ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Μ.Π.Σ. ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΥΡΙΑΚΟΠΟΥΛΟΣ ΠΑΝΑΓΙΩΤΗΣ ΜΕ 09086

ΘΕΜΑ:ΑΝΑΠΤΥΞΗ ΙΣΤΟΣΕΛΙΔΑΣ ΜΕ ΧΡΗΣΗ ΤΕΧΝΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

ΕΙΣΗΓΗΤΗΣ κ. ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

1 Ασφάλεια Δικτύων

1.1 Εισαγωγή

Μια από τις σημαντικότερες απειλές για μια εταιρία η οποία διατηρεί ένα πληροφοριακό σύστημα είναι η πιθανότητα εισβολής ενός hacker στο πληροφοριακό της σύστημα. Σύμφωνα με τον Kim Bayne (2000) κάτι τέτοιο είναι πιθανόν να συμβεί κυρίως γιατί οι μηχανικοί Η/Υ και οι υπεύθυνοι μηχανογράφησης συνήθως υποτιμούν τις ικανότητες ανταγωνιστών,δυσαρεστημένων υπαλλήλων,εισβολέων ή πολύ ικανών και έξυπνων χρηστών που έχουν πολύ χρόνο στη διάθεσή τους.

Η ασφάλεια λοιπόν ενός πληροφοριακού συστήματος θα πρέπει να είναι βασικό μέλημα των κατασκευαστών εφαρμογών λογισμικού. Τα πληροφοριακά συστήματα κινδυνεύουν από διάφορες απειλές και οι κίνδυνοι αυτοί είναι περισσότεροι όταν το πληροφοριακό σύστημα δεν είναι απομονωμένο από τον υπόλοιπο κόσμο αλλά συνδεδεμένο με το Διαδίκτυο και προσβάσιμο από όλους τους υπολογιστές παγκοσμίως που έχουν πρόσβαση σε αυτό. Για παράδειγμα για να ολοκληρωθεί μια ηλεκτρονική αγορά θα πρέπει να γίνει μια ηλεκτρονική πληρωμή. Τα στοιχεία της πληρωμής που θα αποσταλούν από έναν υπολογιστή σε έναν άλλον θα πρέπει να μεταδοθούν με τη μεγαλύτερη δυνατή ασφάλεια έτσι ώστε να διαφυλαχθούν τα συμφέροντα του αγοραστή και το κύρος της ηλεκτρονική επιχείρησης. Γενικά οι βασικές αρχές ασφάλειας δεδομένων είναι οι εξής:

- Εμπιστευτικότητα. Τα δεδομένα θα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα.
- Ακεραιότητα. Τα δεδομένα δεν θα πρέπει σε καμία περίπτωση να διαγραφούν ή να αλλοιωθούν από μη εξουσιοδοτημένα άτομα.
- Προσβασιμότητα. Η πρόσβαση στα δεδομένα από τους εξουσιοδοτημένους χρήστες θα πρέπει να μην διακόπτεται ή εμποδίζεται αλλά να επιτρέπεται στους εξουσιοδοτημένους χρήστες όποτε αυτοί τα χρειάζονται.

1.2 Θέματα Ασφαλείας

Μια δικτυακή εφαρμογή προϋποθέτει την σύνδεση πληροφοριακών συστημάτων μεταξύ τους και την ανταλλαγή δεδομένων με ασφαλή τρόπο μέσω του Διαδικτύου. Συνεπώς η δημιουργία μιας ασφαλούς εφαρμογής έχει ως βασική απαίτηση την ανάπτυξη ενός ασφαλούς δικτύου και τη διασφάλιση του απορρήτου των πληροφοριών που μεταδίδονται. Η υλοποίηση του δικτύου θα πρέπει να παρέχει την ασφάλεια που θα παρείχε αν το δίκτυο αυτό δεν είχε καμία σύνδεση προς εξωτερικά δίκτυα και δε μπορούσε να δεχτεί εξωτερικές επιθέσεις. Σύμφωνα με τη Cisco Hellas, η προστασία διασφαλίζεται, με την ενσωμάτωση στοιχείων προστασίας σε πέντε κρίσιμες περιοχές του δικτύου:

- Ταυτοποίηση. Με τον όρο ταυτοποίηση εννοούμε τη διαδικασία ελέγχου της ταυτότητας ενός χρήστη με τέτοιο τρόπο έτσι ώστε να εγγυάται ότι η πρόσβαση στο δίκτυο δεν θα δοθεί σε μη εξουσιοδοτημένους χρήστες. Τα πρωτόκολλα ταυτοποίησης που χρησιμοποιούνται και εξετάζουμε στη συνέχεια διασφαλίζουν σε μεγάλο βαθμό της εγκυρότητα της διαδικασίας αυτής.

- Περιμετρική Ασφάλεια. Η περιμετρική ασφάλεια έχει να κάνει περισσότερο με τη χρήση προστατευτικών μέσων που μπορούν να αποτρέψουν εξωτερικές επιθέσεις για την απόκτηση πρόσβασης στους πόρους ενός συστήματος. Για το λόγο αυτό χρησιμοποιούνται τα τείχη προστασίας (firewalls) σε μορφή είτε hardware ή software.
- Ασφαλής Σύνδεση. Μια ασφαλής σύνδεση εγγυάται ότι τα μεταδιδόμενα δεδομένα μέσω του δικτύου δεν μπορούν να υποκλαπούν. Η ασφάλεια και μυστικότητα των δεδομένων μπορεί να επιτευχθεί με τη χρήση τεχνικών κρυπτογράφησης που θα εξετάσουμε παρακάτω και που χρησιμοποιούνται σε μεγάλο βαθμό στα Δίκτυα.
- Ασφαλής Παρακολούθηση. Με τη ασφαλή παρακολούθηση, οι διαχειριστές των δικτύων μπορούν να παρακολουθούν τα συμβάντα που καταγράφονται όσον αφορά τα θέματα ασφαλείας και με τη βοήθεια συστημάτων εντοπισμού εξωτερικών επιθέσεων να μπορούν να επέμβουν έγκαιρα.
- Πολιτική Διαχείρισης Ασφάλειας. Η πολιτική διαχείρισης Ασφαλείας καθορίζεται από τους διαχειριστές των δικτύων και εφαρμόζεται από ειδικά εργαλεία που πολλές φορές είναι ενσωματωμένα στο Λειτουργικό Σύστημα του server του δικτύου. Με την πολιτική διαχείρισης ασφαλείας μπορούν οι διαχειριστές να αποδίδουν δικαιώματα σε χρήστες, ομάδες και υπολογιστές του δικτύου διασφαλίζοντας την προστασία του δικτύου.

1.3 Ταυτοποίηση και Ασφαλής Μεταφορά Δεδομένων

Ένα βασικό τμήμα της διακίνησης ιδιωτικών πληροφοριών (με περιορισμούς στην πρόσβαση) μέσω διαδικτύου είναι αφενός η πρόσβαση μόνο από εξουσιοδοτημένους χρήστες και αφετέρου η ασφαλής μετάδοση των πληροφοριών. Έτσι υπάρχουν ιστοσελίδες του Διαδικτύου οι οποίες περιέχουν πληροφορίες που απευθύνονται μόνο σε εξουσιοδοτημένους χρήστες. Η πρόσβαση σε αυτές τις σελίδες γίνεται μόνο αφού ο χρήστης ταυτοποιηθεί μέσω μιας διαδικασίας υποβολής ονόματος χρήστη και κωδικού πρόσβασης. Το πρόβλημα που είναι πιθανόν να δημιουργηθεί είναι το γεγονός ότι οι κωδικοί πρόσβασης μπορεί να υποκλαπούν κατά την υποβολή τους από τον χρήστη στη σελίδα ταυτοποίησης και συνεπώς να αποκτήσουν πρόσβαση στην προστατευμένη περιοχή και χρήστες μη-εξουσιοδοτημένοι. Στη συνέχεια λοιπόν πρέπει να αναλυθούν οι τρόποι με τους οποίους επιτυγχάνεται η ταυτοποίηση χρηστών αλλά και η ασφαλής μετάδοση των κωδικών τους.

