος θα είχε ενημέρωση για αυτή την μη-νόμιμη εκτροπή των προσωπικών στοιχείων των πελατών του και η ζημία περιορίζεται. Για να μπορέσει να γνωρίζει την κατάσταση των αρχείων του πρέπει να εκτελείται το tripwire ανά κάποιο χρονικό διάστημα ελέγχοντας τα αρχεία , αλλά και την βάση δεδομένων. Επίσης δίνει την δυνατότητα να ελέγξει το e-mail που χρησιμοποιεί το ηλεκτρονικό κατάστημα ώστε να μην μπορεί να χρησιμοποιήσει το e-mail του ηλεκτρονικού καταστήματος για να αποσπάσει προσωπικά δεδομένα από τους πελάτες προσποιούμενος ότι είναι ο διαχειριστής. Ένας έμπιστος άνθρωπος δηλαδή.

Μέχρι στιγμής έχουμε αναφέρει με ποια προγράμματα μπορούμε να ελέγξουμε την ποιότητα του λογισμικού και πως μπορεί να επηρεάσει τον πελάτη όταν δεν είναι σωστά

ελεγμένη. Παρόλο που αυτά τα προγράμματα κάνουν αρκετά καλή δουλεία δεν πρέπει να ξεχνάμε τον παράγοντα «άνθρωπο». Αυτό σημαίνει ότι δεν μπορούμε να αρκεστούμε στα αποτελέσματα που βγάζουν τα προγράμματα ,όσο αξιόπιστα και αν είναι, γιατί είναι και αυτά λογισμικό και σίγουρα θα έχουν κάποιες αδυναμίες.

Αυτό που μπορούμε να κάνουμε είναι να αναθέσουμε σε ανθρώπους που έχουν ασχοληθεί με την ασφάλεια, που ξέρουν να παραβιάζουν συστήματα ασφαλείας, να συντηρούν, να ελέγχουν, να προτείνουν λύσεις για να μπορεί να έχει ο πελάτης την μέγιστη ασφάλεια.

Στο επόμενο κεφάλαιο θα αναφερθώ γενικότερα στο τι είναι ασφάλεια, τι είναι ιοί, ποιοι είναι οι χακερς και ποιες οι διαφορές από τους Κρακερς, ποια είναι τα πρότυπα ασφάλειας, κρυπτογραφία.

Κεφάλαιο 3ο:

Ασφάλεια

3.1 Εισαγωγή

Πολλοί από εμάς είτε για λόγους δουλείας, είτε για διασκέδαση, είτε για την αγορά κάποιων προϊόντων, είτε για άλλους λόγους χρησιμοποιούμε το Internet (Διαδίκτυο --Ελληνική Ορολογία --εδώ θα χρησιμοποιούμε το Internet). Τα τελευταία χρόνια το Internet αναπτύσσεται με εκθετικούς ρυθμούς τόσο σε επίπεδο χρηστών, όσο και σε επίπεδο παρεχόμενων υπηρεσιών όπως το ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονικό εμπόριο (e-commerce), η ηλεκτρονική μεταφορά χρημάτων, e-banking, e-services, e-health κτλ. Υπάρχει όντως πρόβλημα ασφάλειας που έχει τρεις βασικές παραμέτρους, τον τελικό χρήστη, γενικά το διαδίκτυο, ειδικότερα τα συστήματα ηλεκτρονικού εμπορίου. Για αυτούς τους λόγους η ανάγκη για καλύτερη και περισσότερη ασφάλεια είναι επιτακτική. Όμως τι είναι ασφάλεια και ποια μέρη του υπολογιστή μας πρέπει να ασφαλίσουμε έτσι ώστε να μπορούμε να αποτρέψουμε στο μέγιστο βαθμό τις κακόβουλες επιθέσεις? Ένας απλός και όχι πλήρης ορισμός για το τι είναι ασφάλεια ενός υπολογιστή θα τον δώσουμε τώρα:

" **Η αποτροπή των επιθέσεων με σκοπό την εκμετάλλευση υπολογιστών καθώς και των πόρων τους τόσο σε επίπεδο software όσο και σε επίπεδο hardware καθώς και η διασφάλιση του λειτουργικού συστήματος και των αρχείων συστήματος.** "

Οι κανόνες για να έχουμε ένα υπολογιστή ασφαλισμένο από κάποιον που θέλει να αλλοιώσει ή να κλέψει τα δεδομένα μας, ισχύουν τόσο σε web συστήματα αλλά και σε συστήματα ηλεκτρονικού εμπορίου, τα οποία είναι διαφορετικά από τα web συστήματα. Η διαφορά μεταξύ των web συστημάτων και των συστημάτων ηλεκτρονικού εμπορίου είναι ότι στα συστήματα ηλεκτρονικού εμπορίου διακινούνται και οι ευαίσθητες πληροφορίες του χρήστη, όπως η πιστωτική του κάρτα ο τραπεζικός λογαριασμός του, το όνομα χρήστη και ο κωδικός πρόσβασης, κλπ.

Στα συστήματα που επιβάλλεται η χρήση της κρυπτογραφίας είναι κυρίως στα συστήματα ηλεκτρονικού εμπορίου (e-commerce system), στα δια-τραπεζικά συστήματα (e-baking) και γενικότερα στα συστήματα όπου διακινούνται ευαίσθητες και προσωπικές πληροφορίες του χρήστη όπως ο αριθμός πιστωτικής κάρτας, ο αριθμός τραπεζικού λογαριασμού, κ.α.

Στο e-baking ο χρήστης μπορεί να μεταφέρει χρήματα, να εξοφλήσει λογαριασμούς, και να κάνει διάφορες συναλλαγές από το σπίτι του, οποιαδήποτε μέρα -ακόμα και Κυριακή - τις αργίες, ολόκληρο το 24ώρο. Η ασφάλεια των συναλλαγών στο e-baking αποτελεί τον μεγαλύτερο πονοκέφαλο των μηχανογράφων και των υπευθύνων στις τράπεζες και σε αυτήν οφείλεται η διστακτικότητα του απλού χρήστη. Για τον λόγο αυτό οι τράπεζες υλοποιούν μια σειρά από ασφαλείς

διαδικασίες όπως η ταυτοποίηση του πελάτη, η κρυπτογράφηση σε υψηλό επίπεδο, και η πιστοποίηση της συναλλαγής με ηλεκτρονικά πιστοποιητικά ή αριθμούς TAN. Το ίδιο ισχύει και στο ηλεκτρονικό εμπόριο αλλά σε μικρότερο βαθμό

3.2 Κατηγορίες Επικίνδυνων Προγραμμάτων

Η κλοπή των πληροφοριών γίνεται είτε με την χρήση των **ατελειών (bugs),** είτε με την χρήση των **cookies,** είτε με την χρήση **ιών (viruses), σκουληκιών (worms), δούρειων ίππων (Trojan horses** ή **Trojans** όπως είναι πιο γνωστά).

- **3.2.1** ***Ιοί (Viruses):*** Οι ιοί είναι προγράμματα μικρά σε μέγεθος, το πολύ μέχρι 2 KB, τα οποία έχουν την δυνατότητα να συνυπάρχουν μέσα σε εκτελέσιμα αρχεία ή άλλα αρχεία. Οι ιοί μπορούν να βρίσκονται στην μνήμη του υπολογιστή ή και στην Κ.Μ.Ε. (Κεντρική Μονάδα Επεξεργασίας). Ο ιός ενεργοποιείται με την ενεργοποίηση ενός συγκεκριμένου γεγονότος που έχει καθοριστεί από τον κατασκευαστή. Οι ιοί χωρίζονται σε 4 βασικές κατηγορίες:

  3.2.1.1: 1η Ιοί Εκκίνησης (Bootstrap Viruses): οι οποίοι ενεργοποιούνται κατά την διαδικασία εκκίνησης του υπολογιστή, πράμα που τους κάνει σχεδόν αόρατους από το antivirus. Αν και σήμερα όλα τα antivirus ελέγχουν το boot sector για ιούς.

  3.2.1.2: 2η Παρασιτικοί Ιοί (Parasitic Viruses): είναι οι ιοί οι οποίοι προσαρτώνται σε εκτελέσιμα προγράμματα. Αυτό έχει σαν αποτέλεσμα ο ιός να εκτελείται όταν εκτελείται το πρόγραμμα στο οποίο έχει αντιγράψει τον κώδικα του.

  3.2.1.3: 3η Συνοδευτικοί Ιοί (Companion Viruses): εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στη διαδρομή αναζήτησης κανονικών προγραμμάτων.

  3.2.1.4: 4η Ιοί Μακροεντολών (Macro Viruses): είναι τμήματα κώδικα τα οποία εισάγονται σε αρχεία δεδομένων που χρησιμοποιούν μακροεντολές. Η εισαγωγή ενός τέτοιου ιού μπορεί να γίνει και με την αποστολή ενός απλού e-mail. Τέτοια αρχεία είναι τα αρχεία του Word (*.doc), Excel (*.xls).

- **3.2.2 *Σκουλήκια (Worms):*** Τα worms είναι ένα είδος ιομορφολογικού λογισμικού. Έχουν διαφορές και ομοιότητες με τους ιούς. Η διαφορά με βάση την οποία ξεχωρίζουμε τους ιούς από τα worms είναι ότι τα worms υπάρχουν ελεύθερα στο διαδίκτυο. Έχουν την δυνατότητα αυτοαναπαραγωγής καθώς και την ικανότητα να κινούνται εύκολα μέσα στον υπολογιστή. Τα worms χρησιμοποιούν τους πόρους του υπολογιστή και ανάλογα με τον σχεδιαστή τους έχουν και την ανάλογη δράση.

- **3.2.3 *Δούρειοι Ίπποι (Trojan Horses):*** Τα trojans ανήκουν στην κατηγορία των ιών αν και διαφέρουν αρκετά από τους ιούς και τα worms. Τα trojans δεν μπορούν να αναπαραχθούν και δεν μπορούν να εξαπλωθούν. Τα trojans εισβάλλουν σε ένα υπολογιστή με την μορφή και ονομασία κάποιον άλλων προγραμμάτων ώστε να μην μπορούν να γίνουν αντιληπτά από το σύστημα. Ο ρόλος τους είναι συγκεκριμένος, δηλαδή να βρουν όλες τις ανοιχτές πόρτες και να αποκαταστήσουν σύνδεση με ένα άλλο υπολογιστή ώστε ο εισβολέας να μπορεί να πάρει τον έλεγχο του θύματος. Μια άλλη λειτουργία των trojans είναι η καταγραφή των κωδικών ασφαλείας και η αποστολή τους στον σχεδιαστή τους χρησιμοποιώντας μια e-mail υπηρεσία.

- **3.2.4 *Cookies:*** Τα cookies είναι μικρά προγράμματα τα οποία τα χρησιμοποιούν οι περισσότερες ιστοσελίδες για την αποθήκευση προσωπικών στοιχείων του χρήστη. Ένα παράδειγμα η ιστοσελίδα του pathfinder χρησιμοποιεί τα cookies για να εμφανίζει την κεντρική σελίδα με τα χρώματα, που θέλει να βλέπει ο χρήστης όταν δίνει το username και το password ή και να τον κρατάει συνδεμένο μέχρι αυτός να αποφασίσει να αποσυνδεθεί. Όμως τα cookies δεν είναι πάντα τόσο «αθώα» όσο δείχνουν, μπορούν να μαζεύουν προσωπικές πληροφορίες για τον υπολογιστή του χρήστη ώστε κάποιος τρίτος να μπορέσει να αποκτήσει πρόσβαση ή μαζεύουν πληροφορίες γύρο από τα ενδιαφέροντα του χρήστη για να μπορέσουν να τις χρησιμοποιήσουν εταιρίες για την πώληση των προϊόντων τους.

- **3.2.5 *Hoaxes Viruses:*** έχουν τα ίδια αποτελέσματα με τους πραγματικούς ιούς χωρίς να έχουν μολύνει τον υπολογιστή. Συνήθως οι Εικονικοί Ιοί στέλνονται με το ηλεκτρονικό ταχυδρομείο (e-mails) για να προειδοποιήσουν τους χρήστες και τους διαχειριστές δικτύου για τον βαθμό κινδύνου ενός καινούριου ιού

χωρίς στην ουσία να υπάρχει αυτός ο ιός. Μέχρι να διαπιστωθεί αν όντως πρόκειται για φάρσα ή όχι οι χρήστες έχουν είδη σταματήσει για μερικές μέρες να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο. Χαρακτηριστικό παράδειγμα εικονικού ιού είναι ο ιός «**Good Time**». Στην αρχή στάλθηκε με το ηλεκτρονικό ταχυδρομείο σαν hoax virus και για 3-4 μέρες οι SMTP Servers ήταν εκτός λειτουργίας. Μερικές μέρες αργότερα και αφού είχε διαπιστωθεί ότι ήταν φάρσα, κάποιοι προγραμματιστές δημιούργησαν ένα ιό και τον ονόμασαν **Good Time** με αποτέλεσμα να μολυνθούν όσοι υπολογιστές άνοιξαν το e-mail.

3.3 Λύση

Σε επίπεδο software τα μέτρα προστασίας βασικά είναι δύο. Το πρώτο είναι η χρήση *Firewall* και το δεύτερο μέτρο είναι η χρήση *Antivirus, Antitrojan.* Άλλα μέτρα προστασίας των δεδομένων είναι η χρήση κωδικών πρόσβασης (passwords), η κρυπτογράφηση των δεδομένων, που θέλουμε να προστατέψουμε. Αναφορικά με την προστασία των δεδομένων, θα πρέπει να έχετε ξεκαθαρίσει ποια κατηγορία δεδομένων θέλετε να προστατέψετε: Πρόκειται για κάποιο mail plug-in, κάποιο data driver, ή κάποιο software που πραγματοποιεί κρυπτογράφηση σε on-line επικοινωνίες; Η προστασία θα αφορά ολόκληρο τον δίσκο ή κάποιο μέρος του δίσκου; Αυτά πρέπει να τα είναι ξεκαθαρισμένα ώστε να μην παραβιαστούν από Hacker's (Χακερς) ή Cracker's (Κράκερ). Η ασφάλεια δεν είναι αρκετή μόνο σε επίπεδο software, αλλά απαιτείται και σε επίπεδο hardware. Πρέπει να υπάρχει ασφάλεια στο φυσικό μέρος του υπολογιστή, δηλαδή να μην υπάρχει η δυνατότητα να καταστραφεί ένας δίσκος. Όταν συνδεόμαστε στο internet κινδυνεύουμε να δεχτούμε επίθεση από: 1)Hackers και 2) Crackers.

3.4 Από ποιους κινδυνεύουμε και γιατί

3.4.1 *Hacker's*

Πριν αναφερθούμε στους hackers θα δώσουμε ένα απλό και όχι ακριβή ορισμό.

" *Το άτομο που προσπαθεί να ανακαλύψει ευαίσθητες πληροφορίες διεισδύοντας παντού, που απολαμβάνει την εξερεύνηση των λεπτομερειών ενός συστήματος και των δυνατοτήτων του συστήματος φτάνοντας το στα όρια του* " ονομάζεται **Χακερ(Hacker)**.

Οι hackers είναι μια από τις πολλές κατηγορίες που εποφθαλμιούν τα πολύτιμα δεδομένα μας (ειδικά όταν είναι αριθμοί πιστωτικών καρτών ή κάποια άλλα προσωπικά δεδομένα), ή να απλώς να παίξουν με το σύστημα μας, ή στην καλύτερη περίπτωση να βρουν τις τρύπες και τα αδύνατα σημεία του λειτουργικού συστήματος και μετά να μας πουλήσουν τις πληροφορίες αυτές. Ένας μέτριος

hacker μπορεί εύκολα να παρακάμψει το firewall που έχουμε εγκαταστήσει και να σπάσει τα κωδικοποιημένα αρχεία. Το μόνο που χρειάζονται είναι χρόνος και αφορμή. Οι hackers βρίσκουν τις ανοιχτές τρύπες στον υπολογιστή του χρήστη ή στον Web Server και στην συνέχεια με την μέθοδο "**brute force attack**" μπορούν να σπάσουν τους κωδικούς πρόσβασης (ειδικά όταν είναι 4 ψηφίων η διαδικασία διαρκεί μερικά δευτερόλεπτα μόνο.). Άρα ο υπεύθυνος για την επίθεση ενός hacker είναι ο διαχειριστής του υπολογιστή. Οι hackers σπάνια "δημιουργούν" τρύπες σε ένα σύστημα, κατά 99% απλώς εκμεταλλεύονται τις υπάρχουσες τρύπες, χρησιμοποιώντας συχνά μάλιστα και standard software που έχει εξελιχθεί για αυτό το σκοπό. (Συνήθως οι hacker's φτιάχνουν μόνοι τους τα προγράμματα τα οποία αργότερα θα χρησιμοποιήσουν για να αποκτήσουν πρόσβαση στον υπολογιστή του θύματος). Σε περίπτωση που κάποιος χρησιμοποιεί προγράμματα έτοιμα και ΔΕΝ τα έχει φτιάξει μόνος του τότε ονομάζεται Lammer Hacker (Λάμερ Χακερ). Όσοι βρίσκουν νέες "τρύπες" δεν τις εντοπίζουν κάνοντας "μαγικά", αλλά απλώς με την διόλου "ρομαντική" μέθοδο δοκιμής και λάθους. Η πλειονότητα των "λαθών" ασφάλειας εντοπίζονται κατά τη διάρκεια άλλων εργασιών από χρήστες ή administrators και μετά τυγχάνουν ευρύτερης εκμετάλλευσης.

