ΤΜΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

<<ΑΝΑΠΤΥΞΗ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ>>

ΕΛΕΝΗ-ΑΝΔΡΙΑΝΑ ΠΑΝΟΒΑΣΙΛΗ Α.Μ:1068

Επιβλέπων καθηγητής:Σωτήρης Χριστοδούλου

Περίληψη

Η συνεχώς αυξανόμενη διάδοση της πληροφορίας και η ανάπτυξη της κοινωνίας της πληροφορίας είχαν σαν αποτέλεσμα και την μετεξέλιξη θεσμών όπως η ψηφοφορία όπου η διάδοση της τεχνολογίας έχει επιφέρει σημαντικά επιτεύγματα στην διαδικασία διεξαγωγής της. Έτσι εντάσσεται μια νέα μορφή ψηφοφορίας η λεγόμενη ηλεκτρονική ψηφοφορία που δεν είναι τίποτα άλλο παρά μια εναλλακτική μορφή άσκησης του εκλογικού δικαιώματος. Η ψηφιοποίηση των εκλογικών διαδικασιών, με την εισαγωγή της ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ή άλλων επικοινωνιακών μέσων, και ιδιαίτερα η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την απαίτηση προσέλευσης του ψηφοφόρου στα εκλογικά τμήματα όπως συμβαίνει σήμερα, αποτελεί σπουδαία καινοτομία, που αναμένεται να αυξήσει τη συμμετοχή των πολιτών στις εκλογικές διαδικασίες.

Η διαρκής μείωση του ποσοστού συμμετοχής των ψηφοφόρων στις διαδικασίες των εκλογών έχει προκαλέσει την έντονη ανησυχία των φορέων διαχείρισης της πολιτικής εξουσίας, αλλά και κάθε πολίτη που ενδιαφέρεται για την εμβάθυνση της Δημοκρατίας. Λόγω της οικονομικής κρίσης που επικρατεί και της κοινωνικής αναταραχής που έχει ως αποτέλεσμα οδήγησε στο να αναζητηθούν νέοι τρόποι με τους οποίους θα τονώσουν το ενδιαφέρον των πολιτών για τις μορφές συμμετοχής στους πολιτικούς θεσμούς του δημοκρατικού πολιτεύματος.

Στα πλαίσια της παρούσας πτυχιακής εργασίας θα μελετήσουμε διεξοδικά την ουσία της ηλεκτρονικής ψηφοφορίας, θα μελετήσουμε τα υπάρχοντα συστήματα και τεχνολογίες που την υποστηρίζουν καθώς και τα θέματα ασφάλειας που την αφορούν και θα σχεδιάσουμε ένα ηλεκτρονικό σύστημα ψηφοφορίας ειδικά σχεδιασμένο για φοιτητές όπου εκεί θα μπαίνουν και θα ψηφίζουν για φοιτητικά θέματα που τους απασχολούν.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Σωτήρη Χριστοδούλου κυρίως για την εμπιστοσύνη που μου έδειξε, και την υπομονή που έκανε κατά τη διάρκεια υλοποίησης της πτυχιακής εργασίας. Όπως επίσης και για την πολύτιμη βοήθεια και καθοδήγηση του, για την επίλυση διάφορων θεμάτων.

Θα θελα επίσης να απευθύνω τις ευχαριστίες μου στους γονείς μου, οι οποίοι στήριξαν τις σπουδές μου με διάφορους τρόπους, φροντίζοντας για την καλύτερη δυνατή μόρφωση μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Η θεαματική ανάπτυξη της πληροφοριακής τεχνολογίας και της τεχνολογίας των επικοινωνιών τα τελευταία χρόνια, οδήγησε σε ένα δυναμικό μετασχηματισμό των δομών της κοινωνικής συμβίωσης, αλλά και του πολιτικού γίγνεσθαι γενικότερα. Τα επιτεύγματα της τεχνολογίας δύναται να εισέλθουν σε όλους τους τομείς της συλλογικής και ατομικής δράσης και να αποτελέσουν εργαλείο βελτίωσης ή πλήρους αναδιαμόρφωσης θεσμοποιημένων διαδικασιών. Μέσα σε αυτό το πνεύμα αναδιάρθρωσης των πολιτικών διαδικασιών εντάσσεται και η συζήτηση για την εισαγωγή της ηλεκτρονικής ψηφοφορίας ως μίας εν2αλλακτικής μορφής άσκησης του εκλογικού δικαιώματος.

Η διαρκής μείωση του ποσοστού συμμετοχής των ψηφοφόρων στις διαδικασίες άσκησης του εκλογικού δικαιώματος έχει προκαλέσει την έντονη ανησυχία των φορέων διαχείρισης της πολιτικής εξουσίας, αλλά και κάθε πολίτη που ενδιαφέρεται για την εμβάθυνση της Δημοκρατίας, οι οποίοι αναζητούν τρόπους με τους οποίους θα κατορθώσουν να αναστρέψουν αυτό το φαινόμενο και να τονώσουν το ενδιαφέρον των πολιτών για τις μορφές συμμετοχής στους πολιτικούς θεσμούς του δημοκρατικού πολιτεύματος.

Η ψηφιοποίηση των εκλογικών διαδικασιών, με την εισαγωγή της ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου ή άλλων επικοινωνιακών μέσων, και ιδιαίτερα η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την απαίτηση προσέλευσης του ψηφοφόρου στα εκλογικά τμήματα όπως συμβαίνει σήμερα, αποτελεί σπουδαία καινοτομία, που αναμένεται να αυξήσει τη συμμετοχή των πολιτών στις εκλογικές διαδικασίες. Στο πλαίσιο αυτής της συζήτησης, σε πολλές χώρες της Ευρωπαϊκής Ένωσης έχει ξεκινήσει ήδη τα τελευταία χρόνια, η πιλοτική εφαρμογή προγραμμάτων αυτού του είδους, σε περιορισμένου εύρους εκλογικές διαδικασίες, οι οποίες πραγματοποιούνται συνήθως σε επίπεδο τοπικών αρχών. Σύμφωνα με τα πρώτα αποτελέσματα η ανταπόκριση του κόσμου υπήρξε θετική, καθώς σημειώθηκε άνοδος του ποσοστού συμμετοχής των εκλογέων.

ΚΕΦΑΛΑΙΟ 2: ΣΚΟΠΟΣ ΚΑΙ ΣΤΟΧΟΙ

Σκοπός της παρούσας μελέτης είναι ο σχεδιασμός ενός ηλεκτρονικού συστήματος ψηφοφορίας ειδικά σχεδιασμένο για φοιτητές. Το συγκεκριμένο σύστημα θα χρησιμοποιείται και άλλα είδη ψηφοφορίας όπως: αξιολογήσεις καθηγητών και μαθημάτων.

Επιμέρους Στόχοι:

- Ανάλυση της διαδικασίας της ψηφοφορίας.
- Ανάλυση της διαδικασίας της ηλεκτρονικής ψηφοφορίας.
- Ανάλυση Ασφάλειας Συστημάτων Ηλεκτρονικής Ψηφοφορίας.
- Παρουσίαση Συστημάτων Ηλεκτρονικής Ψηφοφορίας.
- Παρουσίαση Απαιτήσεων Συστήματος Ηλεκτρονικής Ψηφοφορίας σε Υλικό και Λογισμικό.

ΚΕΦΑΛΑΙΟ 3: ΠΑΡΑΜΕΤΡΟΙ ΤΗΣ ΨΗΦΟΦΟΡΙΑΣ

Οι παράμετροι μιας ψηφοφορίας είναι οι εξής:

3.1 Εκλογές

Για τους πολίτες μιας χώρας οι εκλογές αποτελούν μια προϋπόθεση που αντιπροσωπεύει το δημοκρατικό τους πολίτευμα. Οι εκλογές είναι μια διαδικασία μέσα από την οποία οι πολίτες μιας χώρας με την ψήφο τους καθορίζουν ποιοι θα τους εκπροσωπούν.

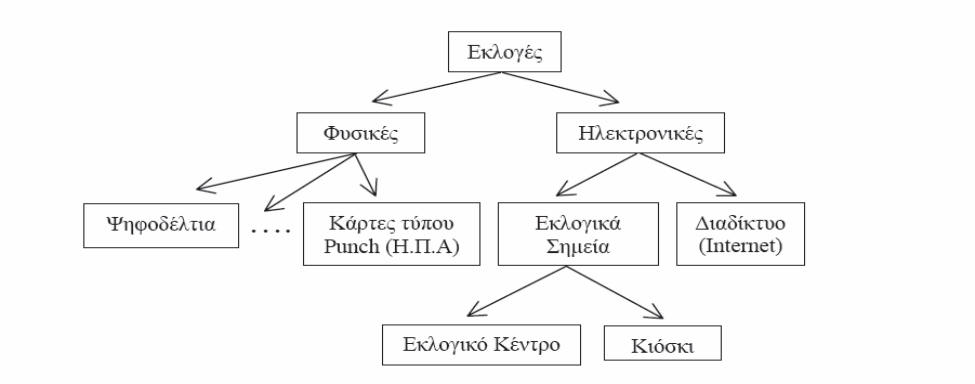
3.2 Εκλογικό σώμα

Το εκλογικό σώμα είναι το σύνολο των πολιτών που έχουν το δικαίωμα της ψήφου (ή το "δικαίωμα του εκλέγειν" ή το "ενεργητικό εκλογικό δικαίωμα").

3.3 Εκλογική διαδικασία

Η εκλογική διαδικασία περιλαμβάνει την διαδικασία κατά την οποία το εκλογικό σώμα πηγαίνει στα εκλογικά τμήματα στα οποία ο κάθε πολίτης είναι εγγεγραμμένος την καθορισμένη ημέρα που έχει οριστεί, εκεί ο ψηφοφόρος καταθέτει την ταυτότητα του η το διαβατήριο του και στην συνέχεια λαμβάνει το σύνολο των ψηφοδελτίων χωρίς να είναι ορατός από τους άλλους, συνήθως πίσω από ένα παραβάν, τοποθετεί στο φάκελο το ψηφοδέλτιο της επιλογής του, στο οποίο εφόσον το επιθυμεί μπορεί να σημειώσει με σταυρό μέχρι ένα συγκεκριμένο αριθμό υποψηφίων. Στη συνέχεια ρίχνει το φάκελο στην κάλπη και το όνομά του διαγράφεται από τη λίστα. Η εκλογική διαδικασία διαρκεί από την ανατολή μέχρι την δύση του

ηλίου. Όταν κλείσουν οι κάλπες γίνεται η καταμέτρηση των ψήφων στα εκλογικά κέντρα στα οποία διεκπεραιώθηκε η εκλογική διαδικασία .Σε αυτήν περιλαμβάνονται μόνο τα θεωρούμενα ως έγκυρα ψηφοδέλτια, σύμφωνα με τους αντίστοιχους κανονισμούς.



Εικόνα 1: Ταξινόμηση μεθόδων ψηφοφορίας

ΚΕΦΑΛΑΙΟ 4: ΗΛΕΚΤΡΟΝΙΚΗ ΨΗΦΟΦΟΡΙΑ

4.1 Ορισμός ηλεκτρονικής ψηφοφορίας

Ως ***ηλεκτρονική ψηφοφορία (electronic voting / e-voting)*** εννοούμε την άσκηση του εκλογικού δικαιώματος με την χρήση ηλεκτρονικών μεθόδων. Στο σύστημα ψηφοφορίας στο οποίο διεξάγεται η ηλεκτρονική ψηφοφορία, τα ηλεκτρονικά δεδομένα καταγράφονται, αποθηκεύονται και υπόκεινται σε επεξεργασία πρωτίστως ως ψηφιακή πληροφορία. Η ψηφιοποίηση των εκλογικών διαδικασιών, με την εισαγωγή της ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ή άλλων επικοινωνιακών μέσων, και ιδιαίτερα η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την απαίτηση προσέλευσης του ψηφοφόρου στα εκλογικά τμήματα όπως συμβαίνει σήμερα, αποτελεί σπουδαία καινοτομία, που αναμένεται να αυξήσει τη συμμετοχή των πολιτών στις εκλογικές διαδικασίες.

Η ηλεκτρονική ψηφοφορία μπορεί να γίνει με αποστολή μηνυμάτων SMS από το κινητό τηλέφωνο, μέσω ειδικών τερματικών που βασίζονται στην «έξυπνη κάρτα» (smart card),σε ειδικά εκλογικά περίπτερα (infokiosks), με τη χρήση των νέων τηλεοράσεων ψηφιακής τεχνολογίας, κυρίως όμως μέσα από το διαδίκτυο και τον προσωπικό υπολογιστή. Πρόκειται για μια (εκλογική) διαδικασία, η οποία καθιστά δυνατή την άσκηση εκλογικού δικαιώματος ή την έκφραση γνώμης, η ψηφοφορία μπορεί να γίνεται χωρίς αυτοπρόσωπη παρουσία του εκλογέα σε ειδικό χώρο (διεξαγωγής εκλογών) αλλά με τη **χρήση αυτοματοποιημένων μεθόδων/δικτύων** (Internet / Intranet).

Βασικό κριτήριο ελέγχου είναι το εκλογικό δικαίωμα να ασκείται σε χώρο και μέσω συσκευών που δεν υπόκεινται στον έλεγχο των αρμόδιων οργάνων. Η ηλεκτρονική ψηφοφορία είναι μια διαδικασία που ορισμένες φορές υπόκειται σε λάθη όπως επίσης και σε διαστρέβλωση του αποτελέσματος για αυτό το λόγω τα άτομα τα οποία διεξάγουν την εκλογική διαδικασία πρέπει να χαρακτηρίζονται από εντιμότητα και εμπειρία .Η ηλεκτρονική ψηφοφορία αποτελεί ένα σημαντικό θέμα ασφάλειας από την καταχώρηση και πιστοποίηση των ψηφοφόρων έως την καθαυτό ψηφοφορία και καταμέτρηση των αποτελεσμάτων, ενώ περικλείει ένα ευρύ φάσμα τεχνολογικών και κοινωνικών προβλημάτων, που πρέπει να ληφθούν υπόψη. Η ψηφιοποίηση των εκλογικών διαδικασιών, με την εισαγωγή της ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ή άλλων επικοινωνιακών μέσων, και ιδιαίτερα η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την απαίτηση

προσέλευσης του ψηφοφόρου στα εκλογικά τμήματα όπως συμβαίνει σήμερα, αποτελεί σπουδαία καινοτομία, που αναμένεται να αυξήσει τη συμμετοχή των πολιτών στις εκλογικές διαδικασίες. Η ηλεκτρονική ψηφοφορία αποτελείται από ένα σύστημα που περικλείει όλες τις τεχνικές ψηφοφορίας εμπεριέχοντας ηλεκτρονικό εξοπλισμό. Για το σκοπό αυτό, η ηλεκτρονική ψηφοφορία μπορεί να είναι ένα πλατύ θέμα που αποτελείται από τις παρακάτω έννοιες:

- **Ηλεκτρονική ψηφοφορία (e-voting):** οποιαδήποτε μέθοδος ψηφοφορίας όπου η πρόθεση των ψηφοφόρων εκφράζεται και συλλέγεται με ηλεκτρονικούς τρόπους.
- **Ηλεκτρονική καταμέτρηση:** συγκεκριμένα χρησιμοποιείται για να καλύψει τεχνολογίες που ηλεκτρονικά καταμετρούν φυσικά ψηφοδέλτια όπως για παράδειγμα οπτικά scanner για χάρτινα ψηφοδέλτια.
- **Θάλαμοι ψηφοφορίας(kiosk voting):** στο γενικό ηλεκτρονικό πλαίσιο, οι θάλαμοι ψηφοφορίας σημαίνουν τη χρήση μηχανών ψηφοφορίας σε εκλογικούς σταθμούς ή σε άλλες ελεγχόμενες τοποθεσίες. Οι ψηφοφόροι αποτυπώνουν την επιλογή τους ηλεκτρονικά (ίσως σε touch sensitive screens) αντί για χάρτινα ψηφοδέλτια. Οι ψήφοι καταμετρούνται σε ατομικές μηχανές και τέλος μεταφέρονται στο κεντρικό σύστημα. Ένα ψηφοδέλτιο μπορεί να εκτυπώνεται και να παραμένει στο κουτί ψηφοδελτίων σαν επιπρόσθετη απόδειξη.
- **Απομακρυσμένη ηλεκτρονική ψηφοφορία (Remote Electronic Voting):** Το REV είναι η πιο πλήρης έννοια για την ηλεκτρονική ψηφοφορία. Αυτή η έννοια μπορεί να περιέχει τη χρήση internet, μηνύματος κειμένου, διαδραστικής ψηφιακής τηλεόρασης ή touchtone τηλέφωνου
- **Voting Server:** Μια γενική έννοια που περιγράφει από τι αποτελείται ο server του συστήματος online ψηφοφορίας..
- **Ίντερνετ ψηφοφορία (i-voting):** Είναι μια συγκεκριμένη περίπτωση του REV όπου η ψήφοι πραγματοποιούνται στο Internet μέσω web site ή applet ψηφοφορίας. Πολλές φορές αυτή η έννοια χρησιμοποιείται και σαν συνώνυμο του REV.
- **On-line σύστημα εκλογών:** το φυσικό σύστημα που είναι υπεύθυνο για τον έλεγχο της online εκλογικής διαδικασίας.

4.2 Ιστορική αναδρομή ηλεκτρονικής ψηφοφορίας

Το 1869 ο Thomas edis Edison λαμβάνει το αμερικανικό δίπλωμα ευρεσιτεχνίας κατασκευάζοντας μια μηχανή ηλεκτρονικής ψηφοφορίας αλλά δεν θα μπορέσει ποτέ να

πουλήσει την εφεύρεση του εν τούτοις από τότε η ηλεκτρονική ψηφοφορία έχει κάνει σημαντική πρόοδο.

Στις αρχές της δεκαετίας του ’60 και ως το τέλος της ίδιας δεκαετίας βλέπουμε την εμφάνιση των διάτρητων καρτών (punch cards), οι οποίες χρησιμοποιήθηκαν σε δύο μορφές ως:**VOTOMATIC** και **DATAVOTE** τις οποίες σταμάτησαν να χρησιμοποιούν λίγα χρόνια αργότερα λόγω προβλημάτων που παρατηρήθηκαν κατά την χρήση τους. Έως το 1960 ιδιαίτερα χρησιμοποιούμενος ήτανε ο μηχανικός τρόπος ψηφοφορίας (paperless voting), με τη βοήθεια μιας μηχανολογικής εγκατάστασης με μοχλό (mechanical-lever machines). Και αυτός όμως αποδείχτηκε μάλλον ανακριβής, ενώ είχε και το επιπρόσθετο μειονέκτημα ότι δεν διατηρούσε κανενός είδους φυσικό αρχείο ψήφων.

Στην δεκαετία του ’70 άρχισαν να χρησιμοποιούνται ηλεκτρονικά συστήματα καταγραφής ψήφων DRE (Direct recording electronic voting systems), έτσι η παραδοσιακή ηλεκτρονική ψηφοφορία αντικαθίσταται από τα τοπικά συστήματα ηλεκτρονικής ψηφοφορίας DRE.Η πρώτη χρήση μηχανής ηλεκτρονικής ψηφοφορίας έγινε σε πραγματικές εκλογές το 1975 στο Streamwood και Woodstock Illinois.

Το 1990 εκδόθηκαν τα πρώτα προαιρετικά VSS (Voting System Standards) από το Federal Election Commission (FEC) Office of Elections Administration (OEA), που πλέον είναι ενσωματωμένη στην Election Assistance Commission (EAC), σύμφωνα με τα οποία στο εξής θα πιστοποιούνταν από τη National Association of State Election Directors (NASED) στα διάφορα από την ίδια εξουσιοδοτημένα ITAs (Independent Testing Authorities) τα εκάστοτε συστήματα ψηφοφορίας, τόσο ως προς το hardware όσο και ως προς το software. Τα συγκεκριμένα standards αναθεωρήθηκαν και έδωσαν τα 2002 VSS, που ισχύουν μέχρι σήμερα. Το Δεκέμβρη του 2005 η EAC ομόφωνα υιοθέτησε τα 2005 VSS, που αυξάνουν σημαντικά τις απαιτήσεις ασφάλειας και διευρύνουν την προσβασιμότητα, προσφέροντας περισσότερες δυνατότητες σε άτομα με ποικίλες «ανικανότητες».Τέθηκαν σε ισχύ το Δεκέμβρη του 2007, αντικαθιστώντας τα VSS 2002.Από το 1991 το Βέλγιο διεξάγει εκλογές μέσω ηλεκτρονικής ψηφοφορίας, η Μεγάλη Βρετανία διεξάγει πιλοτικά τις δημοτικές εκλογές μέσω ηλεκτρονικής ψηφοφορίας και οι Ηνωμένες Πολιτείες Αμερικής χρησιμοποιούν ηλεκτρονικά μέσα για την διεξαγωγή των κοινοβουλευτικών εκλογών. Η πρώτη χώρα που διεξήγαγε ηλεκτρονική ψηφοφορία βασισμένη σε ηλεκτρονικούς υπολογιστές ήτανε η Βραζιλία όπως επίσης και η Γεωργία ήτανε η πρώτη που υιοθέτησε DRE μηχανη για την διεξαγωγή ηλεκτρονικής ψηφοφορίας το 2002.