Με τη διαδικασία της ταυτοποίησης το κάθε μέρος που συμμετέχει θα πρέπει να πιστοποιήσει καταρχήν την ταυτότητα του άλλου μέρους και στη συνέχεια να αποστείλει τα δεδομένα με έναν ασφαλή τρόπο. Όταν οι πληροφορίες ανταλλάσσονται σε μορφή απλού κειμένου είναι πολύ εύκολο να υποκλαπούν από κάποιον ο οποίος παρακολουθεί μια ηλεκτρονική συνομιλία. Δεδομένα όπως κωδικοί πρόσβασης σε ηλεκτρονικές υπηρεσίες μπορούν να καταλήξουν στα χέρια κακόβουλων ατόμων και μη εξουσιοδοτημένων χρηστών. Για την ασφαλή μετάδοση των δεδομένων μέσω ενός δικτύου υπολογιστών ή του Διαδικτύου η πιο διαδεδομένη μέθοδος είναι αυτή της κρυπτογράφησης.

1.3.1 Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία κωδικοποίησης της πληροφορίας σε τέτοια μορφή έτσι ώστε κατά την αποστολή της πληροφορίας να είναι δυνατή η ανάγνωσή της μόνο από τον εξουσιοδοτημένο παραλήπτη της. Οι αλγόριθμοι κρυπτογράφησης λειτουργούν σαν κλειδαριές με συνδυασμό όπου το κλειδί είναι ένας συνδυασμός. Όσα περισσότερα ψηφία έχει ο συνδυασμός τόσο ασφαλέστερη είναι η κλειδαριά και τελικά τόσο πιο δύσκολη η αποκρυπτογράφηση των πληροφοριών. Έτσι τα κλειδιά κρυπτογράφησης όπως θα δούμε ποικίλουν από 56 δυαδικά ψηφία (όπως στην περίπτωση του DES) μέχρι 168 ψηφία (3DES) που αποτελεί και το πιο ασφαλές επίπεδο κρυπτογράφησης.

Υπάρχουν διάφοροι τύποι αλγορίθμων κρυπτογράφησης όπως:

- Συμμετρικοί Αλγόριθμοι (Ιδιωτικό κλειδί)
- Ασύμμετροι Αλγόριθμοι (Δημόσιο κλειδί)
- Αλγόριθμοι Hash.

1.3.2 Συμμετρικοί Αλγόριθμοι

Στους Συμμετρικούς αλγόριθμους κρυπτογράφησης ή αλλιώς Αλγορίθμους Ιδιωτικού κλειδιού, η διαδικασία κρυπτογράφησης βασίζεται στη χρήση ενός και μόνο κλειδιού το οποίο χρησιμοποιείται και στην κρυπτογράφηση και στην αποκρυπτογράφηση της πληροφορίας. Το κλειδί αυτό είναι κοινό και για τον αποστολέα αλλά και για τον παραλήπτη. Ο αποστολέας χρησιμοποιεί το μυστικό αυτό κλειδί για να κρυπτογραφήσει το μήνυμα. Ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί έτσι ώστε να αποκρυπτογραφήσει το κωδικοποιημένο μήνυμα σε απλό κείμενο. Τέτοιοι αλγόριθμοι είναι ο αλγόριθμος RSA RC4 που χρησιμοποιείται στο MPPE (Microsoft Point to Point Encryption), ο αλγόριθμος DES (Data Encryption Standard), ο 3DES και ο IDEA (International Data Encryption Algorithm). Οι συμμετρικοί αλγόριθμοι χρησιμοποιήθηκαν κυρίως σε κλειστά συστήματα και εφαρμόστηκαν τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων.

1.3.3 Ασύμμετροι Αλγόριθμοι

Στους ασύμμετρους αλγορίθμους κρυπτογράφησης που ονομάζονται και Αλγόριθμοι Κρυπτογράφησης Δημόσιου Κλειδιού, χρησιμοποιούνται δύο διαφορετικά κλειδιά , ένα για κάθε χρήστη. Το ένα είναι Ιδιωτικό και ανήκει μόνο σε έναν χρήστη ενώ το δεύτερο είναι ένα δημόσιο κλειδί το οποίο είναι διαθέσιμο σε όλους. Ένας χρήστης χρησιμοποιεί το ιδιωτικό κλειδί για να κρυπτογραφήσει μια πληροφορία, ενώ ο αποδέκτης χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί για να μπορέσει να αποκωδικοποιήσει τη πληροφορία. Τα δύο κλειδιά σχετίζονται μεταξύ τους με μια μαθηματική σχέση η οποία ορίζεται από τον αλγόριθμο κρυπτογράφησης. Συνήθως οι ασύμμετροι αλγόριθμοι χρησιμοποιούν μεγαλύτερα σε μέγεθος κλειδιά σε σχέση με τους συμμετρικούς και συνεπώς απαιτούν μεγαλύτερη επεξεργαστική ισχύ για την αποκωδικοποίηση.

1.3.4 Ψηφιακές υπογραφές

Οι ασύμμετροι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται επίσης και στην περίπτωση των ψηφιακών υπογραφών. Μια ψηφιακή υπογραφή χρησιμοποιεί το ιδιωτικό κλειδί του αποστολέα για να κωδικοποιήσει κάποιο μέρος του μηνύματος. Όταν ο παραλήπτης λαμβάνει το μήνυμα χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί για να αποκωδικοποιήσει τη ψηφιακή υπογραφή του αποστολέα. Αν η αποκρυπτογράφηση είναι επιτυχής αποδεικνύει την ταυτότητα του αποστολέα. Ο αλγόριθμος RSA είναι ένα τυπικό παράδειγμα ασύμμετρου αλγορίθμου. Το ελληνικό Δίκαιο με ειδική πρόβλεψη (Ν. 2672/1999) προτείνει τον όρο "ψηφιακή υπογραφή" αντί για "ηλεκτρονική", και δίνει τον ορισμό της: "Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων".

1.3.5 Αλγόριθμοι Hash

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εισέρχεται και η έννοια της συνάρτησης κατακερματισμού (hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από κάθε μήνυμα παράγεται μια "σύνοψη", η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (fingerprint ή message digest) και αποτελεί ψηφιακή αναπαράσταση του μηνύματος μοναδική για το μήνυμα που αντιπροσωπεύει.

Με τη χρήση αλγόριθμων από μια μεταβλητού μήκους πληροφορία παράγεται πάντα ένας αριθμός με σταθερό πλήθος ψηφίων που ονομάζεται κλειδί hash. Τα κλειδιά αυτά μοιάζουν με τον Κυκλικό έλεγχο περιττότητας (Cyclical redundancy checks CRCs) για τον έλεγχο της ακεραιότητας των δεδομένων. Ο αλγόριθμος hash εφαρμόζεται στα περιεχόμενα του πακέτου και στη συνέχεια το κλειδί hash που δημιουργείται ενσωματώνεται στο IP πακέτο. Κατά τη παραλαβή του πακέτου, αν έστω και ένα bit του μηνύματος έχει αλλαχθεί, τα κλειδιά hash δεν θα ταιριάζουν, με αποτέλεσμα ο παραλήπτης να γνωρίζει ότι η πληροφορία έχει αλλοιωθεί κατά τη μεταφορά. Τέτοιοι αλγόριθμοι είναι και οι MD5 και SHA1.