Δεν είναι μόνο τα bugs τα οποία δίνουν πρόσβαση σε ένα υπολογιστικό σύστημα, αλλά ένας εισβολέας μπορεί να αποκτήσει πρόσβαση με την χρήση **σκουληκιών (worms)** ή **Δούρειων Ίππων (Trojan horses)**. Τα trojan horses μπορούν να περάσουν απαρατήρητα μέσα από αθώα αρχεία ή όταν δεν υπάρχει κάποιο firewall εγκατεστημένο, ενώ τα worms κινούνται συνήθως ελεύθερα στο διαδίκτυο και ψάχνουν για πόρους και μέρος για να αυτοαναπαραχθούν. Σε περίπτωση που υπάρχει κάποιο firewall εγκατεστημένο πρέπει να αφήνει κάποιες εφαρμογές ή δεδομένα να περνάνε διότι είναι αναγκαίες για το σύστημα προκειμένου να δουλέψει. Π.χ. το Outlook.exe. Σε αυτό το σημείο οι hackers "φυτεύουν" ένα Trojan δίνοντας το όνομα κάποιας εφαρμογής του συστήματος. Με αυτόν τον τρόπο παρακάμπτουν τα firewalls (τα trojan είναι ένα από τα πολλά εργαλεία που χρησιμοποιούν προκειμένου να πάρουν πρόσβαση στο σύστημα μας. Τα εργαλεία που χρησιμοποιούν θα τα αναφέρουμε παρακάτω).

3.4.2 *Cracker's*

Με τον όρο Cracker ονομάζουμε αυτόν που *"σπάει" κωδικούς ασφαλείας σε ένα σύστημα. Είναι κάτι που δεν σχετίζεται άμεσα με τον όρο Hacker*." Παρόλο που οι Hackers και οι Crakers μπορούν να χρησιμοποιήσουν τις ίδιες μεθόδους για να αποκτήσουν πρόσβαση σε κάποιον υπολογιστή ο σκοπός τους επιθέσεις είναι τελείως διαφορετικός.

Οι Crackers σαν σκοπό έχουν να "σπάσουν" τους κωδικούς ασφαλείας προσκειμένου να μπορέσουν να πειράξουν αρχεία του λειτουργικού συστήματος και γενικά να προκαλέσουν ζημιές στον υπολογιστή. Για παράδειγμα το CD-ROM να μην δουλεύει ή να σβήσουν αρχεία συστήματος με αποτέλεσμα να μην μπορεί να γίνει εκκίνηση του λειτουργικού συστήματος, κτλ. Αυτό έχει σαν αποτέλεσμα ο

εντοπισμός των Crackers να είναι δύσκολος έως αδύνατος αφού ξέρουν να καλύπτουν τα ίχνη τους. Όμως υπάρχουν περιπτώσεις όπου μετά από μια επίθεση δεν εξαφάνισαν τα ίχνη τους με αποτέλεσμα να συλληφθούν όλοι.

Ο σκοπός του Cracker δεν είναι μόνο να σπάσει τους κωδικούς ασφαλείας από κάποιο υπολογιστή για να έχει πρόσβαση σε αυτό, αλλά σπάει και του κωδικούς που έχουν προγράμματα με σκοπό να τα διανείμει ελεύθερα σε όλους ή να σπάσει κρυπτογραφημένα πακέτα για να δοκιμάσει την δύναμη του κρυπτογραφικού αλγορίθμου που χρησιμοποιήθηκε για την προστασία και ασφάλεια των δεδομένων που στέλνονται. Τα δεδομένα αυτά μπορεί να είναι είτε ευαίσθητα προσωπικά στοιχεία ενός χρήστη ή κάποιας επιχείρησης, ή ένα κείμενο.

3.5 Συλλογή Πληροφοριών για ένα Σύστημα ή Server

Ας υποθέσουμε ότι ένας hacker βλέπει μια διαφήμιση στην τηλεόραση για κάποια επιχείρηση, που πουλάει τα προϊόντα της μέσο του Internet, και αποφασίζει να επιτεθεί. Όμως δεν ξέρει τίποτα για την επιχείρηση, το DNS που έχει, τους Servers, το λειτουργικό σύστημα που χρησιμοποιούν οι υπολογιστές κλπ. Για αυτό το λόγο θα κάνει μια έρευνα ώστε να μπορέσει να συγκεντρώσει τις απαραίτητες πληροφορίες για να μπορέσει να επιτεθεί Η συλλογή των πληροφοριών γίνεται με τα εξής εργαλεία και εντολές:

1. Με την εντολή ***Whois***
2. Με την εντολή ***Nslookup***
3. Με την εντολή ***Traceroute***
4. Χρησιμοποιώντας ***Μηχανές Αναζήτησης (Search Engines)***
5. Χρησιμοποιώντας ***Ping - Port Scanners***
6. Χρησιμοποιώντας ***Passive Monitor.***

3.5.1 Εντολή **Whois:**

Το ***Whois*** είναι ένα πρωτόκολλο με το οποίο μπορούμε να συλλέγουμε πληροφορίες για δίκτυα, οργανισμούς, domains. Σαν αποτελέσματα η εντολή ***Whois*** μας εμφανίζει τους εξυπηρετητές, τα domain names (DNS), τις IP διευθύνσεις, τους διαχειριστές του δικτύου. Η σύνταξη της εντολής αυτής είναι πολύ απλή και δίνεται στο παρακάτω παράδειγμα. Ο Hacker με το ψευδώνυμο **granite** δοκιμάζει πρώτα ένα whois ερώτημα στην βάση δεδομένων InterNIC.net η οποία έχει όλα τα domain name όλων των οργανισμών και επιχειρήσεων. Έστω ότι ψάχνει για την επιχείρηση ElfArrow. Στην γραμμή εντολών ενός συστήματος Unix ([granite:~]$) ο hacker θα πληκτρολογήσει:

[granite: ~]$
και θα πάρει τα εξής αποτελέσματα:

Από τις 3 εγγραφές που πείρε πιο πολύ ταιριάζει η πρώτη εγγραφή. Ο hacker θα ξανακάνει το ερώτημα πιο συγκεκριμένο αυτή τη φορά.

[granite:~]$

Με αυτό το ερώτημα ο hacker έχει στην διάθεση του τις εξής πληροφορίες:

- Το domain name της επιχειρήσεις,
- Την φυσική τοποθεσία της επιχειρήσεις,
- E-mail για επικοινωνία με τον administrator,
- Τον αριθμό τηλεφώνου και τον αριθμό του φαξ για τον administrator,
- Μια διαθέσιμη Subnet διεύθυνση της επιχειρήσεις (209.1.78.0)

3.5.2 Η εντολή **nslookup**

Έχοντας μαζέψει πληροφορίες για το domain name της επιχείρησης και έχοντας μια πιθανή subnet IP χρησιμοποιούμε την εντολή **nslookup** για να μαζέψουμε περισσότερες πληροφορίες για το DNS και τους εξυπηρετητές (servers) που χρησιμοποιεί η επιχείρηση. Αυτό γίνεται για να μπορέσει ο επιτιθέμενος να βρει διαθέσιμους εξυπηρετητές μέσο των οποίων θα μπορέσει να επιτεθεί στο σύστημα.

```
[granite:~]$

Default Server:
Address        :
```

για να μπορέσουμε να πάρει τις πληροφορίες που χρειάζεται ο επιτιθέμενος πρέπει να αλλάξει τον εξυπηρετητή και να συνδεθεί με τον εξυπηρετητή του δικτύου που σχεδιάζει να επιτεθεί. Η αλλαγή αυτή γίνεται με την εντολή **server** του **nslookup :**

```
Default Server:
Address        :

[Kermit.ElfArrow.com]
Received 20 answers (0 records)
```

Με την πρώτη εντολή συνδεόμαστε στον εξυπηρετητή του δικτύου που θέλουμε να επιτεθούμε στην συνέχεια αντιγράφουμε όλους τους διαθέσιμους εξυπηρετητές που έχει η επιχείρηση στο αρχείο **hosts.lst** Για να μπορέσουμε να φύγουμε πληκτρολογούμε την εντολή **exit.** Το **nslookup** δουλεύει μόνο σε λειτουργικά συστήματα *Unix* και *Linux* και σε Windows NT/2000/XP.

Το αρχείο αυτό μας δίνει πολλές χρήσιμες πληροφορίες. Ο Woolly (granite, Woolly είναι το όνομα του) ίσος να έχει δύο έγκυρα IP υποδίκτυα στα οποία μπορεί να επιτεθεί αμέσως εκτός από ένα. Το υποδίκτυο 206.100.29.0 είναι υπό αμφισβήτηση γιατί ο Web εξυπηρετητής μπορεί να είναι σε τοποθεσία εκτός δικτύου. Τέλος το αρχείο μας δείχνει ότι ο DNS server Kermit λειτουργεί και ως FTP εξυπηρετητής. Είναι πιθανό ο Woolly να χρησιμοποίηση την FTP υπηρεσία για να εκθέσει τον DNS εξυπηρετητή και να αλλάξει την cache. Αυτό θα του δώσει την απευθείας πρόσβαση σε οποίο εξυπηρετητή επιθυμεί.

3.5.3 SEARCH ENGINES - Μηχανές Αναζήτησης

Οι μηχανές αναζήτησης είναι μια τέλεια μέθοδος συλλογής πληροφοριών για ένα εσωτερικό δίκτυο ενός οργανισμού. Θα εκπλαγείς από την ποσότητα των πληροφοριών που προκύπτουν από ένα οργανισμό ακόμα και αν συνδεθεί για λίγο στο διαδίκτυο. Αυτό συμπεριλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, newsgroup posts, και ιστοσελίδες από τους Web εξυπηρετητές (με την προϋπόθεση ότι είναι ορατές από το διαδίκτυο).

3.5.4 Η εντολή TRACERT.

Η εντολή tracert μας δείχνει το μονοπάτι του δικτύου από τον ένα εξυπηρετητή στον άλλο. Η σύνταξη την εντολής αυτής είναι: *γραμμή εντολών: tracert όνομα εξυπηρετητή* Η εντολή αυτή μας δείχνει ότι ο Kermit server περνάει:

1) από 12 εξυπηρετητές,
2) το χρόνο που χρειάζεται στον κάθε ένα,
3) το όνομα του εξυπηρετητή,
4) την IP διεύθυνση του.

Μια υλοποίηση της εφαρμογής βασίζεται στην αποστολή μιας ακολουθίας πακέτων με αυξανόμενες τιμές του πεδίου ***time-to-live (TTL)*** ,δηλαδή μέγιστου αριθμού των **hops** που ένα πακέτο μπορεί να κάνει. Στην περίπτωση μας ο μέγιστος αριθμός των hops είναι 30. Οι τιμές αυτές αυξάνονται μέχρι το πακέτο να φτάσει στον παραλήπτη. Αν και αυτός ο τρόπος υλοποίησης είναι απλός και χρησιμοποιείται ευρύτατα, παράγει ένα μεγάλο πλήθος πακέτων.

3.5.5 PING - PORT SCAN

Ένας **ping scanner** στέλνει μια **ICMP** αίτηση στις IP διευθύνσεις που έχει ορίσει ο χρήστης (δίνει μια αρχική και μια τελική IP διεύθυνση) και περιμένει απάντηση στην αίτηση. Αν πάρει απάντηση στην αίτηση που έστειλε τότε ο υπολογιστής σε αυτή την διεύθυνση είναι ενεργός. Στην συνέχεια θα προσπαθήσει να πάρει το όνομα που αντιστοιχεί στον υπολογιστή. Ακόμα και αν βρεθεί ενεργός ο υπολογιστής ΔΕΝ είναι απαραίτητο να βρεθεί το όνομα του. Σε λειτουργικά συστήματα όπως τα Windows ο υπολογιστής στέλνει 4 πακέτα, αντίθετα με *NIX λειτουργικά συστήματα τα οποία στέλνουν **άπειρα** πακέτα. Με το ping βλέπουμε σε πόσο χρόνο έφτασαν τα πακέτα στον υπολογιστή που έχουν ορίσει, αν έφτασαν όλα. Με το ping εκτός ότι βρίσκουμε ένα υπολογιστή αν είναι συνδεμένος σε δίκτυο ή στο διαδίκτυο μπορούμε να βρούμε το λειτουργικό σύστημα που χρησιμοποιεί, από το TTL (TTL=128 το λειτουργικό σύστημα είναι Windows 98/NT/2000/XP). Η σύνταξη της εντολής είναι:

«Ping ip address ή domain name»

Ο **port scanner** ,είναι πρόγραμμα, το οποίο μας επιτρέπει να βρούμε τον αριθμό από τις πόρτες του υπολογιστή που ακούνε, ποιες δεν ακούνε (κλειστές), και ποιες είναι ανοιχτές, και ποιες φιλτράρουν τα δεδομένα που δέχονται. Ο χρήστης δίνει το όνομα του υπολογιστή ή την IP διεύθυνση, από ποιο port να ξεκινάει η ανίχνευση και σε ποιο να σταματάει, και σε ποιο πρωτόκολλο να γίνει η ανίχνευση (TCP - UTP). Στην συνέχεια εμφανίζει τον αριθμό της port και το όνομα της, δηλαδή το **port 21** αντιστοιχεί στον **ftp server, port 23** στο **telnet...** καθώς ποιες από αυτές είναι ανοιχτές και ποιες κλειστές.

Μέχρι εδώ ο επιτιθέμενος έχει μαζέψει αρκετές πληροφορίες για τον οργανισμό που σκοπεύει να επιτεθεί. Τώρα δεν έχει παρά να μαζέψει πληροφορίες για το λειτουργικό σύστημα που χρησιμοποιούν οι υπολογιστές, αν χρησιμοποιούν **Windows** ή **Unix.** Σε περίπτωση που οι υπολογιστές χρησιμοποιούν λειτουργικό **Windows NT/2000** ή **Windows XP** τα πράγματα για τον επιτιθέμενο είναι αρκετά εύκολα αφού μπορεί να κάνει **null session** και να αποκτήσει πλήρη πρόσβαση στον δίσκο **χωρίς να δώσει username** και **password!** Το **null session** μπορεί και να μην δουλέψει να ο διαχειριστής το έχει απενεργοποιήσει από το registry. Για να βεβαιωθούμε ότι δεν είναι απενεργοποιημένο χρησιμοποιούμε την εντολή *net stat*. Ο τρόπος για να βρει το λειτουργικό λέγεται **Passive Monitoring.**

3.5.6 Passive Monitoring

Για να μπορέσει ο επιτιθέμενος να βρει περισσότερα στοιχεία όσο αφορά την κίνηση του δικτύου, και το λειτουργικό που χρησιμοποιεί εγκαθιστά ένα πρόγραμμα μικρού μεγέθους

ώστε να μην γίνεται αντιληπτό, το οποίο συλλέγει πληροφορίες και στην συνέχεια τις στέλνει στον κατασκευαστή του. Οι πληροφορίες που παίρνουμε συνήθως είναι:

1. Η γλώσσα που χρησιμοποιείται,
2. την ανάλυση της οθόνης,
3. τα χρώματα που υποστηρίζει η κάρτα οθόνης,
4. το λειτουργικό σύστημα,
5. ο επεξεργαστής που χρησιμοποιείται,
6. ο φυλλομετρητής που έχει ο υπολογιστής και την έκδοση του.

Τα 3 τελευταία μας ενδιαφέρουν περισσότερο και είναι τα πιο ενδιαφέροντα. Έχοντας αυτές τις πληροφορίες ο επιτιθέμενος μπορεί να καθορίσει τον τρόπο με τον οποίο θα επιτεθεί στο σύστημα και από πού θα κάνει την επίθεση του. (Τα προγράμματα που κάνουν αυτή την δουλεία φτιάχνονται από τους Hacker's ή τους Cracker's και είναι μικρού μεγέθους). Τώρα ο επιτιθέμενος έχει όλες τις πληροφορίες που χρειάζεται για να επιτεθεί στον οργανισμό. Το ερώτημα που τίθεται είναι ποια επίθεση θα χρησιμοποίηση για να έχει τα αποτελέσματα που επιθυμεί.

3.6 ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ

Η επίθεση μπορεί να γίνει σε δυο επίπεδα 1) σε επίπεδο hardware (υλικού), και 2) σε επίπεδο software (λογισμικού).

Όταν ένας hacker ή cracker αποφασίζει να επιτεθεί στο hardware στην ουσία εκμεταλλεύεται τις αδυναμίες των πρωτοκόλλων για να μπορέσει να κλέψει πακέτα ή να αποκτήσει πρόσβαση στο σύστημα μέσο των πρωτοκόλλων. Το πρωτόκολλο IP είναι πολύ ευάλωτο σε τέτοιου είδους επιθέσεις όπως είναι η *sequence number attack* με την οποία ο επιτιθέμενος βρίσκει τον αποστολέα και τον παραλήπτη των πακέτων. Στην συνέχεια αλλάζει την διεύθυνση του παραλήπτη με αποτέλεσμα να κλέψει τα πακέτα. Για να εξασφαλιστεί η ασφάλεια σε αυτό το επίπεδο δημιουργήθηκε ένα άλλο πρωτόκολλο το οποίο χρησιμοποιείται στο επίπεδο του IP πρωτοκόλλου κ.α. ονομάζεται *Network Layer Security Protocol (NLSP)*. Το πρωτόκολλο αυτό χρησιμοποιεί την κρυπτογραφία για να ασφαλίσει τα περιεχόμενα των πακέτων και τα στοιχεία του χρήστη.

Τα πράγματα είναι πιο εύκολα όταν ένας hacker ή cracker αποφασίζει να επιτεθεί σε ένα σύστημα εκμεταλλευόμενος τις αδυναμίες του λειτουργικού συστήματος. Η ασφάλεια στο λογισμικό είναι ελλείπεις επειδή ο χρήστης δεν έχει γνώση για τους κινδύνους που διατρέχει όταν είναι συνδεμένος στο διαδίκτυο με αποτέλεσμα να μην κάνει σωστή χρήση ή και καθόλου χρήση των λογισμικών που κυκλοφορούν και τα

οποία είναι σχεδιασμένα για να τον προστατεύουν. Έτσι ο επιτιθέμενος έχει πολλές επιλογές όσο αφορά τον τρόπο με τον οποίο θα επιτεθεί.