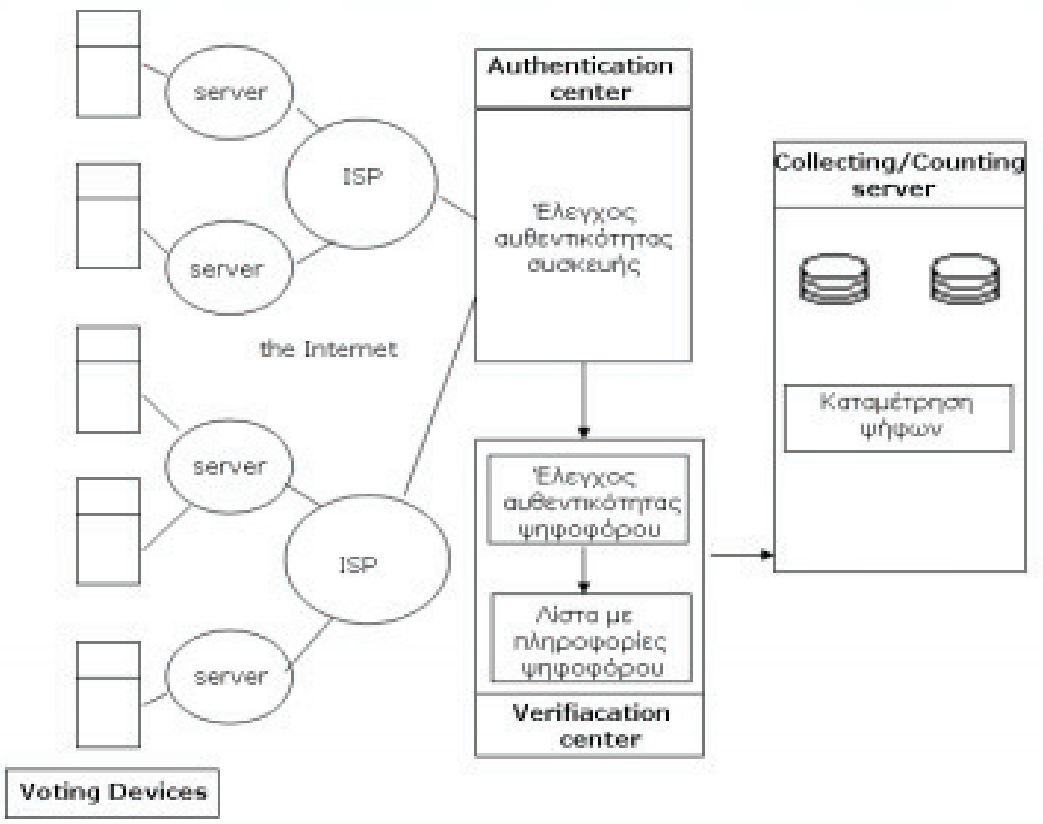
Στη χώρα μας, κατά τη διάρκεια της Ελληνικής Προεδρίας της Ευρωπαϊκής Ένωσης το Υπουργείο Εξωτερικών της Ελλάδος προώθησε ένα πρόγραμμα ηλεκτρονικής ψηφοφορίας,

που είναι γνωστό ως e-Vote. Το e-Vote, την εκπόνηση του οποίου ανέλαβε η ελληνική εταιρία Quality & Reliability, του ομίλου Πουλιάδη προσέφερε στους πολίτες της Ευρωπαϊκής Ένωσης τη δυνατότητα συμμετοχής στην διαδικασία λήψης αποφάσεων και χάραξης της δημόσιας πολιτικής των χωρών της Ευρωπαϊκής Ένωσης. Για να πραγματοποιήσει τον σκοπό αυτό, η Ελληνική Προεδρία δημιούργησε μία ιστοσελίδα, η οποία περιείχε διαφόρων ειδών ερωτήσεις ομαδοποιημένες σε δώδεκα ερωτηματολόγια. Οι ερωτήσεις σχετίζονταν τόσο με την Ευρωπαϊκή Ένωση, όσο και με τα διάφορα προβλήματα που καλείται να αντιμετωπίσει η ευρωπαϊκή κοινότητα, όπως η μετανάστευση, τα ναρκωτικά και η μόλυνση του περιβάλλοντος. Ακόμη ο δήμος Αμαρουσίου διοργάνωσε ηλεκτρονικό «δημοψήφισμα» για να εκφράσουν οι δημότες τις απόψεις τους για τους Ολυμπιακούς του 2004. Το έργο χρηματοδοτήθηκε κατά 50% από την Ευρωπαϊκή Ένωση μέσα στα πλαίσια του προγράμματος IST (Information Society Technologies).

4.3 Αρχιτεκτονική συστημάτων ηλεκτρονικής ψηφοφορίας

Υπάρχουν διάφορα συστήματα ηλεκτρονικής ψηφοφορίας, που να διαφέρουν μεταξύ τους σε αρκετά σημεία. Για κάθε τέτοιο σύστημα, υπάρχει μια αρχιτεκτονική που το αντιπροσωπεύει και παρουσιάζει τον τρόπο λειτουργίας του. Μπορούμε όμως να παρουσιάσουμε μια γενική αρχιτεκτονική, βάσει των ερευνών που έχουν γίνει και των άρθρων που έχουν γραφτεί, σχετικά με το θέμα, η οποία παρουσιάζει τη δομή ενός συστήματος ηλεκτρονικής ψηφοφορίας, καθώς και τις βασικές του λειτουργίες.

Υπάρχουν οι ηλεκτρονικές συσκευές, μέσω των οποίων ψηφίζουν οι ψηφοφόροι. Κάθε συσκευή είναι συνδεδεμένη με ένα server, ο οποίος συνδέεται με άλλα δίκτυα, τα οποία με τη σειρά τους συνδέονται με τους ISP's που χρησιμοποιούνται από το Verification Center. Τα ψηφοδέλτια και όλες οι σχετικές πληροφορίες που χρειάζονται κατά τη διάρκεια της ψηφοφορίας διακινούνται μεταξύ των ηλεκτρονικών συσκευών και των servers μέσω του διαδικτύου. Το verification center είναι υπεύθυνο για να συγκεντρώνει τα κωδικοποιημένα (encrypted) ηλεκτρονικά ψηφοδέλτια, που έχουν αποστείλει οι ψηφοφόροι μέσω του διαδικτύου και για κάθε ψηφοδέλτιο να ελέγχει την αυθεντικότητα πρώτα της συσκευής και στη συνέχεια του ψηφοφόρου, για τον οποίο κρατά μία λίστα με τις πληροφορίες του. Στη συνέχεια μεταφέρει τα ψηφοδέλτια στο collecting/counting server, όπου θα γίνει η καταμέτρηση τους. Σε αυτό το σημείο, οι ψήφοι αποκωδικοποιούνται (decrypted) και είναι έτοιμες για καταμέτρηση. Η διαδικασία αυτή γίνεται ηλεκτρονικά και υπολογίζεται το αποτέλεσμα.



Εικόνα 2: Διακρίσεις ηλεκτρονικής ψηφοφορίας ανάλογα με το χώρο άσκησης του εκλογικού δικαιώματος

Η ηλεκτρονική ψηφοφορία είναι δυνατόν να πραγματοποιηθεί είτε στα παραδοσιακά εκλογικά τμήματα είτε, σε οποιοδήποτε άλλο χώρο από τον οποίο υπάρχει η δυνατότητα πρόσβασης στο διαδίκτυο. Σύμφωνα με τα παραπάνω, προκύπτει μια ουσιαστική διάκριση μεταξύ των μορφών που μπορεί να λάβει η ηλεκτρονική ψηφοφορία, η οποία συναρτάται με το χώρο από τον οποίο ο εκλογέας επιλέγει να ασκήσει το εκλογικό του δικαίωμα:

- ***Ηλεκτρονική ψηφοφορία εντός των εκλογικών τμημάτων (poll site e-voting):*** Στην περίπτωση αυτή, η ψηφοφορία γίνεται στα εκλογικά κέντρα, υπό την εποπτεία των αρμόδιων διοικητικών αρχών, οι οποίες έχουν την ευθύνη για τον έλεγχο της καλής λειτουργίας του υλικού και του λογισμικού του υπολογιστικού συστήματος, καθώς και την εποπτεία του περιβάλλοντος χώρου. Με την ύπαρξη εποπτείας, διαφυλάσσεται ο

μυστικός χαρακτήρας της διαδικασίας και αποτρέπονται φαινόμενα άσκησης πιέσεων επί των εκλογέων, όπως απειλές, εκφοβισμός, ή άσκηση βίας, προκειμένου να διαμορφώσουν την ψήφο τους κατά συγκεκριμένο τρόπο.

- ***Ηλεκτρονική ψηφοφορία που πραγματοποιείται από απόσταση (remote e-voting):*** Η άσκηση του ηλεκτρονικού δικαιώματος γίνεται από οποιοδήποτε ιδιωτικό χώρο, όπου το μηχάνημα, μέσω του οποίου καταθέτει την ψήφο του ο εκλογέας, ελέγχεται από τον ίδιο ή κάποιον τρίτο. Ο χώρος αυτός μπορεί να είναι η οικία, ο επαγγελματικός χώρος του ψηφοφόρου, ή κάποιος δημόσιος χώρος, όπως τα "internet café". Η ηλεκτρονική ψηφοφορία από απόσταση με τη χρήση του διαδικτύου, αποτελεί επιμέρους κατηγορία των λεγόμενων **RVEM** (Remote Voting by Electronic Means) δηλαδή ψηφοφορία από απόσταση με τη χρήση ηλεκτρονικών μέσων.

  Άλλα τέτοια μέσα μπορεί να αποτελούν:

  - ***Ψηφοφορία με τη χρήση τηλεφώνου.*** Αυτός ο τύπος του συστήματος μπορεί να λειτουργήσει είτε με τη χρήση των γραμμών της σταθερής τηλεφωνίας ή με τη χρήση κινητών τηλεφώνων.
  - ***Η ψήφος με την αποστολή μηνυμάτων μέσω κινητού τηλεφώνου*** (SMS - Short Message Service),
  - ***Χρήση της ψηφιακής διαδραστικής τηλεόρασης*** (Interactive Digital Television). Η τεχνολογία αυτή αξιοποιεί τη δυνατότητα διάδρασης των νέων τύπων τηλεόρασης για να διευκολύνει τους ψηφοφόρους να καταθέσουν την ψήφο τους.

4.4 Γιατί διεξάγονται ηλεκτρονικές ψηφοφορίες

Η ηλεκτρονική ψηφοφορία διεξάγεται κυρίως για να προβληθεί η γνώμη του κόσμου πάνω σε ένα θέμα με κοινωνικό ή πολιτικό ή άλλο ενδιαφέρον. Αν παρατηρήσουμε την καθημερινότητα μας η ηλεκτρονική ψηφοφορία είναι γύρω μας,δίνεται η δυνατότητα να εκφράσουμε την γνώμη μας και την συμπάθια μας για ένα άτομο και αυτό γίνεται μέσω ενός τηλεφωνήματος, ενός μηνύματος, ενός ηλεκτρονικού υπολογιστή και με ακόμα ποικίλους τρόπους που διαφοροποιούνται ανάλογα με την τις επιταγές της τεχνολογίας.

4.5 Πεδία εφαρμογής ηλεκτρονικής ψηφοφορίας

Η ηλεκτρονική ψηφοφορία μπορεί να εφαρμοστεί επίσης:

- Επιχειρήσεις (Εκλογή οργάνων διοίκησης – Διατύπωση γνώμης – Επιχειρησιακές και ενδοεπιχειρησιακές έρευνες)
- Σφυγμομετρήσεις (Ενδεικτικός/συμβουλευτικός χαρακτήρας)

- Γενικές εκλογές/Δημοψηφίσματα (Εθνικό/τοπικό επίπεδο)

- Θεσμοί αντιπροσώπευσης (Εκλογή οργάνων / διατύπωση γνώμης-θέσης)
  - ✓ Πολιτικά Κόμματα.
  - ✓ Εθελοντικές Οργανώσεις (χωρίς λειτουργία αντιπροσώπευσης).
  - ✓ Επαγγελματικές οργανώσεις (Επιμελητήρια/Συνδικάτα κλπ.)
  - ✓ Φοιτητικούς συλλόγους

4.6 Προσδοκίες ηλεκτρονικής ψηφοφορίας

Οι βασικές προσδοκίες της ηλεκτρονικής ψηφοφορίας είναι οι εξής:

- Αναστροφή της πορείας αποχωρισμού των πολιτών από τις πολιτικές διαδικασίες και τις διαδικασίες συμμετοχής.
- Μείωση του μέσο-μακροπρόθεσμου κόστους των εκλογών, και ταυτόχρονη βελτίωση της διοικητικής αποτελεσματικότητας.
- Διευκόλυνση συμμετοχής – εκπαίδευση στη συμμετοχή.

4.7 Στάδια διεξαγωγής ηλεκτρονικής ψηφοφορίας

- **Εγγραφή (registration)**

  Είναι η διαδικασία που οι ψηφοφόροι υποβάλουν τα στοιχεία που αποδεικνύουν πως έχουν δικαίωμα ψήφου και στην συνέχεια προστίθενται στους εκλογικούς καταλόγους.
- **Ψηφοφορία (voting)**

  Η ψηφοφορία χωρίζεται σε δύο φάσεις:

✓ **Επιβεβαίωση (Validation)**

Περιλαμβάνει τον έλεγχο της εγκυρότητας αυτών που επιχειρούν να ψηφίσουν και επιτρέπει μόνο στους νόμιμους ψηφοφόρους που δεν έχουν ακόμη ψηφίσει να προχωρήσουν στη διαδικασία.

- ✓ **Συλλογή (Collection)**
  Διαδικασία συλλογής των έγκυρων ψήφων.
- **Εξακρίβωση (identification)**
  Οι ψηφοφόροι υποβάλουν την ψήφο τους
- **Καταμέτρηση ψήφων (Tallying)**
  Οι ψήφοι καταμετρούνται και τέλος ανακοινώνεται το αποτέλεσμα των εκλογών

4.8 Θεμελιώδης αρχές ηλεκτρονικής ψηφοφορίας

Οι θεμελιώδεις αρχές της ηλεκτρονικής ψηφοφορίας είναι οι εξής:

- **Καθολικότητα:** Η αρχή της καθολικότητας ορίζει ότι κανένας δεν μπορεί να αποκλειστεί από την διαδικασία της ηλεκτρονικής ψηφοφορίας η να υποστεί κάποιου είδους διάκριση.

- **Ισότητα:** Η αρχή της ισότητας ορίζει ότι ο σχεδιασμός, η δομή και η εμφάνιση του συστήματος/ιστότοπου και των «ψηφοδελτίων» πρέπει να είναι τέτοια ώστε να μην έχουν ως αποτέλεσμα διακρίσεις υπέρ ή κατά συγκεκριμένων επιλογών/υποψηφίων. Όλοι οι συμμετέχοντες πρέπει να έχουν ισότιμη πρόσβαση στα εργαλεία/στοιχεία/διαδικασίες του εκλογικού συστήματος ώστε να ελέγχουν και να επιβεβαιώνουν τη διαφανή και νόμιμη λειτουργία του.

- **Ελευθερία:** Η αρχή της ελευθερίας ορίζει ότι κατά τη λήψη απόφασης/άσκησης δικαιώματος πρέπει να αποτρέπεται η βία, ο καταναγκασμός και η χειραγώγηση.Να δίνεται η δυνατότητα της ελεύθερης επιλογής.

- **Μυστικότητα:** Κανένας από τους συμμετέχοντες στη διαδικασία (οργανωτές, διοίκηση, εκλογείς, πάροχοι υπηρεσιών, έμπιστες τρίτες οντότητες) δεν πρέπει να είναι σε θέση να συσχετίζει μία ψήφο με έναν εκλογέα, ο ανάστροφος συσχετισμός πρέπει να αποκλειστεί. Η μυστικότητα πρέπει να εναρμονίζεται τεχνολογικά και οργανωτικά με τη

διαφάνεια και την ελεγξιμότητα της διαδικασίας..Η μυστικότητα είναι προϋπόθεση της ελεύθερης επιλογής. Η αρχή της μυστικότητας πρέπει να γίνεται σεβαστή σε όλη τη διάρκεια της διαδικασίας ψηφοφορία/μεταφορά/λήψη/συλλογή και καταμέτρηση των ψήφων).Οι λειτουργικές απαιτήσεις της μυστικότητας είναι: Καμία ταυτοποίηση κατά την ψηφοφορία: σαφής και προφανής διάκριση μεταξύ εγγραφής, ταυτοποίησης/αυθεντικοποίησης και ψηφοφορίας)

- **Αυθεντικοποίηση:** των ψήφων και διαχωρισμός από ταυτοποίηση εκλογέων.
- **Επιβεβαίωση της ψήφου**: έναντι του εκλογέα αλλά όχι του περιεχομένου της ψήφου προς αποφυγή της εκμετάλλευσης/εκποίησης του.
- **Διαφάνεια – ελεγξιμότητα:** Η διαφάνεια είναι απούσα στην ηλεκτρονική ψηφοφορία: ο μέσος εκλογέας και ο μέσος κομματικός αντιπρόσωπος δεν είναι σε θέση να αντιληφθούν πως λειτουργεί το σύστημα. Η έλλειψη της διαφάνειας, είναι αντιληπτή ως απώλεια της άμεσης ελεγξιμότητας, μπορεί να χάσει την εμπιστοσύνη στο σύστημα της ψηφοφορίας και τη νομιμοποίησή του. Η απώλεια της διαφάνειας πρέπει να εξισορροπηθεί με εμπιστοσύνη στο σύστημα που χρησιμοποιείται. Οι σχετικές πληροφορίες πρέπει να είναι διαθέσιμες χωρίς να διακυβεύεται η ασφάλεια.
- ***Προστασία δεδομένων***: Τα δεδομένα που συλλέγονται κατά την εγγραφή, ταυτοποίηση, αυθεντικοποίηση, επιβεβαίωση της ψηφοφορίας είναι δεδομένα προσωπικού χαρακτήρα. Η νομοθεσία για την προστασία προσωπικών δεδομένων εφαρμόζεται σε διαδικασίες έκφρασης γνώμης καθώς και σε εκλογικές διαδικασίες, εφόσον δεν υφίσταται ειδική ρύθμιση που αναφέρεται σε δικαιώματα εκλογέων, διαδικασίες κλπ. Ακόμη και στην περίπτωση ύπαρξης ειδικού κανονιστικού πλαισίου αυτό πρέπει να βρίσκεται σε αρμονία προς τις αρχές και τις επιταγές της νομοθεσίας για την προστασία προσωπικών δεδομένων.Επιφύλαξη στην περίπτωση ύπαρξης συνταγματικής θεμελίωσης.

4.9 Χαρακτηριστικά και Προσδοκίες από ένα συστήματος ασφαλούς ηλεκτρονικής ψηφοφορίας

Βασικός στόχος ενός συστήματος ηλεκτρονικής ψηφοφορίας είναι η υποστήριξη όλων των απαιτούμενων υπηρεσιών για την οργάνωση και διεξαγωγή μιας εκλογικής διαδικασίας. Ανάλογα με τον τύπο της εκλογικής διαδικασίας, το σύστημα υποστηρίζει τον καθορισμό, την καταχώριση των συνδυασμών και των υποψηφίων, τη δημιουργία ηλεκτρονικών ψηφοδελτίων, την εισαγωγή των στοιχείων των ψηφοφόρων για τη δημιουργία εκλογικών καταλόγων, τη δημιουργία μέσων αυθεντικοποίησης για τους ψηφοφόρους, την αυτόματη καταμέτρηση των ψήφων μετά το τέλος της εκλογικής διαδικασίας. Βασική προϋπόθεση για την επιτυχία των συστημάτων ηλεκτρονικής ψηφοφορίας είναι:

- Να εξασφαλίζεται η ευκολία χρήσης τους από τους ενδιαφερόμενους χωρίς απαραίτητη προϋπόθεση την ύπαρξη εξειδικευμένων γνώσεων.
- Η λειτουργία του συστήματος να μην απαιτεί την εγκατάσταση εξειδικευμένου υλικού η λογισμικού στον υπολογιστή του ψηφοφόρου.

Όπως είναι φυσικό, τα θέματα ασφάλειας και διαφύλαξης της ιδιωτικότητας του ψηφοφόρου είναι μεγάλης σημασίας και καθορίζουν σε σημαντικό βαθμό την ευρεία αποδοχή ή μη αποδοχή του συστήματος. Ως εκ τούτου, οι μηχανισμοί ασφάλειας και εμπιστοσύνης που ενσωματώνονται από τα συστήματα ηλεκτρονικής ψηφοφορίας είναι εξαιρετικά πολύπλοκοι, αξιοποιώντας στο μέγιστο βαθμό τις δυνατότητες που παρέχουν οι πρόσφατες τεχνολογικές εξελίξεις.