1.3.6 Αποστολή και λήψη δεδομένων με τη χρήση ψηφιακών υπογραφών

Η αποστολή και λήψη δεδομένων ανάμεσα στα δύο μέρη της συναλλαγής με τη χρήση και επαλήθευση της ψηφιακής υπογραφής γίνεται ως εξής:

Ο Αποστολέας δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (hash). Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων. Στη συνέχεια χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

Στη συνέχεια ο Παραλήπτης παραλαμβάνει το μήνυμα και αποσπά την ψηφιακή υπογραφή που είναι κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή). Αν οι δύο συνόψεις βρεθούν ίδιες, το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

1.3.7 Πιστοποιητικά

Στους συμμετρικούς αλγόριθμους ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί, πράγμα που σημαίνει ότι το κλειδί αυτό θα πρέπει να έχει αποσταλεί στον παραλήπτη πριν από την αποστολή του κρυπτογραφημένου μηνύματος. Αυτό εγκυμονεί τον κίνδυνο το κλειδί να υποκλαπεί και η μυστικότητα του μηνύματος να διαβληθεί. Αντίθετα στους ασύμμετρους αλγορίθμους, ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα ενώ ο παραλήπτης χρησιμοποιεί ένα δημόσιο κλειδί για την αποκωδικοποίηση το οποίο διατίθεται σε οποιονδήποτε πρόκειται να παραλάβει το κρυπτογραφημένο ή ηλεκτρονικά υπογραφόμενο μήνυμα. Με τη λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο αποστολέας αρκεί να διαφυλάξει μυστικό το ιδιωτικό κλειδί. Ο παραλήπτης επίσης θα πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος και κάτοχος του ιδιωτικού κλειδιού είναι όντως αυτός που ισχυρίζεται ότι είναι. Συνεπώς απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή, και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται λοιπόν ένας φορέας πιστοποίησης που θα πιστοποιεί στον παραλήπτη την ταυτότητα του προσώπου με το δημόσιο κλειδί.

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι ένας φορέας που βεβαιώνει με ακρίβεια τη σχέση ενός φυσικού προσώπου με το δημόσιο κλειδί του, με την έκδοση ενός ηλεκτρονικού πιστοποιητικού, στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Κύριος τύπος ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificates). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει. Η συσχέτιση ενός δημόσιου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Πάροχου Υπηρεσιών Πιστοποίησης, ο οποίος υπογράφει το πιστοποιητικό του δικαιούχου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο Πάροχος Υπηρεσιών Πιστοποίησης δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) [Microsoft, 1999].

Με την ηλεκτρονική υπογραφή επιτυγχάνονται οι εξής στόχοι:

- Η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει
- Η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και
- Η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, ότι δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί τη συμμετοχή του στην εν λόγω συναλλαγή

1.3.8 Πρωτόκολλα Ασφαλείας

Για την ασφαλή ανταλλαγή των δεδομένων κατά την ηλεκτρονική συναλλαγή έχουν αναπτυχθεί διάφορα πρωτόκολλα ασφαλείας. Ένα από αυτά είναι το πρωτόκολλο για Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)

Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, απολαμβάνει μεγάλης αποδοχής από την τραπεζική κοινότητα. Στην πράξη όμως η χρήση των ψηφιακών πιστοποιητικών πραγματοποιείται με την εφαρμογή του Secure Sockets Layer (SSL). Το SSL χρησιμοποιείται κυρίως στις συναλλαγές που γίνονται στον Παγκόσμιο Ιστό και εγγυάται ότι τα υποβαλλόμενα από το χρήστη του Internet δεδομένα θα μεταφερθούν με ασφαλή τρόπο στην ηλεκτρονική επιχείρηση. Επίσης η χρήση του SSL πιστοποιεί την ταυτότητα του ιδιοκτήτη της ηλεκτρονικής επιχείρησης και επιπλέον παρουσιάζει το πιστοποιητικό αυτό στους χρήστες του Διαδικτύου.

Κατά τη χρήση του πρωτόκολλου SSL στο Παγκόσμιο Ιστό, ως πρωτόκολλο μεταφοράς δεδομένων υπερκειμένου δεν χρησιμοποιείται πλέον το HTTP αλλά το ασφαλές HTTPS.

2 Εφαρμογή

2.1 Web εφαρμογή

Μια Web εφαρμογή στηρίζεται στην Client - Server αρχιτεκτονική. Ένας δικτυακός τόπος περιέχει ιστοσελίδες HTML και στοιχεία εκτελέσιμου κώδικα, τα οποία είναι αποθηκευμένα σε έναν Web server. Από την άλλη πλευρά υπάρχουν εργαλεία όπως οι φυλλομετρητές (Internet browser) στους υπολογιστές των χρηστών που συνδέονται με τον Web Server και γίνονται αποδέκτες του περιεχομένου των ιστοσελίδων. Ο χρήστης ζητάει το περιεχόμενο από τον Web Server στέλνοντας μια αίτηση σε μια συγκεκριμένη URL (Unified Reference Location), το περιεχόμενο αποστέλλεται και οι φυλλομετρητές αναλαμβάνουν να εμφανίσουν το περιεχόμενο στο χρήστη.

Η γλώσσα HTML είναι μια markup γλώσσα περιγραφής περιεχομένου των ιστοσελίδων που πρόκειται να είναι προσβάσιμες στον Παγκόσμιο Ιστό. Σχεδιάστηκε για να μπορεί να οργανώσει και να περιγράψει τον τρόπο με τον οποίο θα εμφανίζεται το περιεχόμενο μέσα σε μια ιστοσελίδα.

Η λύση των Cascading Style Sheets (CCS) επιτρέπει στον φυλλομετρητή να λάβει οδηγίες αναφορικά με τη μορφή του περιεχομένου μιας ιστοσελίδας. Ένα CSS που μπορεί να είναι ένα αρχείο ξεχωριστό από την ιστοσελίδα περιγράφει τον τρόπο με τον οποίο θα παρουσιαστεί η πληροφορία μέσα στην ιστοσελίδα. Έτσι γίνεται διαχωρισμός της παρουσίασης του περιεχομένου από τη δομή του και επίσης διασφαλίζεται ο ενιαίος τρόπος με τον οποίο θα εμφανίζεται το περιεχόμενο μέσα από οποιονδήποτε browser.

Τέλος η JavaScript είναι μια γλώσσα προγραμματισμού η οποία μπορεί να χρησιμοποιηθεί μέσα σε ιστοσελίδες. Ο κώδικας ενσωματώνεται μέσα στις ιστοσελίδες και εκτελείται από τον φυλλομετρητή στο περιβάλλον του client δίνοντας έτσι τη δυνατότητα στις ιστοσελίδες να αλληλεπιδρούν με τις κινήσεις του χρήστη κατά την πλοήγησή του.

2.1.1 PHP

Οι ιστοσελίδες περιέχουν κώδικα γραμμένο σε γλώσσα HTML (Hyper Text Markup Language). Σε μια Web εφαρμογή όμως εκτός των περιεχομένων, οι ιστοσελίδες περιέχουν ενσωματωμένο και εκτελέσιμο κώδικα ο οποίος εκτελείται στον Server χωρίς να είναι ορατός στον τελικό χρήστη. Τέτοιες σελίδες είναι οι PHP σελίδες (Hypertext Preprocessor). Η PHP ξεκίνησε αρχικά σαν μια σύντομη έκδοση της Perl από τον Rasmus Lerdorf το 1994.

Βασικό της χαρακτηριστικό είναι ότι οι σελίδες αυτές σχεδιάζονται δυναμικά ανάλογα με την εκτέλεση του κώδικα. Τα βασικά χαρακτηριστικά των δυναμικών PHP σελίδων είναι τα εξής:

- Είναι πολύ εύκολη η εκμάθηση της PHP
- Υποστηρίζει πολλές πλατφόρμες (Windows, Linux, Unix, κα)
- Υπάρχει συμβατότητα με σχεδόν όλους τους servers (Apache, IIS, κα)
- Παρέχει εύκολη συνδεσιμότητα με Βάσεις Δεδομένων όπως MySQL, Oracle, Sybase, PostgreSQL, Generic ODBC κα.