3.7 Γνωστές Μέθοδοι Επίθεσης

3.7.1 *Brute Force Attack*

Η **brute force attack** είναι μια από τις πιο γνωστές επιθέσεις που γίνονται σε υπολογιστές. Με την επίθεση αυτή ο επιτιθέμενος μπορεί να «σπάσει» τους κωδικούς πρόσβασης και να συνδεθεί στο σύστημα σαν ένας από τους χρήστες του συστήματος. Επειδή οποιαδήποτε απόπειρα στους κωδικούς ασφαλείας καταγράφεται ο επιτιθέμενος δημιουργεί ένα αντίγραφο του αρχείο που έχει τους κωδικούς πρόσβασης, και στην συνέχεια τους αποθηκεύει στον υπολογιστή του, εκτός και αν είναι σε θέση να μαντέψει τον κωδικό ασφαλείας γνωρίζοντας το όνομα χρήστη. Ένα από τα πιο γνωστά προγράμματα είναι το «John the Ripper». Μπορεί να σπάσει κωδικούς 4 ψηφίων μεταξύ 4 έως 18 δευτερολέπτων!!!

3.7.2 *Spoofing*

Μια άλλη γνωστή επίθεση είναι το **Spoofing.** Ο επιτιθέμενος κρύβει την δική του IP με την IP κάποιου άλλου υπολογιστή , η οποία μπορεί να είναι πραγματική ή και ψεύτικη, και με αυτόν τον τρόπο μπορεί να στείλει πακέτα, να τροποποίηση πακέτα, ή και ακόμη να συνδεθεί στο σύστημα. Η επίθεση αυτή αφήνει ψεύτικα ίχνη με αποτέλεσμα ο εντοπισμός του να γίνεται δύσκολα και ακόμη δυσκολότερος όταν χρησιμοποιεί δημόσιους **proxy servers.** Οι proxy servers λέγονται και «ενδιάμεσοι» και έχουν σαν σκοπό να καλύπτουν τα πραγματικά στοιχεία του χρήστη όσο είναι συνδεμένος στο διαδίκτυο.

3.7.3 *Denial of Service (DoS) Attack*

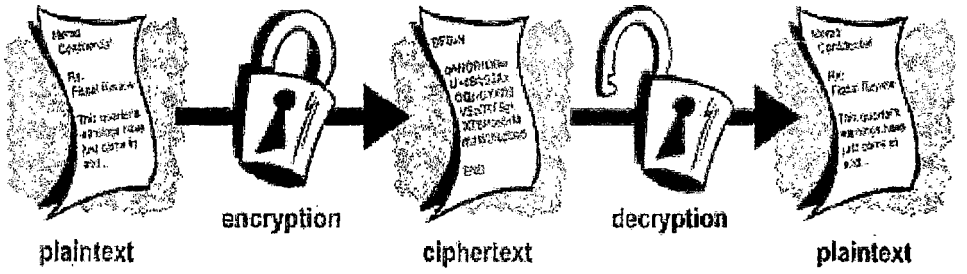
Με την DoS ο επιτιθέμενος έχει σαν σκοπό να βγάλει εκτός λειτουργία ,για ένα χρονικό διάστημα, ένα server που προσφέρει κάποιες υπηρεσίες σε χρήστες. Αυτό έχει σαν αποτέλεσμα να προκληθεί πρόβλημα όταν ζητηθεί από κάποιον χρήστη μια υπηρεσία. Ο λόγος που οι περισσότεροι επιτιθέμενοι χρησιμοποιούν την Άρνηση Υπηρεσίας (DoS) είναι ότι όταν βγει έκτος λειτουργίας ο server κάνοντας Spoof την IP του μπορούν να δουν τους υπολογιστές του δικτύου και τα πακέτα που πιθανός να στείλουν, να γίνουν αποδεκτά αφού τα στέλνει μια έμπιστη οντότητα. Μπορούν να πάρουν πρόσβαση και να δουν ή να τροποποιήσουν αρχεία.

3.8 *ΚΡΥΠΤΟΓΡΑΦΙΑ*

Η κρυπτογραφία είναι ένα μέρος της συνολικής ασφάλειας των δεδομένων που στέλνουμε ή παραλαμβάνουμε όταν είμαστε συνδεμένοι στο διαδίκτυο. Αυτό όμως δεν σημαίνει ότι με την χρήση της κρυπτογραφίας ότι έχουμε ασφαλίσει πλήρως τα δεδομένα μας και οποιαδήποτε απόπειρα για να κλαπούν τα δεδομένα μας ,ειδικά όταν είναι αριθμοί πιστωτικών καρτών, ή να παραποιηθούν θα πέσει στο κενό. Ας δούμε όμως τι είναι η κρυπτογραφία και πως μας βοηθάει στην ασφάλεια των προσωπικών μας στοιχείων.

Η κρυπτογραφία είναι **μια επιστήμη για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων.** Είναι μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. 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).Αυτό μετατρέπεται από μια συνάρτηση που έχει ως παράμετρο ένα κλειδί. Το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext) (Σχήμα 1).



Σχήμα 1: Συμμετρική Κρυπτογραφία

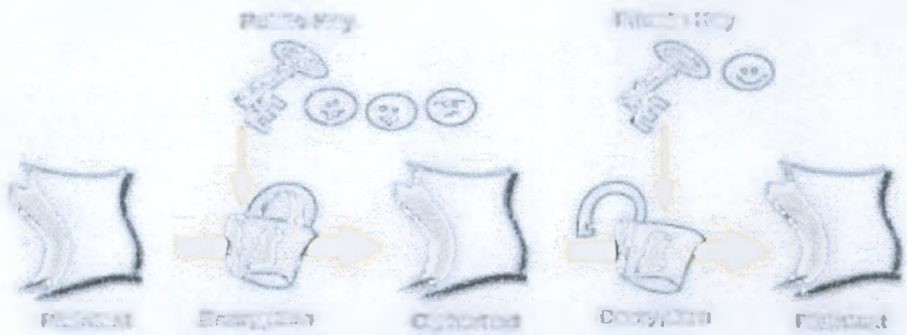
3.8.1 Συμμετρική Κρυπτογραφία

Για να μπορέσει ένα απλό κείμενο να κρυπτογραφηθεί χρησιμοποιείται είτε η **συμμετρική κρυπτογραφία**, είτε η **ασύμμετρη κρυπτογραφία**. Η συμμετρική κρυπτογραφία χρησιμοποιεί ένα **δημόσιο κλειδί** για να κρυπτογραφήσει και να αποκρυπτογραφήσει το κείμενο και για αυτό το λόγο ονομάζεται και *αλγόριθμος μυστικού κλειδιού*, εφ' όσον το κλειδί είναι γνωστό μόνο σε εξουσιοδοτημένα μέρη. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα

χρησιμοποιείται. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο το κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

3.8.2 Ασύμετρη Κρυπτογραφία

Αντίθετα η ασύμμετρη κρυπτογραφία ,(αυτός ο τύπος είναι γνωστός και σαν *κρυπτογραφία δημόσιου κλειδιού*), χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται **δημόσιο κλειδί (public key)** και το άλλο καλείται **ιδιωτικό κλειδί (private key)**. (σχήμα2) *Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κλειδί κρατείται μυστικό*. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.



Σχήμα 2: Ασύμμετρη Κρυπτογραφία.

Σε περίπτωση που η κρυπτογραφία που χρησιμοποιούμε είναι πολύ δυνατή δηλαδή δεν μπορεί να βρεθεί εύκολα το κλειδί, οι hacker's ή οι cracker's ΔΕΝ επιτίθονται στον κρυπτογραφικό αλγόριθμο αλλά στα συστήματα (τα οποία έχουν και τις περισσότερες αδυναμίες) που χρησιμοποιούν τον κρυπτογραφικό αλγόριθμο. Ας δώσουμε μερικά παραδείγματα για να γίνει πιο κατανοητό.

Πολλές από τις πρόσφατες επιθέσεις εναντίον των εφαρμογών SSL της Netscape ήταν επιθέσεις στο Netscape Navigator παρά του ίδιου SSL πρωτοκόλλου. Σε μια δημοσιευμένη επίθεση, οι ερευνητές ανακάλυψαν ότι η γεννήτρια τυχαίων αριθμών

δεν ήταν ακριβώς τυχαία. Ήταν δυνατό για του επιτιθέμενους να παρακολουθήσουν προσεκτικά τον υπολογιστή στον οποίο "έτρεχε" η εφαρμογή και να προβλέπουν κάθε φορά την διαμόρφωση της γεννήτριας τυχαίων αριθμών. Έτσι καθόριζαν ποιο ήταν το επιλεγμένο κλειδί με έναν τίμιο τρόπο. Σε άλλη επίθεση ερευνητές ανακάλυψαν ότι μπορούν εύκολα να τροποποιήσουν το ίδιο το πρόγραμμα έτσι ώστε η γεννήτρια τυχαίων αριθμών να μην μπορεί να εκτελεστεί. Έτσι δεν χρειάζεται να μαντέψουμε το κλειδί.

Ένα καλό παράδειγμα τέτοιας επίθεσης είναι ο VC-I Video, κρυπτογραφικός αλγόριθμος που χρησιμοποιούταν για την δορυφορική μετάδοση προγράμματος τηλεόρασης παλαιότερα. Για πολλά χρόνια υπήρχαν πειρατές που πουλούσαν αποκωδικοποιητές που μπορούσαν να υποκλέψουν τα κλειδιά μεταφοράς και ύστερα να τα χρησιμοποιήσουν για να αποκρυπτογραφήσουν την μετάδοση. Ο VC-I κρυπτογραφικός αλγόριθμος ήταν ασφαλής, αλλά το σύστημα σαν σύνολο ήταν αδύνατο. (Αυτό επίσης δείχνει ότι όταν γίνεται λόγος για πολλά χρήματα, οι άνθρωποι συχνά βρίσκουν ελαττώματα στα κρυπτογραφικά συστήματα και εκμεταλλεύονται αυτά τα ελαττώματα.) Η επιθέσεις αυτές είναι γνωστές και σαν **system-based attack - επιθέσεις βασισμένες στο σύστημα.**

3.8.3 *Πλεονεκτήματα Κρυπτογράφησης*

Η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες :

- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες αποθηκευμένες στον υπολογιστή μας από πρόσβαση ενός τρίτου, με ή χωρίς άδεια.

- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες κατά την διάρκεια της μεταφοράς από ένα υπολογιστικό σύστημα στο άλλο.

- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να εμποδίσει και για να εντοπίσει τυχαίες ή σκόπιμες αλλαγές στα δεδομένα μας.

- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού.

Πέρα από αυτά τα πλεονεκτήματα, υπάρχουν και κάποια όρια τα οποία πρέπει να γνωρίζουμε για να αποφεύγουμε τα ανεπιθύμητα αποτελέσματα :

- Η κρυπτογράφηση δεν μπορεί να προφυλάξει τα δεδομένα μας από

κάποιον εισβολέα που θέλει να σβήσει τα δεδομένα μας όπως είναι.

- Ένας εισβολέας μπορεί να έχει τροποποιήσει και να εκθέτει ένα πρόγραμμα κρυπτογράφησης από μόνος του, έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Ή μπορεί να κρατά σε ένα αρχείο όλα τα κλειδιά για να τα χρησιμοποιήσει αργότερα.

- Ένας εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα κρυπτογραφήσουμε και αφού τα αποκρυπτογραφήσουμε.

- Ένας εισβολέας ίσως βρει έναν άγνωστο και σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα μηνύματα που εμείς κρυπτογραφούμε με κάποιο αλγόριθμο.

Για όλους αυτούς του λόγους, η κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολικής στρατηγικής ασφαλείας που έχουμε, και όχι σαν υποκατάστατο άλλων μέτρων ασφαλείας που πρέπει να έχουμε, όπως είναι ο κατάλληλος έλεγχος πρόσβασης στον υπολογιστή μας. Άλλωστε δεν πρέπει να ξεχνάμε ότι τα ευαίσθητα και προσωπικά στοιχεία του χρήστη ή μιας επιχείρησης μπορούν να κλαπούν πριν από την κρυπτογράφηση των στοιχείων ή μετά την αποκρυπτογράφηση των στοιχείων αυτών.

3.9 Ασφάλεια με την χρήση πρωτοκόλλων

3.9.1 Εισαγωγή

Για να μπορέσουν να ασφαλίσουν τις πληροφορίες αυτές πρέπει πρώτα να ασφαλίσουν τα πρωτόκολλα που κάνουν χρήση των πληροφοριών. Παράδειγμα για το πρωτόκολλο **HTTP** έχει φτιαχτεί το **SHTTP** το οποίο ασφαλίζει τις πληροφορίες που διακινούνται στο επίπεδο εφαρμογής ή το **SET** το οποίο ασφαλίζει τους αριθμούς των πιστωτικών καρτών με την χρήση της κρυπτογραφίας ή το **SSL** το οποίο με την χρήση κρυπτογραφικών αλγορίθμων ασφαλίζει τις επικοινωνίες στο επίπεδο μεταφοράς (κρυπτογραφικούς αλγόριθμους χρησιμοποιούν και το SHTTP και το SET). Ας δούμε όμως τι είναι η κρυπτογραφία και πως βοηθάει στην ασφάλεια των προσωπικών δεδομένων του χρήστη σε ένα ηλεκτρονικό κατάστημα. Παρακάτω θα αναφερθώ αναλυτικότερα στα πρωτόκολλα αυτά και πως μπορούμε να καταλάβουμε ότι γίνεται χρήση των πρωτοκόλλων αυτών.

3.9.2 SET (Secure Electronic Transactions)

Το SET είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο για την αποστολή κρυπτογραφημένων αριθμών πιστωτικών καρτών μέσω του Internet. Το πρωτόκολλο αυτό είναι ακόμα υπό ανάπτυξη.

Υπάρχουν τρία μέρη που αποτελούν το SET : ένα "ηλεκτρονικό πορτοφόλι" που υπάρχει στον υπολογιστή του χρήστη, ένας server που τρέχει στα εμπορικά web sites, και ο SET server πληρωμής που τρέχει στις διάφορες τράπεζες των εμπόρων.

Για να χρησιμοποιήσουμε το SET σύστημα, πρέπει να εισάγουμε πρώτα τον αριθμό της πιστωτικής μας κάρτας μέσα στο πρόγραμμα του "ηλεκτρονικού πορτοφολιού". Οι περισσότερες εφαρμογές αποθηκεύουν τον αριθμό της πιστωτικής κάρτας σε ένα κρυπτογραφημένο αρχείο στον σκληρό μας δίσκο ή σε μια κάρτα (smart card). Το πρόγραμμα επίσης δημιουργεί ένα δημόσιο και ένα μυστικό κλειδί για την κρυπτογράφηση διάφορων οικονομικών πληροφοριών μας που θα σταλούν μέσω του Internet.

Όταν εμείς θελήσουμε να αγοράσουμε κάτι, ο αριθμός της πιστωτικής μας κάρτας κρυπτογραφείται και στέλνεται στον έμπορο. Το πρόγραμμα του έμπορου υπογράφει ψηφιακά το μήνυμα πληρωμής και το προωθεί στην τράπεζα όπου επεξεργάζεται. Έτσι ο SET server πληρωμής αποκρυπτογραφεί όλες τις πληροφορίες και χρεώνει την πιστωτική κάρτα. Τελικά, μια απόδειξη είσπραξης στέλνεται πίσω και σε εμάς, τους πελάτες, αλλά και στον έμπορο.

Οι Τράπεζες που επεξεργάζονται τις πιστωτικές κάρτες είναι ενθουσιασμένες για το SET επειδή αυτές κρατούν τους αριθμούς των πιστωτικών καρτών μακριά από τα χέρια των εμπόρων. Αυτό θα περιόριζε σημαντικά τις απάτες που γίνονται, γιατί είναι έμποροι, και όχι νεαροί hackers, που αυτοί είναι υπεύθυνοι για τις απάτες των πιστωτικών καρτών σήμερα.

Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς κρυπτογραφούνται χρησιμοποιώντας τον RSA αλγόριθμο. Αλλά δεν προσφέρει εμπιστευτικότητα (και κατά συνέπεια μυστικότητα) για τα υπόλοιπα στοιχεία της συναλλαγής του χρήστη. Αυτή ήταν μια αναγκαία συμβιβαστική λύση για να κερδισθεί η έγκριση για εξαγωγή του SET προγράμματος χωρίς περιορισμούς. Το SET παρέχει ακεραιότητα, αναγνώριση ταυτότητας και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές.

3.9.3 SSL (Secure Socket Layer)

Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης. Το SSL χρησιμοποιείται συχνά με το TCP/IP πρωτόκολλο του Internet. Το SSL είναι το κρυπτογραφικό σύστημα που χρησιμοποιείται από τους web browsers όπως είναι ο Netscape Navigator και ο Microsoft Internet Explorer, αλλά μπορεί να χρησιμοποιηθεί σε οποιοδήποτε υπηρεσία TCP/IP.

Οι SSL συνδέσεις συχνά ξεκινούν από την πλευρά του web browser εξαιτίας της χρήσης ενός ειδικού προθέματος στην URL διεύθυνση. Για παράδειγμα το πρόθεμα "https://" χρησιμοποιείται για να υποδείξει μια SSL κρυπτογραφημένη http σύνδεση, ενώ "snews://" χρησιμοποιείται για να υποδείξει μια SSL κρυπτογραφημένη NNTP σύνδεση.

Το SSL προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

Περίληψη

Μέχρι στιγμής έχουμε δει δυο από τα πιο σημαντικά πρωτόκολλα ασφαλείας που χρησιμοποιούνται για να ασφαλίζουν τις ηλεκτρονικές συναλλαγές στο ηλεκτρονικό εμπόριο. Όμως δεν είναι και τα μόνα που υπάρχουν. Υπάρχουν και άλλα πρωτόκολλα όπως το e-cash, e-wallets, e-checks, smart cards, τα οποία ασφαλίζουν τις ηλεκτρονικές συναλλαγές του χρήστη. Οι smart cards χρησιμοποιούν ειδικό υλικό προκειμένου να μπορέσει να προστατέψει και να χρησιμοποίηση τα δεδομένα για την πραγματοποίηση της ηλεκτρονικής συναλλαγής.