Ενδεικτικά, κάποιες από τις απαιτήσεις που πρέπει να καλύπτει ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι οι ακόλουθες:

• Στην ψηφοφορία συμμετέχουν μόνον όσοι έχουν δικαίωμα συμμετοχής.

• Κάθε ψηφοφόρος μπορεί να ψηφίσει μόνο μια φορά.

• Κανένας δεν μπορεί να συσχετίσει ψηφοδέλτια με ψηφοφόρους.

• Κανένας δεν μπορεί να αποδείξει τι ψήφισε.

• Κανένας δεν μπορεί να αναπαράξει το δικό του ψηφοδέλτιο ή το ψηφοδέλτιο κάποιου τρίτου.

• Κανένας δεν μπορεί να τροποποιήσει το ψηφοδέλτιο άλλου ψηφοφόρου.

•Κανένας δεν μπορεί να τροποποιήσει το εκλογικό αποτέλεσμα, αγνοώντας κάποιες έγκυρες ψήφους ή προσμετρώντας κάποιες άκυρες ψήφους.

• Οποιαδήποτε ανεξάρτητη οντότητα έχει τη δυνατότητα να εξετάσει και να διαπιστώσει ότι το σύνολο των ψήφων έχει καταμετρηθεί σωστά.

• Το σύστημα είναι συμβατό με το Ελληνικό και Ευρωπαϊκό Νομικό και Κανονιστικό πλαίσιο, κυρίως σε θέματα που σχετίζονται με τη νομοθεσία και την προστασία προσωπικών δεδομένων.

4.10 Τα πλεονεκτήματα ηλεκτρονικής ψηφοφορίας

Η ηλεκτρονική ψηφοφορία πέρα από τα σημαντικά πλεονεκτήματα που έχει επιφέρει στον χώρο στον ψηφοφοριών παρουσιάζει και ορισμένα μειονεκτήματα κάποια από τα οποία παρουσιάζονται παρακάτω:

- Μειώνεται σημαντικά το κόστος στην εκλογική διαδικασία.
- Ο τρόπος διεξαγωγής της ηλεκτρονικής ψηφοφορίας γίνεται εξ' αποστάσεως και έτσι μειώνονται οι μετακινήσεις του πληθυσμού και με αυτό τον τρόπο αυξάνεται η συμμετοχή διότι ο καθένας μπορεί να ψηφίσει από τον χώρο τον οποίο βρίσκεται η από τον χώρο όπου θα βρίσκονται οι καθορισμένοι τερματικοί σταθμοί.
- Μειώνεται ο χρόνος διεξαγωγής των αποτελεσμάτων καθώς τα μηχανήματα είναι αυτοματοποιημένα και έχουν εξελιχθεί τόσο που μπορούν να υπολογίσουν το αποτέλεσμα με πολύ μεγάλη ακρίβεια.
- Η αμεσότητα είναι ακόμη ένα πλεονέκτημα της ηλεκτρονικής ψηφοφορίας καθώς θα μπορεί να οργανώνεται εύκολα και γρήγορα μια ψηφοφορία χωρίς να κοστίζει τίποτα έτσι χωρίς καμία επιβάρυνση θα μπορεί να ακούγεται η γνώμη του κόσμου.
- Τα ψηφοδέλτια θα μπορούν να είναι και σε άλλες γλώσσες.
- Ο περιορισμός της επέμβασης του ανθρώπινου παράγοντα και κατ ' επέκταση της νοθείας.
- Η μεγάλη ταχύτητα στην έκδοση των αποτελεσμάτων.
- Μείωση των άκυρων ψηφοδελτίων καθότι δεν υπάρχει η δυνατότητα ρίψης μιας ψήφου που να μην είναι ορθή, αφού το σύστημα θα την απορρίψει.

4.11 Θετικές συνέπειες ηλεκτρονικής ψηφοφορίας

Με την εισαγωγή της ηλεκτρονικής ψηφοφορίας αναμένεται να αυξηθεί το πλήθος των πολιτών που συμμετέχουν σε εκλογικές διαδικασίες. Πλήθος επιστημονικών και δημοσιογραφικών άρθρων έχουν γραφτεί για τις προσδοκίες που υπάρχουν μετά από την εμφάνιση της ηλεκτρονικής ψηφοφορίας. Βασική επιδίωξη πριν κατασκευαστεί ένα σύστημα είναι να έχει την κατάλληλη ισορροπία μεταξύ ασφάλειας, προσβασιμότητας και ευκολίας χρήσης ώστε να

επιτραπεί να χρησιμοποιηθεί σε πραγματικές συνθήκες εκλογής. Η αύξηση του ποσοστού των ψηφοφόρων που θα κινητοποιηθεί ώστε να συμμετάσχει στις εκλογές οφείλεται κυρίως:

- Στην αύξηση της ευκολίας συμμετοχής των ψηφοφόρων (votersconvenience), λόγω των εναλλακτικών λύσεων που προσφέρονται στον τρόπο άσκησης του εκλογικού δικαιώματος, όπως είναι η επέκταση της εκλογικής περιόδου.
- Σημαντική ώθηση στην εκλογική συμμετοχή, εξάλλου, θεωρείται ότι θα επιφέρει η προσέλκυση που θα ασκήσει το διαδίκτυο καθ' αυτό ιδιαίτερα στους νεότερους σε ηλικία ψηφοφόρους, οι οποίοι αποτελούν και τη μερίδα εκείνη του πληθυσμού που παρουσιάζουν τη μεγαλύτερη εξοικείωση με τις νέες τεχνολογίες.
- Ακόμη λόγω του αυτοματοποιημένου χαρακτήρα του όλου εγχειρήματος, θα υπάρξει μείωση του κόστους των εκλογών και ταυτόχρονη βελτίωση της διοικητικής αποτελεσματικότητας. Η καταμέτρηση των ψήφων θα πραγματοποιείται γρηγορότερα και με μεγαλύτερη ακρίβεια, μειώνοντας την πιθανότητα αμφισβητήσεως των εκλογικών αποτελεσμάτων και ανάγκης για επανάληψη της εκλογικής διαδικασίας.

4.12 Αρνητικές συνέπειες ηλεκτρονικής ψηφοφορίας

Οι επιδράσεις της ηλεκτρονικής ψηφοφορίας στην αναδιοργάνωση της εκλογικής διαδικασίας και στην αύξηση της ευκολίας των ψηφοφόρων, αναμφισβήτητα αποτελούν σημαντικά στοιχεία στην επιχειρηματολογία των δημιουργών αυτής της μεθόδου. Εντούτοις, εξίσου ισχυρός είναι και ο αντίλογος όσων υποστηρίζουν ότι η ψηφιοποίηση της εκλογικής διαδικασίας κρύβει πολλούς κινδύνους για τις κατακτήσεις που έχουν πραγματοποιηθεί στο χώρο των πολιτικών δικαιωμάτων και οι οποίες ως ένα βαθμό αποτελούν θεσμικό κεκτημένο. Ειδικότερα, υποστηρίζουν ότι η εισαγωγή της ηλεκτρονικής ψηφοφορίας δεν είναι σε θέση, με την υπάρχουσα υποδομή της πληροφοριακής τεχνολογίας να διασφαλίσει τις προϋποθέσεις ασφάλειας, που είναι απαραίτητο να παρέχει ένα αξιόπιστο εκλογικό σύστημα. Η ασφάλεια σε γενικές γραμμές μπορεί να αφορά:

- ***Την ακεραιότητα της ψήφου, την εγγύηση*** δηλαδή, ότι το περιεχόμενο της δεν θα μεταβληθεί στο στάδιο που μεσολαβεί από την άσκηση του εκλογικού δικαιώματος του ψηφοφόρου μέχρι την καταμέτρηση της ψήφου από το κεντρικό υπολογιστικό σύστημα. Η μη εξουσιοδοτημένη πρόσβαση στα εκλογικά δεδομένα και η απόπειρα πρόκλησης δυσλειτουργιών στην εξέλιξη της διαδικασίας, λόγω του συγκεντρωτικού τρόπου με τον

οποίο λειτουργούν τέτοιου είδους συστήματα, είναι δυνατόν να οδηγήσει σε αυτοματοποιημένη λαθροχειρία μεγάλης κλίμακας.

- ***Τη μυστικότητα της ψήφου*** την δυνατότητα δηλαδή των εκλογέων να ρίξουν την ψήφο τους, χωρίς την υποχρέωση να προσέλθουν στα εκλογικά τμήματα επιβάλλει, εκ των πραγμάτων, τη θέσπιση αυστηρότερων προϋποθέσεων για την ανάγκη εξακρίβωσης της ταυτότητας του ψηφοφόρου. Οι προϋποθέσεις αυτές πιθανά θα συνίσταται στη χορήγηση ψηφιακών υπογραφών ή κωδικών πρόσβασης, ανάλογα με τις συγκεκριμένες προδιαγραφές με τις οποίες έχει σχεδιαστεί το κάθε ηλεκτρονικό σύστημα. Παρά την ικανότητα που παρουσιάζουν οι συγκεκριμένες μέθοδοι να προστατεύσουν το περιεχόμενο της ψήφου των εκλογέων, αλλά και να αποστρέψουν τον κίνδυνο αποκάλυψης της ταυτότητας του ψηφοφόρου, εντούτοις αμφισβητείται ευρέως η αποτελεσματικότητα τους σε εφαρμογές μεγάλης κλίμακας και ιδιαίτερης συνθετότητας, όπως είναι η ηλεκτρονική ψηφοφορία.

  Παράλληλα, παρά την εντυπωσιακή διάδοση, τα τελευταία χρόνια, της χρήσης των μέσων πληροφοριακής τεχνολογίας και ιδιαίτερα του διαδικτύου, εξακολουθεί να υπάρχει διαφοροποιημένη πρόσβαση στις νέες τεχνολογίες μεταξύ των κοινωνικών ομάδων. Συνεπώς, η εισαγωγή της ηλεκτρονικής ψηφοφορίας ενδεχομένως να ευνοήσει τους ψηφοφόρους εκείνους που έχουν εξοικειωθεί με τις νέες τεχνολογίες και να οδηγήσει στον αποκλεισμό των υπολοίπων από τις διαδικασίες λήψης αποφάσεων.

  Η ψηφιοποίηση μίας διαδικασίας, η οποία αποτελεί τον κορυφαίο θεσμό της δημοκρατίας, χάριν ικανοποίησης ατομικιστικών επιδιώξεων (ευκολία συμμετοχής) υποβιβάζει την άσκηση ενός θεμελιώδους πολιτικού δικαιώματος στο επίπεδο των ηλεκτρονικών συναλλαγών στις οποίες προβαίνει καθημερινά ο πολίτης. Οι εκλογές αποσκοπούν στο να ενδυναμώσουν την ιδιότητα του πολίτη, υπενθυμίζοντας την σημασία του να θέτει κανείς το ευρύτερο δημόσιο συμφέρον πάνω από τις στενές του ατομικές επιδιώξεις. Η δημοκρατική συμμετοχή πάντα θα συνεπάγεται ένα μικρό ποσοστό αναστάτωσης για τον πολίτη, όπως άλλωστε συμβαίνει με τις περισσότερες σημαντικές δραστηριότητες στη ζωή. Η αντιμετώπιση της ηλεκτρονικής ψηφοφορίας ως μια επέκταση των εφαρμογών του διαδικτύου παραγνωρίζει βασικές αρχές του συνταγματικού βίου και υπονομεύει την ίδια αρχή της λαϊκής κυριαρχίας.

4.13 Θεσμικό και νομικό πλαίσιο ηλεκτρονικής ψηφοφορίας

Η ανάπτυξη της τεχνολογίας ηλεκτρονικής ψηφοφορίας και η διαμόρφωση του θεσμικού και νομικού πλαισίου βρίσκονται σε μία δυναμική διαδραστική σχέση. Η ανάπτυξη και εφαρμογή της τεχνολογίας προϋποθέτει τη διαμόρφωση του θεσμικού και νομικού πλαισίου και αντιστρόφως η διαμόρφωση του θεσμικού και νομικού πλαισίου προϋποθέτει τον εντοπισμό των προβλημάτων που ανακύπτουν από την εφαρμογή της σχετικής τεχνολογίας. Για να αποφευχθεί το προφανές αδιέξοδο απαιτείται μία παράλληλη πορεία, όπου οι βασικές θεσμικές παρεμβάσεις θα επιτρέψουν την αρχική εφαρμογή της τεχνολογίας και τα συμπεράσματα της αξιολόγησης της εφαρμογής της τεχνολογίας θα δώσουν τη δυνατότητα για επέκταση του νομικού και θεσμικού πλαισίου. Τα συστήματα ηλεκτρονικής ψηφοφορίας θα μπορούσαν, για παράδειγμα, αρχικά να εφαρμοστούν σε εσωτερικές εκλογικές διαδικασίες (σε συλλόγους, εταιρείες, επαγγελματικές ενώσεις κ.λπ.), καθώς και για την έκφραση της γνώμης των πολιτών σε επίπεδο τοπικής αυτοδιοίκησης. Οι απαιτούμενες θεσμικές και νομικές παρεμβάσεις αφορούν τρεις άξονες: (α) την προστασία των δικαιωμάτων του πολίτη, (β) τη διασφάλιση των δημοκρατικών αρχών και (γ) την αλλαγή των διαδικασιών
διεξαγωγής των εκλογικών διαδικασιών, ώστε να είναι εφικτή η ενσωμάτωση των τεχνολογιών ηλεκτρονικής ψηφοφορίας.

- ***Προστασία των δικαιωμάτων του πολίτη:*** Οι πολιτικές πεποιθήσεις των πολιτών κατοχυρώνονται από την υφιστάμενη νομοθεσία ως ευαίσθητα προσωπικά δεδομένα. Η εισαγωγή, όμως, των τεχνολογιών ηλεκτρονικής ψηφοφορίας δημιουργεί νέες απειλές κατά της ιδιωτικότητας του πολίτη. Κατά συνέπεια το θεσμικό πλαίσιο θα πρέπει να επεκταθεί ώστε να καλύπτει και αυτές τις απειλές. Για παράδειγμα, είναι ανάγκη να αντιμετωπιστούν ζητήματα όπως η "οικογενειακή ψήφος", οι ψηφοφορίες στον εργασιακό χώρο, οι υποχρεώσεις των εταιρειών που παρέχουν υπηρεσίες τηλεπικοινωνιών και πρόσβασης στο διαδίκτυο, η διασφάλιση της μυστικότητας της ψήφου κατά τη διάρκεια της εκλογικής διαδικασίας και κατά την καταμέτρηση των ψήφων κ.ά. Είναι προφανές πως αυτά τα ζητήματα είναι ιδιαίτερα σύνθετα και απαιτείται περαιτέρω μελέτη και ανοικτός διάλογος για τη διαμόρφωση των απαιτούμενων ρυθμίσεων.
- ***Διασφάλιση των δημοκρατικών αρχών:*** Οι θεμελιώδεις δημοκρατικές αρχές, αφορούν κάθε δημοκρατική διαδικασία ανεξάρτητα από την εμβέλειά της (εθνική, τοπική, κ.λπ.). Κατά συνέπεια θα πρέπει να αποφευχθεί η ανεξέλεγκτη χρήση

τεχνολογιών ηλεκτρονικής ψηφοφορίας που δεν σέβονται τις θεμελιώδεις δημοκρατικές αρχές, καθώς ένα τέτοιο γεγονός, εκτός από τις προφανείς επιπτώσεις στην ποιότητα της Δημοκρατίας, θα αποτελούσε και δυσφήμιση για τις τεχνολογίες και τα συστήματα ηλεκτρονικής ψηφοφορίας, με αποτέλεσμα να υπονομεύσει την ανάπτυξη της σχετικής αγοράς. Συνεπώς, οι ρυθμιστικές παρεμβάσεις είναι απαραίτητες και μπορούν να λάβουν πολλές μορφές, όπως αυτορρύθμιση, πιστοποίηση συστημάτων και διαδικασιών, ρυθμιστικές παρεμβάσεις ανεξάρτητων διοικητικών αρχών κ.ά.

Τα υφιστάμενα συστήματα δεν φαίνεται να έχουν τη δυνατότητα να υποστηρίξουν βουλευτικές εκλογές, εκτός εάν η ψηφοφορία πραγματοποιείται αποκλειστικά σε εκλογικά κέντρα. Σε κάθε περίπτωση, τα συστήματα ηλεκτρονικής ψηφοφορίας θα πρέπει να ικανοποιούν τις εξής αρχές, που απορρέουν από το Ελληνικό και τα Ευρωπαϊκά Συντάγματα:

- **Αρχή της καθολικής ψηφοφορίας:** Σύμφωνα με την αρχή της καθολικής ψηφοφορίας κάθε πολίτης, ο οποίος πληροί τις σύμφωνα με τον νόμο προϋποθέσεις εκλογιμότητας, μπορεί να συμμετέχει στην εκλογική διαδικασία.
- ***Εκλογιμότητα και εγγραφή στους εκλογικούς καταλόγους και ταυτοποίηση:*** Η διαδικασία αυτή αποσκοπεί στο να διασφαλίσει ότι το εκλογικό δικαίωμα περιορίζεται σε αυτούς που πληρούν τις προϋποθέσεις για να το ασκήσουν, αλλά και ότι κάθε ψηφοφόρος ψηφίζει μόνο μία φορά.
- ***Αρχή της ισότητας της ψήφου και της ψηφοφορίας:***Με την αρχή της ισότητας επιδιώκεται η ίση συμμετοχή των πολιτών στην εκλογική διαδικασία. Αυτό συνεπάγεται ότι κάθε πολίτης έχει στη διάθεση του μόνο μία ψήφο και ότι όλες οι ψήφοι είναι μεταξύ τους ισοδύναμες.
- **Ισότητα των υποψηφίων που μετέχουν στις εκλογές:** Αναφέρεται στην ανάγκη παροχής ίσων ευκαιριών σε όλους τους πολιτικούς σχηματισμούς και υποψηφίους που διαγωνίζονται στον πολιτικό στίβο.
- ***Αρχή της μυστικότητας της ψήφο.*** Η αρχή της μυστικότητας της ψήφου έχει ως στόχο να προστατεύσει τη γνησιότητα και αυθεντικότητα της ψηφοφορίας, διασφαλίζοντας το απόρρητο των πολιτικών επιλογών του εκλογέα.
- ***Αρχή της ελευθερίας της ψήφου και της ψηφοφορίας.*** Ελεύθερη είναι η εκλογική διαδικασία κατά την οποία η βούληση του λαού πραγματώνεται σε συνθήκες απουσίας εξαναγκασμών και πιέσεων, βίας, απόπειρας χειραγώγησης ή εκφοβισμού.
- ***Αρχή της αμεσότητας της ψήφου και της ψηφοφορίας.*** Μεταξύ της άσκησης του εκλογικού δικαιώματος από τον ψηφοφόρο και της ανακοίνωσης του εκλογικού

αποτελέσματος δεν πρέπει να παρεμβάλλεται καμία άλλη βούληση, διαδικασία ή όργανο, όπως στις περιπτώσεις της έμμεσης εκλογής.

Με βάση το παραπάνω πλαίσιο και το σύγχρονο τεχνολογικό περιβάλλον προσδιορίζονται και οι βασικές απαιτήσεις που θα πρέπει να πληροί ένα σύστημα ηλεκτρονικής ψηφοφορίας. Σε αυτές περιλαμβάνονται:

- Ορθότητα, ακρίβεια και επαληθευσιμότητα των αποτελεσμάτων.
- Ταυτοποίηση των ψηφοφόρων με βάση τους εκλογικούς καταλόγους και διασφάλιση της μοναδικότητας της ψήφου.
- Προστασία της ιδιωτικότητας του ψηφοφόρου και της μυστικότητας της ψήφου.
- Ανθεκτικότητα του συστήματος.
- Διασφάλιση της ελευθερίας της ψήφου (μη-εξαναγκασμός, uncoercibility).
- Αμεροληψία.
- Επαληθεύσιμη συμμετοχή.
- Ευκολία συμμετοχής των ψηφοφόρων.
- Ευελιξία και αποδοτικότητα. Οι απαιτήσεις αυτές δεν είναι εφικτό να ικανοποιούνται πάντα και για όλες τις κατηγορίες εκλογικών διαδικασιών και κατά συνέπεια θα πρέπει να εξετάζονται κατά περίπτωση.