- Ανήκει στην κατηγορία του Λογισμικού Ανοικτού Κώδικα (Open Source software – OSS).
- Συνεργάζεται με την επίσης Ανοικτού Κώδικα βάση Δεδομένων MySQL.
- Η χρήση είναι δωρεάν.
- Ο προγραμματισμός σε PHP είναι οικείος σε προγραμματιστές C, Perl και Java.

2.1.2 Βάση Δεδομένων MySQL

Βασικό συστατικό μιας web εφαρμογής είναι μια βάση δεδομένων για την καταχώρηση, συντήρηση και προβολή πληροφοριών στους χρήστες. Στην πλευρά του server υπάρχει ένα σύστημα Διαχείρισης Βάσης Δεδομένων συνήθως Σχεσιακής (Relational Database System - RDBMS) όπου καταχωρούνται τα δεδομένα. Ανάλογα με τις ενέργειες και τις αιτήσεις του χρήστη, ο server επικοινωνεί με το σύστημα διαχείρισης της βάσης δεδομένων εκτελώντας ερωτήματα στη γλώσσα SQL.

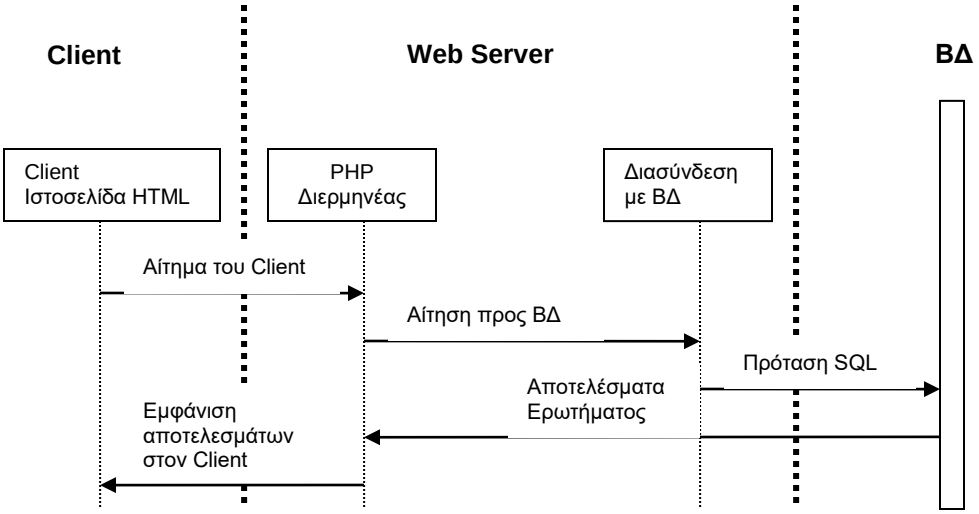
Το σύστημα διαχείρισης της Βάσης Δεδομένων απαντάει σε αυτά τα ερωτήματα του server είτε αποστέλλοντας τα δεδομένα που προέκυψαν σαν αποτελέσματα των ερωτημάτων ή εκτελώντας κάποια εισαγωγή ή διαγραφή δεδομένων. Η επικοινωνία μεταξύ Server εφαρμογής και Βάσης Δεδομένων γίνεται με τη χρήση οδηγών (Database Connectivity drivers).

Στη συγκεκριμένη εφαρμογή χρησιμοποιείται η MySQL. Η MySQL είναι ένα Σύστημα Διαχείρισης Σχεσιακής Βάσης Δεδομένων και περιέχει και έναν μικρό server της βάσης. Αναπτύχθηκε σαν μια εφαρμογή της γλώσσας SQL από την TcX. Είναι αρκετά σταθερό σύστημα και πολύ ευέλικτο. Υποστηρίζει όλες τις λειτουργίες και τους τύπους δεδομένων της standard.

2.1.3 PHP – MySQL

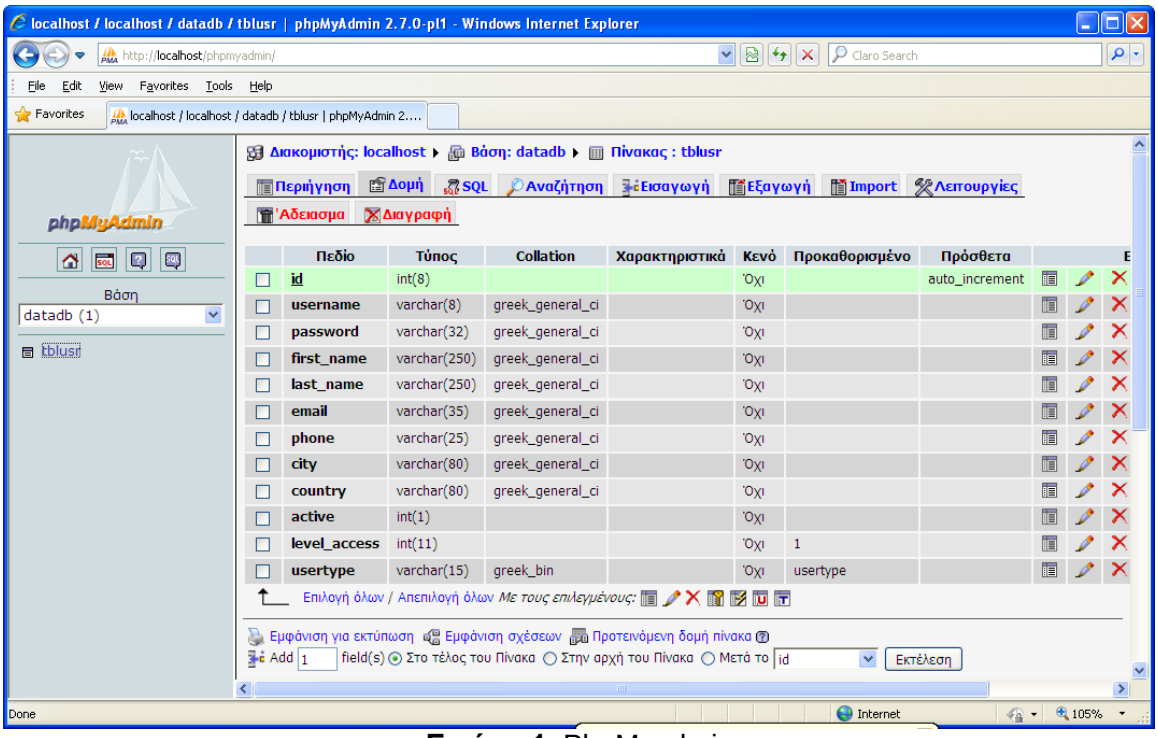
Ο συνδυασμός της γλώσσας PHP και της ΒΔ MySQL έχει σαν βασικό πλεονέκτημα ότι υποστηρίζεται από σχεδόν όλες τις πλατφόρμες. Έχουν κοινά χαρακτηριστικά όπως είναι το γεγονός ότι ανήκουν και οι δύο στις εφαρμογές Ανοικτού Κώδικα και τα δικαιώματα χρήσης τους είναι δωρεάν. Εξαιτίας των κοινών αυτών χαρακτηριστικών, έχουν αναπτυχθεί Web Servers που υποστηρίζουν τα δύο αυτά λογισμικά και την άμεση συνδεσιμότητα μεταξύ τους.

Η βασική λειτουργία του συνδυασμού των δύο τεχνολογιών είναι η εξής: Ένας δυναμικός δικτυακός τόπος αποτελείται από PHP σελίδες. Η λειτουργικότητα που παρέχουν οι σελίδες αυτές στο χρήστη στηρίζεται στον εκτελέσιμο κώδικα που είναι ενσωματωμένος. Οι δυναμικές σελίδες PHP περιέχουν κώδικα ο οποίος εκτελείται στον server. Ο κώδικας αυτός εκτελεί ερωτήματα σε SQL τα οποία μεταβιβάζονται μέσω του ειδικού driver της MySQL στη βάση MySQL. Ανάλογα με την αίτηση του χρήστη μπορεί να γίνει μια καταχώριση, τροποποίηση ή διαγραφή δεδομένων στη Βάση. Επίσης ο χρήστης μπορεί να αιτηθεί την ανάκτηση κάποιας πληροφορίας. Η αίτηση μεταβιβάζεται στη Βάση Δεδομένων και τα αποτελέσματα επιστρέφουν στο Web Server. Στη συνέχεια τα δεδομένα χρησιμοποιούνται στη δημιουργία της σελίδας που τελικά αποστέλλεται στο χρήστη και του προβάλει το περιεχόμενο που ζήτησε. Το περιεχόμενο παρουσιάζεται στο χρήστη από τον αντίστοιχο browser. Η διαδικασία παρουσιάζεται στο Σχήμα 2.