Συμπεράσματα

Ο πελάτης όπως είναι φυσικό δεν μπορεί να διακινδυνέψει να δώσει τον αριθμό της πιστωτικής του κάρτας χωρίς να είναι απόλυτα σίγουρος ότι τα προσωπικά στοιχεία του θα είναι ασφαλείς. Για τον λόγο αυτό ο πελάτης πρέπει να ενημερώνεται

1. σχετικά με τους τρόπους διασφάλισης των προσωπικών δεδομένων του,
2. ποιοι άλλοι εναλλακτικοί τρόποι πληρωμής του προσφέρονται και με τι κόστος,
3. αν υπάρχει κάποια εταιρεία (Έμπιστη Τρίτη Οντότητα) η οποία να πιστοποιεί την γνησιότητα του έμπορα,
4. μια εγγύηση για τα προϊόντα που αγοράζει.

Έχοντας όλα αυτά υπ' όψιν του ο πελάτης τότε θα είναι πλέον σίγουρος για την διασφάλιση των προσωπικών του στοιχείων από την μεριά του έμπορα και θα είναι σε θέση να πραγματοποίηση και να ολοκληρώσει την ηλεκτρονική συναλλαγή.

Το ερωτηματολόγιο που ακολουθεί είναι σχεδιασμένο για να μπορεί να το απαντήσουν όλοι όσοι χρησιμοποιούν το διαδίκτυο και γενικότερα όσοι χρησιμοποιούν τον υπολογιστή ανεξάρτητα με την εμπειρία που έχουν στο χώρο της πληροφορικής.

Κεφάλαιο 4°:

Ερωτηματολόγιο

4.1 Σκοπός του ερωτηματολογίου

Στα 3 πρώτα κεφάλαια αναφέρομαι σε γνωστούς ορισμούς και σε γεγονότα τα οποία είναι γνωστά σε άλλους λιγότερο και σε άλλους περισσότερο. Το ερωτηματολόγιο που ακολουθεί στην πραγματικότητα πρόκειται για μια τεκμηρίωση ,όσων αναφέρω παραπάνω, με αριθμούς. Οι ερωτήσεις διαμορφώθηκαν με τέτοιο τρόπο έτσι ώστε να καλύπτουν ένα ευρύ φάσμα όσο αφορά τις γνώσεις των Ελλήνων χρηστών. Για να υπάρχει μια αντικειμενικότερη άποψη για τους έλληνες χρήστες το ερωτηματολόγιο δημοσιεύτηκε στο διαδίκτυο, ώστε να απαντήσουν χρήστες. Οι ηλικία κυμαίνεται από 15 έως 45+ ετών και τα αποτελέσματα είναι εντυπωσιακά αφού επαναλαμβάνονται οι ίδιες ερωτήσεις με διαφορετική διατύπωση και ο ίδιος χρήστης έχει δώσει ,κατά μεγάλο ποσοστό, διαφορετική απάντηση.

4.2 Ερωτηματολόγιο

Ακολουθεί το ερωτηματολόγιο όπως βγήκε στο διαδίκτυο , καθώς και ο κώδικας που υπάρχει πίσω από το ερωτηματολόγιο για την συλλογή και αποθήκευση των απαντήσεων, καθώς και τα αποτελέσματα αναλυμένα.

1. Ξέρετε τι είναι ηλεκτρονικό εμπόριο?
Α)*ΝΑΙ*
Β)*Όχι*

2. Έχετε γνώση των κινδύνων που διατρέχετε κάθε φορά που συνδέεστε στο διαδίκτυο?
Α) *ΝΑΙ*
Β) *ΟΧΙ*
Γ) *Υπάρχει κάποιος που μπορεί να με βλάψει όσο είμαι συνδεμένος στο διαδίκτυο?*

3. Στο ηλεκτρονικό εμπόριο πρέπει να υπάρχει ενημέρωση των πελατών σχετικά με την σχετικά με την ασφάλεια των προσωπικών δεδομένων τους.
   Α) *ΝΑΙ*
   Β) *ΟΧΙ*

4. Η ασφάλεια πρέπει ,κατά την γνώμη σας, να υπάρχει σε ολόκληρη την ιστοσελίδα ή στην φόρμα που συμπληρώνονται τα προσωπικά στοιχεία του χρήστη.
   Α) *Σε ολόκληρη την ιστοσελίδα*
   Β) *Μόνο στην σελίδα που συμπληρώνω τα προσωπικά στοιχεία μου.*

5. Πιστεύεται ότι η δομή του ηλεκτρονικού εμπορίου πρέπει να είναι το ίδιο ασφαλή, όσο και τα πρωτόκολλα που χρησιμοποιούνται για την ασφάλεια.
   Α)*ΝΑΙ*
   Β) *Όχι*

6. Μια τοποθεσία χαρακτηρίζεται ασφαλής όταν:
   Α) *στην κάτω γραμμή του explorer υπάρχει ένα ανοιχτό λουκέτο,*
   Β) *όταν υπάρχει ένα κλειστό λουκέτο.*

7. Κρίνεται απαραίτητη την χρήση των «ψηφιακών υπογραφών» (Digital ID's) για την πιστοποίηση ενός μέλους στο ηλεκτρονικό εμπόριο?
   Α) *Ναι, είναι απαραίτητη,*
   Β) *Όχι, δεν είναι απαραίτητη,*
   Γ) *Ο κωδικός πρόσβασης είναι αρκετός για την πιστοποίηση του μέλους.*

8. Με την αποστολή του αριθμού της πιστωτικής κάρτας, πρέπει να στέλνεται η «ψηφιακή υπογραφή» και η «ψηφιακή ταυτότητα» του χρήστη για την ολοκλήρωση της συναλλαγής?
   Α) *Ναι, το θεωρώ απαραίτητο,*
   Β) *Όχι, δεν είναι απαραίτητα,*
   Γ) *Αρκεί ένα πολύ καλό επίπεδο ασφάλειας για την αποστολή.*

9. Η χρήση «έξυπνων καρτών» (smart cards) διασφαλίζουν τα προσωπικά δεδομένα. Θεωρείται ότι είναι απαραίτητες στο ηλεκτρονικό εμπόριο?
   Α)*Ναι, είναι απαραίτητες,*
   Β) *Όχι, δεν είναι απαραίτητες,*
   Γ) *Πρώτη φορά της ακούω, δεν ξέρω την χρησιμότητα τους.*

10. Εκτός από την χρήση των πιστωτικών καρτών στο ηλεκτρονικό εμπόριο, πρέπει να υπάρχει και άλλος τρόπος για την αγορά των προϊόντων?
    Α)*ΝΑΙ,*
    Β) *ΟΧΙ*

11. Η ύπαρξη μιας έμπιστης τρίτης οντότητας η οποία θα διασφαλίζει την πιστοποίηση του πελάτη και του εμπόρου μειώνει τον κίνδυνο κλοπής των προσωπικών στοιχείων του πελάτη, καθώς και την περίπτωση εξαπάτησης. Η ύπαρξη της :

Α)*μειώνει την δυσπιστία του χρήστη στο ηλεκτρονικό εμπόριο,*

Β) *βοηθάει στην διασφάλιση των προσωπικών στοιχείων χωρίς να γίνεται αντιληπτό από τον χρήστη,*

Γ) *και τα δυο.*

12. Θα πραγματοποιούσατε ηλεκτρονική συναλλαγή σε ηλεκτρονικό κατάστημα στην Ελλάδα?

Α) *Αν υπάρχει διασφάλιση των προσωπικών δεδομένων, φυσικά,*

Β) *Αν υπάρχουν και άλλοι τρόποι πληρωμής εκτός από την πιστωτική κάρτα.*

Παρακαλώ συμπληρώστε τα παρακάτω πεδία. Παρακαλώ να ανταποκρίνονται στην πραγματικότητα όποια πεδία έχουν το *. Ευχαριστώ.

Ψευδώνυμο:
***Εμπειρία σχετική με το θέμα:**
***Επάγγελμα:**
***Ηλικία:**
***Χώρα:**

Πατήστε το κουμπί «Αποστολή».

Ευχαριστώ που απαντήσατε στο ερωτηματολόγιο. Για απορίες στείλτε e-mail.

4.2 *Κώδικας ερωτηματολογίου*

4.2.1 *PHP*

Όνομα αρχείου: Data.php

```
<?php
   /* Connecting, selecting database */

//Here put server ip, username , password
  $link = mysql_connect("localhost", "ODBC", "")
```

```
  or die("Could not connect : " . mysql_error());
   /*print "Connected successfully";*/
   mysql_select_db("Questions") or die("Could not select database");

   /* Performing SQL query */
   $query = "INSERT INTO data
(text1,text2,text3,text4,text5,text6,text7,text8,text9,text10,text11,text12,name,empiri
a,age,country,job) VALUES
('$text1','$text2','$text3','$text4','$text5','$text6','$text7','$text8','$text9','$text10','$text
11','$text12','$name','$empiria','$age','$country','$job')";

//Execute the query

   $result = mysql_query($query) or die("Query failed : " . mysql_error());

?>
```

Όνομα αρχείου: show_data.php

```
<?php
mysql_connect("localhost","ODBC","") or die ("Could not connect in the database");
mysql_select_db("Questions");
$query = "SELECT * FROM data";
$result = mysql_query($query);
while($line=mysql_fetch_array($result, MYSQL_ASSOC))
{
echo "apanthsh1 ";
echo $line["text1"];
echo "<br>";
echo "apanthsh2 ";
echo $line["text2"];
echo "<br>";
echo "apanthsh3 ";
echo $line["text3"];
echo "<br>";
echo "apanthsh4 ";
echo $line["text4"];
echo "<br>";
echo "apanthsh5 ";
echo $line["text5"];
echo "<br>";
echo "apanthsh6 ";
echo $line["text6"];
echo "<br>";
```

```
echo "apanthsh7 ";
echo $line["text7"];
echo "<br>";
echo "apanthsh8 ";
echo $line["text8"];
echo "<br>";
echo "apanthsh9 ";
echo $line["text9"];
echo "<br>";
echo "apanthsh10 ";
echo $line["text10"];
echo "<br>";
echo "apanthsh11 ";
echo $line["text11"];
echo "<br>";
echo "apanthsh12 ";
echo $line["text12"];
echo "<br>";
echo "name ";
echo $line["nickname"];
echo "<br>";
echo "empiria ";
echo $line["empiria"];
echo "<br>";
echo "age ";
echo $line["age"];
echo "<br>";
echo "job ";
echo $line["job"];
echo "<br>";
echo "country ";
echo $line["country"];
//mysql_free_result($result);
}
?>
```

Αυτό που κάνουν τα PHP αρχεία είναι να αποθηκεύουν και να εμφανίζουν τις απαντήσεις που δίνουν οι ερωτηθέντες. Για λόγους ασφάλειας των αποτελεσμάτων τα αρχεία είναι γραμμένα στην γλώσσα προγραμματισμού PHP η οποία εκτελείται μόνο από την μεριά του εξυπηρετητή και όχι από την μεριά που πελάτη με αποτέλεσμα ο παραπάνω κώδικας να μην είναι ορατός όταν προσπαθήσει κάποιος να δει τα αποτελέσματα ή που αποθηκεύονται και πως. Για κάθε κενή απάντηση η ΒΑΣΗ ΔΕΔΟΜΕΝΩΝ έβαζε την τιμή «Δεν ξέρω / Δεν απαντώ».

4.2.2 *HTML*

Όνομα αρχείου: Questions1.html

```
//Questioner code
<html>
<head><title>Ερωτηματολόγιο στα πλαίσια της πτυχιακής </title>
</head>
<body link=blue alink=blue vlink=blue>
<h2 align="center">Ερωτηματολόγιο για την ασφάλεια στο ηλεκτρονικό
εμπόριο</h2><br>
<p>Πληκτρολογήστε την απάντηση στα <input type="text" disable="true"> ή
μαρκάρετε την απάντηση και κάνετε copy και paste  στο <input type="text"
disable="true">.
<br>
<br>
<br>
<form method="post" action="data1.php">
<ol>
<li>Ξέρετε τι είναι το ηλεκτρονικό εμπόριο?
<ul>
<li>Ναι
<li>Όχι
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text1" size=40 value="
">       <a
href="help.html#r1">Επεξηγήσεις</a>
<br>
<br>

<li>Έχετε γνώση των κινδύνων που διατρέχετε κάθε φορά που είστε συνδεμένος
στο διαδίκτυο?
<ul>
<li>Ναι
<li>Όχι
<li>Υπάρχει κάποιος που μπορεί να με βλάψει όσο είμαι συνδεμένος στο διαδίκτυο?
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text2" size=40 value="
">       <a
href="help.html#r2">Επεξηγήσεις</a>
<br>
<br>
```

Στο ηλεκτρονικό εμπόριο πρέπει να υπάρχει ενημέρωση των πελατών σχετικά με την ασφάλεια των προσωπικών δεδομένων τους

Ναι
Όχι

<label>Απάντηση:</label><input type="text" name="text3" size=40 value=" ">

Η ασφάλεια πρέπει να υπάρχει σε ολόκληρη την ιστοσελίδα ή μόνο στην φόρμα που συμπληρώνονται τα προσωπικά στοιχεία του χρήστη.

Σε ολόκληρη την ιστοσελίδα
Μόνο στην σελίδα που συμπληρώνονται τα προσωπικά στοιχεία του πελάτη.

<label>Απάντηση:</label><input type="text" name="text4" size=40 value=" ">

Πιστεύεται ότι η δομή του ηλεκτρονικού εμπορίου πρέπει να είναι το ίδιο ασφαλή, όσο και τα πρωτόκολλα που χρησιμοποιούνται για την ασφάλεια των προσωπικών στοιχείων.

Ναι
Όχι

<label>Απάντηση:</label><input type="text" name="text5" size=40 value="
">   Τι είναι δομή?   Τι είναι πρωτόκολλο?

Πότε θα χαρακτηρίζατε μια τοποθεσία ηλεκτρονικού εμπορίου ασφαλής:

όταν στην κάτω γραμμή του φυλλομετρητή υπάρχει ένα κλειστό λουκέτο,
όταν στην κάτω γραμμή του φυλλομετρητή δεν υπάρχει τίποτα


```
<br>
<label>Απάντηση:</label><input type="text" name="text6" size=40 value="
">       <a
href="help.html#r7">Επεξηγήσεις</a>
<br>
<br>

<li>Κρίνεται απαραίτητη την χρήση των "ψηφιακών υπογραφών" (Digital
Signatures) για την πιστοποίηση ενός μέλους στο ηλεκτρονικό εμπόριο?
<ul>
<li>Ναι, είναι απαραίτητη,
<li>Όχι, δεν είναι απαραίτητη,
<li>Ο κωδικός πρόσβασης είναι αρκετός για την πιστοποίηση του μέλους.
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text7" size=40 value=" ">
<br>
<br>

<li>Με την αποστολή του αριθμού της πιστωτικής κάρτας, πρέπει να στέλνονται και
η "ψηφιακή υπογραφή" και η " ψηφιακή ταυτότητα" του χρήστη για την ολοκλήρωση
της συναλλαγής?
<ul>
<li>Ναί, το θεωρώ απαραίτητο,
<li>Όχι, δεν χρειάζεται,
<li>Αρκεί ένα πολύ καλό επίπεδο ασφάλειας για την αποστολή.
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text8" size=40 value="
">       <a
href="help.html#r8">Επεξηγήσεις</a>
<br>
<br>

<li>Η χρήση "έξυπνων καρτών" (smart cards) διασφαλίζουν τα προσωπικά
δεδομένα. Θεωρείται ότι είναι απαραίτητες στο ηλεκτρονικό εμπόριο?
<ul>
<li>Ναί, είναι απαραίτητες
<li>Όχι,
<li>Πρώτη φορά τις ακούω, δεν ξέρω κατά πόσο χρησιμεύουν στο ηλεκτρονικό
εμπόριο.
</ul>
```

```
<br>
<label>Απάντηση:</label><input type="text" name="text9" size=40 value="
">       <a
href="help.html#r9">Επεξηγήσεις</a>
<br>
<br>

<li>Εκτός από την χρήση των πιστωτικών καρτών στο ηλεκτρονικό εμπόριο, πρέπει
να υπάρχει και άλλος εναλλακτικός τρόπος πληρωμής?
<ul>
<li>Ναί,
<li>Όχι
</ul>
```

```
<br>
<label>Απάντηση:</label><input type="text" name="text10" size=40 value=" ">
<br>
<br>

<li>Η Έμπιστης Τρίτη Οντότητα έχει σαν σκοπό την πιστοποίηση του πελάτη για
τον έμπορο, αλλά και την πιστοποίηση του εμπόρου για τον πελάτη με αποτέλεσμα
να μειώνεται ο κίνδυνος κλοπής ή εξαπάτησης. Η ύπαρξη της:
<ul>
<li>μειώνει την δυσπιστία του χρήστη στο ηλεκτρονικό εμπόριο,
<li>βοηθάει στην διασφάλιση, των προσωπικών στοιχείων του χρήστη,
<li> και τα δύο
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text11" size=40 value="
">       <a
href="help.html#r10">Επεξηγήσεις</a>
<br>
<br>

<li>Θα πραγματοποιούσατε ηλεκτρονική συναλλαγή σε ηλεκτρονικό κατάστημα
στην Ελλάδα?
<ul>
<li>Αν υπάρχει διασφάλιση των προσωπικών στοιχείων μου, φυσικά
<li>Αν υπάρχουν και άλλοι τρόποι πληρωμής εκτός από την πιστωτική κάρτα.
</ul>

<br>
<label>Απάντηση:</label><input type="text" name="text12" size=40 value=" ">
```

```
</ol>
<br>
<br>
<b>Παρακαλώ συμπληρώστε τα παρακάτω στοιχεία. <u>ΔΕΝ</u> είναι απαραίτητο
να ανταποκρίνονται στην πραγματικότητα όσα δεν έχουν το <font
color="red">*</font></b>
<br><br>
<table>
<tr><td><label>Ψευδόνυμο/Nickname:</label></td><td><input type="text"
name="nickname" value=" "></td>
<tr><td><label><font color="red">*</font>Εμπειρία:</label></td><td><input
type="text" name="empiria" value=" "></td>
<tr><td><label>Επάγγελμα:</label></td><td><input type="text" name="job" value="
"></td>
<tr><td><label><font color="red">*</font>Ηλικία:</label></td><td><input
type="text" name="age" value=" "></td>
<tr><td><label><font color="red">*</font>Χώρα:</label></td><td><input type="text"
name="country" value=" "></td>
</table>
<br>

<input type="submit" value="Αποστολή φόρμας">
</form>

</body>
</html>
```