4.14 Ψηφοφορία με σταθερή συσκευή Vs Ψηφοφορία με κινητή συσκευή

Η ηλεκτρονική ψηφοφορία, βάσει της αρχιτεκτονικής που έχουμε δει προηγουμένως, γίνεται μέσω του διαδικτύου. Ανάλογα με το αν η σύνδεση που θα χρησιμοποιήσουμε για τη διαδικασία της ψηφοφορίας είναι ασύρματη ή ενσύρματη, τότε θα έχουμε αντίστοιχα την ηλεκτρονική ψηφοφορία με κινητή συσκευή και την ηλεκτρονική ψηφοφορία με σταθερή συσκευή. Για παράδειγμα, αν η ψηφοφορία γίνει με χρήση ενός σταθερού ηλεκτρονικού υπολογιστή, τότε έχουμε ψηφοφορία με σταθερή συσκευή, ενώ αν γίνει με χρήση ενός κινητού τηλεφώνου, τότε έχουμε ψηφοφορία με κινητή συσκευή. Όταν η σύνδεση είναι ενσύρματη και η ψηφοφορία γίνει με χρήση σταθερής συσκευής, θα έχουμε στη διάθεσή μας μεγάλο bandwidth σε αντίθεση με την ασύρματη σύνδεση, όπου το bandwidth είναι αρκετά μικρότερο. Κατά συνέπεια, με την ασύρματη σύνδεση δεν θα μπορούμε να εκτελέσουμε λειτουργίες στις οποίες γίνεται καταχώρηση στη βάση δεδομένων ή ανάκτηση δεδομένων από αυτή πολύ μεγάλου όγκου. Τέτοιες λειτουργίες, θα γίνονται με χρήση ενσύρματης σύνδεσης μέσω σταθερής συσκευής.

Στην ψηφοφορία με σταθερή συσκευή, υπάρχει μεγαλύτερη ασφάλεια. Στην ψηφοφορία με κινητή συσκευή υπάρχουν περισσότεροι κίνδυνοι που απειλούν την ασφάλεια της διαδικασίας της ψηφοφορίας. Ο βασικότερος κίνδυνος είναι η παραβίαση της μυστικότητας της ψήφου, η οποία μπορεί να γίνει λόγω της χρήσης ασύρματης σύνδεσης. Καθώς γίνεται η μεταφορά της κωδικοποιημένης ψήφου στο server, μπορεί να ανιχνευθεί και να διαβαστεί από τρίτους και με τον τρόπο αυτό να παραβιαστεί η μυστικότητά της. Λαμβάνοντας υπ' όψιν τα πιο πάνω, λοιπόν, που είναι οι βασικότερες διαφορές μεταξύ ψηφοφορίας με σταθερή συσκευή και ψηφοφορίας με κινητή συσκευή, θα πρέπει να είμαστε πολύ προσεχτικοί ανάλογα με το σύστημα ψηφοφορίας που θέλουμε να δημιουργήσουμε ή να εισαγάγουμε. Έτσι, ανάλογα με το σύστημα, θα πρέπει να υλοποιηθούν μόνο οι λειτουργίες που μπορεί να υποστηρίξει και να υποστηριχτούν όλα τα αναγκαία θέματα ασφάλειας, έτσι ώστε να μην υπάρχει κανένας κίνδυνος που να απειλεί το σύστημα.

4.15 Εφαρμογή ηλεκτρονικής ψηφοφορίας σε φοιτητικούς συλλόγους

Η ηλεκτρονική ψηφοφορία σε έναν φοιτητικό σύλλογο θα μπορούσε να χρησιμοποιηθεί οπουδήποτε απαιτείται η καταμέτρηση ψήφων προκειμένου να εξαχθεί ένα συγκεκριμένο αποτέλεσμα. Τέτοιες περιπτώσεις αποτελούν όργανα όπως η Γενική Συνέλευση φοιτητών και εκλογικές διαδικασίες όπως οι φοιτητικές εκλογές. Στις γενικές συνελεύσεις κρίνονται όλα τα ζητήματα που αφορούν τους φοιτητές, και η διαδικασία κλείνει με την ψήφιση κάποιου εκ των προτεινόμενων πλαισίων. Στις φοιτητικές εκλογές εκλέγονται μέλη για το Διοικητικό Συμβούλιο Φοιτητών και εκπρόσωποι για τα όργανα συνδιοίκησης, όπως η γενική συνέλευση τμήματος. Ωστόσο η έλλειψη της ταυτοπροσωπίας, ένα από τα σημαντικά μειονεκτήματα της ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου, μοιάζει να αποτελεί το κύριο πρόβλημα της χρήσης της. Πιο συγκεκριμένα, στον φοιτητικό κόσμο υπάρχει μεγάλη έλλειψη εμπιστοσύνης μεταξύ των παρατάξεων, κάτι το οποίο πηγάζει από δείγματα νοθείας που έχουν παρατηρηθεί κατά καιρούς. Η έλλειψη αυτή καθιστά την ταυτοπροσωπία των ψηφοφόρων αναγκαία, λ.χ. για να μην γίνεται εξαγορά ψήφων.

ΚΕΦΑΛΑΙΟ 5: ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

Πληθώρα επιστημονικών αλλά και δημοσιογραφικών κειμένων αναφέρονται στις δυνατότητες των συστημάτων ηλεκτρονικής ψηφοφορίας και τις προοπτικές που ανοίγουν για μια περισσότερο συμμετοχική δημοκρατία, αλλά ταυτόχρονα αναδεικνύουν τους περιορισμούς τους, τους κινδύνους και τις αδυναμίες που αντιμετωπίζουν, όπως επίσης και τους κοινωνικούς προβληματισμούς που εγείρουν. Για παράδειγμα, η πιθανότητα κακόβουλης επίθεσης εναντίον υπολογιστικών συστημάτων συνδεδεμένων στο διαδίκτυο που χρησιμοποιούνται για την ηλεκτρονική ψηφοφορία, δεν πρέπει να αγνοηθεί. Μια τέτοια επίθεση θα μπορούσε να οδηγήσει σε άρνηση εξυπηρέτησης, δηλαδή στην αδυναμία σύνδεσης στο δίκτυο, με τελικό αποτέλεσμα την αδυναμία άσκησης του εκλογικού δικαιώματος. Θα μπορούσε, επίσης, να οδηγήσει στη μαζική εισαγωγή στην ηλεκτρονική κάλπη τροποποιημένων ψηφοδελτίων ή στη μαζική αποκάλυψη της ψήφου ομάδων πολιτών.

Αρκετοί πιστεύουν ότι παρά τις προκλήσεις αυτές, είναι τεχνολογικά δυνατό να κατασκευαστεί σύστημα ηλεκτρονικής ψηφοφορίας που να είναι τουλάχιστον όσο ασφαλές είναι και τα ήδη υπάρχοντα συστήματα επιστολικής ψήφου. Σε κάθε περίπτωση, οι περισσότεροι ειδικοί στον τομέα συμφωνούν ότι πρέπει να επιτευχθεί η κατάλληλη ισορροπία μεταξύ ασφάλειας, προσβασιμότητας και ευκολίας χρήσης πριν ένα σύστημα ηλεκτρονικής ψηφοφορίας επιτραπεί να χρησιμοποιηθεί σε πραγματικές συνθήκες εκλογής. Πέρα όμως από τους τεχνολογικούς κινδύνους, κανείς δεν επιτρέπεται να αγνοεί κινδύνους κοινωνικής ή και πολιτικής φύσης, όπως για παράδειγμα τον κίνδυνο ουσιαστικού αποκλεισμού από την εκλογική διαδικασία ομάδων πολιτών που αντιμετωπίζουν δυσχέρειες ή εμφανίζουν απροθυμία χρήσης της τεχνολογίας, αν οι εκλογές μέσω διαδικτύου αποτελούν τη μοναδική επιλογή συμμετοχής. Το κατά πόσο όλοι οι κίνδυνοι και οι αδυναμίες που σχετίζονται με τα συστήματα ηλεκτρονικής ψηφοφορίας μπορούν να αντιμετωπιστούν με την ήδη υπάρχουσα και την αναπτυσσόμενη τεχνολογία είναι συζητήσιμο. Άλλωστε, δεν θα ήταν δίκαιο να απαιτεί κανείς ένα σύστημα ηλεκτρονικής ψηφοφορίας να είναι περισσότερο ασφαλές από το χειρογραφικό του ισοδύναμο.

Η τελική απόφαση για τη χρήση ή μη μιας συγκεκριμένης τεχνολογίας θα πρέπει να συνυπολογίζει τόσο τους ενδεχόμενους κινδύνους, όσο και τα αναμενόμενα οφέλη. Φαίνεται πάντως ότι, αν και η ψηφοφορία μέσω του διαδικτύου αναμφίβολα δίνει στους ψηφοφόρους άνεση και ευκολία προσβασιμότητας, επιτρέποντάς τους να ψηφίζουν από οποιοδήποτε σημείο υπάρχει πρόσβαση στο διαδίκτυο, αυτός ο τρόπος ψηφοφορίας παρουσιάζει και σημαντικά προβλήματα ασφάλειας και εγείρει κοινωνικά ζητήματα που πρέπει να αντιμετωπιστούν αποτελεσματικά σε τεχνολογικό, οργανωτικό, επιχειρησιακό, αλλά και πολιτικό επίπεδο, πριν

αποτελέσει εναλλακτική επιλογή για τη διεξαγωγή πραγματικών εκλογικών αναμετρήσεων. Σε κάθε περίπτωση, η κοινωνία της πληροφορίας επηρεάζει κάθε πλευρά της καθημερινής μας ζωής και αλλάζει τον τρόπο που ζούμε, που εργαζόμαστε, που επικοινωνούμε, που διασκεδάζουμε, που διοικούμε και διοικούμαστε. Είναι, λοιπόν, καθαρά θέμα χρόνου πριν αλλάξει και τον τρόπο που συμμετέχουμε στα κοινά, που διαμορφώνουμε τις πολιτικές μας απόψεις, που συμβάλλουμε στη διαμόρφωση των απόψεων των άλλων, που επηρεάζουμε τις πολιτικές αποφάσεις που μας αφορούν, που συμμετέχουμε στα κοινά, που εκλέγουμε τους αντιπροσώπους μας και, τελικά, τον τρόπο που βιώνουμε τη δημοκρατία.

5.1 Τεχνικά ζητήματα

Τα τεχνικά ζητήματα της ηλεκτρονικής ψηφοφορίας είναι άρρηκτα συνδεδεμένα με την προσπάθεια εφαρμογής των βασικών αρχών των δημοκρατικών εκλογικών διαδικασιών και περιστρέφονται γύρω από το θέμα της ασφάλειας του συστήματος ηλεκτρονικής ψηφοφορίας.Ως παράδειγμα τεχνικών ζητημάτων που ανακύπτουν και πρέπει να αντιμετωπισθούν μπορούν να αναφερθούν τα θέματα που ανακύπτουν στα διάφορα στάδια της ηλεκτρονικής ψηφοφορίας μέσω του διαδικτύου.

- Προηγούνται της διενέργειας των εκλογών
  - Ο κάθε ψηφοφόρος πρέπει να εγγραφεί στους εκλογικούς καταλόγους, όπως ακριβώς συμβαίνει και με τον παραδοσιακό τρόπο ψηφοφορίας.
  - Κάθε ψηφοφόρος που επιθυμεί να ασκήσει το εκλογικό του δικαίωμα ηλεκτρονικά (μέσω internet) θα πρέπει να αιτηθεί αυτή του την επιθυμία εγγράφως
  - Σε περίπτωση θετικής κρίσης της αίτησης ενός ψηφοφόρου πρέπει να του αποσταλούν, με ασφαλή και αξιόπιστο τρόπο, οι απαραίτητες πληροφορίες για το πώς θα μπορεί να πιστοποιήσει την ταυτότητα του ηλεκτρονικά (π.χ με ψηφιακή υπογραφή).
- Στάδια κατά τη διενέργεια των εκλογών :
  - Εξασφάλιση επαρκούς επιπέδου ασφάλειας εκλογικής υποδομής. Αυτό είναι εύκολο να επιτευχθεί στην περίπτωση που η ψηφοφορία θα γίνεται από ειδικά διαμορφωμένα κέντρα με σύνδεση στο διαδίκτυο. Στην περίπτωση όμως που ψηφοφόρος θα ψηφίσει από τον προσωπικό του υπολογιστή ίσως είναι απαραίτητη η λήψη κάποιων πρόσθετων μέτρων ασφαλείας.
  - Η ταυτότητα του ψηφοφόρου πρέπει να εξακριβωθεί με επιστημονικά και τεχνολογικά άρτιο τρόπο. Έπειτα ο ψηφοφόρος πρέπει να αιτηθεί την αποστολή ψήφου.

- Λήψη κατάλληλου ψηφοδελτίου (που να αντιστοιχεί στην εκλογική περιφέρεια του συγκεκριμένου ψηφοφόρου).
- Συμπλήρωση ψηφοδελτίου από τον χρήστη. Η διαδικασία αυτή είναι πιθανό να περιλαμβάνει περισσότερες από μια ενέργειες για τον ψηφοφόρο.
- Επιβεβαίωση επιλογών χρήστη.
- Αποστολή της ψήφου και άσκηση του εκλογικού δικαιώματος. Η αποστολή της ψήφου πρέπει να γίνει με άρτιο τεχνικά τρόπο ο οποίος θα διασφαλίζει τις αρχές των δημοκρατικών εκλογικών διαδικασιών.
- Υποδοχή ψήφου στο κεντρικό σύστημα και ανατροφοδότηση για επιβεβαίωση επιτυχούς καταχώρησης ψήφου.

- Έπονται της διενέργειας των εκλογών:
  - Επικύρωση ψήφου και διαχωρισμός των στοιχείων του ψηφοφόρου από αυτήν («ανωνυμοποίηση»).
  - Επαλήθευση της ψήφου. Κάθε ψηφοφόρος πρέπει να έχει την δυνατότητα να ελέγχει ηλεκτρονικά (μέσω internet) ανά πάσα στιγμή όχι μόνο αν η ψήφος του καταχωρήθηκε με επιτυχία αλλά και αν καταμετρήθηκε ως έγκυρη.
  - Έλεγχος και επανάληψη καταμέτρησης. Πρέπει να υπάρχει η τεχνική δυνατότητα ελέγχου του αποτελέσματος αλλά και ανακαταμέτρησης των ψήφων όπως ακριβώς ισχύει και στον παραδοσιακό τρόπο ψηφοφορίας.

.

5.2 Τεχνικές απαιτήσεις

Εξίσου σημαντική με τη νομική διάσταση είναι και η τεχνολογική διάσταση του ζητήματος της ηλεκτρονικής ψηφοφορίας. Στις παραγράφους που ακολουθούν παρουσιάζονται οι τεχνικές απαιτήσεις που πρέπει να καλύπτει
ένα σύστημα ηλεκτρονικής ψηφοφορίας.Αρχικά,παρουσιάζουμε τα κύρια χαρακτηριστικά που ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να έχει.Τα χαρακτηριστικά αυτά είναι:

- Το σύστημα θα πρέπει να υποστηρίζει όλες εκείνες τις διαδικασίες που απαιτούνται για την ομαλή οργάνωση και διεξαγωγή των εκλογών. Ανάλογα του είδους των εκλογών οι υπηρεσίες που το σύστημα παρέχει ενδέχεται να περιλαμβάνουν την εγγραφή των ψηφοφόρων, την αυθεντικοποίησή τους, την ίδια τη ψήφο, τον υπολογισμό και την επιβεβαίωση του τελικού αποτελέσματος.

- Το σύστημα θα πρέπει να υποστηρίζει όλες τις συμμετέχουσες οντότητες (ρόλους). Χαρακτηριστικά αναφέρονται οι οργανωτές των εκλογών, οι εκπρόσωποι των κομμάτων οι υποψήφιοι, οι ψηφοφόροι κα.
- Το σύστημα πρέπει να παρέχει ένα φιλικό στο χρήστη περιβάλλον, ώστε να μπορεί να χρησιμοποιείται από οποιοδήποτε απλό φυλλομετρητή του Διαδικτύου (Web Browser).
- Το σύστημα πρέπει να υποστηρίζει ένα σύνολο υπηρεσιών και ενεργειών, ώστε να μπορεί να διευκολύνει το χρήστη κατά την χρησιμοποίησή του.
- Το σύστημα πρέπει να είναι σε θέση να υπολογίζει το τελικό αποτέλεσμα της καταμέτρησης των ψήφων.Ωστόσο, από τα παραπάνω γίνεται φανερό ότι ένα σύστημα ηλεκτρονικής ψηφοφορίας ορίζει ένα μεγάλο αριθμό ευκαιριών σε επίδοξους επιτιθέμενους, οι οποίοι ενδέχεται να οδηγήσουν το σύστημα σε κατάρρευση και κατ' επέκταση σε διακοπή (ακύρωση) της εκλογής διαδικασίας.Στο πλαίσιο αυτό γίνεται εμφανές ότι ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να σχεδιάζεται με τέτοιο τρόπο, ώστε να εγγυάται τη διατήρηση της ασφάλειας και της ιδιωτικότητας των συμμετεχόντων οντοτήτων. Το σύστημα, επομένως, πρέπει να βασίζεται σε ένα πρωτόκολλο ψηφοφορίας (voting protocol) το οποίο θα είναι σε θέση να αποτρέπει ευκαιρίες ενδεχόμενης απώλειας της ιδιωτικότητας του χρήστη.

Για την σχεδίαση ενός συστήματος ηλεκτρονικής ψηφοφορίας είναι σημαντικό να καθορίσουμε τις **απαιτήσεις ασφάλειας και πρακτικότητας**. Έτσι ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει λοιπόν να είναι:

- **Ασφαλές**
- **Δημοκρατικό (Democratic).**
  Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους.Κανένας ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.
- **Ακριβές (Accurate)**. Καμία ψήφος δεν είναι δυνατόν:

✓ Να αλλοιωθεί,
✓ Να καταμετρηθεί περισσότερες από μια φορές,
✓ Να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς/εξωτερικούς εχθρούς.

- **Μυστικό (Secret).**

- ✓ Όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων.
- ✓ Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε.

- **Ανθεκτικό (Robust).** Όλες οι απαιτήσεις ασφάλειας ικανοποιούνται πλήρως, παρά τα όποια τυχαία σφάλματα ή τις κακόβουλες συμπεριφορές ορισμένων οντοτήτων (ψηφοφόροι, Αρχές, εσωτερικοί/εξωτερικοί εχθροί).
- **Πρακτικό**

Το σύστημα πρέπει να είναι εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π), λειτουργικό (Στις εκλογές του 2000 στην Florida των Η.Π.Α ένας μεγάλος αριθμός άκυρων ψήφων υποβλήθηκε λόγω ελλιπούς σχεδίασης των ψηφοδελτίων), και να απευθύνεται σε όλες τις κατηγορίες πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet.

Το σύστημα επίσης πρέπει να υποστηρίζει μια ποικιλία από format ψήφων, συμπεριλαμβανομένων και των λεγόμενων «λευκών» ή άκυρων ψήφων ενώ ταυτόχρονα θα πρέπει να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλεκτορικού σώματος ή των υποψηφίων (scalability). Οι υπηρεσίες ασφάλειας που προσφέρει θα πρέπει να είναι διαφανείς (transparent) στον χρήστη.

Ωστόσο η σημερινή τεχνολογία δεν επιτρέπει την υλοποίηση άτρωτων, αδιάβλητων και χωρίς σφάλματα συστημάτων ψηφοφορίας. Δεκάδες μελέτες βεβαιώνουν ότι μπορεί να παραβιαστεί η κρυπτογραφική ασφάλεια στην ηλεκτρονική ψηφοφορία μέσω internet. Πρόσβαση στα υπολογιστικά συστήματα ηλεκτρονικής ψηφοφορίας έχουν οι κατασκευαστές και οι διαχειριστές του συστήματος, αλλά και οι hackers, ενώ η εφορευτική επιτροπή πολύ περιορισμένη, οι δε υποψήφιοι και οι ψηφοφόροι σχεδόν μηδενική. Η εφορευτική επιτροπή παραμένει διακοσμητική και περιθωριακή στην όλη διαδικασία αναμένοντας την έκδοση των αποτελεσμάτων από το ειδικό πρόγραμμα του υπολογιστή και δεν μπορεί να ελέγξει ή να εποπτεύσει σχεδόν τίποτα. Η διαδικασία αυτή δεν μπορεί να συγκριθεί ή να υποκαταστήσει εκλογές που προϋποθέτουν την άμεση και φυσική παρουσία των προσώπων που ψηφίζουν σε κάλπη, υπό την εποπτεία και ευθύνη των μελών της εφορευτικής επιτροπής. Το κλασικό αυτό σύστημα που διαμορφώθηκε ανά τους αιώνες παραμένει το πιο ασφαλές και δημοκρατικό.

5.3 Επιθέσεις σε συστήματα ηλεκτρονικής ψηφοφορίας

Κανείς δεν παραγνωρίζει ότι τα κίνητρα για μια επίθεση στην ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας, είναι πολλά (πολιτικές επιδιώξεις, χρηματική αμοιβή, διεκδίκηση εξουσίας, εμπλοκή μυστικών υπηρεσιών, τρομοκρατικές οργανώσεις). Το είδος και η μορφή των επιθέσεων είναι η εξής:

.