Σχήμα 1 Ακολουθιακό Διάγραμμα

Στην εικόνα 1 παρουσιάζεται το εργαλείο δημιουργίας και διαχείρισης της βάσης δεδομένων MySQL, το PHPMyadmin.



Εικόνα 1 PhpMyadmin

Στην συγκεκριμένη εφαρμογή δημιουργήθηκε ο πίνακας tblUsr ο οποίος περιέχει τα στοιχεία των εξουσιοδοτημένων χρηστών της εφαρμογής. Τα πεδία του πίνακα είναι τα εξής:

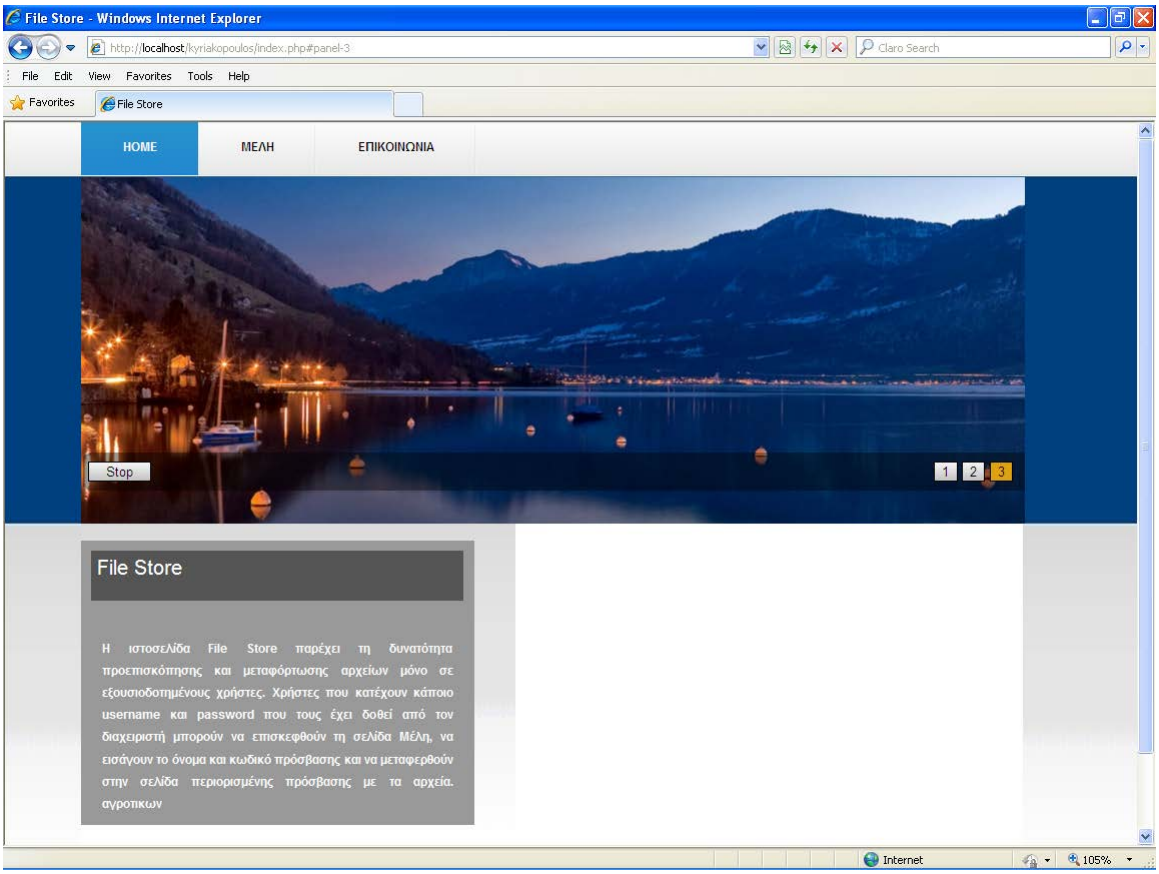
Username:Όνομα χρήστη
Password: Κωδικός πρόσβασης
First_Name : Όνομα
Last_Name: Επώνυμο
Email: Διεύθυνση Ηλεκτρονικού Ταχυδρομείου
Phone: Τηλέφωνο
City: Πόλη Διαμονής
Country: Χώρα
Active: Ενεργός ή Ανενεργός Χρήστης
Level_Access: Επίπεδο Πρόσβασης (1 ή 2)
Usertype:Τύπος Χρηστη

Τα πεδία Username, Password και UserType χρησιμοποιούνται όπως θα δούμε στη συνέχεια για τον έλεγχο της πρόσβασης στις προστατευόμενες ιστοσελίδες.

2.2 Αρχική Σελίδα

Η αρχική σελίδα ονομάζεται index.php και περιέχει κάποιες πληροφορίες για την εφαρμογή και το κεντρικό Menu. Η μορφή βασίζεται σε ένα template του οποίου η περιγραφή περιέχεται στο αρχείο style.css. Η χρήση του συγκεκριμένου style γίνεται με τη χρήση της εντολής :

```
<link rel="stylesheet" href="style.css" type="text/css" media="all">
```