Όνομα αρχείου: help.html

```
<html><head><title>Ερωτήσεις -- Απαντήσεις</title></head>
<body>

<h2 align="center"> Ερωτήσεις -- Απαντήσεις</h2>
<br>
<br>
<center><b><a name="er1">Τι είναι ηλεκτρονικό εμπόριο?</a></b></center>
<p align="justify">Με τον όρο ηλεκτρονικό εμπόριο εννοούμε αγορά ή πώληση
αγαθών ή υπηρεσιών προς καταναλωτές ή και επιχειρήσεις
από επιχειρήσεις.

 </p>

<center><b><a name="er2">Ποίοι είναι οι κίνδυνοι που υπάρχουν στο
διαδίκτυο?</a></b></center>
<p align="justify">Όταν ένας χρήστης συνδέεται στο διαδίκτυο αυτόματα μπορεί
```

κάποιος άλλος χρήστης ή πρόγραμμα να βρει την IP του.
Με βάση την IP και με την βοήθεια μερικών προγραμμάτων μπορεί να αποκτήσει πρόσβαση ένας τρίτος. Όταν πάρει πρόσβαση
στον υπολογιστή μπορεί να κάμει ότι θέλει στο σύστημα από μια απλή μετακίνηση των αρχείων μέχρι και διαγραφή του λειτουργικού συστήματος.
Ο λόγος είναι απλός.... το κάνει για να διασκεδάσει!!! Έκτος ότι κάποιος τρίτος μπορεί
να συνδεθεί με τον υπολογιστή, είναι δυνατόν να εγκατασταθούν στο δίσκο του υπολογιστή ιοί, σκουλήκια, και δούρειοι ίπποι,
τα οποία μπορούν να δώσουν πρόσβαση σε τρίτους, αλλά και να προκαλέσουν ζημιές στο λειτουργικό σύστημα.

Τι εννοείται όταν λετε δομή του "ηλεκτρονικού εμπορίου"?
Με τον όρο δομή εννοούμε τον κώδικα με τον οποίο είναι φτιαγμένο ένα ηλεκτρονικό κατάστημα.
Π.χ αν χρησιμοποιεί PHP, MySQL, C, C++,...

Τι είναι το πρωτόκολλο και ποιος ο ρόλος του στην ασφάλεια?
Πρωτόκολλο είναι ένα είδος λογισμικού το οποίο χρησιμοποιείται για την επικοινωνία των επιπέδων του
συστήματος OSI, στην επικοινωνία δυο υπολογιστών, αλλά και στην ασφάλεια των προσωπικών στοιχείων του χρήστη.
Τα πρωτόκολλα δεν χρησιμοποιούνται σε όλα τα επίπεδα, με αποτέλεσμα να έχουμε διαφορετικό επίπεδο ασφάλειας.
Π.χ. το πρωτόκολλο SET χρησιμοποιείται αποκλειστικά και μόνο για την κρυπτογράφηση του αριθμού των πιστωτικών καρτών,
ενώ το SSL χρησιμοποιείται για την διασφάλιση των στοιχείων στο επίπεδο μεταφοράς.

Πως χαρακτηρίζεται μια τοποθεσία ασφαλής?
Μια τοποθεσία χαρακτηρίζεται ασφαλείς όταν στην κάτω γραμμή του φυλλομετρητή (η οποία λέγεται status bar)
εμφανίζεται ένα λουκέτο κλειστό.

Τι είναι οι "ψηφιακές υπογραφές" και τι είναι οι "ψηφιακές ταυτότητες"?
<u>Ψηφιακές Υπογραφές</u>
Οι "ψηφιακές υπογραφές" είναι ένα κομμάτι πληροφορίας το οποίο χρησιμοποιείται για να πιστοποιεί την
γνησιότητα ενός εγγράφου. Οι "ψηφιακές υπογραφές" χορηγούνται από την Έμπιστη Τρίτη Οντότητα. Χρησιμοποιούν αλγόριθμους κρυπτογράφησης για την προστασία των δεδομένων. Ένα μέρος του κλειδιού το

κρατάει η Ε.Τ.Ο για λόγους ασφάλειας.
Οι "ψηφιακές ταυτότητες" χρησιμοποιούνται όπως οι πραγματικές ταυτότητες που έχουμε στην κατοχή μας και μπορούμε να την πάρουμε από
ένα μέρος μόνο. Έχουν δηλαδή την ίδια ακριβός λειτουργία με την μόνη διαφορά ότι είναι ηλεκτρονικές. Η μόνη αρμόδια για την έκδοση
είναι η Ε.Τ.Ο (Έμπιστη Τρίτη Οντότητα).

Τι είναι οι "έξυπνες κάρτες"?
Οι "έξυπνες κάρτες" μοιάζουν με τις πιστωτικές κάρτες, αλλά η χρησιμότητα τους είναι τελείως διαφορετική.
Μπορούν να αποθηκεύουν χρηματικές μονάδες, μέχρι και να επεξεργαζονται, να κρυπτογραφουν, να αποκρυπτογραφούν, και να μεταφέρουν
δεδομένα που θέλει ο χρήστη. Για να μπορέσουν να λειτουργήσουν σωστά ο χρήστης πρέπει να έχει είδικα τερματικά τα οποία λεγονται
readers και μόνο με αυτά μπορεί να χρησιμοποιήσει τις "έξυπνες κάρτες". Οι γνώστες, σε όλους μας τηλεκάρτες, είναι ένα είδος
"έξυπνης κάρτας" η οποία έχει ήδη αποθηκευμένες χρηματικές μονάδες και χρησιμοποιείται από ειδικές τηλεφωνικές συσκευές.
Μόλις τελειώσουν οι χρηματικές μονάδες η κάρτα βγαίνει εκτός λειτουργίας και δεν μπορεί να ξαναχρησιμοποιηθεί.

Τι είναι και τι κάνει η Έμπιστη Τρίτη Οντότητα?
Η Έμπιστη Τρίτη Οντότητα είναι ένας οργανισμός ο οποίος μεσολαβεί για να μπορέσει να πιστοποίηση την
ταυτότητα τόσο από την μεριά του πελάτη, όσο και από την μεριά του πωλητή. Επίσης εκδίδει "ψηφιακές υπογραφές" και
"ψηφιακές ταυτότητες", και κρατάει ένα μέρος του κλειδιού που χρησιμοποιούν οι δυο πλευρές, ώστε να μην μπορεί η μια πλευρά να
εξαπάτηση την άλλη.

</body>
</html>

4.3 Ανάλυση των αποτελεσμάτων

Ανάλυση των αποτελεσμάτων του ερωτηματολογίου το οποίο είχε διάρκεια 1 μήνα και απάντησαν 77 άτομα, όλοι χρήστες του διαδικτύου η εμπειρία τους είναι από καθόλου (0) έως τέλεια (10).

Τα διαγράμματα μπορείται να τα δείτε στην προσωπική μου σελίδα http://www.psiloriths.com/pp/~yskapell/ptixiaki/diagrammata.html

Ερώτηση 1: «Ξέρετε τι είναι το ηλεκτρονικό εμπόριο?»

Στην ερώτηση 1 το **94,81%** των ερωτηθέντων απάντησαν ότι γνωρίζουν *τι είναι το ηλεκτρονικό εμπόριο*, ενώ μόλις το **5,19%** των ερωτηθέντων *δεν γνωρίζουν τι είναι το ηλεκτρονικό εμπόριο*. Κρίνοντας από τα αποτελέσματα μπορούμε να συμπεράνουμε ότι οι περισσότεροι Έλληνες γνωρίζουν την υπηρεσία αυτή του διαδικτύου και πιθανόν να την έχουν χρησιμοποιήσει αν και το ηλεκτρονικό εμπόριο στην Ελλάδα κάνει ακόμη τα πρώτα του βήματα.

Ερώτηση 2: «Έχετε γνώση των κινδύνων που διατρέχετε κάθε φορά που είστε συνδεμένος στο διαδίκτυο ?»

Στην δεύτερη ερώτηση το **81,82%** απάντησε ότι *γνωρίζει τους κινδύνους, από ποιους κινδυνεύει όταν είναι συνδεμένος στο διαδίκτυο*. Από αυτό το αποτέλεσμα ότι ένα μεγάλο ποσοστό των Ελλήνων χρηστών κάνει χρήση anti-virus και firewall για να μπορέσει να προστατέψει τα αρχεία του και τα προσωπικά του δεδομένα από μη-εξουσιοδοτημένους χρήστες του διαδικτύου. Παράλληλα όταν πραγματοποιούν μια συναλλαγή με κάποιο ηλεκτρονικό κατάστημα βοηθάνε στην καλύτερη διασφάλιση των προσωπικών στοιχείων τους, αφού οι περισσότερες επιθέσεις για την κλοπή πιστωτικών καρτών γίνεται στον υπολογιστή του χρήστη και όχι τόσο πολύ στο ηλεκτρονικό κατάστημα.

Αντίθετα, ένα μικρό ποσοστό των ερωτηθέντων, **10,39%** *δεν γνωρίζει τους κινδύνους του διαδικτύου* με αποτέλεσμα να μην χρησιμοποιεί τα κατάλληλα εργαλεία για να τους περιορίσει. Αυτό έχει σαν αποτέλεσμα οι ευαίσθητες πληροφορίες που πιθανόν να διακινήσει στο διαδίκτυο να κλαπούν ευκολότερα.

Τέλος το **7,79%** *απάντησε ότι ναι μεν γνωρίζουν τους κινδύνους όταν είναι συνδεμένοι στο διαδίκτυο (virus, worm, Trojans), αλλά δεν γνωρίζουν ότι μπορεί κάποιος τρίτος να τους βλάψει, χωρίς λόγο.* Αυτό έχει σαν αποτέλεσμα να χρησιμοποιούν τα anti-virus και τα firewalls μόνο όταν τους παρουσιαστεί κάποιο πρόβλημα.

Ερώτηση 3: «Στο ηλεκτρονικό εμπόριο πρέπει να υπάρχει ενημέρωση των πελατών σχετικά με την ασφάλεια των προσωπικών δεδομένων τους.»

Η ερώτηση αυτή είναι ένα από τα χαρακτηριστικά του ηλεκτρονικού εμπορίου. Το **90,91%** απάντησε ότι *η ενημέρωση από τα ηλεκτρονικά καταστήματα όσο αφορά την ασφάλεια των προσωπικών δεδομένων τους, είναι απαραίτητη*. Υπάρχουν ηλεκτρονικά καταστήματα στην Ελλάδα τα οποία δεν αναφέρουν αν τα προσωπικά στοιχεία του χρήστη ασφαλίζονται.

Το **5,19%** απάντησε ότι *δεν είναι απαραίτητη* η ενημέρωση των πελατών σχετικά με την ασφάλεια των προσωπικών δεδομένων τους, ίσος γιατί το θεωρούν αυτονόητο ότι πρέπει να προστατεύονται τα στοιχεία τους, μόλις το **3,90%** *δεν απάντησε σε αυτή την ερώτηση.*

Ερώτηση 4: «Η ασφάλεια πρέπει να υπάρχει σε ολόκληρη την ιστοσελίδα ή μόνο στην φόρμα που συμπληρώνονται τα προσωπικά στοιχεία του χρήστη?»

Ένα μεγάλο ποσοστό των Ελλήνων χρηστών του διαδικτύου , **70,13%** , απάντησε ότι *η ασφάλεια που έχει ένα ηλεκτρονικό κατάστημα πρέπει να υπάρχει σε ολόκληρη την ιστοσελίδα.* Δηλαδή να τον ακολουθεί από την στιγμή που θα «μπει» στο ηλεκτρονικό κατάστημα μέχρι και την στιγμή που θα λάβει το ευχαριστήριο e-mail.
Αντίθετα το **24,68%** θεωρούν ότι *η ασφάλεια πρέπει να υπάρχει μόνο στην φόρμα που συμπληρώνονται τα προσωπικά στοιχεία του χρήστη* κάτι που γίνεται ήδη στα περισσότερα ηλεκτρονικά καταστήματα.
Το μόλις **5,19%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

Ερώτηση 5: «Πιστεύεται ότι η δομή του ηλεκτρονικού εμπορίου πρέπει να είναι το ίδιο ασφαλή, όσο και τα πρωτόκολλα που χρησιμοποιούνται για την ασφάλεια των προσωπικών στοιχείων.»

Η ερώτηση αυτή είναι καθοριστική για το ηλεκτρονικό εμπόριο, αφού ένας πολύ καλός Χακερ με πολύ καλές γνώσεις προγραμματισμού μπορεί να εκμεταλλευτεί την έλλειψη ασφάλειας στην δομή του ηλεκτρονικού εμπορίου, για να κλέψει τα προσωπικά στοιχεία του χρήστη. (Για περισσότερες λεπτομέρειες στο κεφάλαιο 1 -> [δομή] της πτυχιακής μου.)
Το **81,82%** απάντησε ότι *η ασφάλεια στην δομή του ηλεκτρονικού εμπορίου είναι το ίδιο σημαντική,* όσο σημαντική είναι και η ασφάλεια των προσωπικών στοιχείων του χρήστη, ενώ μόλις το **10,93%** απάντησε ότι *η ασφάλεια στην δομή δεν είναι τόσο σημαντική* όσο είναι η ασφάλεια των προσωπικών στοιχείων του χρήστη.
Σε αυτή την ερώτηση το **7,79%** *δεν ήξερε να απαντήσει.*

Ερώτηση 6: «Πότε θα χαρακτηρίζατε μια τοποθεσία ηλεκτρονικού εμπορίου ασφαλής.»

Στην ερώτηση το **76,62%** απάντησε ότι *γνωρίζει πότε βρίσκεται σε μια ασφαλή τοποθεσία*. Το αναγνωριστικό είναι το λουκέτο που εμφανίζεται στην κάτω μεριά του φυλλομετρητή και φυσικά όταν είναι κλειστό, ενώ το **11,69%** απάντησε ότι *δεν ξέρει πότε βρίσκεται σε ασφαλή τοποθεσία* και το ίδιο (**11,96%**) ποσοστό *δεν ήξερε και δεν απάντησε σε αυτή την ερώτηση.*

Ερώτηση 7: «Κρίνεται απαραίτητη την χρήση «ψηφιακών υπογραφών» για την πιστοποίηση ενός μέλους στο ηλεκτρονικό εμπόριο?»
Το **55,84%** των ερωτηθέντων απάντησε ότι *κρίνει απαραίτητη την χρήση των «ψηφιακών πιστοποιητικών» για την πιστοποίηση ενός μέλους*, αφού ο κωδικός πρόσβασης μπορεί να κλαπεί ή και να αλλαχτεί (Αυτό μπορεί να γίνει εύκολα όταν ο κωδικός πρόσβασης είναι 4 ψηφίων ή έχει κάποια σχέση με τον χρήστη π.χ. ημερομηνία γεννήσεως, έτος γεννήσεως, επώνυμο, κλπ.).

Το **10,39%** *ΔΕΝ θεωρεί ότι είναι απαραίτητη η χρήση των «ψηφιακών υπογραφών»*, ενώ το 24,68% πιστεύει ότι ο κωδικός πρόσβασης είναι αρκετός για να την πιστοποίηση του μέλους.

Τέλος, το **9,09%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

Ερώτηση 8: «Με την αποστολή του αριθμού της πιστωτικής κάρτας, πρέπει να στέλνονται και η «ψηφιακή υπογραφή και η ψηφιακή ταυτότητα» του χρήστη για την ολοκλήρωση της συναλλαγής?»

Το **55,84%** των ερωτηθέντων απάντησαν *ότι είναι απαραίτητο να στέλνονται (η ψηφιακή ταυτότητα και η ψηφιακή υπογραφή) για την ολοκλήρωση της συναλλαγής.* Με αυτό τον τρόπο αισθάνονται σίγουροί ότι δεν θα χρεωθούν προϊόντα που δεν θα έχουν παραγγείλει.

Αντίθετα το **10,39%** *δεν θεωρεί την απαραίτητη για την ολοκλήρωση της συναλλαγής*, σε σχέση με το 24,68% που πιστεύουν ότι εφ' όσον *υπάρχει ένα καλό επίπεδο ασφάλειας* των προσωπικών δεδομένων τους οι «ψηφιακές υπογραφές» και οι «ψηφιακές ταυτότητες» είναι περιττές στον χώρο του ηλεκτρονικού εμπορίου.

Τέλος, το **9,09%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

Ερώτηση 9: «Η χρήση «έξυπνων καρτών (smart card)» διασφαλίζουν τα προσωπικά δεδομένα. Θεωρείται ότι είναι απαραίτητες στο ηλεκτρονικό εμπόριο?»