- **Ηλεκτρονική Ψηφοφορία (Γενικά).** Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πιο εύκολα από ότι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από *εσωτερικούς εχθρούς* (insider attacks) καθώς και σε επιθέσεις άρνησης εξυπηρέτησης (Denial Of Service–DOS). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας επίσης διαθέτουν ανεπαρκή *στοιχεία ελέγχου* (audit trail) και δεν παρέχουν οικουμενική, επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση.

- **Ψηφοφορία μέσω Internet.** Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Internet είναι περισσότερο ευάλωτες σε *επιθέσεις καταναγκασμού* (coercion) όπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου. Επιπρόσθετα, σε ένα σύστημα εξ' αποστάσεως ψηφοφορίας οι ψηφοφόροι ενδεχομένως θα πρέπει να δημιουργήσουν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), π.χ. προτού υποβάλλουν τη ψήφο τους .Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Internet παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web. Παράλληλα, τα συστήματα ψηφοφορίας μέσω Internet είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

✓ *Στα συστήματα-πελάτες*: Ιοί τύπου «*σκουλήκια*» (worms) ή «*δούρειοι ίπποι*» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή

αυθεντικοποιηθεί. Επίσης, ο εισβολέας μπορεί εξ' αποστάσεως να εκμεταλλευτεί λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web.

- ✓ *Στο επίπεδο της επικοινωνίας*: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις *πλαστοπροσωπίας* (spoofing) DNS ονομάτων ή IP διευθύνσεων, και οι *επιθέσεις ενδιάμεσης οντότητας* (man in the middle). Η επικοινωνία μεταξύ πελάτη και εξυπηρετητή μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π.

- ✓ *Στα συστήματα-εξυπηρετητές*: Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με αυτές στα συστήματα-πελάτες. Εδώ βέβαια οι επιθέσεις Άρνησης Εξυπηρέτησης (DOS), όπως IP fragmentation ή υπερχείλιση καταχωρητών (buffer overflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία. Το πρόβλημα της *συμφόρησης* (bottleneck) είναι παρόμοιο, ως προς τις συνέπειες του, με μια επίθεση Άρνησης Εξυπηρέτησης, με τη διαφορά ότι η συμφόρηση προκαλείται από υπερβολικά μεγάλο αριθμό ταυτόχρονων νομίμων αιτήσεων για σύνδεση με τον εξυπηρετητή, και όχι απαραίτητα από κακόβουλη επίθεση.

Στην ηλεκτρονική ψηφοφορία δύο είναι οι βασικοί τύποι **επιθέσεων** οι *εσωτερικές* και οι *εξωτερικές*:

- **Εσωτερικές**

  Οι **νόμιμοι χρήστες** ενός REV συστήματος ίσως επιδιώξουν τη κακή χρήση η ζημιά στο εκλογικό σύστημα και ίσως να έχουν τεχνικές ικανότητες για να υπονομεύσουν το σύστημα. Επειδή είναι νόμιμοι χρήστες υπόκεινται και σε νομικές κυρώσεις αν η επίθεση επικεντρώνεται σε αυτούς. Οι **διαχειριστές REV συστήματος** πολύ συχνά εκμεταλλεύονται τη προνομιούχο θέση τους. Μπορούν να συγκεντρώνουν πληροφορίες από κυβερνητικούς υπαλλήλους, υπαλλήλους οργανισμών αλλά και εξωτερικούς υπάλλήλους. Όλες αυτές οι πληροφορίες τους δίνουν γνώση για τα δικαιώματα προσβασιμότητας. Ίσως το κίνητρο τους είναι να εξαπατηθούν οι εκλογές για οικονομικό κέρδος, για προσωπική ικανοποίηση ή και για πολιτικούς λόγους. Οι διαχειριστές υπηρεσιών και οι κυβερνητικοί υπάλληλοι υπόκεινται εύκολα σε κυρώσεις αν η επίθεση επικεντρώνεται σε αυτούς. Οι **υπόλοιποι** κάτοχοι μυστικών πληροφοριών

(κυβερνητικοί υπάλληλοι) που έχουν πρόσβαση στο REV σύστημα αλλά δεν συσχετίζονται με τη φροντίδα των εκλογικών υπηρεσιών ίσως καθοδηγήσουν εσωτερικές επιθέσεις. Αυτά τα άτομα ίσως έχουν οικονομικό, προσωπικό ή πολιτικό κίνητρο.

- **Εξωτερικές**

  Κάποιοι **Hackers** ίσως προσπαθήσουν να δημιουργήσουν διακοπή ή αναστάτωση στο σύστημα λόγω προσωπικού φθόνου, επειδή πιστεύουν ότι η επίθεση σε ένα κυβερνητικό σύστημα είναι πρόκληση ή επειδή θέλουν να διαμαρτυρηθούν στη κυβέρνηση. Πολλοί **εγκληματικοί οργανισμοί** και άλλοι, όπως οικονομικοί μεσάζοντες ίσως θελήσουν να έχουν πρόσβαση στο σύστημα για να επωφεληθούν από προσωπικές πληροφορίες.Ο**μάδες διαμαρτυρίας** επιδιώκουν να επιτεθούν στα συστήματα με σκοπό να δείξουν την αντίθεση τους με το REV, να διακόψουν τους ηλεκτρονικούς μηχανισμούς, να εκμεταλλευτούν πληροφορίες και για σκοπούς φθοράς. Επίσης ενδιαφέρονται πολλές φορές να διαπεράσουν το σύστημα για να αλλάξουν το αποτέλεσμα ενός διαγωνισμού ή μιας πολιτικής εκλογής. **Ξένες υπηρεσίες πληροφοριών** θέλουν να αποκτήσουν προσωπικές πληροφορίες για γνώση και ανάλυση. Επιπρόσθετα θέλουν να έχουν πρόσβαση στα συστήματα για συλλογή πολιτικών πληροφοριών και την διαχείριση τους με σκοπό την αλλαγή έκβασης του αποτελέσματος.

✓ **Άλλου είδους επιθέσεις**

- Εξαγορά ψήφων/πώληση και εξαναγκασμός η εξαγορά ψήφων και οι δραστηριότητες πώλησης και εξαναγκασμού δημιουργούν σοβαρή απειλή για το σύστημα REV καθώς δεν υπάρχει φυσικός τρόπος για να παρατηρηθεί η ρίψη των ψήφων. Οι μηχανισμοί που υπάρχουν για να υπολογίσουν αυτές τις απειλές είναι σε πειραματική/ερευνητική μορφή.
- Κλοπή ή παραποίηση ενός μέρους ψήφων. Η κλοπή και η παραποίηση ενός μέρους των ψήφων μπορεί να γίνει είτε ηλεκτρονικά είτε όχι. Αν γίνει χρήση κλεμμένων ή παραποιημένων ψήφων δημιουργείται πρόβλημα στο σύστημα Rev που δεν μπορεί να υπολογίσει τη νομιμότητα των ψήφων. Οι μηχανισμοί που υπάρχουν για να υπολογίζουν αυτές τις απειλές είναι σε πειραματική/ερευνητική μορφή.
- Σκόπιμη άρνηση της συναλλαγής ,κάποιος επιτιθέμενος μπορεί πιθανότατα να πάει στα μέσα ενημέρωσης και να παραπονεθεί ότι δήθεν δεν ψήφισε. Με αυτό το τρόπο θα

μπορούσε αναμφισβήτητα να προκαλέσει πρόβλημα στο σύστημα.Αυτές οι απειλές δημιουργούν μεγάλα προβλήματα στα μη εποπτευόμενα REV συστήματα. Μέχρι να γίνουν ουσιαστικοί οι μηχανισμοί μετρήσεων αυτών των απειλών μπορούμε να λέμε ότι αυτές οι απειλές είναι γνωστές αλλά απροσδιορίστου κινδύνου.

- ✓ **Μη προβλέψιμες απειλές**

- Χρήστες:Οι νόμιμοι χρήστες μπορούν να προκαλέσουν ακούσια, κακή χρήση του REV ή πιθανή ζημιά του συστήματος. Μεγάλος αριθμός ψηφοφόρων χρησιμοποιεί το σύστημα λανθασμένα και μπορεί να οδηγήσει στη περιττή απώλεια απόδοσης ή ακόμα και να καταστραφεί.

- Χειριστές:Οι χειριστές ίσως λόγω κακής κατάρτισης να προκαλέσουν ζημιά στο σύστημα ή απώλεια δεδομένων. Αυτά τα άτομα δεν είναι παρακινημένα να προκαλέσουν μια τέτοια επίθεση αλλά λόγω των προνομιούχων δικαιωμάτων τους, μπορούν ασυναίσθητα να βρεθούν υπαίτιοι μιας τέτοιας κατάστασης.

- Εξοπλισμός:δηλαδή η λάθος επιλογή εξοπλισμού ή του προγράμματος μπορεί να οδηγήσει σε αναστολή της υπηρεσίας ή σε απώλεια δεδομένων.

- Ενέργειες Ανωτέρας Βίας:δηλαδή ένα ατύχημα ή ένα φυσικό φαινόμενο μπορεί να καταστρέψει τη παροχή υπηρεσιών ή τις αποθηκευμένες πληροφορίες.

Η χρήση των ηλεκτρονικών ψηφοφοριών παγκοσμίως, παραμένει μια σχετικά ασυνήθιστη πρακτική, αν και συνεχώς η σκέψη αυτή αλλάζει, καθώς πολλές χώρες πειραματίζονται με διάφορες μορφές ηλεκτρονικών μεθόδων ή επεκτείνουν τις ήδη υπάρχουσες ηλεκτρονικές ψηφοφορίες. Επιπλέον, η ηλεκτρονική ψηφοφορία δεν περιορίζεται στην Ευρώπη και στην Βόρεια Αμερική αφού χώρες όπως η Βραζιλία και η Ινδία έχουν αναπτύξει εφαρμογές περισσότερο ολοκληρωμένες.

Οι πιο συνήθεις απειλές για συστήματα ηλεκτρονικής ψηφοφορίας, που έχουν εντοπιστεί μέχρι σήμερα, καταγράφονται συνοπτικά στον παρακάτω πίνακα.

Απειλή	**Επίπεδο ικανοτήτων που απαιτούνται**	**Συνέπειες**	**Πιθανότητες να συμβεί**	**Μέτρα Αντιμετώπισης**
Denial of Service attack	Χαμηλό	Παραβίαση πολιτικών Δικαιωμάτων (πιθανώς επιλεκτικά)	σύνηθες στο Internet	όχι με απλά μέσα: απαιτεί ώρες εργασίας από μηχανικούς δικτύων
Trojan horse attack στο pc με στόχο να παρεμποδιστεί η ψηφοφορία	Χαμηλό	Παραβίαση πολιτικών δικαιωμάτων	Υπάρχουν εκατομμύρια τρόποι για να πραγματοποιηθεί μια τέτοια σύνθετη εργασία	μπορεί να μετριασθεί ο κίνδυνος με προσεχτικό έλεγχο του λογισμικού
on-screen electioneering	Χαμηλό	Ενόχληση ψηφοφόρου, απογοήτευση, περισπασμός, Ανάρμοστη επιρροή	Υπερβολικά εύκολο με τη σημερινή web τεχνολογία	Ο ψηφοφόρος δεν έχει τη δυνατότητα να το εμποδίσει - απαιτείται νέος νόμος
Spoofing (εξαπάτηση διαφόρων ειδών)	Χαμηλό	κλοπή ψήφων, διακύβευση απορρήτου, παραβίαση πολιτικών δικαιωμάτων	σύνηθες και σχετικά εύκολο	Δεν αντιμετωπίζεται με κάποιο τρόπο πολύ πιθανόν να μην ανιχνευθεί
Εξαπάτηση ψηφοφόρου	Χαμηλό	Παραβίαση πολιτικών δικαιωμάτων	π.χ. : παραποίηση αδειών στα αρχεία cookie	δύσκολο να προβλεφθούν και κυρίως να ανιχνευθούν όλες οι πιθανές απόπειρες εξαπάτησης
Εσωτερικές επιθέσεις στους servers του συστήματος	Μέσο	Ολοκληρωτική διακύβευση της Εκλογικής διαδικασίας	είναι οι πιο συνήθεις, επικίνδυνες και οι πιο δύσκολα ανιχνεύσιμες παραβιάσεις	επιθυμητό να επαληθεύει ο ψηφοφόρος την ψήφο του
Αγοραπωλησία	Μέσο	κατάλυση της	Απόλυτα	Δεν υπάρχουν– η

Ο πίνακας περιγράφει, για κάθε πιθανή απειλή των συστημάτων ηλεκτρονικής ψηφοφορίας, τι ικανότητες απαιτούνται από τον εισβολέα, ποιες είναι οι συνέπειες μιας επιτυχημένης τελικά επίθεσης, πόσο πιθανό είναι να παρουσιαστεί η καθεμία και με ποιον τρόπο μπορεί να αντιμετωπιστεί

5.4 Προϋποθέσεις ασφάλειας ενός συστήματος ηλεκτρονικής ψηφοφορίας

Για να είναι ασφαλής ένα σύστημα ηλεκτρονικής ψηφοφορίας θα πρέπει:

- Να υιοθετεί ασφαλής κρυπτογραφικές μέθοδους καθώς και επαρκή στοιχεία ελέγχου με οικουμενική επαληθευσιμότητα ώστε τα ηλεκτρονικά συστήματα ψηφοφορίας να τύχουν ευρείας αποδοχής . Οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας. Επίσης για λόγους αξιοπιστίας, το σύστημα πρέπει να έχει υλοποιηθεί με χρήση ανοικτού λογισμικού (open source)

- Οι εκλογές μέσω διαδικτύου θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της εγγραφής έως και το στάδιο της καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής υποδομή δημοσίου κλειδιού (Public Key Infrastructure – PKI) , όπου οι απαιτήσεις της ακρίβειας και της μυστικότητας στην επικοινωνία μέσω διαδικτύου θα υποστηρίζονται με ισχυρές ψηφιακές υπογραφές και τεχνολογίες κρυπτογράφησης. Επίσης, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως SSL/TLS (Secure Socket Layer/Transport Layer Security) και SSH (Secure Shell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.
- Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία firewalls στα συστήματα-πελάτες, καθώς και συστήματα ελέγχου εισβολής (Intrusion Detection Systems) και firewalls στα συστήματα- εξυπηρετητές. Παράλληλα επιβάλλεται η χρήση διαδικασιών πλεονασμού (redundancy),ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές

clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ.ενσύρματα/ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται.

- Τέλος, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής πολιτικής ασφάλειας που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις . Επίσης, επιβάλλεται η ύπαρξη νομολογίας που θα κατοχυρώνει το δικαίωμα των ψηφοφόρων για μυστική ψήφο (π.χ. στον χώρο εργασίας) και θα αντιμετωπίζει επιθέσεις όπως καταναγκασμός του ψηφοφόρου,ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π

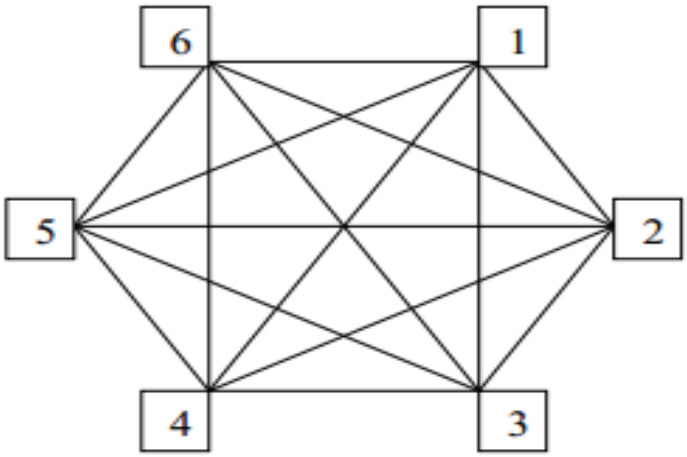
5.5 Μηχανισμοί και τεχνικές κρυπτογραφίας

Στα σημερινά υπολογιστικά και δικτυακά περιβάλλοντα η ασφάλεια καλείται να καλύψει τόσο φυσικούς πόρους, λειτουργικά συστήματα και λογισμικά εφαρμογών, όσο και τα δεδομένα τα οποία αυτά αποθηκεύουν και επεξεργάζονται. Επιπλέον, ο έλεγχος της πρόσβασης σε δίκτυα, τα τείχη προστασίας (firewalls) και άλλες τεχνολογίες «φιλτραρίσματος» θεωρούνται πλέον απαραίτητες ώστε να προστατευθούν τα όρια των εκάστοτε δικτυακών υποδομών. Έξω από αυτά τα όρια τα μη προστατευμένα δεδομένα που στέλνονται και λαμβάνονται από τον αντίστοιχο οργανισμό πάνω από τα διάφορα δίκτυα είναι ευάλωτα σε αποκάλυψη, τροποποίηση, διαγραφή και άλλων ειδών επιθέσεις. Προκειμένου να προστατεύονται τα μεταφερόμενα δεδομένα πάνω από μη αξιόπιστα δίκτυα, η μόνη εφαρμόσιμη και οικονομικά συμφέρουσα τεχνολογία είναι η κρυπτογραφία, η οποία βρίσκεται στο επίκεντρο σε ό,τι αφορά τόσο τα εικονικά ιδιωτικά δίκτυα (virtual private networks, VPNs) όσο και τις τεχνολογίες δημόσιου κλειδιού (public key infrastructures).

5.5.1 Κρυπτογραφία μυστικού κλειδιού

Η συμμετρική κρυπτογραφία μυστικού κλειδιού (Secret Key Cryptography) χρησιμοποιεί ίδιο κλειδί για την κρυπτογράφηση και κατόπιν αποκρυπτογράφηση ενός κειμένου. Προκειμένου n οντότητες να επικοινωνούν με ασφάλεια μεταξύ τους, ένα σύστημα κρυπτογράφησης μυστικού κλειδιού θα απαιτεί n*(n-1)/2 κλειδιά (Σχήμα), παρόλο που κάθε

οντότητα χρειάζεται να γνωρίζει μόνο n κλειδιά. Για ένα σύνολο έξι χρηστών, αυτό σημαίνει απλά 15 κλειδιά. Αλλά για ένα σύνολο 1000 χρηστών, για παράδειγμα, η διαχείριση και ασφαλής ανταλλαγή σχεδόν μισού εκατομμυρίου μυστικών κλειδιών είναι πρακτικά μη εφαρμόσιμη.



Εικόνα 3: Μυστικά κλειδιά στην περίπτωση 6 χρηστών

5.5.2 Κρυπτογραφικά συστήματα δημόσιου κλειδιού

Σε αντίθεση με τα παραπάνω, τα κρυπτογραφικά συστήματα δημόσιου κλειδιού (public key cryptosystems, PKCs) χρησιμοποιούν ζεύγη συσχετιζόμενων κλειδιών που δημιουργούνται μαζί. Το κρυπτογραφημένο κείμενο που παράγεται από το ένα κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο μέλος του ίδιου ζεύγους κλειδιών. Το ένα από τα κλειδιά αυτά παραμένει μυστικό (ιδιωτικό κλειδί, private key) και το άλλο δημοσιοποιείται και μπορεί να χρησιμοποιηθεί από όλους (δημόσιο κλειδί, public key). Για την απόκρυψη ενός

μηνύματος κατά τη μεταφορά, ώστε μόνο ο επιθυμητός παραλήπτης να μπορεί να το διαβάσει, το αρχικό κείμενο κρυπτογραφείται με το δημόσιο
κλειδί του παραλήπτη. Μόνο το μυστικό κλειδί του παραλήπτη μπορεί να αποκρυπτογραφήσει το μεταφερόμενο κρυπτογραφημένο κείμενο. Παρόμοια, για την εξακρίβωση της ακεραιότητας και αυθεντικότητας ενός μηνύματος, είναι πιθανό να κρυπτογραφούνται πληροφορίες με το ιδιωτικό κλειδί του αποστολέα. Αυτό επιτρέπει σε όλους όσους έχουν πρόσβαση στο δημόσιο κλειδί αυτού του αποστολέα να επικυρώνουν το μήνυμα αποκρυπτογραφώντας το επιτυχώς.