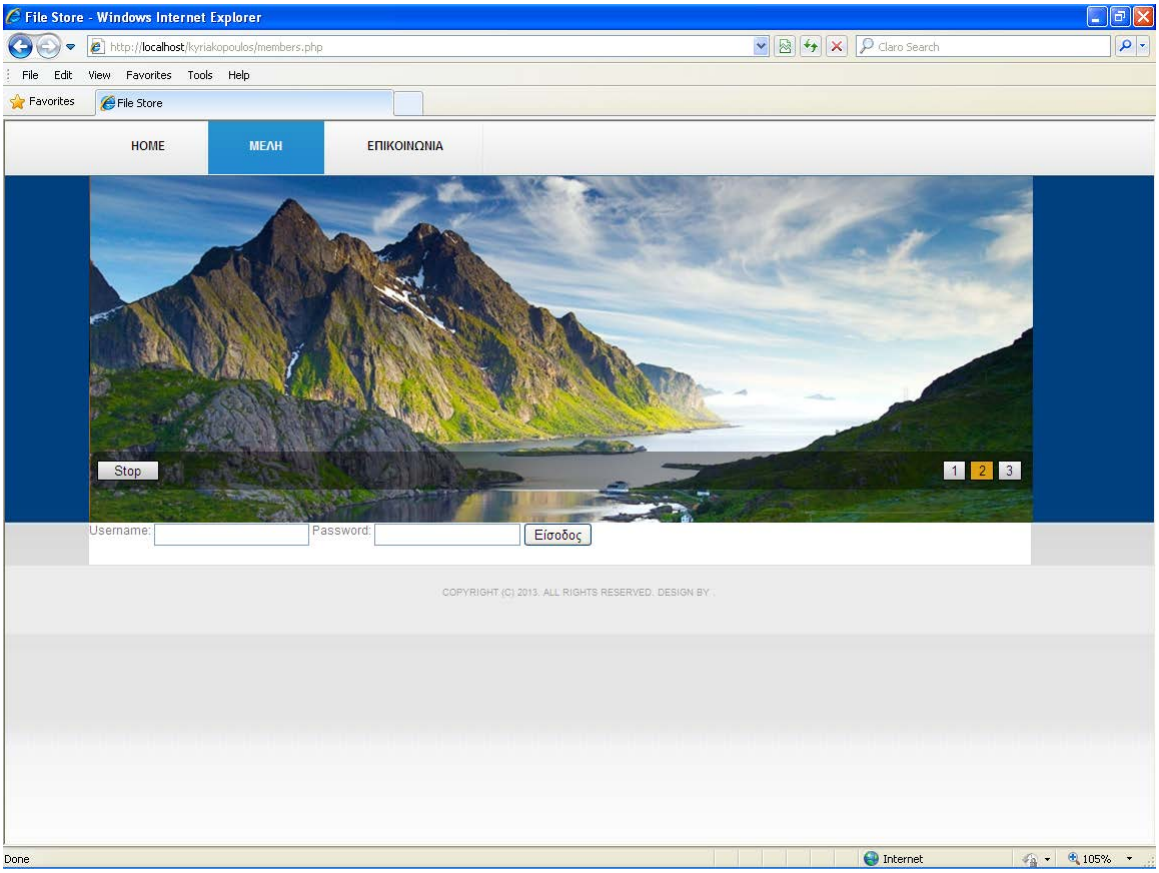
Εικόνα 2 Index.php

2.3 Σελίδα Μέλη

Πατώντας στην επιλογή Μέλη από το menu επιλογών ο χρήστης μεταφέρεται στη σελίδα member.php που περιέχει τη φόρμα εισαγωγής του username και του password για την ταυτοποίηση και την είσοδο σε περιοχή που απευθύνεται μόνο σε εξουσιοδοτημένους χρήστες. Η φόρμα αποτελείται από τον παρακάτω κώδικα.

```
<form id="form1" method="post" action="./member/loginmember.php">
            <fieldset>
            <label for="inputtext1">Username:</label>
            <input id="inputtext1" type="text" name="inputtext1"
value="" size="20" />
            <label for="inputtext2">Password:</label>
            <input id="inputtext2" type="password" name="inputtext2"
value="" size="20" />
            <input id="inputsubmit1" type="submit" name="inputsubmit1"
value="Είσοδος" />
            </fieldset>
</form>
```

Οι τιμές των πεδίων αποστέλλονται με τη μορφή παραμέτρων στη σελίδα loginmember.php που βρίσκεται στην περιοχή member. Το πρωτόκολλο επικοινωνίας σε αυτή την περίπτωση δεν είναι το HTTP αλλά το HTTPS που χρησιμοποιεί κρυπτογράφηση για την αποστολή του username και password.



Εικόνα 3 Member.php

2.4 Σελίδα Ταυτοποίησης

Η σελίδα αποτελείται από κώδικα php ο οποίος δέχεται τις τιμές των παραμέτρων 'inputtext1' και 'inputtext2' για το username και password αντίστοιχα. Στη συνέχεια εκτελεί ένα SELECT query στον πίνακα tblusr για τον έλεγχο της ύπαρξης του χρήστη και της επιβεβαίωσης του κωδικού. Το script εκτελείται στον server όπου είναι αποθηκευμένη και η βάση δεδομένων. Αν ο χρήστης δεν είναι καταχωρημένος στη βάση ή έχει δώσει λάθος κωδικό ή είναι ανενεργός (active=0) τότε απορρίπτεται η είσοδος στην προστατευμένη περιοχή και ο χρήστης μεταφέρεται στην κεντρική σελίδα. Αν το query επιστρέψει την εγγραφή τότε σημαίνει ότι ο χρήστης είναι καταχωρημένος και ενεργός και ανάλογα με το επίπεδο πρόσβασης (1 ή 2) του δίνεται και αντίστοιχος ρόλος χρήστη ή διαχειριστή σε μια session μεταβλητή (μεταβλητή συνόδου) που θα τον συνοδεύει στη προστατευόμενη περιοχή. Ο χρήστης οδηγείται στη σελίδα admin.php της περιοχής member. Οι παραπάνω διαδικασίες γίνονται από τον παρακάτω κώδικα:

```
<?php
session_start();
include 'datadbinfo.php';
$username='';
$password='';
$username = addslashes($_POST['inputtext1' ]);
$password=addslashes($_POST['inputtext2']);

$query=mysql_query("select * from tblusr where username
='".$username."'");
if (mysql_num_rows($query)==0)
    {
      mysql_close($link);
      ?>
      <script language="javascript">
      window.alert("Μη αποδεκτό Username");
      window.location="../index.php";
      </script>
<?php    }
else if
((mysql_result($query,0,"password")!=$password)||(mysql_result($query,0
,"active")==0))
    {
      mysql_close($link);
      ?>
      <script language="javascript">
      window.alert("Μη αποδεκτός χρήστης");
      window.location="../index.php";
      </script>
<?php
    }
else
{
$_SESSION['currentuser']=$username ;
if (mysql_result($query,0,"level_access")==1)
{
$_SESSION['usertype']="tradertp" ;
}
```

```
else if (mysql_result($query,0,"level_access")==2)
{
$_SESSION['usertype']="admintp" ;
}
      mysql_close($link);
?>

      <script language="javascript">
      window.alert("Συνδέθηκες επιτυχώς");
      window.location="admin.php";
      </script>
<?php


} ?>
```

2.5 Προστατευόμενη Σελίδα

Η σελίδα admin.php περιέχει στην αρχή την εντολή session_start() για την ενεργοποίηση συνόδου. Στη συνέχει χρησιμοποιοεί τον παρακάτω έλεγχο για να διαπιστώσει αν η σελίδα έχει ανοίξει από κάποιον χρήστη που έχει κάνει νωρίτερα ταυτοποίηση και το usertype έχει οριστεί σε ρόλο εξουσιοδοτημένου χρήστη, διαφορετικά ο επισκέπτης ανακατευθύνεται στην αρχική σελίδα της εφαρμογής:

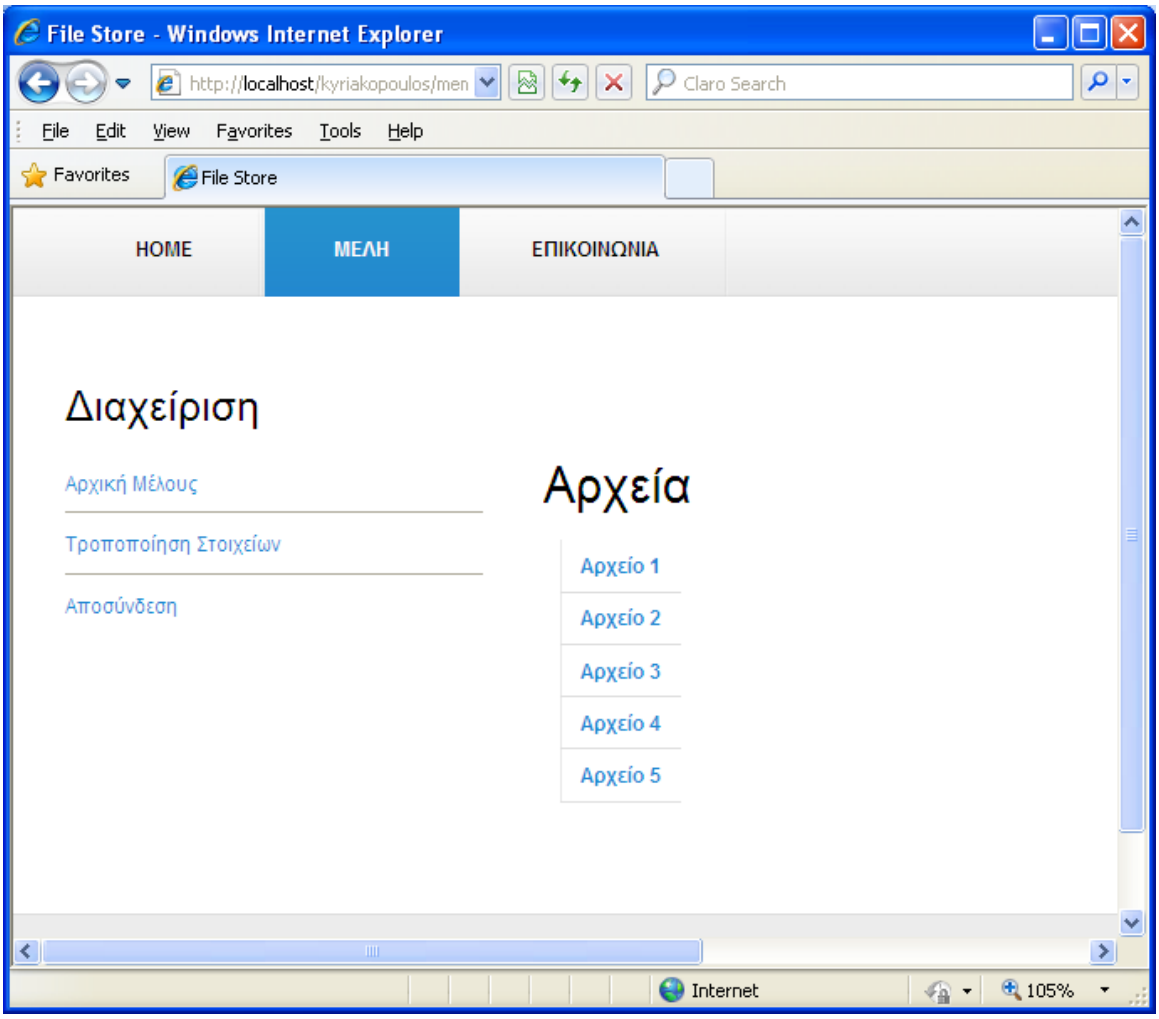
```
session_start();
if
((!(isset($_SESSION['usertype'])))||($_SESSION['usertype']!="tradertp")
){
header( 'Location: ../index.php');
}
```