Το **38,96%** *θεωρεί ότι είναι απαραίτητες στο ηλεκτρονικό εμπόριο*, αντίθετα το **10,39%** *θεωρεί ότι δεν χρειάζονται στο ηλεκτρονικό εμπόριο*. Η πλειοψηφία των Ελλήνων χρηστών του διαδικτύου ,δηλαδή το **41,56%** , *δεν γνωρίζει τι είναι οι έξυπνες κάρτες και κατά πόσο χρησιμεύουν στο ηλεκτρονικό εμπόριο.*

Το μόλις **9,09%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

Ερώτηση 10: «Εκτός από την χρήση πιστωτικών καρτών στο ηλεκτρονικό εμπόριο, πρέπει να υπάρχει και άλλος εναλλακτικός τρόπος πληρωμής?»

Το **77,92%** των ερωτηθέντων θεωρούν ότι *πρέπει να υπάρχουν εναλλακτικοί τρόποι πληρωμής στο χώρο του ηλεκτρονικού εμπορίου,* σε αντίθεση με το **12,99%** το οποίο *θεωρεί ότι η χρήση της πιστωτικής κάρτας είναι ένας καλός τρόπος πληρωμής*.

Το **9,09%** *δεν ήξεραν να απαντήσουν σε αυτή την ερώτηση.*

Ερώτηση 11: «Η Εμπιστη Τρίτη Οντότητα έχει σαν σκοπό την πιστοποίηση του πελάτη για τον έμπορο, αλλά και την πιστοποίηση του εμπόρου για τον πελάτη με αποτέλεσμα να μειώνεται ο κίνδυνος κλοπής ή εξαπάτησης. Η ύπαρξη της: »

Μειώνει την δυσπιστία του χρήστη στο ηλεκτρονικό εμπόριο απάντησε το **3,90%** των ερωτηθέντων, ενώ το **14,29%** απάντησε ότι η Εμπιστη Τρίτη Οντότητα *βοηθάει στην διασφάλιση των προσωπικών στοιχείων του χρήστη*.

Ένα μεγάλο ποσοστό των ερωτηθέντων το **70,13%** απάντησε ότι η Έμπιστη Τρίτη Οντότητα *βοηθάει και στα δυο*, δηλαδή στο να μειώσει την δυσπιστία του χρήστη στο ηλεκτρονικό εμπόριο αλλά ταυτόχρονα να διασφαλίζει και τα προσωπικά στοιχεία του.

Το **11,69%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

Ερώτηση 12: «θα πραγματοποιούσατε ηλεκτρονική συναλλαγή σε ηλεκτρονικό κατάστημα στην Ελλάδα?»

Το **55,84%** των ερωτηθέντων απάντησε ότι *θα πραγματοποιούσε ηλεκτρονική συναλλαγή με την προϋπόθεση ότι τα προσωπικά στοιχεία του θα διασφαλίζονταν*, ενώ το **35,06%** *αν υπήρχαν και άλλοι τρόποι πληρωμής εκτός από την πιστωτική κάρτα.*

Τέλος, το **9,09%** *δεν ήξερε να απαντήσει σε αυτή την ερώτηση.*

4.4 Συμπεράσματα απο το ερωτηματολόγιο:

Με τα αποτελέσματα των ερωτήσεων από το ερωτηματολόγιο καταλήγω στα εξής συμπεράσματα:

- Αν και οι περισσότεροι Έλληνες χρήστες του διαδικτύου θέλουν να υπάρχουν εναλλακτικοί τρόποι πληρωμής στο ηλεκτρονικό εμπόριο, εν τούτοις δύσκολα θα αποχωριζόντουσαν την πιστωτική τους κάρτα ακόμα και για τις ηλεκτρονικές αγορές τους.

- Το γεγονός ότι πολλοί Έλληνες χρήστες γνωρίζουν τι είναι ηλεκτρονικό εμπόριο και τους κινδύνους που διατρέχουν όταν είναι στο διαδίκτυο, μπορεί να βοηθήσει το ηλεκτρονικό εμπόριο να βελτιωθεί αρκετά και ειδικά στον τομέα της ασφάλειας. Στον τομέα του ηλεκτρονικού εμπορίου ανεξάρτητα τα πρωτόκολλα και τις

μεθόδου ασφάλειας που χρησιμοποιούνται, πρέπει και ο χρήστης να φροντίζει να ασφαλίζει και το δικό του ηλεκτρονικό υπολογιστή, για να μην μπορέσει ο επιτιθέμενος να κλέψει τα ευαίσθητα προσωπικά δεδομένα του. Έχει αποδειχτεί ότι όταν ένας επιτιθέμενος δεν μπορεί να περάσει στο σύστημα ασφάλειας ενός ηλεκτρονικού καταστήματος, τότε επιτίθεται στον αγοραστή γιατί ξέρει ότι δεν δυσκολευτεί στον να «μπει» και να κλέψει τις πληροφορίες που τον ενδιαφέρουν.

- Το ηλεκτρονικό εμπόριο στην Ελλάδα θα αναπτυχθεί περισσότερο όταν καθιερωθεί μια Έμπιστη Τρίτη Οντότητα. Με την ύπαρξη της οι ηλεκτρονικές συναλλαγές θα αυξάνονταν αφού ο Έλληνας θα ήξερε ότι δεν θα τον εξαπατούσαν. Η Έμπιστη Τρίτη Οντότητα έχει αρχίσει να κάνει τα πρώτα της βήματα στην Ελλάδα με την έκδοση ψηφιακών πιστοποιητικών τόσο για επιχειρήσεις όσο και για απλούς χρήστες. Τα «ψηφιακά πιστοποιητικά» είναι ακόμη σε πειραματικό στάδιο από το 2000, αλλά παρόλο ότι δεν έχουν δοθεί ακόμη επίσημα στην κυκλοφορία οποιοσδήποτε μπορεί να αγοράσει «ψηφιακό πιστοποιητικό» πληρώνοντας ένα μικρό ποσό.

- Παρόλο που η Ελλάδα είναι η δεύτερη χώρα με τους περισσότερους χρήστες στο διαδίκτυο (2.000.000 χρήστες) στον τομέα του ηλεκτρονικού εμπορίου είναι αρκετά πίσω όσο αφορά τους τρόπους πληρωμής, αλλά και τους τρόπους διασφάλισης προσωπικών δεδομένων.

Πολλοί από τους χρήστες δεν έχουν ακούσει και δεν ξέρουν τι είναι και πως μπορούν να βοηθήσουν στις ηλεκτρονικές συναλλαγές οι «Έξυπνες Κάρτες» (Smart Card). Οι «Έξυπνες Κάρτες» έχουν φτιαχτεί για να ασφαλίζουν τα ευαίσθητα προσωπικά δεδομένα του χρήστη, αλλά και να ασφαλίζουν με τον καλύτερο δυνατό τρόπο της ηλεκτρονικές συναλλαγές του. Για να επιτευχθεί αυτό οι «Έξυπνες Κάρτες» χρησιμοποιούν ειδικούς αναγνώστες οι οποίοι συνδέονται με τον ηλεκτρονικό υπολογιστή, διαβάζουν τα δεδομένα από την κάρτα και στην συνέχεια πραγματοποιούν την συναλλαγή. Υπάρχουν «Έξυπνες Κάρτες» οι οποίες επιτρέπουν στον

χρήστη να βάλει δικό του κωδικό πρόσβασης και να διαλέξει την μέθοδο και το κλειδί, για την κρυπτογράφηση των προσωπικών δεδομένων του.
Στην Ελλάδα οι «Έξυπνες Κάρτες» δεν χρησιμοποιούνται καθόλου για τις ηλεκτρονικές συναλλαγές.

4.5 Έρευνα σε 5 Ελληνικά Ηλεκτρονικά Καταστήματα

Με βάση τα παραπάνω αποτελέσματα από το ερωτηματολόγιο και τις απαντήσεις που έδωσαν οι Έλληνες χρήστες πραγματοποιήθηκε μια έρευνα σε 5 ελληνικά ηλεκτρονικά καταστήματα μέσω του διαδικτύου. Ο λόγος που έγινε η έρευνα αυτή είναι για να δούμε τι εναλλακτικές λύσεις έχει ο Έλληνας χρήστης για τις ηλεκτρονικές αγορές του. Διαπιστώθηκε ότι το ηλεκτρονικό εμπόριο στην Ελλάδα είναι πολύ πίσω σε σχέση με άλλα ηλεκτρονικά καταστήματα της Ευρώπης. Στα ηλεκτρονικά καταστήματα εξετάσθηκαν όλα στα εξής μέρη:

1) Δημιουργία Μέλους,
2) Αν υπάρχει ασφάλεια σε όλο το site ή μόνο στα προσωπικά δεδομένα
3) Αν δίνουν εναλλακτικού τρόπους πληρωμής εκτός πιστωτικών καρτών
4) Δομή τους
5) Δομή τους με βάση των κώδικα που χρησιμοποιούν.

Τα ηλεκτρονικά καταστήματα εξετάσθηκαν σε αυτούς τους τομείς με βάση το ερωτηματολόγιο που αναρτήθηκε και με βάση τις απαντήσεις που έδωσαν οι Έλληνες εν δυνάμει (όσοι ξέρουν να χρησιμοποιούν Η/Υ και το διαδίκτυο) πελάτες.

Σημείο 1ο: Δημιουργία Μέλους

Παπασωτηρίου

Στο ηλεκτρονικό κατάστημα του Παπασωτηρίου ,http://www.papasotiriou.gr, για να μπορέσει ένας χρήστης του διαδικτύου να πραγματοποίηση μια αγορά πρέπει να γίνει μέλος πρώτα και στην συνέχεια μπορεί να αγοράσει τα προϊόντα που επιθυμεί. Για να γίνει μέλος δίνει *όνομα χρήστη(username) κωδικό πρόσβασης (password)* και κάποια άλλα προσωπικά δεδομένα. Τα στοιχεία αυτά στέλνονται στους servers του καταστήματος με την χρήση ασφαλούς καναλιού SSL 128 bit *.
Η παραγγελία στέλνεται μέσο ασφαλούς καναλιού SSL 128 bit. Επίσης στην είσοδο των μελών χρησιμοποιείται το SSL για την ασφαλή μετάδοση τους.

*Τα περισσότερα ηλεκτρονικά καταστήματα χρησιμοποιούν αυτή τη μέθοδο, γιατί έχει αποδειχτεί ότι είναι σταθερή και προστατεύει τα δεδομένα που στέλνονται.

E-Shop.gr

Το e-shop.gr ζητάει από τον χρήστη να γίνει μέλος ,αν το επιθυμεί να γίνει μέλος δίνει *όνομα χρήστη(username) κωδικό πρόσβασης (password)* και κάποια άλλα προσωπικά

δεδομένα και την ίδια στιγμή μπορεί να πραγματοποίηση τις αγορές του, αλλά σε περίπτωση που δεν γίνει μέλος δεν σημαίνει ότι δεν μπορεί να πραγματοποίηση την αγορά των προϊόντων του.
Με αυτό τον τρόπο κρατάει την ανωνυμία των πελατών του προσφέροντας παράλληλα μια ασφαλή αποστολή της παραγγελίας αφού γίνεται και εδώ χρήση του πρωτοκόλλου SSL στα 128 bit. Αν κάποιος πελάτης θελήσει να γίνει μέλος δίνει τα προσωπικά του στοιχεία μέσα από μια ασφαλή τοποθεσία, ζητώντας εκτός των άλλων με τι τρόπο θα πληρώνει κάθε φορά που θα αγοράζει ένα προϊόν. Τα δεδομένα αυτά μπορούν να αλλάξουν (και εδώ γίνεται χρήση του SSL). Στην είσοδο μελών χρησιμοποιείται το πρωτόκολλο SSL.

Πλαίσιο

Στο ηλεκτρονικό κατάστημα του Πλαισίου ,http://www.plaisio.gr, απαιτεί την δημιουργία χρήστη για να μπορέσει να κάνει ένας χρήστης μια αγορά από το σπίτι του. Για την λήψη των προσωπικών στοιχείων του πελάτη ΔΕΝ χρησιμοποιείται κάποιο πρωτόκολλο ασφάλειας όπως στα παραπάνω καταστήματα, αλλά χρησιμοποιείται μια διαφορετική μέθοδος αποστολής της παραγγελίας. Η αποστολή γίνεται με την υπογραφή της VeriSign. Για την είσοδο των μελών του στο σύστημα χρησιμοποιείται η VeriSign για λόγους ασφαλείας.

MicroLand

Στο ηλεκτρονικό κατάστημα της MicroLand ,http://www.eml.gr, για να μπορέσει ένας χρήστης να κάνει μια αγορά, πρέπει να γίνει πρώτα μέλος. Κατά την είσοδο των μελών στο σύστημα, αλλά και κατά την δημιουργία μελών ΔΕΝ χρησιμοποιείται κάποιο σύστημα ασφάλειας. Αντίθετα, όμως με τα άλλα ηλεκτρονικά καταστήματα, το κατάστημα της MicroLand διαθέτει «Ψηφιακό Πιστοποιητικό» κάτι το οποίο ΔΕΝ ΔΙΑΘΕΤΟΥΝ τα άλλα τα ηλεκτρονικά καταστήματα.

Media Power

Το ηλεκτρονικό κατάστημα της Media Power ,http://www.thewebpower.com, δεν απαιτεί την δημιουργία μελών για την πραγματοποίηση αγοράς. Για την μετάδοση των προσωπικών δεδομένων, γίνεται χρήση ασφαλούς κέλυφους (SSH) και του πρωτοκόλλου SSL.

Σημείο 2ο: Ασφάλεια σε όλο το site

Τα ηλεκτρονικά καταστήματα που αναφέρθηκαν παραπάνω έχουν όλα ένα κοινό σημείο: Κανένα δεν κάνει χρήση κάποιου πρωτοκόλλου ασφαλείας όπως το SSL, αλλά χρησιμοποιούν πρωτόκολλα ασφαλείας (SSL) στην μετάδοση προσωπικών στοιχείων του χρήστη στην φόρμα παραγγελίας, στην είσοδο μελών στο σύστημα, και κάποια από αυτά και στην φόρμα για την δημιουργίας χρηστών.

Η χρήση κάποιου πρωτόκολλου ασφαλείας δεν είναι απαραίτητο να υπάρχει στα ηλεκτρονικά καταστήματα ,αν η δομή του κώδικα είναι σωστή και χωρίς λάθη, και αν ο

server στον οποίο βρίσκεται το ηλεκτρονικό κατάστημα προσφέρει την μέγιστη ασφάλεια. Όμως το να γίνεται χρήση πρωτόκολλου ασφαλείας σε ολόκληρο το ηλεκτρονικό κατάστημα, δίνει την αίσθηση της ασφάλειας στους πελάτες του ηλεκτρονικού καταστήματος.

Σημείο 3ο: Εναλλακτικοί Τρόποι Πληρωμής

Όλα τα ηλεκτρονικά καταστήματα που μελετήθηκαν, προσφέρουν και άλλους τρόπους πληρωμής εκτός από την πιστωτική κάρτα. Οι εναλλακτικοί τρόποι πληρωμής που προσφέρουν είναι:

- Αντικαταβολή,
- Κατάθεση του ποσού σε λογαριασμό τράπεζας (μια ή και περισσότερες τράπεζες)

Το ηλεκτρονικό κατάστημα του Πλαισίου εκτός από τους παραπάνω τρόπους πληρωμής δίνει και ένα άλλο πληρωμής. Αυτός είναι ο πελάτης να πληρώσει και να πάρει τα προιόντα που έχει παραγγείλει από το ηλεκτρονικό κατάστημα, πηγαίνοντας στο κοντινότερο κατάστημα του Πλαισίου που υπάρχει!!! Το πλαίσιο δίνει αυτή την δυνατότητα γιατί έχει καταστήματα σε όλη σχεδόν την Ελλάδα.

Αυτό που είναι εξαιρετικά ενδιαφέρον είναι το γεγονός ότι κανένα κατάστημα δεν δίνει την δυνατότητα για χρήση smart card, e-wallets, κάρτες προπληρωμένου χρόνου, για να μπορεί να κάνει τις αγορές του ο χρήστης ολόκληρο το 24ωρο και χωρίς να κινδυνεύει να χάσει όλα του τα χρήματα από επιδέξιους χακερς. Η αντικαταβολή είναι ο ασφαλέστερος τρόπος για τους πελάτες, αλλά το κόστος είναι λίγο μεγαλύτερο μια που έχει να πληρώσει ένα ποσό για την μεταφορική. Το ποσό αυτό κυμαίνεται και το κόστος του μπορεί να φτάσει από 5 - 10 ευρό. (Εξαρτάται αν είναι εντός ή εκτός Αθηνών). Το μειονέκτημα που έχει αυτός ο τρόπος πληρωμής είναι ότι πρέπει ο πελάτης να βρίσκεται στο σπίτι του όταν πρόκειται να φτάσει το προϊόν, σε αντίθεση με τις άλλες πληρωμές όπου μπορεί να πάει από το ταχυδρομείο να το πάρει όταν αυτός μπορεί.

Σημείο 4ο: Δομή

Αυτό το σημείο είναι το πιο σημαντικό για τα ηλεκτρονικά καταστήματα γιατί ανάλογα πως είναι δομημένα και πόσο εύκολη πλοήγηση προσφέρουν ο χρήστης θα περιηγηθεί ή όχι στο ηλεκτρονικό κατάστημα.

Παπασωτηρίου

Στο κατάστημα του Παπασωτηρίου η δομή του είναι αρκετά καλή ,δίνοντας την δυνατότητα να πλοηγηθεί και πιο άπειρος χρήστης. Με αυτό τον τρόπο ο χρήστης μπορεί να δει τα προϊόντα που προσφέρει στις τιμές και αν τον ενδιαφέρει κάποιο από αυτά μπορεί να το αγοράσει. Δίνει την δυνατότητα στον χρήστη να κάνει αναζήτηση προϊόντων είτε γενικά σε όλα τα προϊόντα, είτε να κάνει αναζήτηση με βάση την κατηγορία (π.χ. Βιβλία, CD, ...) είτε με τον κωδικό του προϊόντος. Στην τελευταία περίπτωση η αναζήτηση γίνεται πιο συγκεκριμένη και είναι για χρήστες που ξέρουν το προϊόν που θέλουν να αγοράσουν.