5.5.3 Η ανάγκη για υποδομή δημόσιου κλειδιού

Τα συστήματα δημόσιου κλειδιού βασίζουν την αποτελεσματικότητά τους στην ακεραιότητα κάθε δημόσιου κλειδιού και στη διασύνδεσή του με μια συγκεκριμένη οντότητα, όπως ένα άτομο, έναν οργανισμό ή ένα τμήμα δικτύου. Χωρίς μηχανισμούς διασφάλισης της ακεραιότητας και αυθεντικότητας, οι χρήστες είναι ευάλωτοι σε επιθέσεις «μεταμφίεσης» μέσω αντικατάστασης του δημόσιου κλειδιού. Ας υποθέσουμε, για παράδειγμα, ότι ο οργανισμός Α θέλει να στείλει ένα απόρρητο μήνυμα στον Β, χωρίς κανείς άλλος να μπορεί να το διαβάσει. Ο Α θα μπορούσε να χρησιμοποιήσει το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα, ωστόσο για καλύτερη επίδοση ο Α θα χρησιμοποιούσε μάλλον συμμετρικό αλγόριθμο για την κρυπτογράφηση και αλγόριθμο δημόσιου κλειδιού για να κρυπτογραφήσει το συμμετρικό κλειδί. Αν όμως ο Α «ξεγελαστεί» και αντ' αυτού χρησιμοποιήσει το δημόσιο κλειδί ενός τρίτου οργανισμού Γ σα να ήταν του Β, τότε ο Γ θα μπορούσε να αποκρυπτογραφήσει το μήνυμα.
Η τεχνική αυτή είναι γνωστή ως απάτη δημόσιου κλειδιού. Μια τέτοια απάτη από πλευράς του Γ θα εμπόδιζε από την άλλη τον Β να διαβάσει το μήνυμα του Α, όπως έπρεπε αρχικά. Έτσι μια τέτοια επίθεση θα συνεχιζόταν με τον Γ να επανακρυπτογραφεί τα μηνύματα του Α, χρησιμοποιώντας το πραγματικό δημόσιο κλειδί του Β, και να τα στέλνει τελικά στον Β. Μια τέτοια παρεμπόδιση και επανακρυπτογράφηση αποτελεί παράδειγμα επίθεσης ενδιάμεσου (man-in-the-middle attack).
Ένα άλλο παράδειγμα ρήξης της σύνδεσης ανάμεσα σε ένα δημόσιο κλειδί και τον ιδιοκτήτη του περιλαμβάνει την εξακρίβωση ηλεκτρονικών υπογραφών. Ας υποθέσουμε ότι ο Α θέλει να επαληθεύσει την υπογραφή του Β. Αν ο Γ μπορεί να ξεγελάσει τον Α ώστε ο τελευταίος να χρησιμοποιήσει το δικό του δημόσιο κλειδί σα να ήταν του Β, τότε ο Γ θα μπορούσε να υπογράφει μηνύματα μεταμφιεζόμενος ως Β χρησιμοποιώντας το δικό του (του Γ)

ιδιωτικό κλειδί. Ο Α θα χρησιμοποιούσε ακούσια το δημόσιο κλειδί του Γ και θα νόμιζε εσφαλμένα ότι το μήνυμα όντως έχει υπογραφεί από τον Β.

Συμπερασματικά, τόσο για ψηφιακές υπογραφές όσο και για υπηρεσίες κρυπτογράφησης, κάθε χρήστης πρέπει να χρησιμοποιεί το δημόσιο κλειδί του σωστού «συνομιλητή», προκειμένου να εξασφαλίζεται η ασφάλεια. Υπάρχουν πολλοί φυσικοί, *ηλεκτρονικοί* και υβριδικοί μηχανισμοί για τη διανομή δημόσιων κλειδιών με αξιόπιστο τρόπο, ώστε κάθε χρήστης να είναι σίγουρος ότι έχει το σωστό δημόσιο κλειδί για κάθε άλλο χρήστη με τον οποίο συνδιαλέγεται. Αυτοί οι μηχανισμοί για τη διανομή και δέσμευση δημόσιων κλειδιών είναι γνωστοί ως υποδομή δημόσιου κλειδιού (Public Key Infrastructure).

5.5.4 Πιστοποιητικό δημόσιου κλειδιού: Το πιστοποιητικό X.509

Η αντίστοιχη τεχνική χρησιμοποιεί ένα πιστοποιητικό δημόσιου κλειδιού, το οποίο έχει εκδοθεί από μια αξιόπιστη οντότητα, την CA (certification authority, CA). Μια CA εκδίδει πιστοποιητικά δημόσιου κλειδιού στους διάφορους συνδρομητές συγκεντρώνοντας τα στοιχεία τους και υπογράφοντας τα στοιχεία αυτά με το ιδιωτικό της κλειδί. Το γενικά αποδεκτό πρότυπο για τα ψηφιακά πιστοποιητικά δημόσιου κλειδιού είναι το X.509 version. Το πιστοποιητικό κάθε CA περιέχει τις ακόλουθες πληροφορίες κλειδιού:

- Αριθμός έκδοσης του χρησιμοποιούμενου προτύπου.
- Σειριακός αριθμός (serial number) του πιστοποιητικού (μοναδικός για κάθε πιστοποιητικό που εκδίδει η CA)
- Ο αλγόριθμος και οι σχετικές παράμετροι που χρησιμοποιήθηκαν από τη CA για την υπογραφή του πιστοποιητικού.
- Το όνομα της CA.
- Η χρονική περίοδος για την οποία ισχύει το πιστοποιητικό.
- Το όνομα του συνδρομητή.
- Το δημόσιο κλειδί του συνδρομητή, ο αλγόριθμος δημόσιου κλειδιού και οι σχετικές παράμετροι.
- Ο μοναδικός αναγνωριστικός αριθμός της CA (προαιρετικό).
- Ο μοναδικός αναγνωριστικός αριθμός του συνδρομητή (προαιρετικό).
- Επεκτάσεις (προαιρετικό).
- Η ψηφιακή υπογραφή της CA.

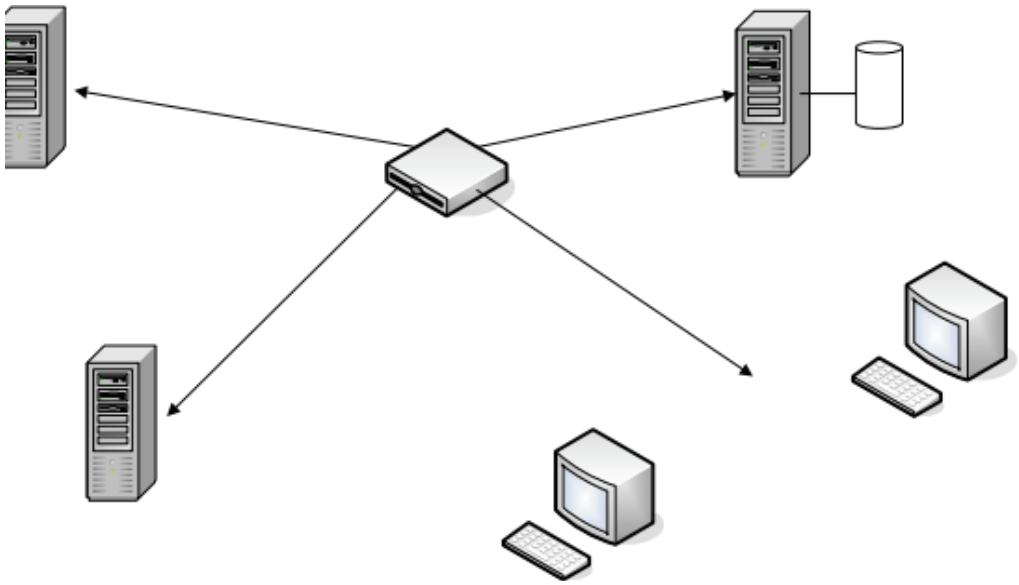
Κάθε χρήστης πρέπει να γνωρίζει το δημόσιο κλειδί της CA, ώστε να μπορεί να επαληθεύει την ψηφιακή υπογραφή στα πιστοποιητικά που εκδίδονται από αυτή, και να το

εμπιστεύεται. Αυτό το δημόσιο κλειδί λαμβάνεται κατά τη διαδικασία εγγραφής. Μόλις οι υπογραφές επαληθευτούν, οι χρήστες μπορούν να χρησιμοποιήσουν το όνομα και το δημόσιο κλειδί του συνδρομητή στο πιστοποιητικό, με τόση εμπιστοσύνη στην ακρίβεια της πληροφορίας, όση έχουν και στην αξιοπιστία της CA. Σε κάποιες περιπτώσεις η CA ίσως χρειαστεί να ακυρώσει τη σύνδεση ενός συνδρομητή με το δημόσιο κλειδί του. Το ιδιωτικό κλειδί του συνδρομητή, για παράδειγμα, μπορεί να έχει υποκλαπεί. Εφόσον ένα πιστοποιητικό δημόσιου κλειδιού είναι ένα ηλεκτρονικό αντικείμενο και μπορεί να βρίσκεται σε διάφορα μέρη την ίδια στιγμή, δεν είναι ούτε εφαρμόσιμο ούτε πιθανό να ανακληθούν ή διαγραφούν ή σβηστούν όλα τα αντίγραφα ενός τέτοιου πιστοποιητικού σε ένα κατανεμημένο περιβάλλον. Έτσι προκειμένου να ακυρώσει ένα πιστοποιητικό παύοντας τη συσχέτιση ανάμεσα στο συνδρομητή και στο δημόσιο κλειδί του, η CA δημιουργεί μια λίστα από άκυρα πιστοποιητικά, τη λίστα ανακληθέντων πιστοποιητικών (certificate revocation list, CRL). Οι χρήστες πρέπει να ελέγχουν ότι ένα πιστοποιητικό δεν ανήκει στη λίστα προτού χρησιμοποιήσουν το δημόσιο κλειδί στο πιστοποιητικό. Αν το πιστοποιητικό είναι στη λίστα, ο χρήστης δεν πρέπει να το χρησιμοποιήσει. Η CA υπογράφει τη λίστα, ώστε οι χρήστες να επαληθεύουν την ακεραιότητα και αυθεντικότητά της. Οι πληροφορίες κλειδιού στην CRL X.509 version 2 είναι οι εξής:

- Αριθμός έκδοσης του χρησιμοποιούμενου προτύπου CRL.
- Ο αλγόριθμος και οι σχετικές παράμετροι που χρησιμοποιήθηκαν από τη CA για την υπογραφή του πιστοποιητικού.
- Η χρονική στιγμή έκδοσης αυτής της CRL.
- Η χρονική στιγμή έκδοσης της επόμενης CRL (προαιρετικό).
- Η λίστα με τα ανακληθέντα πιστοποιητικά (για καθένα δίνονται τα ακόλουθα):
  - ✓ Σειριακός αριθμός (serial number) του πιστοποιητικού.
  - ✓ Η στιγμή κατά της οποία η CA ενημερώθηκε για την ανάκληση.
  - ✓ Επεκτάσεις που σχετίζονται με το ανακληθέν πιστοποιητικό (προαιρετικό).
- Επεκτάσεις σχετικές με το CRL (προαιρετικό).
- Η ψηφιακή υπογραφή της CA.

5.5.5 Υποδομή Δημοσίου Κλειδιού

Κάθε ομάδα χρηστών, η οποία προστατεύεται από μία CA, ονομάζεται πεδίο (domain). Στους συνδρομητές κάθε πεδίου διανέμονται πιστοποιητικά δημοσίου κλειδιού από την Αρμόδια CA. Το Σχήμα παρουσιάζει τους συμμετέχοντες σε μια Υποδομή Δημοσίου Κλειδιού για ένα πεδίο. Η CA είναι υπεύθυνη για την παραγωγή πιστοποιητικών και για την παραγωγή της CRL. Στέλνει αυτά τα υπογεγραμμένα αντικείμενα σ' έναν καταχωρητή, μέσω του οποίου μπορούν οι έμπιστοι συμμετέχοντες να τα ανασύρουν. Επίσης αρχειοθετεί τα πιστοποιητικά και τις λίστες ανακληθέντων πιστοποιητικών, σε περίπτωση που ζητηθούν στον μέλλον για την επίλυση διαφωνιών ανάμεσα στους συνδρομητές και στους έμπιστους συμμετέχοντες.



Εικόνα 4: Συμμετέχοντες στην υποδομή δημασίου κλειδιού για ένα πεδίο

Η Αρχή Εγγραφής (Registration Authority RA) είναι ο έμπιστος πράκτορας της CA και είναι υπεύθυνη για την εξακρίβωση της ταυτότητας του συνδρομητή. Ουσιαστικά πραγματοποιεί τις ακόλουθες εργασίες:

• Εξακριβώνει την ταυτότητα που ο συνδρομητής ισχυρίζεται ότι κατέχει. Για παράδειγμα, η RA θα μπορούσε να ζητά από τον συνδρομητή μια σε ισχύ ταυτότητα με φωτογραφία, όπως είναι η άδεια οδήγησης και το διαβατήριο.

• Μέσω του συνδρομητή αποκτά το δημόσιο κλειδί του.

• Προμηθεύει το συνδρομητή με το CA δημόσιο κλειδί, το οποίο ο συνδρομητής εμπιστεύεται. Η εμπιστοσύνη αυτή, γενικά, επιτυγχάνεται μέσω της λήψης του δημοσίου κλειδιού από μία έμπιστη πηγή, όπως π.χ. «χέρι με χέρι» ή μέσω Secure Sockets Layer (SSL) από έναν έμπιστο ή γνωστό δικτυακό τόπο.

• Στέλνει το αίτημα για τη δημιουργία του πιστοποιητικού στην CA. Τυπικά η RA δημιουργεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο περιέχει το όνομα του συνδρομητή και το δημόσιο κλειδί του, το υπογράφει ψηφιακά και το στέλνει στην CA. Άλλα μέσα μεταφοράς (π.χ. Διαδίκτυο) είναι επίσης κατάλληλα, με την προϋπόθεση να παραμένουν η ταυτότητα του συνδρομητή και το δημόσιο κλειδί του αναλλοίωτα.

5.5.6 Πολιτική του ψηφιακού πιστοποιητικού

Για να διασφαλιστεί η ασφάλεια της Υποδομής Δημοσίου Κλειδιού, οι συνιστώσες της είναι απαραίτητο να λειτουργούν με υψηλό βαθμό ασφάλειας. Για παράδειγμα:

• Τα ιδιωτικά κλειδιά πρέπει να παραμένουν εμπιστευτικά.

• Τα ιδιωτικά κλειδιά πρέπει να χρησιμοποιούνται μόνο από τους ιδιοκτήτες των κλειδιών.

• Πρέπει να διασφαλίζεται η ακεραιότητα του δημοσίου κλειδιού.

• Η αρχική ταυτοποίηση του συνδρομητή (δηλ. η κατοχή του ιδιωτικού κλειδιού και το θέμα του πιστοποιητικού δημοσίου κλειδιού) πρέπει να εξασφαλίζει ότι δεν πραγματοποιήθηκε υποκλοπή ταυτότητας κατά την δημιουργία του πιστοποιητικού.

Τα συστήματα υπολογιστών των CA και RA πρέπει να προστατεύονται από τυχόν αλλοιώσεις. Επιπρόσθετα με τις απαιτήσεις ασφαλείας, με σκοπό να διευκολυνθεί το ηλεκτρονικό εμπόριο, η Υποδομή Δημοσίου Κλειδιού πρέπει να απευθύνει υποχρεώσεις προς όλες τις μονάδες συνεργασίας και ευθύνες σε περίπτωση διαφωνίας. Αυτά τα θέματα ασφάλειας, ευθυνών και υποχρεώσεων υλοποιούνται μέσω μιας πολιτικής πιστοποιητικών (certificate policy, CP).

Σύμφωνα με το στάνταρτ X.509 τουAmerican National Standards Institute (ANSI), ένα πιστοποιητικό είναι ένα «σετ κανόνων» που καταδεικνύει την «προσαρμοστικότητα» ενός πιστοποιητικού στα πλαίσια μιας συγκεκριμένης κοινότητας ή/ και μιας κλάσης εφαρμογών με κοινές απαιτήσεις ασφαλείας. Ο χρήστης του πιστοποιητικού μπορεί να χρησιμοποιήσει μια πολιτική πιστοποιητικών για να αποφασίσει εάν ένα πιστοποιητικό, ή η σύνδεση που

πραγματοποιείται ανάμεσα στο πιστοποιητικό και τον ιδιοκτήτη του, είναι επαρκώς άξιο εμπιστοσύνης για μια συγκεκριμένη εφαρμογή.

Η CP απευθύνει απαιτήσεις ασφαλείας και υποχρεώσεις προς όλες τις συνιστώσες της Υποδομής Δημοσίου Κλειδιού, και όχι μόνο προς την CA: αυτές περιλαμβάνουν τις CA και RA, καταχωρητές, συνδρομητές και έμπιστους συμμετέχοντες. Μια πιο λεπτομερής περιγραφή των πρακτικών που ακολουθεί η CA κατά την έκδοση και τη διαχείριση των πιστοποιητικών, περιέχεται σε μια δήλωση πρακτικών πιστοποίησης (certification practice statement, CPS), η οποία εκδίδεται από την CA. Αν και μια CP και μια CPS καλύπτουν τα ίδια πεδία, η Πολιτική Πιστοποιητικών προσδιορίζει τις απαιτήσεις ασφαλείας και τις υποχρεώσεις για μια Υποδομή Δημόσιου Κλειδιού και η CPS περιγράφει πώς αυτές οι απαιτήσεις ικανοποιούνται από την Πολιτική Δημοσίου Κλειδιού. Επίσης όμως, χρησιμοποιούνται διαφορετικά. HCP αποτελεί τη βάση για την πιστοποίηση μέσα στα όρια της Υποδομής Δημοσίου Κλειδιού, με σκοπό να προωθήσει το ασφαλές ηλεκτρονικό εμπόριο. Ένα αντικείμενο αναγνώρισης (Object Identifier, OID) που αναπαριστά την CP και χρησιμοποιείται για να δημιουργεί ένα πιστοποιητικό, μπορεί να συμπεριληφθεί στις «πολιτικές πιστοποιητικών» των πιστοποιητικών X.509.

Το OID επιτρέπει στους έμπιστους συμμετέχοντες να ενημερώνονται για την προσοχή που λήφθηκε κατά την δημιουργία των πιστοποιητικών, την προτεινόμενη χρήση και τις υποχρεώσεις των διαφόρων συμμετεχόντων. Η CPS επιτρέπει στην Υποδομή Δημοσίου Κλειδιού να χρησιμοποιεί και να διαχειρίζεται τις διάφορες συνιστώσες της. Ακόμα αποτελεί τη βάση όπου πραγματοποιούνται οι έλεγχοι για το αν οι συνιστώσες της Υποδομής Δημοσίου Κλειδιού λειτουργούν σύμφωνα με τις προδιαγραφές της CPS.

5.5.7 Αλγόριθμοι κρυπτογράφησης

Οι κυριότεροι αλγόριθμοι που χρησιμοποιούνται σήμερα στην κρυπτογραφία, είναι οι εξής: οι συμμετρικοί αλγόριθμοι που χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση και είναι πιο γρήγοροι από τους ασύμμετρους και οι αλγόριθμοι ψηφιακών υπογραφών, για τη δημιουργία και επαλήθευση των οποίων χρησιμοποιούνται ασύμμετροι αλγόριθμοι σε συνδυασμό με αλγόριθμους κατακερματισμού.

5.5.8 Συμμετρικοί αλγόριθμοι

Το πρότυπο DES (Data Encryption Standard), το Τριπλό DES (Triple DES) και ο αλγόριθμος IDEA (International Data Encryption Algorithm) είναι συμμετρικά συστήματα τμηματικής

(block) κρυπτογράφησης, που χρησιμοποιούν «κομμάτια» δεδομένων των 64 bits. Ο αλγόριθμος DES επιλέχθηκε ως επίσημο Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφορίας(Federal Information Processing Standard, FIPS) των ΗΠΑ το1976 και συνεπώς υιοθετήθηκε διεθνώς. Καθώς το μικρό κλειδί του (56 bits) καθιστά τον DES μη ασφαλή, ο Τριπλός DES θεωρήθηκε ως ένας απλός τρόπος αύξησης του μεγέθους κλειδιού χωρίς να απαιτείται η μετάβαση σε νέο αλγόριθμο. Ο τελευταίος διενεργεί, στην ουσία, τρεις διαδοχικές εκτελέσεις του DES, με αποτέλεσμα ένα κλειδί μήκους 192 bits (συμπεριλαμβανομένων των bits ισοτιμίας). OIDEA ήταν από τις πρώτες προτάσεις αντικατάστασης του DES με κλειδί μήκους 128 bits. Χρησιμοποιήθηκε στο πρόγραμμα PGP (Pretty Good Privacy) σαν εναλλακτική και θεωρείται αρκετά ασφαλής.

Ο αλγόριθμος AES (Advanced Encryption Standard) είναι από τους δημοφιλέστερους αλγόριθμους στη συμμετρική κρυπτογραφία. Θεωρείται πολύ ασφαλής και η Επιτροπή Εθνικής Ασφάλειας (National Security Agency, NSA) των ΗΠΑ τον συμπεριλαμβάνει στην «Κατηγορία Β» των κρυπτογραφικών αλγορίθμων που προτείνονται ως η βάση για την προστασία τόσο μη απόρρητων όσο και πολύ απόρρητων πληροφοριών X[8]X. Ο AES έχει σταθερό μέγεθος block 128 bits και μέγεθος κλειδιού128, 192 ή 256 bits.

Ο Blowfish αποτελεί έναν ακόμα αλγόριθμο με σταθερό μέγεθος block 64 bits. Χρησιμοποιείται σε μεγάλο αριθμό εφαρμογών και προϊόντων κρυπτογραφίας και θεωρείται αρκετά ασφαλής. Το μέγεθος κλειδιού του μπορεί να μεταβάλλεται και φτάνει τα 448 bits. Στην πράξη το συνηθέστερο μήκος κλειδιού είναι128 bits.