Ο χρήστης μπορεί να κατεβάσει ένα από τα αρχεία ή κάνει αποσύνδεση. Η αποσύνδεση γίνεται από τη σελίδα logout η οποία καθαρίζει το περιεχόμενο των μεταβλητών συνόδου:

```
<?php
session_start();
$_SESSION['currentuser']='' ;
$_SESSION['usertype']='';
unset($_SESSION['currentuser']);
unset($_SESSION['usertype']);
?>

      <script language="javascript">
      window.alert("Αποσυνδεθήκατε επιτυχώς");
      window.location="../index.php";
      </script>
```

Σε περίπτωση που ο χρήστης επιθυμεί να τροποποιήσει τα στοιχεία του επιλέγει την Τροποποίηση Στοιχείων και μεταφέρεται στη σελίδα UpdateMember.php.



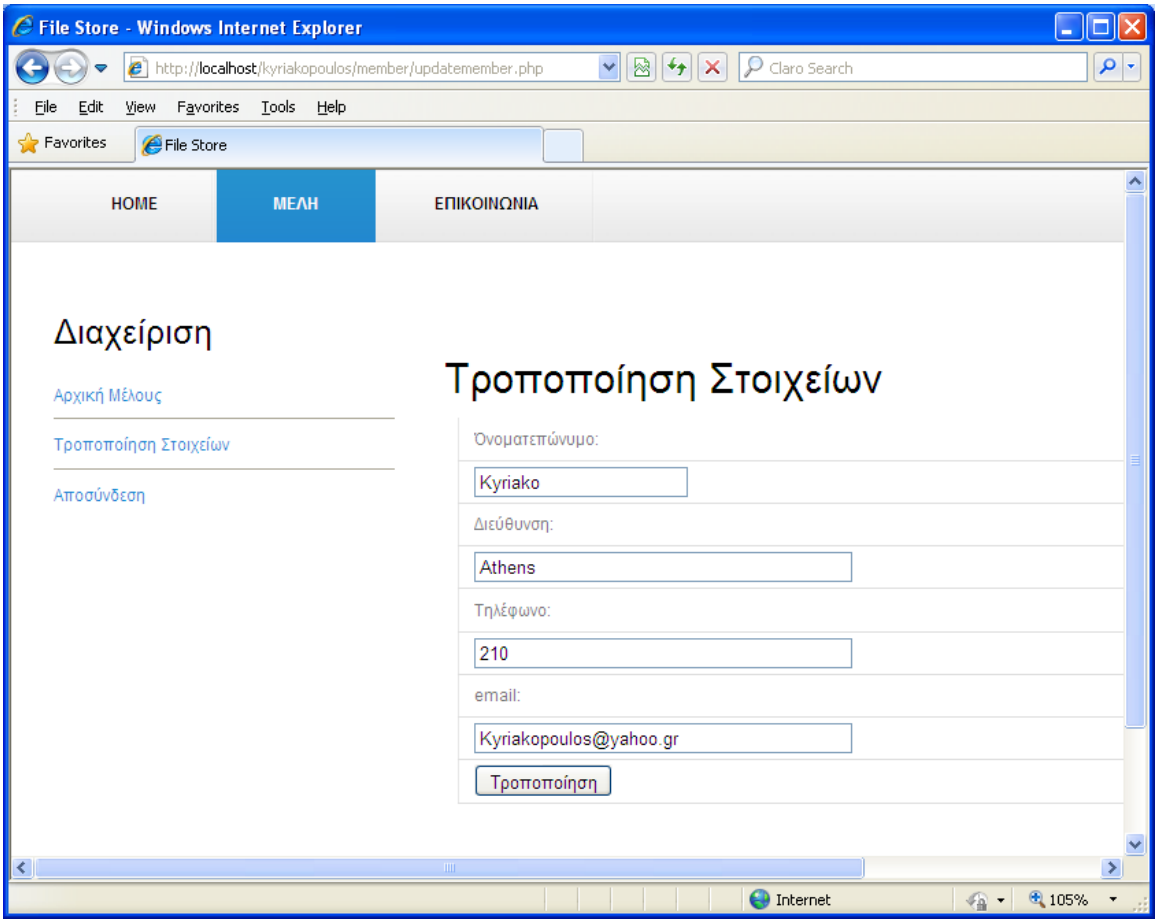
Εικόνα 4 Admin.php

2.6 Τροποποίηση Στοιχείων -UpdateMember.php

Στη σελίδα αυτή ο χρήστης συμπληρώνει σε μια φόρμα τις τροποποιημένες τιμές των στοιχείων του στα αντίστοιχα πεδία. Τα στοιχεία με τη μορφή παραμέτρων περνάνε στη σελίδα AlterMember.php η οποία με τον παρακάτω κώδικα εκτελεί ένα update query στον πίνακα tblusr.

```
$username=$_SESSION['currentuser'];
$firstname=$_POST['firstname'];
$address = $_POST['address' ];
$phone = $_POST['phone'];
$email = $_POST['email'];
include 'datadbinfo.php';

mysql_query("update tblusr set
first_name='".$firstname."',phone='".$phone."',city='".$address."',emai
l='".$email."' where username='".$username."'");
mysql_close($link);
```



Εικόνα 5 UpdateMamber.php

3 Εγκατάσταση

3.1.1 Οδηγίες εγκατάστασης εφαρμογής

Το Wamp είναι ένα λογισμικό το οποίο μας εγκαθιστά την Mysql μαζί με το PhpMyadmin και τον Apache server για Windows τοπικά στο μηχάνημά μας για να εκτελέσουμε μια εφαρμογή php στον υπολογιστή μας. Αφού το εγκαταστήσουμε και εκκινήσουμε τις υπηρεσίες (εικονίδιο κάτω δεξιά) κάνουμε την εξής διαδικασία.

1.Φόρτωση Βάσης
Αρχικά δημιουργούμε μια βάση δεδομένων με την εφαρμογή phpMyadmin κάνοντας κλικ κάτω δεξιά στο εικονίδιο του WAMP. Το όνομα της βάσης θα είναι datadb. Στη συνέχεια επιλέγουμε την επιλογη SQL και αντιγράφουμε το περιεχόμενο του αρχείου sql.txt και πατάμε εκτέλεση. Ο πίνακας της βάσης δημιουργείται.