Εκτός από τις μηχανές αναζήτησης το κατάστημα δίνει ένα κατάλογο με τις κατηγορίες και τις υποκατηγορίες που έχουν ταξινομήσει τα προϊόντα για να μπορεί να μετακινηθεί σε εκείνες τις κατηγορίες χωρίς να κάνει συνέχεια αναζητήσεις.

Το μενού που έχει τοποθετήσει στην αρχή είναι γενικό και αναφέρει τι προϊόντα έχει και αν έχει καινούρια προϊόντα. Το μενού αυτό θα μπορούσαμε να πούμε ότι αναφέρεται σε πελάτες που θέλουν να πλοηγηθούν και να ρίξουν μια ματιά στο κατάστημα.
Στην πρώτη σελίδα έχει βάλει σε εμφανές σημείο βασικές επεξηγήσεις για τους χρήστες ξεκαθαρίζοντας ότι τα προσωπικά στοιχεία του χρήστη είναι απόλυτα διασφαλισμένα και αναφέρει με πιο τρόπο ασφαλίζονται. Επίσης αναφέρει για πιο λόγο κάνει χρήση των cookies και σε περίπτωση που ο χρήστης έχει αποφασίσει για δική του ασφάλεια να μην δέχεται cookies από κανένα διαδικτυακό τόπο, δεν θα έχει στην διάθεση του κάποιες βασικές υπηρεσίες που δίνει το κατάστημα, όπως τα προϊόντα που έχει αγοράσει.

E-Shop.gr

Το e-shop.gr έχει στην αρχική του σελίδα μια μηχανή αναζήτησης για κάθε κατηγορία , η οποία δίνει την δυνατότητα να κάνει αναζήτηση ο χρήστης στις υποκατηγορίες ή στην βασική κατηγορία. Έχει τοποθετήσει ένα μενού στο πλάι το οποίο είναι ευδιάκριτο και αναφέρει δείχνει τις βασικές κατηγορίες. Αν έχει υποκατηγορίες τότε ο χρήστης θα τις δει μόνο όταν ενεργοποιήσει την αντίστοιχη κατηγορία.

Έχει τοποθετήσει ένα δεσμό βοήθειας ο οποίος οδηγεί σε μια άλλη ιστοσελίδα όπου εκεί αναφέρονται όλες οι συχνές ερωτήσεις που μπορεί να κάνει ο χρήστης όσο αφορά,

1. την παραγγελία,
2. τους τρόπους πληρωμής,
3. πως θα παραλάβει τα προϊόντα του και σε πόσο χρονικό διάστημα,
4. και το πιο σημαντικό με τι τρόπο διασφαλίζονται τα προσωπικά δεδομένα σε περίπτωση που αποφασίσει να χρησιμοποίηση την πιστωτική του κάρτα.

Όπως και το κατάστημα του Παπασωτηρίου έτσι και αυτό χρησιμοποιεί τα cookies για την διευκόλυνση των πελατών του, αλλά χωρίς να αναφέρονται οι λόγοι που γίνεται κάτι τέτοιο.

Πλαίσιο

Το πλαίσιο δίνει σε εμφανές σημείο μια μηχανή αναζήτησης η οποία κάνει αναζήτηση σε ολόκληρο το σύστημα αφού δεν μπορεί να συγκεκριμενοποίηση ο χρήστης την αναζήτηση του. Σε εμφανές σημείο είναι και το μενού το οποίο είναι χωρισμένο στις βασικές κατηγορίες που έχει ορίσει το κατάστημα. Ο τρόπος με τον οποίο είναι σχεδιασμένο το ηλεκτρονικό κατάστημα σε ωθεί στο να μείνεις και να δεις τι σου προσφέρει. Εκεί που διαφέρει από τα άλλα καταστήματα είναι ότι σε ένα δευτερεύον αλλά ευδιάκριτο μενού ο χρήστης μπορεί να πάρει πληροφορίες για τους τρόπους πληρωμής, τους τρόπους με τον οποίο θα παραλάβει τα προϊόντα του και πληροφορίες για το κατάστημα. Γενικά η δομή του είναι πολύ φιλική προς τον χρήστη και δίνει την αίσθηση της ασφάλειας, παρόλο που δεν χρησιμοποιούν πρωτόκολλο ασφάλειας σε ολόκληρο την ιστοσελίδα.

MicroLand

Το κατάστημα της MicroLand έχει ένα βασικό μενού το οποίο είναι στην αρχική σελίδα και ένα δεύτερο μενού στο πλάι το οποίο δίνει κάποιες δευτερεύουσες επιλογές. Αυτό που μπορεί να διακρίνει ο χρήστης είναι μια μηχανή αναζήτησης και το μενού. Η δομή του δεν είναι πολύ καλή γιατί κάνει χρήση frames και απευθύνεται κυρίως σε έμπειρους χρήστες. Όσο αφορά την ενημέρωση των πελατών γίνεται με την χρήση των συχνών ερωτήσεων (Frequently Asked Questions FAQ) όπου σε εκείνη την σελίδα αναφέρει τους τρόπους πληρωμής, πως θα παραλάβουν τα προϊόντα και άλλες ερωτήσεις που κάνουν συχνά οι χρήστες.

Media Power

Η Media Power δίνει την δυνατότητα στον χρήστη να πλοηγηθεί στον διαδικτυακό τόπο με την βοήθεια του μενού. Ο χρήστης μπορεί να ενημερωθεί για τα πάντα με ένα κλικ αφού έχει προβλέψει για ότι μπορεί να ρωτήσει ο χρήστης. Στο βασικό μενού ο χρήστης μπορεί να περιηγηθεί και να δει τις υπηρεσίες που προσφέρει, και στο δεύτερο μενού που έχει στο πλάι μπορεί να μάθει ότι τον ενδιαφέρει.

Σημείο 5ο: Δομή στον κώδικα

Στα ηλεκτρονικά καταστήματα που μελετήθηκαν διαπιστώθηκε ότι στα περισσότερα καταστήματα ο κώδικας είναι σωστά δομημένος με αποτέλεσμα την σταθερότητα των σελίδων, δηλαδή όλες οι σελίδες θα εμφανιστούν χωρίς κάποιο πρόβλημα. Σε μερικά ηλεκτρονικά καταστήματα γινόταν χρήση απλού HTML και JavaScript κώδικα για να εμφανίζει τα προϊόντα και να δημιουργεί τα μενού. Σε πιο σημαντικές σελίδες όπως την σελίδα για την είσοδο και πιστοποίηση του χρήστη στο σύστημα χρησιμοποιήθηκαν άλλες γλώσσες προγραμματισμού όπου ο κώδικας τους δεν είναι ορατός από τον χρήστη , π.χ. PHP,ASP, JAVA,... , γιατί εκτελούνται πάνω στον εξυπηρετητή και όχι στον υπολογιστή του χρήστη όπως γίνεται με την HTML και την JavaScript.

Η χρήση αυτών των γλωσσών προγραμματισμού δίνει την δυνατότητα στον διαχειριστή του ηλεκτρονικού καταστήματος να μπορεί να γνωρίζει ποιος μπήκε στο σύστημα, από που, για πόσο, τι έκανε, κλπ. Αυτό δεν γίνεται αντιληπτό από τον χρήστη, αλλά είναι απαραίτητο για την ασφάλεια των προσωπικών στοιχείων του χρήστη και του συστήματος γενικότερα.

Συμπέρασμα:

Τα συμπεράσματα που μπορούν να βγουν από την μελέτη που έγινε στα ηλεκτρονικά καταστήματα είναι ότι ενώ υπάρχει μια αρκετά καλή υποδομή για την μέγιστη ασφάλεια των ηλεκτρονικών συναλλαγών, δεν έχουμε φτάσει ούτε στο ελάχιστο. Παρόλο που χρησιμοποιούνται δυνατά πρωτόκολλα ασφάλειας όπως το SSL, SET, τα οποία κρυπτογραφούν και στέλνουν με ασφάλεια τους αριθμούς πιστωτικών καρτών, ΔΕΝ είναι

αρκετό. Πρέπει να αρχίσουν τα ηλεκτρονικά καταστήματα να υποστηρίζουν την χρήση

- **έξυπνων καρτών** (Smart Cards),
- **ηλεκτρονικών πορτοφολιών** (e-wallets),
- **καρτών προπληρωμένου χρόνου,**

για τις αγορές μέσο του διαδικτύου.

Οι Έλληνες χρήστες του διαδικτύου δεν γνωρίζουν τους εναλλακτικούς τρόπους πληρωμής που υπάρχουν, την ασφάλεια που προσφέρουν, με αποτέλεσμα ή να συνεχίζουν να πραγματοποιούν τις αγορές με τις πιστωτικές κάρτες ή να μην τις πραγματοποιούν καθόλου. Σε έρευνα που έγινε μέσο του διαδικτύου σε 75 Έλληνες χρήστες ανεξαρτήτως ηλικίας, το μεγαλύτερο μέρος θα ήθελε να του έδιναν εναλλακτικούς τρόπους πληρωμής εκτός από τις πιστωτικές κάρτες, αλλά και τα ηλεκτρονικά καταστήματα να τους δείχνουν ένα πιστοποιητικό όσο αφορά την ασφάλεια των συναλλαγών και τις εγκυρότητας του.

Κεφάλαιο 5°:

Σύστημα Ασφάλειας

5.1 *Εισαγωγή*

Έχοντας ολοκληρώσει την έρευνα που έγινε με την μορφή ερωτηματολογίου από το διαδίκτυο και έχοντας μελετήσει 5 ηλεκτρονικά καταστήματα στην Ελλάδα προτείνω ένα σύστημα ασφάλειας το οποίο προφέρει στον πελάτη την αίσθηση της διαφάλησης των προσωπικών του στοιχείων που ζητάει το ηλεκτρονικό κατάστημα, αλλά και την διασφάλιση από την μεριά του ηλεκτρονικού καταστήματος ότι ο πελάτης του είναι έμπιστος.

5.2 *Ανάλυση του συστήματος ασφαλείας*

Στην Ελλάδα η EBEA μπορεί να εκδώσει "ψηφιακά πιστοποιητικά" τόσο για επιχειρήσεις όσο και για απλούς χρήστες. Η ασφάλεια στηρίζεται στην χρήση των "ψηφιακών πιστοποιητικών" από την μεριά των χρηστών.

Προϋποθέσεις από την μεριά του χρήστη

1. **Με την χρήση "ψηφιακού πιστοποιητικού"**
   - Έστω ότι ένας χρήστης έχει "ψηφιακό πιστοποιητικό" και θέλει να πραγματοποίηση μια αγορά μέσα από το διαδίκτυο, από το ηλεκτρονικό κατάστημα www.kapellakis.gr . Το ηλεκτρονικό κατάστημα θα ζητήσει από τον χρήστη να στείλει το "ψηφιακό πιστοποιητικό" που έχει. Ο χρήστης στέλνει το "ψηφιακό πιστοποιητικό" και το ηλεκτρονικό κατάστημα επιβεβαιώνει την γνησιότητα του με την βοήθεια τις εκδοτικής αρχής (EBEA στην περίπτωση μας). Αν το "ψηφιακό πιστοποιητικό" είναι γνήσιο και υπάρχει τότε ο χρήστης συνδέεται στο ηλεκτρονικό κατάστημα μέσα από ασφαλή μονοπάτια (SSL, SET). Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα είναι κρυπτογραφημένη και θα αποκρυπτογραφείται με το δημόσιο κλειδί του ηλεκτρονικού καταστήματος. Αφού το ηλεκτρονικό κατάστημα πιστοποιήσει τον χρήστη θα του στείλει το δικό του δημόσιο κλειδί για να αποκρυπτογραφήση την ιστοσελίδα. Αυτό το μέτρο έχει σαν σκοπό να μην μπορούν να διαβάσουν τις σελίδες, όλοι όσοι μπορέσουν και αποφύγουν το honey pot.

   - Στην περίπτωση που ο χρήστης αρνηθεί για οποιονδήποτε λόγο να στείλει το "ψηφιακό πιστοποιητικό" είτε γιατί δεν έχει , είτε γιατί δεν θέλει να το στείλει τότε το ηλεκτρονικό κατάστημα τον εκτρέπει σε ένα μεμονωμένο εξυπηρετητή(server)ο οποίος είναι ένα πιστό αντίγραφο του πραγματικού ηλεκτρονικού καταστήματος, χωρίς να έχει αληθή προσωπικά δεδομένα, και ο

οποίος είναι πολύ ευάλωτος σε όλες τις επιθέσεις!!!

Με αυτό τον τρόπο το ηλεκτρονικό κρατάει τους hackers απασχολημένους σε ένα ηλεκτρονικό κατάστημα που το βλέπουν μόνο οι hackers χωρίς να κινδυνεύουν τα προσωπικά στοιχεία των πελατών.

1. **Χωρίς την χρήση "ψηφιακού πιστοποιητικού"**
   - Στην περίπτωση που ο πελάτης θελήσει να περιηγηθεί απλώς στο ηλεκτρονικό κατάστημα τότε εκτρέπεται στον μεμονωμένο εξυπηρετητή, μια που αποτελεί πιστό αντίγραφο του πραγματικού. Αν θελήσει να πληρώσει προϊόντα που επιθυμεί να αγοράσει τότε θα πρέπει να στείλει το "ψηφιακό πιστοποιητικό ", αλλιώς η αγορά γίνεται τηλεφωνικά και μόνο με αντικαταβολή.

Όπως έδειξα στην εικόνα 2 του κεφαλαίου 2 ένας hacker τροποποιώντας μια απλή φόρμα μπορεί να εκτρέψει την αποθήκευση των προσωπικών στοιχείων του χρήστη από το προκαθορισμένο αρχείο, σε ένα άλλο αρχείο πιο προσβάσιμο όπως είναι το αρχείο passwd.

5.2.1 *Προϋποθέσεις από την μεριά του ηλεκτρονικού καταστήματος*

Για να μπορέσει να αντιμετωπίσει αυτού του είδους τις επιθέσεις το ηλεκτρονικό κατάστημα θα πρέπει να χρησιμοποιεί 2 από τα πιο βασικά προγράμματα:

1. το nessus το οποίο βρίσκει τρύπες στο σύστημα και προτείνει τρόπους αντιμετώπισης,

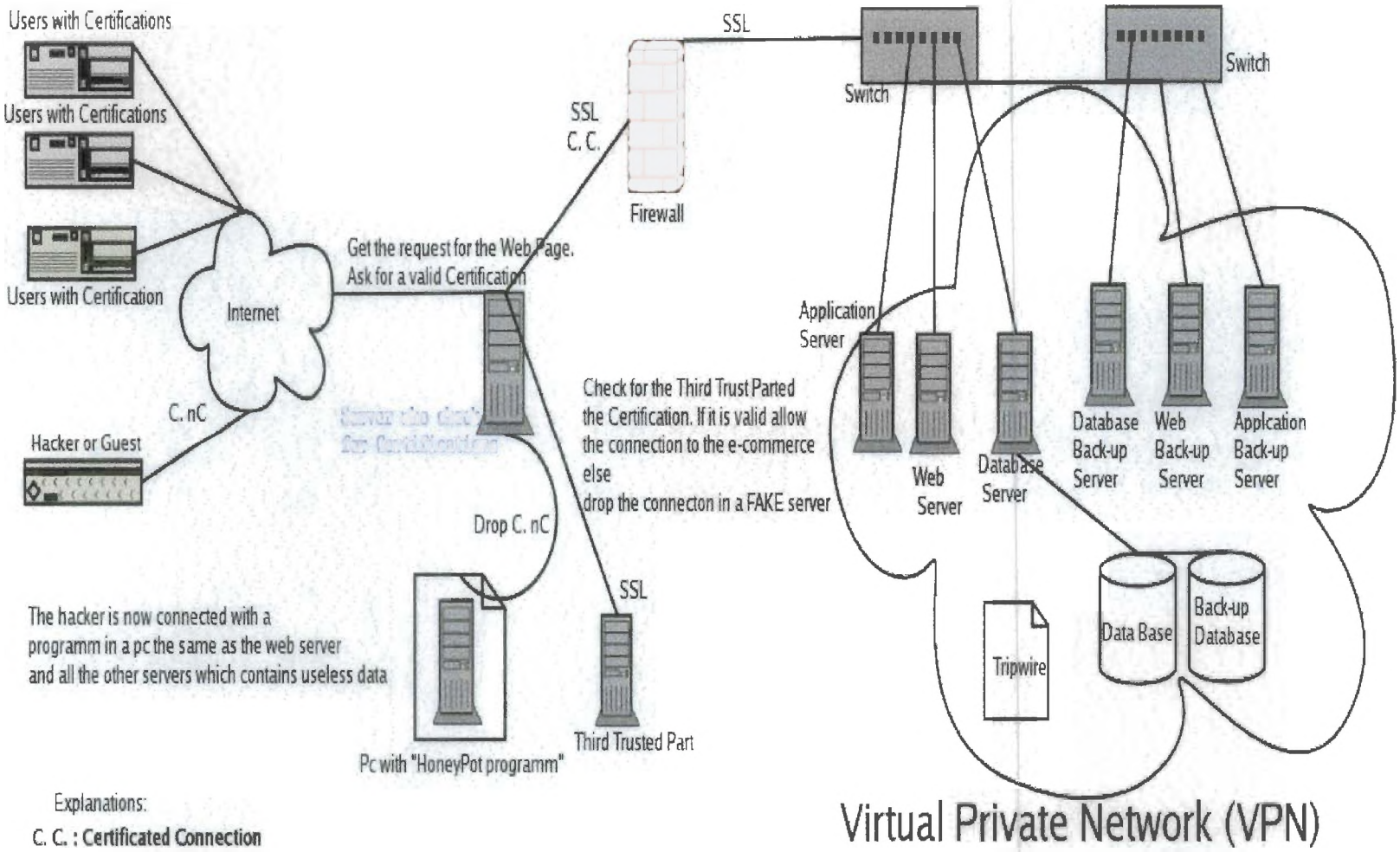
2. το tripwire το οποίο ελέγχει την ακεραιότητα των αρχείων του συστήματος και της βάσης δεδομένων. Σε περίπτωση που μπορέσει να τροποποιήσει ένας hacker κάποιο αρχείο το tripwire θα βγάλει ένα μήνυμα στον διαχειριστή του συστήματος ότι το αρχείο data.dat περιέχει ιό ή ότι η φόρμα για την συλλογή των προσωπικών στοιχείων ΔΕΝ αντιστοιχεί στο αρχείο data.dataαλλά στο αρχείο /etc/passwd.