Οι αλγόριθμοι Rivest Ciphers 2 (RC2) και 5 (RC5) σχεδιάστηκαν από τον Ronald Rivest. Ο RC2 είναι ένας αλγόριθμος τμηματικής κρυπτογράφησης με μήκος κλειδιού που μεταβάλλεται από 8 έως 128 bits και μήκος block 64 bits, ενώ ο RC5 έχει μεταβλητό μήκος κλειδιού μέχρι τα2048 bits αλλά επιπλέον, σε αντίθεση με την πλειοψηφία των σχημάτων, μεταβλητό μέγεθος block.

Ο Rivest Cipher 4 (RC4) του ίδιου σχεδιαστή είναι ένας συμμετρικός αλγόριθμος με κυμαινόμενο μέγεθος κλειδιού. Σε αντίθεση με τους δύο προηγούμενους είναι κρυπτογράφησης ροής (stream cipher) και χρησιμοποιείται σε δημοφιλή πρωτόκολλα, όπως τοSSL (Secure Socket Layer).

5.5.9 Ψηφιακές υπογραφές

Οι αλγόριθμοι σύνοψης μηνύματος Message Digest Algorithms 2 (MD2) και 5 (MD5) συνιστούν κρυπτογραφικές συναρτήσεις κατακερματισμού (hash functions) και αναπτύχθηκαν από τον Ronald Rivest. Παράγουν και οι δύο μια τιμή κατακερματισμού μήκους 128 bits.Κατά μία έννοια, ο MD5 αντικατέστησε τον MD2, παρόλο που και ο τελευταίος χρησιμοποιείται ακόμα σε μεγάλο βαθμό. Εφαρμόζονται κυρίως σε Υποδομές Δημόσιου Κλειδιού ως μέρος των ψηφιακών πιστοποιητικών, συνήθως με τον ασύμμετρο κρυπτογραφικό αλγόριθμο RSA. Ο αλγόριθμος RSA (Ronald Rivest, Adi Shamir, Leonard Adleman) αναπτύχθηκε το 1977 και είναι ένα από τα πρώτα κρυπτογραφικά σχήματα δημόσιου κλειδιού, ενώ σήμερα αποτελεί το ευρύτερα αποδεκτό και υλοποιούμενο. Τα κλειδιά RSA έχουν συνηθέστερα μήκος1024-2048 bits.

5.6 Κρυπτογραφικά μοντέλα ασφάλειας

Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι τέσσερα:

- Το μοντέλο MIX-net
- Το μοντέλο των «τυφλών» υπογραφών (blind signatures)
- ΤΟ μοντέλο του Benaloh
- Το ομομορφικό μοντέλο

5.6.1 Το μοντέλο MIX-net

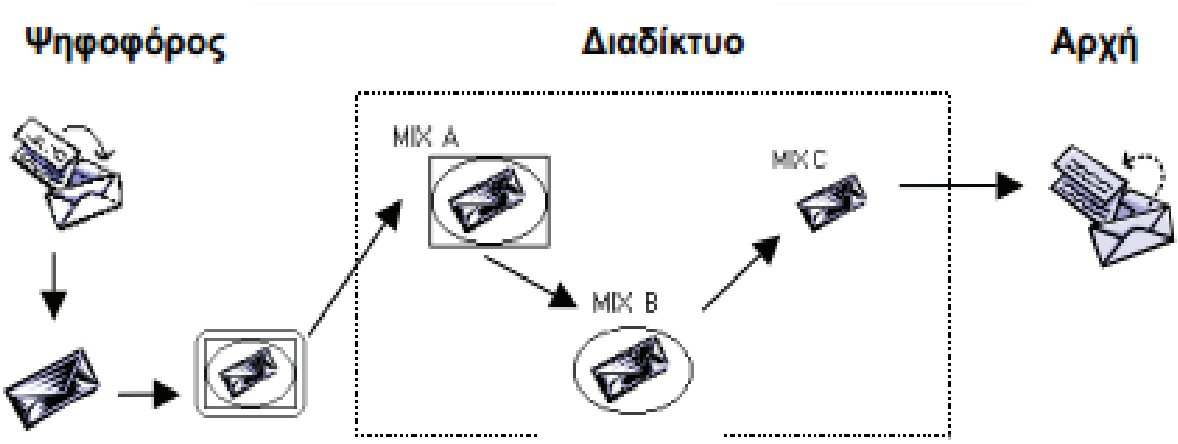
Ο Chaum εισήγαγε την έννοια των δικτύων MIX-net (MIX networks) τα οποία αποτελούν έναν κρυπτογραφικό μηχανισμό για την κατασκευή ανώνυμων καναλιών (anonymous channels) σε εφαρμογές υψηλής ασφάλειας. Ένα δίκτυο MIX-net αποτελείται από έναν αριθμό εξυπηρετητών, συνδεδεμένων μεταξύ τους, που καλούνται κόμβοι MIX. Κάθε κόμβος MIX λαμβάνει ως είσοδο (input) ένα σύνολο μηνυμάτων (π.χ. τις κρυπτογραφημένες ψήφους), κάνει ορισμένους τυχαίους μετασχηματισμούς και επιστρέφει στην έξοδο (output) ένα διαφορετικό σύνολο (των ίδιων, μετασχηματισμένων) μηνυμάτων, κατά τρόπο ώστε τα μηνύματα της εξόδου να μη μπορούν να συνδεθούν με τα μηνύματα της εισόδου. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι οι κόμβοι) δε μπορεί να καθορίσει ποια ψήφος αντιστοιχεί σε ποιόν

ψηφοφόρο.Κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη της σειράς των κόμβων.

Η ψήφος κρυπτογραφείται πρώτα με το δημόσιο κλειδί του MIXC που θα παραλάβει τελευταίο τη λίστα με τις κρυπτογραφημένες ψήφους, στη συνέχεια με το κλειδί του προτελευταίου MIXB και τέλος με το δημόσιο κλειδί του πρώτου τη τάξει MIXA. Κάθε κόμβος MIX αποκρυπτογραφεί τη λίστα των ψήφων που του αποστέλλονται, τη μετασχηματίζει (π.χ. προσθέτοντας τυχαιότητα σε κάθε ψήφο και αναδιατάσσοντας τη λίστα με τις ψήφους που προκύπτει), και στη συνέχεια την προωθεί στον επόμενο κόμβο. Αυτός ο τύπος δικτύου καλείται MIX-net αποκρυπτογράφησης.

Εναλλακτικά, σε ένα παραπλήσιο μοντέλο, σε κάθε κόμβο MIX λαμβάνει χώρα μόνον ο μετασχηματισμός των ψήφων, και στη συνέχεια όλοι οι κόμβοι συνεργάζονται για την αποκρυπτογράφηση της τελικής λίστας των ψήφων. Ένας άλλος τύπος είναι το MIX-net επανακρυπτογράφησης , όπου όλες οι ψήφοι κρυπτογραφούνται με το δημόσιο κλειδί του πρώτου κόμβου MIX, και στη συνέχεια σε κάθε κόμβο MIX λαμβάνει χώρα ο μετασχηματισμός και η κρυπτογράφηση με το δημόσιο κλειδί του επόμενου κόμβου, κατά τρόπο επαληθεύσιμο (μεταξύ των κόμβων ή και για τους εξωτερικούς παρατηρητές). Οι πλέον χρήσιμες ιδιότητες των δικτύων MIX-net, ειδικά για εκλογές μεγάλης κλίμακας, είναι η οικουμενική επαληθευσιμότητα της ορθότητας των μετασχηματισμών και της αποκρυπτογράφησης που προσφέρουν, καθώς και η ανθεκτικότητα τους έναντι συνεργιών μεταξύ (έως) ενός ορισμένου αριθμού κακόβουλων ή δυσλειτουργικών κόμβων MIX που επιχειρούν να παρακωλύσουν την εκλογική διαδικασία ή να καταλύσουν τη μυστικότητα των ψήφων ή και την ορθότητα των αποτελεσμάτων . Επίσης, τα δίκτυα MIX-net θεωρούνται αποδοτικά:

- Για τους εξωτερικούς παρατηρητές (που επιχειρούν να επαληθεύσουν την ορθότητα των πράξεων), αν και εφόσον ο υπολογιστικός φόρτος για τον παρατηρητή είναι σταθερός και ανεξάρτητος από τον αριθμό των κόμβων MIX που συμμετέχουν στη διαδικασία
- Για τους ψηφοφόρους, αν και εφόσον ο υπολογιστικός φόρτος για κάθε ψηφοφόρο είναι επίσης ανεξάρτητος του αριθμού των κόμβων MIX.
- Για τους εξυπηρετητές (κόμβοι MIX), αν και εφόσον η υπολογιστική πολυπλοκότητα για κάθε κόμβο είναι ανεξάρτητη από τον αριθμό των υπολοίπων κόμβων που συμμετέχουν στη διαδικασία.



Εικόνα 5: Παράδειγμα δικτύου MIX-net με τρεις κομβους MIX

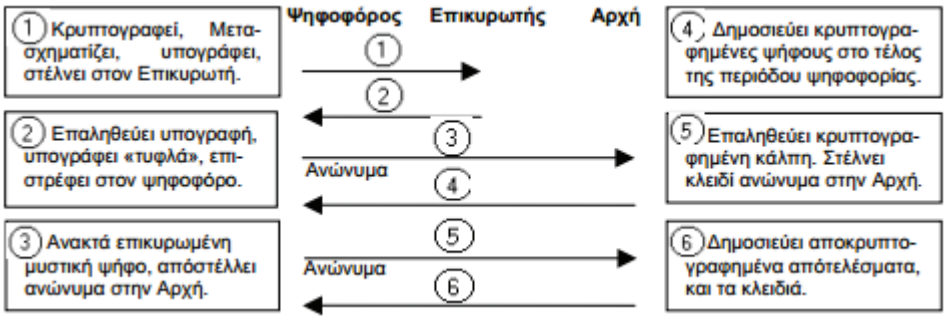
5.6.2 Το μοντέλο των «τυφλών» υπογραφών

Η έννοια της «τυφλής» υπογραφής (blind signature) παρουσιάστηκε αρχικά από τον Chaum ως μια κρυπτογραφική μέθοδος για την υπογραφή ενός μηνύματος χωρίς τη γνώση του μηνύματος καθ' αυτού. Ένα ιδιαίτερο χαρακτηριστικό λοιπόν των «τυφλών» υπογραφών είναι η μη συνδεσιμότητα τους (unlinkability) . Αυτή η μέθοδος, αν και εφαρμόστηκε αρχικά σε εφαρμογές ανώνυμου ηλεκτρονικού χρήματος (e-cash), χρησιμοποιήθηκε επίσης από τους Fujioka, Okamoto και Ohta για την επίλυση του προβλήματος της Επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητας τους: κάθε ψηφοφόρος κρυπτογραφεί τη ψήφο του και στη συνέχεια την υποβάλλει σε έναν Επικυρωτή από τον οποίο λαμβάνει πίσω μια «τυφλή» υπογραφή στο κρυπτογράφημα της ψήφου. Ο ψηφοφόρος στέλνει το επικυρωμένο κρυπτογράφημα σε μια Αρχή (μπορεί να είναι ο Επικυρωτής ή κάποια άλλη ανεξάρτητη οντότητα - για επιπρόσθετη ασφάλεια) χρησιμοποιώντας ένα ανώνυμο κανάλι επικοινωνίας. Στο τέλος της περιόδου υποβολής ψήφων, η Αρχή δημοσιεύει τις κρυπτογραφημένες ψήφους σε έναν πίνακα ανακοινώσεων (bulletin board). Κάθε ψηφοφόρος ελέγχει εάν η ψήφος του είναι δημοσιευμένη στον πίνακα ανακοινώσεων (αν όχι, τότε μπορεί να καταγγείλει τη διαδικασία, επίσης ανώνυμα.

Εάν η ψήφος του έχει δημοσιευτεί κανονικά, ο ψηφοφόρος υποβάλλει το κλειδί αποκρυπτογράφησης στην Αρχή, χρησιμοποιώντας ξανά το ανώνυμο κανάλι επικοινωνίας. Η Αρχή αποκρυπτογραφεί όλες τις ψήφους και δημοσιεύει τα αποτελέσματα στον πίνακα ανακοινώσεων. Έως σήμερα έχουν προταθεί αρκετά σχήματα που βασίζονται στον μηχανισμό των «τυφλών» υπογραφών . Επίσης, αρκετά τέτοια συστήματα έχουν υλοποιηθεί πιλοτικά σε

εκλογές μικρής κλίμακας. Ένα πλεονέκτημα των συστημάτων που ακολουθούν το μοντέλο των «τυφλών» υπογραφών είναι ότι απαιτούν χαμηλό επικοινωνιακό φόρτο και υπολογιστικό κόστος, ακόμα και όταν ο αριθμός των ψηφοφόρων είναι μεγάλος (scalability). Επιπλέον, η μυστικότητα των ψήφων επαφίεται στους ψηφοφόρους, κάτι που ευνοεί την εύκολη και ασφαλή διαχείριση του συστήματος από την (συνήθως μια) Αρχή. Τέλος, τα ανωτέρω σε συνδυασμό με την εγγενή υποστήριξη πολλαπλών υποψηφίων, καθιστούν τα συστήματα αυτά ιδιαίτερα ελκυστικά όχι μόνο για εκλογές μικρής/μεγάλης κλίμακας, αλλά και για σφυγμομετρήσεις, δημοσκοπήσεις, κ.λ.π

Ένα σημαντικό μειονέκτημα των συστημάτων «τυφλής» υπογραφής είναι ότι απαιτούν από τον ψηφοφόρο να είναι ενεργός (online) σε όλα τα στάδια της ψηφοφορίας. Από τη σκοπιά της ασφάλειας, τα συστήματα αυτά προσφέρουν μόνο ατομική επαληθευσιμότητα και είναι ιδιαίτερα ευάλωτα στο πρόβλημα των απεχόντων ψηφοφόρων: εάν ένας εγγεγραμμένος ψηφοφόρος επικυρώσει τη ψήφο του αλλά στη συνέχεια απέχει από τη ψηφοφορία, τότε ένας κακόβουλος Επικυρωτής μπορεί να υποβάλλει μια πλαστή ψήφο εκ μέρους του ψηφοφόρου.



Εικόνα 6: Ένα παράδειγμα ηλεκτρονικής ψηφοφορίας με τυφλές υπογραφές

5.6.3 Το μοντέλο του Benaloh

Το μοντέλο αυτό χρησιμοποιεί ένα σχήμα ομομορφικού διαμοιρασμού μυστικών (homomorphic secret sharing). Σε τέτοια ομομορφικά σχήματα υπάρχει μια Πράξη $\oplus$ ορισμένη στο σύνολο των μεριδίων, τέτοια ώστε το «άθροισμα» των μεριδίων οποιονδήποτε δυο μυστικών x1,x2 να ισούται με ένα μερίδιο του «αθροίσματος» x1$\oplus$ x2.Στο σχήμα του Benaloh κάθε ψηφοφόρος διαμοιράζει τη ψήφο του σε Αρχές, χρησιμοποιώντας ένα (t,n) threshold διαμοιρασμού μυστικού. Τα μερίδια κρυπτογραφούνται με το δημόσιο κλειδί της κάθε Αρχής-παραλήπτη, υπογράφονται ψηφιακά και δημοσιεύονται σε έναν Πίνακα Ανακοινώσεων.

Μετά το τέλος της περιόδου υποβολής ψήφων κάθε Αρχή προσθέτει όλα τα μερίδια που έχει λάβει ώστε, βάσει της ομομορφικής ιδιότητας της συνάρτησης διαμοιρασμού, να αποκτήσει ένα μερίδιο του αθροίσματος των ψήφων της κάλπης. Τέλος, οι Αρχές συνδυάζουν τα μερίδια τους ώστε να σχηματίσουν την τελική κάλπη. Η ορθότητα της καταμέτρησης βασίζεται στην ιδιότητα των τεχνικών threshold: τουλάχιστον t από τις n Αρχές πρέπει να συνδυάσουν τα μερίδια τους ώστε τα αποτελέσματα να είναι οικουμενικά επαληθεύσιμα. Τα συστήματα αυτής της κατηγορίας , παρότι σχετικά απλά στη δομή τους, έχουν υψηλό επικοινωνιακό φόρτο: κάθε ψηφοφόρος πρέπει να υποβάλλει τη ψήφο του χρησιμοποιώντας n κανάλια επικοινωνίας.

5.7 Βασικά κρυπτογραφικά εργαλεία

Τα βασικά εργαλεία που χρησιμοποιούνται από τα περισσότερα κρυπτογραφικά πρωτόκολλα ηλεκτρονικής ψηφοφορίας είναι τα εξής:

- **Πίνακες Ανακοινώσεων (Bulletin Boards):** Πρόκειται για κανάλια δημόσιας εκπομπής (public broadcast channels) που επιτρέπουν στους χρήστες (π.χ. ψηφοφόροι) να επικοινωνούν με τις Αρχές του συστήματος, με πλήρη διαφάνεια. Στα κανάλια αυτά η επικοινωνία αυθεντικοποιείται με τη χρήση ψηφιακών υπογραφών. Μια πρακτική και ασφαλής υλοποίηση των πινάκων ανακοινώσεων αποτελεί το κατανεμημένο σύστημα Rampart.

- **Ανώνυμα Κανάλια Επικοινωνίας (Anonymous Channels):** Τα κανάλια αυτά εξασφαλίζουν την ανωνυμία των χρηστών του συστήματος. Εκτός από τα δίκτυα MIX-net, υπάρχουν και τα συστήματα ανωνυμίας με τη χρήση διαμεσολαβητή (proxy systems) , όπως επίσης και τα υβριδικά συστήματα (hybrid systems) ανωνυμίας .

- **Κρυπτογραφία τύπου Threshold (threshold cryptography)**

  Τα συστήματα κρυπτογράφησης τύπου threshold κατανέμουν τη λειτουργικότητα των κρυπτογραφικών πρωτοκόλλων ώστε να επιτύχουν ανθεκτικότητα (robustness). Για παράδειγμα, σε μια ψηφοφορία η διαδικασία της καταμέτρησης μπορεί να κατανεμηθεί μεταξύ n Αρχών Ψηφοφορίας, με τη χρήση ενός (t,n) threshold κρυπτογραφικού συστήματος δημοσίου κλειδιού (π.χ. threshold ElGamal. Σε αυτήν την περίπτωση υπάρχει μόνον ένα δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί διαμοιράζεται στις Αρχές με τη χρήση τεχνικών διαμοιρασμού μυστικού . Κάθε ψηφοφόρος κρυπτογραφεί τη ψήφο του με το δημόσιο κλειδί των Αρχών, και η τελική κάλπη αποκρυπτογραφείται από κοινού με τη συνεργασία τουλάχιστον t Αρχών.

  Η μμυστικότητα της ψήφου και η ακρίβεια των αποτελεσμάτων εξασφαλίζεται εφόσον δεν υπάρχουν περισσότερες από t-1 βουλες ή απλά δυσλειτουργικές Αρχές. Ο αριθμός αποτελεί τη τιμή threshold του κρυπτογραφικού συστήματος. Τα συστήματα threshold μπορούν να ενισχυθούν, για προστασία από επιθέσεις υποκλοπής κλειδιού (key confiscation), με μηχανισμούς όπως προ-ενεργή ασφάλεια (proactive security) καθώς και με τεχνικές ισχυρής χρονικής ασφάλειας

- **Αποδείξεις με Μηδενική Γνώση (Zero Knowledge Proofs)**

  Οι αποδείξεις αυτές χρησιμοποιούν πρωτόκολλα Απόδειξης/Επαλήθευσης με αλληλεπίδραση (interactive), στα οποία ο Αποδεικνύων (Prover) επιβεβαιώνει σε έναν Επαληθευτή (Verifier) την ορθότητα μιας δήλωσης, κατά τέτοιον τρόπο ώστε ο Επαληθευτής να μη μπορεί να μάθει τίποτε περισσότερο, εκτός από το γεγονός ότι η δήλωση είναι ορθή . Τα πρωτόκολλα απόδειξης με μηδενική γνώση χρησιμοποιούνται ευρέως σε ηλεκτρονικά πρωτόκολλα ψηφοφορίας. Για παράδειγμα, τέτοια πρωτόκολλα χρησιμοποιούνται προκειμένου να αποδειχθεί η ορθότητα των μετασχηματισμών στα συστήματα ψηφοφορίας που χρησιμοποιούν δίκτυα MIX-net για την ανωνυμία των

ψήφων, για να αποδειχτεί η εγκυρότητα των κρυπτογραφημένων ψήφων στις ομομορφικές εκλογές, για την ορθότητα των κρυπτογραφήσεων στα πρωτόκολλα προστασίας από καταναγκασμό, καθώς και για την ορθότητα των επικυρωμένων ψήφων στα συστήματα που βασίζονται στο μοντέλο των «τυφλών» υπογραφών.