Στη συνέχεια μέσα στο αρχείο dabas.php στον υποφάκελο lib της εφαρμογής μας εισάγουμε το username, το password και το όνομα της βάσης. Συνήθως για τον WAMP είναι ορισμένα ως "root", "" και το όνομα της βάσης που δημιουργήσαμε στο phpmyadmin αντίστοιχα.

```
<?php
//db.php
//το όνομα του server μας
$host = "localhost";
//το όνομα του χρήστη που θα χρησιμοποιήσουμε
$user = "root";
//το αντίστοιχο password για τον προηγούμενο χρήστη
$pass = "";
//η βάση μας, στο συγκεκριμένο παράδειγμα
$db = "datadb";
?>
```

3. Σε έναν υποφάκελο πχ site στο φάκελο www μέσα στο φάκελο C:\wamp αντιγράφουμε όλα τα αρχεία php και τους φακέλους του zip.

4. Για την είσοδο στη πρώτη σελίδα index.php ο χρήστης θα πρέπει να εισάγει στη διεύθυνση του browser την εξής διεύθυνση: https://localhost/site.

5. Για την είσοδο στη σελίδα Μέλη ο χρήστης θα πρέπει να εισάγει
Username: kyriako
Password: kyriako

3.1.2 Οδηγίες εγκατάστασης SSL σε WAMP

Βήμα 1ο
Ανοίγοντας το παράθυρο DOS command μεταφερόμαστε στον κατάλογο bin του wamp apache χρησιμοποιώντας την παρακάτω εντολή:

"cd /d c:\" και μετά "cd wamp\bin\apache\apache2.2.22\bin".

και ανάλογα με την έκδοση του apache (στην προκειμένη περίπτωση έχουμε την έκδοση 2.2.22)
Μετά από αυτό λογικά στο DOS φαίνεται το εξης:
C:\wamp\bin\apache\apache2.2.22\bin >

Βήμα 2ο
Για να δημιουργηθεί ένα ιδιωτικό κλειδί με κρυπτογράφηση1024 bits, πρέπει αρχικά να εκτελεστεί η εντολή στο command prompt:
"openssl genrsa -des3 -out server.key 1024"
Στην ερώτηση για μια φράση κλειδί εισάγουμε μια οποιαδήποτε φράση.

Βήμα 3ο
Αφαιρούμε τη φράση από το RSA ιδιωτικό κλειδί (αφού κρατήσουμε ένα back up του αρχικού αρχείου) πληκτρολογώντας την εξής εντολή:
"copy server.key server.key.org"
Και στη συνέχεια
"openssl rsa -in server.key.org -out server.key"
Στη συνέχεια ζητείται η φράση κλειδί που πληκτρολογήθηκε νωρίτερα.

Βήμα 4ο
Για τη δημιουργία ενός προσωπικά υπογεγραμμένου πιστοποιητικού (X509 structure) με το RSA κλειδί που μόλις δημιουργήθηκε , εισάγουμε την εντολή :
"openssl req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt -config C:\wamp\bin\apache\apache2.2.22\conf\openssl.cnf".
Υπάρχει η περίπτωση να χρειάζεται διόρθωση για την διαδρομή του αρχείου config openssl.cnf . Στα windows δεν εμφανίζεται η επέκταση ".cnf" αλλά σε DOS εμφανίζεται το πλήρες όνομα openssl.cnf.

Βήμα 5ο
Αντιγραφή των αρχείων server.key και server.crt.
α)
Στο φάκελο conf του apache , δημιουργούμε δύο υποφακέλους με όνομα ssl.key και ssl.crt

β)
Αντιγράφουμε το αρχείο server.key στον φάκελο ssl.key και το αρχείο server.crt στον φάκελο ssl.crt

Βήμα 6ο
Στη συνέχεια τροποποιούμε τα αρχεία httpd.conf file και php.ini.
α)
Στο αρχείο httpd.conf αφαιρούμε τα σχόλια '#' από τη γραμμή που αναφέρει :
LoadModule ssl_module
modules/mod_ssl.so

β)
Στο αρχείο httpd.conf αφαιρούμε τα σχόλια '#' από τη γραμμή που αναφέρει :
Include
conf/extra/httpd_ssl.conf

Στη συνέχεια μεταφέρουμε αυτή τη γραμμή μετά το block <IfModule ssl_module>....
</IfModule>

γ)
Ανοίγουμε το αρχείο php.ini που βρίσκεται στον φάκελο apache2.....\bin folder, και αφαιρούμε τα σχόλια ';' μετά τη γραμμή που αναφέρει:
extension=php_openssl.dll

Βήμα 7ο

Τροποποιούμε το αρχείο httpd_ssl.conf στον φάκελο extra
α)
Εντοπίζουμε τη γραμμή που αναφέρει "SSLMutex ...." και την αλλάζουμε σε "SSLMutex default"

β)
Εντοπίζουμε τη γραμμή που αναφέρει: <VirtualHost _default_:443>.
Αμέσως μετά τροποποιούμε τη γραμμή που αναφέρει :
"DocumentRoot ..." σε
DocumentRoot "C:/wamp/www/"
Τροποποιούμε τη γραμμή που αναφέρει : "ErrorLog...." σε Errorlog logs/sslerror_log.
τροποποιούμε τη γραμμή που αναφέρει : "TransferLog ...." σε TransferLog logs/sslaccess_log

γ)
Για το αρχείο SSL crt τροποποιούμε τη γραμμή που αναφέρει :"SSLCertificateFile ...." σε SSLCertificateFile " C:\wamp\bin\apache\apache2.2.22\conf/ssl.crt/server.crt"

δ)
Για το αρχείο SSL key τροποποιούμε τη γραμμή που αναφέρει "SSLCertificateKeyFile ...." σε SSLCertificateKeyFile " C:\wamp\bin\apache\apache2.2.22\
conf/ssl.key/server.key"

ε)
Τροποποιούμε τη γραμμή που αναφέρει <Directory "C:/Program Files/Apache Software Foundation/Apache2.2/cgi-bin"> ή παρόμοια σε <Directory "C:/wamp/www/">
και προσθέτουμε τις ακόλουθες γραμμές μέσα στα tags <Directory ... >...</Directory>

Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
allow from all

στ)
Επιβεβαιώνουμε ότι η γραμμή CustomLog "logs/ssl_request_log" \
δεν είναι μέσα σε σχόλιο διαφορετικά σβήνουμε το #.

Βήμα 8ο
Στο προηγούμενο παράθυρο DOS εισάγουμε την εντολή httpd -t . Αν αυτή εμφανίζει Sysntax is OK, τότε προχωράμε στο βήμα 9 διαφορετικά διορθώνουμε τυχόν λάθη στην προηγούμενη διαδικασία και επαναλαμβάνουμε τον παραπάνω έλεγχο.

Βήμα 9ο
Κάνουμε επανεκκίνηση του Apache server.

Βήμα 10ο
Αν η επανεκκίνηση είναι επιτυχής ανοίγουμε τον browser και εισάγουμε στη διεύθυνση το localhost.

Αν ο υπολογιστής είναι συνδεδεμένος σε router, ρυθμίζουμε τον router ώστε να επιτρέπει τη θύρα 443 να κάνει forward στον υπολογιστή μας. Αν επίσης ο Η/Υ έχει ενεργοποιημένο firewall, ρυθμίζουμε το firewall να επιτρέπει εισερχόμενα αιτήματα σύνδεσης στη θύρα 443

Βιβλιογραφία

1. www.microsoft.com/security
2. Kim M.Bayne “The Internet Marketing Plan, Second Edition”, John Wiley and Sons Inc., 2000
3. Cisco Systems, Inc “Reference Guide A Primer for Implementing a Cisco Virtual Private Network”, Aug 2000
4. Microsoft, “Virtual Private Networking in Windows 2000: An Overview” White Paper 1999