3. με την σωστή χρήση firewall και με την χρήση VPN μπορεί να εγγυηθεί για την ασφάλεια των ηλεκτρονικών συναλλαγών του χρήστη αλλά και για την προστασία των προσωπικών δεδομένων στο ακέραιο.

Το μόνο που πρέπει να αλλάζει είναι τα log αρχεία του συστήματος και τίποτα άλλο.

Αυτά τα μέτρα μπορούν να προσφέρουν την μέγιστη προστασία όταν χρησιμοποιούνται από λειτουργικό σύστημα με τις λιγότερες ευπάθειας όπως το Solaris, BSD, Linux.

Για τον λόγο αυτό προτείνω το ηλεκτρονικό κατάστημα να χρησιμοποιεί τεχνολογία Sparc 64 bit και Solaris στα 64 bit και ανάλογα με τις υπηρεσίες που προσφέρει να έχει ένα server για κάθε υπηρεσία που προσφέρει και ένα backup server για κάθε server. Αυτό βοηθάει στην περίπτωση που πετύχει μια DOS attack να χαθεί ΜΟΝΟ η συγκεκριμένη υπηρεσία (π.χ. e-mail) και ΟΧΙ ΟΛΟ το σύστημα. Στην περίπτωση που έχει για κάθε server έχει ένα backup server, τότε η υπηρεσία θα μπορέσει να λειτουργεί κανονικά χωρίς να αντιληφθεί ο χρήστης το παραμικρό. Το συγκεκριμένο μέρος από το ηλεκτρονικό κατάστημα είναι σίγουρο ότι θα δουλέψει, γιατί έχει δοκιμαστεί πρώτα και τις δοκιμές τις πέρασε με μεγάλη επιτυχία. Η δομή των εξυπηρετητών είναι η ίδια με την δομή που είχαν οι εξυπηρετητές στους Ολυμπιακούς Αγώνες την Αθήνας. Σε περίπτωση που κάποιος από τους Unix Servers για κάποιο λόγο έχανε την επαφή με το δίκτυο, τότε η ροή των δεδομένων όπως θα περίμενε κάποιος θα σταματούσε για το χρονικό διάστημα που θα έκανε να επισκευαστεί. Όπως ήταν δομημένο το σύστημα ακόμα και αν έχανε την επαφή με το δίκτυο κάποιος από τους servers η ροή των δεδομένων δεν σταματούσε γιατί έμπαινε σε λειτουργεία αυτόματα ο δεύτερος server. Επομένως για να μην μπορεί να χρησιμοποιήσει ένας χρήστης τις υπηρεσίες του ηλεκτρονικού καταστήματος, μετά από μια DoS attack [βλ. κεφάλαιο 3] θα πρέπει ο hacker να «ρίξει» και τον εφεδρικό server του ηλεκτρονικού καταστήματος ή και τα 2 switches. Παρακάτω μπορούμε να δούμε το σύστημα ασφάλειας σχηματικά.



Explanations:

C. C. : Certificated Connection

C. nC : Connection not Certifivated

SSL: Secure Socket Layer Protocol

Σχήμα 3: Σχηματική αναπαράσταση του συστήματος ασφαλείας

Ο χρήστης έχοντας την «ψηφιακή υπογραφή» του (η οποία αποτελείται από ένα ζεύγος ιδιωτικού-δημόσιου κλειδιού) αποκτά από την E.T.O το «ψηφιακό πιστοποιητικό» το οποίο αργότερα θα το χρησιμοποιήσει ως «δημόσιο κλειδί» για να μπορεί το ηλεκτρονικό κατάστημα να πιστοποιεί την ταυτότητα του χρήστη από την E.T.O. Η E.T.O. γνωρίζοντας την «ψηφιακή υπογραφή» του χρήστη και γνωρίζοντας την αυθεντικότητα των στοιχείων του, τον πιστοποιεί στο ηλεκτρονικό κατάστημα. Στην περίπτωση που το «ψηφιακό πιστοποιητικό έχει λήξει ή έχει αλλαχτεί, τότε η είσοδος του χρήστη σε https:// δεν είναι δυνατή, αλλά σε http:// ακόμη και αν είναι μέλος του ηλεκτρονικού καταστήματος.

5.3 Ψευδοκώδικας

main.php

Ο παρακάτω ψευδοκώδικας που ακολουθεί αντιστοιχεί στο σημείο όπου ο χρήστης θα πρέπει να πιστοποιήσει την ταυτότητα του. Αν έχει «ψηφιακό πιστοποιητικό» τότε μπαίνει σε ένα site το οποίο αποκρυπτογραφείται με την είσοδο του και σε ολόκληρο το site γίνεται χρήση του πρωτοκόλλου SSL. Θυμίζω ότι το SSL σημαίνει Secure Socket Layer. Ο ψευδοκώδικας αφορά μόνο την κεντρική σελίδα και χωρίζεται σε δυο βασικά - δυναμικά αρχεία:
1) στο CLIENT και
2) στο CREATE CUSTOMERS

File: *CLIENT*

//This file check if the user has a Digital Certificate Or Not
//This is a secure page

SHOW MESSAGE 1 "ENTRANCE "

Select case:

1) using "Digital Certificate": //The user is member.

Enter the key:

Connect via https and dynamic-decrypted the web site;
/*The whole web-site is dynamic, secure using SSL*/
/*In this server the member will be able to use Credit Card, smart cart, e-cash, e-check, etc*/

Goto key.php;

break;

2) not using "Digital Certificate": //The user is not member ,yet

Connect via http in a simple html web site;
/*Not Using SSL*/
/*This is the server with Honey Pot the file for hackers. The customer can not use Credit Card or to Send Personal data through internet for security reasons. If the user want to use Credit Card must be a member first with Digital Certificate*/

Goto simple.html
break;

3) New Member: Goto register.php
End Select

End of file CLIENT

FILE: *CREATE CUSTOMERS*

BEGIN FILE

//This file creates users for the e-commerce
//This is a secure page

Create link "New Member"

Display the terms of the E-COMMERCE

select case

Accept) Display form1(); break;

Cancel) Display Main Page /*Or CLIENT file */; break;

end select

form1()

//This function gets the personal data in a secure mode and use SSL for the transmission and the storage

BEGIN function

Enter "Digital Certificate" /*D.G.*/

```
        Call Check(results);

        check=Check(results);

        if check is FALSE

                Display message " You can not be a member with out a Digital Certificate"; exit(-1);
        End if

        Enter Fullname;
        Enter dd/mm/YYYY; /* d=DATE, m=MONTH, Y=YEAR*/
        Enter sex;
        Enter Address;
        Enter e-mail;

Show Buttons "Submit" "Clear Form"

        if "submit" is TRUE

                Use SSL;
                Connect in the database;
                Store the data;
                Display thanks page;
                Send e-mail with instruction about authentication;

        else if "clear" is TRUE

                clear all the fields;

           end if

        end if

END function

Check(results)

//This function checks if the user enter the right Certificate and if the Certificate is true!

BEGIN function

        Use SSL;

        Send the Certificate for authentication;

        Return the results;

END function
```

END of file CREATE CUSTOMERS

Για λόγους λειτουργηκότητας έχω χωρίσει τα 2 βασικά αρχεία σε άλλα μικρότερα. Το αρχείο **client.php** έχει σπάσει σε 3 αρχεία:

1) *key.php* ,
2) *simple.html*
3) *register.php*

,ενώ το αρχείο create client έχει σπάσει σε 2 βασικά αρχεία:

1) *register.php* το οποίο βρίσκεται στην main.php και
2) στο *new_members.php*

το οποίο είναι το αρχείο που κάνει όλη την δουλειά γιατί ελέγχει και καταχωρεί τα δεδομένα σε ασφαλεί βάση δεδομένων.

Ο κώδικας που ακολουθεί είναι δοκιμασμένος και δούλευει. Δοκιμάστηκε σε συστήμα Linux με Web Server Apache. Πριν δοκιμάσετε τα script πρέπει να φτιάξετε μια βάση δεδομένων mysql με το όνομα members και πεδία:

- realname -> *varchar*
- public -> *varchar*
- secret -> *password*
- email ->*varchar*
- date_created -> *date*
- hash -> *varchar* (μόνο για την σελίδα new_members

Αν δεν θέλετε να αντιγράφετε τα scripts μπορείται να τα κατεβάσετε με την μορφή txt από την ηλεκτρονική διεύθυνση http://www.psiloriths.com/pp/~yskapell/free_code.php

Script - Code

Key.php

```
<?php

$filename="public_key.txt"; //In this file is stored the public key of the customer

$fd=fopen($filename, "r") or die ("Could not open the $filename");
$read=fread($fd, filesize($filename) );
//echo $read;
//echo "<input type=\"text\" value=$read>";

echo "Please enter for confirmation your <br><br>";
echo "<form method=POST action=\"http://localhost/ptixiaki/confirm.php\">";
//echo "<input type=\"hidden\" name=\"readfile\" value=$read>";
echo "public key: <input type=\"password\" name=t1 value=\"$read \"> <br><br>";
echo "password: <input type=\"password\" name=p1 value=\"\"><br><br>";
echo "<input type=\"submit\" value=\"Confirm ID\"> <input type=\"reset\" value=\"Clear &
Cancel\">";
echo "</form>";
```

```
fclose($fd);
?>
```

confirm.php //This is the file which verify the public key and the user password

```
<?php
$username="root";
$database="members";
$localhost="localhost";

$link=mysql_connect($localhost,$username) or die ("Could not connect in the specific database");

mysql_select_db($database) or die ("Could not connect in the database. Please check!!!");

$query="SELECT realname, public, secret FROM users";

$query1=mysql_query($query);

$line=mysql_fetch_array($query1, MYSQL_ASSOC);

$public_key=$_POST['t1'];
$password=$_POST['p1'];

if (($line["public"] == $public_key)&&($line["secret"] == $password))
{
                    echo "Welcome "; echo $line["realname"];
}
else
{
                echo "Please your public key or your password";
                        header("Location: /key.php");
}


?>
```

simple.html

This is just a simple html page. Nothing more, nothing less

register.php This is the page which the user can be a member

```
<?php

require_once('new_members.php');

if ($submit=='Mail confirmation')
{
```

```
                    $feedback=user_register();
}
else
{
$feedback_str='';
}

//----------------
//DISPLAY THE FORM
//----------------

site_header('Registration');

$php_self=$_SERVER['PHP_SELF'];

$reg_str=<<<EOREGSTR

echo "Display your text or html code here ";

$feedback_str

echo "Display the form as you wish";


EOREGSTR; //HERE ENDS THE HTML CODE

//echo $reg_str;

//site_footer();
?>
```

new_members.php //This file select and check the data for the user

```
<?php
//This is the file for new members
/*Here starts code for MySql*/
$localhost="localhost";
$username="root";
$database="members";

mysql_connect($localhost,$username) or die ("Could not connect in the $localhost");

$link1=mysql_select_db($database) or die ("Could not connect in the $database. Please

contact with your administator and check");
/*Here ends the MySql code*/
```

```
$super_secret_hash_padding='A string that is used to pad out to short ';
function

user_register()
{
global $super_secret_hash_padding;

if (strlen($_POST['realname'])<=25 && strlen($_POST['public'])<=50 &&

strlen($_POST['pass1'])<=50 && ($_POST['pass1'] == $_POST['pass2']) &&

strlen($_POST['email']) && validate_email($_POST['email']))
                                        {
if (account_validname($_POST['public']) || strlen($_POST['pass1'])>=6){

$email=$_POST['email'];

$query="SELECT user_id FROM user WHERE

public='$public' AND email='$email'";
$result=mysql_query($query);

                    if($result && mysql_num_rows($results)>0)
                    {

                   $feedback='ERROR - Public Key or E-Mail address already exists';

                   return $feedback;
                   }
                 else

                {
$realname=$_POST['realname'];


$public=md5($_POST['public']);

$password=md5($_POST['pass1']);

$hash=md5($email.$super_secret_hash_padding);

$query="INSERT INTO user (realname, public, secret, email, hash, is_confirmed,

date_created)VALUES('$realname','$public','$pass1','$email','$hash','0',NOW())";
```

```
$result=mysql_query($query);

if(!$result)


{
$feedback='ERROR - Database Error';
return $feedback;
}
else
{

$encoded_email=urlencode($_POST['email']);
mail($email,'electrickeye.gr Registration
Confirmation',$mail_body,'From:noreply@electriceye.gr');
}
}
}else{ $feedback='Error';return $feedback;}
}

function account_validname()
{
if (strspn($_POST['public'],"123456789")!=strlen($public)){return false;}
}

function validate_email()
{
return(ereg('^[-!#$%&\'*+\\./0-9=?A-Z^_`a-z{|}~+'. '@'.
'[-!#$%&\'*+\\/0-9=?A-Z^_`a-z{|}~]+\.' . '[~!#$%&\'*+\\./0-9=?A-Z^_`a-z{|}~]+$',
$_POST['email']));
}
}
?>
```

main.php

```
<html>
<head>
<title>Electric EYE</title>
<body bgcolor="skyblue" link="blue" alink="blue" vlink="blue">
<?php
//Here starts the PHP code****/


echo "<center><b>Electric EYE</b></center>"; echo"<BR>";
echo "<BR>";
```

```
echo "<FORM NAME=\"f1\" method=\"POST\" action=\"client.php\">";
echo "<INPUT TYPE=\"radio\" NAME=\"r1\" VALUE=\"dc\">Entrance for Members Only<br>";
echo "<INPUT TYPE=\"radio\" NAME=\"r1\" VALUE=\"ndc\">Entrace for Visitors<br>";
echo "<INPUT TYPE=\"radio\" NAME=\"r1\" VALUE=\"new\">New Member<br>";
echo "<BR>";
echo "<INPUT TYPE=\"submit\" NAME=\"submit\" VALUE=\"Entrance\">";
echo "<INPUT TYPE=\"reset\" VALUE=\"Cancel\">";
echo "</FORM>";

?>
</body></html>
```

Όμως δεν αρκεί ένα πολύ καλό σύστημα ασφάλειας για να τους αποτρέψει ή να τους αποθαρρύνει, αλλά χρειάζεται και συντήρηση από ανθρώπους που έχουν τις σωστές γνώσεις. Άλλωστε την πλειοψηφία των hackers μπορούμε να την αποτρέψουμε και να προστατέψουμε τα προσωπικά στοιχεία των πελατών μας, αλλά υπάρχει και μια μειοψηφία όπου δύσκολα θα μπορέσουμε να την αποτρέψουμε. Εκτός από τα μέτρα ασφαλείας που ΠΡΕΠΕΙ να έχει ένα ηλεκτρονικό κατάστημα, ΠΡΕΠΕΙ και ο χρήστης να παίρνει κάποια μέτρα ασφάλειας γιατί οι περισσότερες κλοπές προσωπικών δεδομένων γίνονται όταν πληκτρολογεί τα στοιχεία ο χρήστης χάρη στην βοήθεια key spyiers (προγράμματα που διαβάζουν το πληκτρολόγιο) οπότε το ηλεκτρονικό κατάστημα δεν έχει καμία εύθηνη για την απώλεια των προσωπικών στοιχείων του χρήστη.

Συμπεράσματα

Λαμβάνοντας υπ' όψιν τα αποτελέσματα που προέκυψαν από το ερωτηματολόγιο καταλήγουμε στο συμπέρασμα ότι ασφάλεια 100% στο ηλεκτρονικό εμπόριο δεν είναι εφικτή. Ο λόγος που δεν μπορούμε να πετύχουμε την απόλυτη ασφάλεια στις ηλεκτρονικές συναλλαγές οφείλεται στην δυσπιστία του χρήστη και στην έλλειψη γνώσεων όσο αφορά τους κινδύνους. Όπως και να είναι δομημένα τα ηλεκτρονικά καταστήματα, όσο καλά πρωτόκολλα ασφαλείας χρησιμοποιούν, αν ο χρηστής δεν κάνει το βήμα να μάθει, τότε το ερώτημα "Υπάρχει ασφάλεια στις ηλεκτρονικές συναλλαγές?" θα είναι ένα κρίσιμο ερώτημα το οποίο δεν θα μπορεί να απαντηθεί πλήρως.

Βιβλιογραφία

- Maximum Security
- Hacking Exposed Network Solutions
- Δίκτυα Υπολογιστών Συγγραφέας:Tanenbaum

Ηλεκτρονική Βιβλιογραφία

[illegible]

PDF documents

- [illegible]

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω για την άριστη συνεργασία και την πολύτιμη βοήθεια την κ. Στεφανή Αντωνία, εισηγήτρια της πτυχιακής εργασίας « Ασφάλεια στο Ηλεκτρονικό Εμπόριο » , καθώς και τους γονείς μου ,την αδερφή μου, την Μαριάνθη, την Ασπασία για την αμέριστη συμπαράσταση και βοήθεια στην διεκπεραίωση της πτυχιακής εργασίας. Επίσης θέλω να ευχαριστήσω τον κ. Στρατάκη Μανώλη για τις πολύτιμες συμβουλές και την πολύτιμη βοήθεια του.