Οι αλληλεπιδραστικές αποδείξεις με μηδενική γνώση είναι μη μεταφέρσιμες (non transferable): ο Επαληθευτής δε μπορεί να αποδείξει σε κάποιον τρίτο την ορθότητα μιας δήλωσης. Εν τούτοις είναι δυνατόν αυτές οι αποδείξεις να μετασχηματιστούν σε αποδείξεις που είναι μεταφέρσιμες, επομένως οικουμενικά επαληθεύσιμες, με την ευριστική προσέγγιση των Fiat-Shamir. Στην περίπτωση αυτή η ασφάλεια βασίζεται στο μοντέλο random oracle.

ΚΕΦΑΛΑΙΟ 6: ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

6.1 Περιπτώσεις εφαρμογής ηλεκτρονικής ψηφοφορίας στο εξωτερικό και τα προβλήματα που παρουσιάστηκαν

Βασικότερο όλων, σχετικά με την εφαρμογή των ηλεκτρονικών ψηφοφοριών, είναι η ταχύτητα και η αμεσότητα που προσφέρουν στους ψηφοφόρους, καθώς και τον μεγάλο βαθμό ευκολίας και για τους εκλογείς και για την διενέργεια της εκλογικής διαδικασίας.Ακόμα βέβαια, οι ηλεκτρονικές ψηφοφορίες, δεν χρησιμοποιούνται για την διενέργεια δημοψηφισμάτων, αλλά η λογική λέει πως αυτά θα είναι το επόμενο άμεσο βήμα. Οι ηλεκτρονικές ψηφοφορίες δίνουν την δυνατότητα για δημοψηφίσματα, γρήγορα και άμεσα. Δημοψηφίσματα για να αποφασίζουν οι πολίτες για το κάθε τι, για παλαιούς και νέους νόμους (κυρίως), για αποφάσεις της κυβέρνησης ή και των τοπικών αρχών (περιφέρειες και δήμοι), για τα πάντα που αφορούν και επηρεάζουν την ζωή τους.Η δημοκρατία όπως ορίζεται η έννοια της με την συμμετοχή και την αμεσότητα των πολιτών στην λήψη των αποφάσεων, χωρίς ενδιάμεσους ή αντιπρόσωπους,αντικαταστάτες. Με αυτό τον τρόπο, με την βοήθεια της τεχνολογίας θα μπορέσει επιτέλους να γίνει το μεγάλο βήμα από τον κοινοβουλευτισμό στην δημοκρατία.

Επειδή όμως είμαστε και ρεαλιστές, καταλαβαίνουμε ότι στην χώρα μας, την Ελλάδα, τα πράγματα θα “αργήσουν” αρκετά ακόμα. Έχουμε υπομονή και επιμονή και κυρίως εμπιστοσύνη στην τεχνολογία και το διαδίκτυο που εκτός από την “αναγκαστική” πρόοδο που έχουν φέρει και θα φέρουν στις ζωές μας, κάποια στιγμή θα φέρουν και την εφαρμογή

της πραγματικής δημοκρατίας. Η χρήση των ηλεκτρονικών ψηφοφοριών παγκοσμίως, παραμένει μια σχετικά ασυνήθιστη πρακτική, αν και συνεχώς η σκέψη αυτή αλλάζει, καθώς πολλές χώρες πειραματίζονται με διάφορες μορφές ηλεκτρονικών μεθόδων ή επεκτείνουν τις ήδη υπάρχουσες ηλεκτρονικές ψηφοφορίες. Επιπλέον, η ηλεκτρονική ψηφοφορία δεν περιορίζεται στην Ευρώπη και στην Βόρεια Αμερική αφού χώρες όπως η Βραζιλία και η Ινδία έχουν αναπτύξει εφαρμογές περισσότερο ολοκληρωμένες. Στον παρακάτω πίνακα συνοψίζονται τα κυριότερα διεθνή έργα, τα οποία σχετίζονται με το ζήτημα της ηλεκτρονικής ψηφοφορίας. Σε κάθε έργο αναφέρεται και ο ιστοτόπος όπου ο αναγνώστης μπορεί να βρει σχετικές αναλυτικές πληροφορίες.

Project Acronym	Full Project Name	Partners	Status / Comments	URL
e-VOTE	An Internet Based Electronic Voting System IST-2000-29518	Quality and Reliability S.A. (Coordinator), University of the Aegean (Greece), Municipality of Amaroussion (Greece), Cryptomathic S.A. (Denmark), University of Regensburg (Germany), Self Governing Region of Kosice (Slovakia)	The project started in October 2001 and will end in April 2004.	http://www.instore.gr/evote/
E-Poll	Electronic polling System for remote voting operations IST-1999-21109	Siemens Informatica (Coordinator), The Italian Ministry of the Interior, Ancitel (Italy), Municipium (Poland), AEC (France), France Telecom	The project started in September 2000 and will end in August 2002.	http://www.e-poll-project.net/
	A secure and Trustable IntErnet Voting system based on PKI IST-2000-29424, IST-2000-29424D	POSTECOM (Coordinator) (Italy), University of Amsterdam, Abacus Spa (Italy), CGIL Lombardia (Italy), Glocal Ltd (Finland), London Borough of Newham (UK), Certinomis Sas (France), Associazione Smile (Italy), University of Milan (Italy)	Start Date: 2001-10-01 End Date: 2003-03-31	http://www.true-vote.net/

Project Acronym	Full Project Name	Partners	Status / Comments	URL
CYBERVOTE 	An innovative cyber voting system for Internet terminals and mobile phones IST-1999-20338	Mairie d' Issy les Moulineaux (France), Kista Stadsdelsnaemnd (Sweden), Katholieke Universiteit Leuven (Belgium), Freie Hansestadt Bremen (Germeny),Technische Universiteit Eindhoven (Netherlands), Nokia Corporation (Finland), British Telecommunications Plc (UK)	Start Date: 2000-09-01 End Date: 2003-02-28 Duration: 30 months	http://www.eucybervote.org/
AGORA 2000 	Innovative IST platforms & services to support a democratic regional/urban planning process IST-1999-20982	S.A.T.A. Applicazione Tecnologie Avanzate Srl (Italy), Aquitaine Europe Communication (France), Ayuntamiento de Valencia (Spain), Business Flow Consulting Sarl BFC Sarl (France), Universidad Politecnica de Madrid (Spain), Universidad Politecnica de Valencia (Spain), Amministrazione Regionale Toscana (Italy), Municipality of Anatoli (Greece), Ergon Consulting and Systems Sa (Greece)	Start Date: 2000-09-01 End Date: 2003-02-28 Duration: 30 months	http://www.agora2000.org/
DEMOS DELPHI MEDIATION ONLINE SYSTEM	Delphi mediation on-line system IST-1999- 20530	Pixelpark Ag (Germany), Ibermatica S.A. (Spain), IPSOS-RSL Limited (UK), Nexus-Intern. Broadcasting Association (Italy), GMD-Forschungszentrum Informationstechnik Gmbh (Germany), Frei und Hansestadt Hamburg (Germany), Comune di Bologna (Italy)	Start Date: 2000-09-01 End Date: 2003-02-28 Duration: 30 months	http://www.demos.nexus.org
euro-citi	EUROpean CITIes platform for on-line transaction services IST-1999-21088	Comunicacion Interactiva S.L (Spain), Archetypon S.A. (Greece), Institut Municipal d'Informatica (Spain), Municipality of Athens Development Agency S.A. (Greece) London Borough of Brent (Brent) (UK), Schlumberger Systemes S.A. (France), T-Nova Deutsche Telekom Innovationsgesellschaft Mbh (Germany)	Start Date: 2000-09-01 End Date: 2002-08-31 Duration: 24 months The main objective of EURO-CITI is to develop and demonstrate a set of new public transaction services, namely tele-voting, electronic submission of forms and tele-consulting, that can be accessed via the Internet and GSM	http://www.euro-citi.org
WEB ORACY	Web Technologies Supporting Direct Participation in Democratic Processes IST-1999-20364	Juvier S.r.o. (Slovakia), University of Wolverhampton (UK), Wolverhampton Metropolitan Borough Council (UK), The Local Authority Kosice - City Ward Tachanovce (Slovakia), Citec Engineering Oy Ab (Finland), Universitaet Gesamthochschule Essen (Germany), The Local Authority Kosice - City Ward Dargovskych Hrdinov (Slovakia)	Start Date: 2000-10-01 End Date: 2003-09-30 Duration: 36 months Project aims to empower citizens with innovative communication, access and voting system supporting increased participation in democratic processes.	http://esprit.ekf.tuke.sk/webocracy
E.D.E.N.	Electronic Democracy European Network IST-1999-20230	Telepolis Antwerpen (Belgium), Info Centrum - Consortium Nisko (Poland) , Yana Research S.R.l. (Italy), Napier University (UK), Universitaet Bremen (Germany), Omega Generation S.R.l. (Italy), Archivio Osvaldo Piacentini - Onlus (Italy), Freie Hansestadt Bremen (Germany), Public Voice Lab (Austria), Stadt Wien (Austria)	Start Date: 2001-02-01 End Date: 2003-07-31 The EDEN project will contribute to stimulate and support the citizens' participation in the decision-making process, specifically in the area of urban planning, through the development of Natural Language Processing (NLP)	http://www.edentool.org

Project Acronym	Full Project Name	Partners	Status / Comments	URL
E-POWER	European Programme for an Ontology-based Working Environment for Regulations and legislation IST-2000-28125	Universiteit Van Amsterdam (Netherlands), O & I Management Partners B.V. (Netherlands), Mega International (France), Librt B.V. (Netherlands), De Verzekeringen Van Fortis Bank Nv (Belgium), Application Engineers Nv. (Belgium),	Start Date: 2001-09-01 End Date: 2003-08-31 E-POWER will implement a knowledge management solution by providing a method and tools that help to improve the quality of legislation whilst facilitating the enforcement of law.	http://www.belastingdienst.nl/epower
VSIIS	Voluntary Organisations and Social Inclusion in the Information Society IST-2000-25427	Models Research, an independent research company specialising in information society issues in Ireland and Europe	Start Date: 2001-02-01 End Date: 2001-08-31 Project Status: Completed Key objectives include to identify potential implications for future policy activities on social inclusion in the information society, and to write the research report.	http://www.models-research.ie/projects/vsiis.html
E-COURT	Electronic Court: judicial IT-based management IST-2000-28199	Intrasoft International Sa (Luxembourg), Ministero della Giustizia (Italy), Cryptomathic A/s (Denmark), Ministry of Justice (Poland), Universite Paul Sabatier (France), Sema Group, S.a.e. (Spain) Consiglio Nazionale delle Ricerche (Italy), Universiteit Van Amsterdam (Netherlands)	Start Date: 2001-06-01 End Date: 2003-11-30 The e-Court solution consists in a shared technological platform aimed at acquiring, storing and exchanging standard electronic-based information among the European Justice community.	http://laplace.intrasoft-intl.com/e-court/
	The Caltech-MIT Voting Technology Project	Caltech, MIT	Tasks of this project include to establish and propose uniform attributes and quantitative guidelines for performance and reliability of voting systems	http://www.vote.caltech.edu
	Internet Policy Institute's report from the National Workshop on Internet Voting	National Science Foundation (Sponsor), Univ. of Maryland, Freedom Forum (Host)	On October 11 & 12, 2000, the IPI conducted a workshop to examine the issues associated with conducting public elections via computer networks, sponsored by the National Science Foundation (NSF) The workshop was part of a request by the White House to study the feasibility of Internet voting.	http://www.netvoting.org/
	California Internet Voting Task Force	The California Internet Voting Task Force was convened by Secretary of State Bill Jones to study the feasibility of using the Internet to conduct lections in California.	The report was published on January 18, 2000	http://www.ss.ca.gov/executive/ivote/
	Administration and Cost of Elections Project	International Foundation for Election Systems (IFES), International Institute for Democracy and Electoral Assistance (International IDEA), and the United Nations Department of Economic and Social Affairs (UN-DESA)	The ACE Electronic Publication provides information resources on election administration to electoral policymakers and administrators.	http://www.aceproject.org/
The EVOX Voting System		The Cryptography and Information Security research group of MIT's Laboratory for Computer Science, sponsored by DARPA Original implementation was done by Mark Herschberg as part of his Master's thesis "Secure Electronic Voting Over the World Wide Web".	Part of their research has been the implementation of the EVOX voting scheme, and testing its use in MIT campus-wide student elections.	http://theory.lcs.mit.edu/~cis/voting/voting.html#evox http://theory.lcs.mit.edu/~cis/voting/herschberg-thesis/index.html Herschberg's thesis
	California Voter Foundation		CVF is a non profit organisation aiming to provide information to those interested in issues of voting technology (systems, standards,	http://www.calvoter.org/

Project Acronym	Full Project Name	Partners	Status / Comments	URL
			legislation etc)	
VoteHere	VoteHere	In partnership with Compaq, Cisco and Entrust	VoteHere election systems support private, public and military (!) elections	http://www.votehere.net
	GNU.FREE (Free Referenda & Elections Electronically) - Internet Voting system		Design work first started in April 1999 and is progressing. A free software project creating Java electronic voting software released under the General Public License (GPL). It is database and platform independent.	http://www.free-project.org/
SAFEVOTE		Safevote is a software company with technology for Internet voting It targets diverse markets in private, government and Internet sectors.	They offer a variety of products supporting both public and private elections	http://www.safevote.com/
	election.com The Global Election Company	election.com is a global (US, UK, France, New Zealand, Australia) election software and services company.	They provide election management solutions—voter registration and database management, poll site and remote electronic voting, advance security solutions, accurate tabulation, and custom demographic reporting for political jurisdictions and private sector clients.	http://www.election.com/
e-lection.com Defining the Digital E-lection Process		LDE Inc. and e-lection.com were founded together in the Summer of 1998 with the goal of creating a solid online voting system.	They provide digital elections hosting and consulting	http://www.e-lection.com/

Πίνακας 2: Τα κυριότερα διεθνή έργα ηλεκτρονικής ψηφοφορίας.
Πηγή:*Kenneth Benoit, 'Experience of Electronic Voting Overseas*

Οι παραπάνω εφαρμογές ηλεκτρονικών ψηφοφοριών διαφέρουν αρκετά τόσο σε τεχνολογικό επίπεδο όσο και επίπεδο λειτουργικότητας. Μερικές περιλαμβάνουν περιοδικό έλεγχο ψήφων μέσω χαρτιού ενώ άλλες όχι. Κάποιες εισάγουν την ηλεκτρονική ψήφο ταυτόχρονα με ένα σύστημα χαρτιού ενώ άλλες έχουν επιλέξει να εισάγουν τις ψήφους χωρίς αυτή την επιλογή. Τέλος, πολλά συστήματα μεταχειρίζονται διαφορετικά τον τρόπο που οι ψηφοφόροι θέλουν να καταστρέψουν την ψήφο τους ή να ψηφίσουν λευκό. Παρακάτω θα αναφερθούν τρόποι με τους οποίους κάποιες χώρες χρησιμοποίησαν την ηλεκτρονική ψηφοφορία και αποτίμησαν τις εμπειρίες τους. Κανένα σύστημα δεν είναι απαλλαγμένο από προβλήματα και αμφισβητήσεις, όμως είναι αξιοπρόσεκτο ότι τα συστήματα ηλεκτρονικής ψηφοφορίας που έχουν εφαρμοστεί σε εθνική κλίμακα δεν έχουν υποστεί κάποια σημαντικά υπολογιστικά λάθη και δεν έχουν υπάρξει εκτεταμένες δημόσιες αντιδράσεις. Πολλές εκλογικές επιτροπές που είναι υπεύθυνες για τη λήψη αποφάσεων υιοθέτησαν ηλεκτρονικές διαδικασίες για την αποφυγή υπολογιστικών λαθών. Τέλος το πλεονέκτημα της χρήσης ηλεκτρονικών ψηφοφοριών είναι η αύξηση της συγκέντρωσης ατόμων και κατά συνέπεια η ποιότητα δημοκρατίας στα αποτελέσματα των εκλογών.

6.1.1 Ενδεικτικές Περιπτώσεις χωρών

- **Βραζιλία:** Η Βραζιλία, το μεγαλύτερο έθνος στη νότια Αμερική, βρίσκεται στη πρώτη γραμμή ηλεκτρονικών ψηφοφοριών παγκοσμίως. Σήμερα, όλοι οι ψήφοι στη Βραζιλία υπολογίζονται από ηλεκτρονικές μηχανές. Το ανώτατο εκλογικό δικαστήριο της Βραζιλίας επέτρεψε την χρήση ηλεκτρονικής ψηφοφορίας το 1996 στις δημοτικές εκλογές. Αυτή η χρήση επεκτάθηκε το 1998 όταν πάνω από 60 εκατομμύρια ψηφοφόροι (57% εκλογικού σώματος) χρησιμοποίησαν την ηλεκτρονική ψηφοφορία. Το 2000, η κυβέρνηση της Βραζιλίας μετέτρεψε το σύστημα σε πλήρως ηλεκτρονικό και κατασκεύασε πάνω από 400.000 ηλεκτρονικά εκλογικά περίπτερα.

  Οι ψηφοφόροι στη Βραζιλία χρησιμοποιούν τα συστήματα ηλεκτρονικής ψηφοφορίας,τα μηχανήματα είναι ένα ενοποιημένο σύστημα οθόνης και πληκτρολογίου σε μικρή αναλογία(30x40x20). Η επιλογή ενός υποψήφιου χρειάζεται μόνο το πάτημα του αριθμού που τον καθορίζει. Έπειτα εμφανίζεται η φωτογραφία του υποψηφίου και οι ψηφοφόροι μπορούν να επιβεβαιώσουν, να απορρίψουν ή και να επιλέξουν άλλο υποψήφιο. Το ηλεκτρονικό σύστημα της Βραζιλίας θεωρείται εξαιρετικό αφού κατά το τέλος των εκλογών παρέχει ψηφιακές και εκτυπωμένες αναφορές με τον αριθμό των ψήφων που πήρε ο κάθε υποψήφιος.Οι ανησυχίες σχετικά με την ακρίβεια των αυτοελεγχόμενων συστημάτων οδήγησε στο να οριστούν συσκευές επαλήθευσης, 3% του όλου αριθμού των συσκευών (περίπου 12.000 μηχανές) για την παραγωγή έντυπου ψηφοδελτίου που ο ψηφοφόρος θα μπορούσε να ρίξει σε ένα κουτί για δεύτερη καταμέτρηση.

  Οι μηχανές σε συνδυασμό με την ρίψη του έντυπου ψηφοδελτίου που οι συσκευές παράγουν,χρησιμοποιήθηκαν επιτυχώς κατά τη διάρκεια των εκλογών στις 6 οκτωμβρίου του 2002.Μετά την επίδειξη αξιοπιστίας των μηχανών,η χρήση του χαρτιού είχε εγκαταληφθεί για τις επόμενες εκλογές.Μετά από μια μακρά συζήτηση για τα πλεονεκτήματα και τα μειονεκτήματα της επιλογής έντυπων ψηφοδελτίων,η κυβέρνηση κατέληξε στο συμπέρασμα ότι η εξάλειψη της χρήσης των εκτυπωτών στο πλαίσιο του συστήματος θα εξοικονομούσε στη Βραζιλία περίπου 100 εκ. δολάρια.Επιπλέον,η υιοθέτηση σε μηχανές χωρίς εκτυπωτές θα κάνουν την ψηφοφορία πολύ πιο γρήγορη.

- **Ιταλία:** Το ιταλικό τμήμα καινοτομίας και τεχνολογιών μαζί με το Υπουργείο Εσωτερικών ανακοίνωσαν το Φεβρουάριο του 2004, ότι στις εκλογές για το Ευρωπαϊκό

Κοινοβούλιο θα πραγματοποιηθεί πειραματικά ένα πρόγραμμα με θέμα τον υπολογισμό ψήφων μέσω ηλεκτρονικής ψηφοφορίας. Η πρωτοβουλία που ονομάστηκε «Ηλεκτρονική διερεύνηση» θα πραγματοποιούνταν παράλληλα με την παραδοσιακή χειρωνακτική ψηφοφορία κατά την διάρκεια των Ευρωπαϊκών εκλογών στις 12 και 13 Ιουνίου αλλά χωρίς οποιαδήποτε νομική αξία. Περίπου 1.500 εκλογικά τμήματα συμμετείχαν στο πρόγραμμα το οποίο προετοίμασε το έδαφος για το μέλλον. Σύμφωνα με την Ιταλική κυβέρνηση, τα κύρια πλεονεκτήματα ενός ερευνητικού ηλεκτρονικού συστήματος είναι οι γρήγορες και εύκολες λειτουργίες, οι πιο ακριβής μετρήσεις,γρήγορες και ασφαλής μεταφορές αποτελεσμάτων και γενικότερη αύξηση της αποδοτικότητας των εκλογών. Στο Βιντζεβάνο της βόρειας Ιταλίας δοκιμάστηκε ένα σύστημα που αποτελούνταν από μια οθόνη αφής και παρείχε μια ηλεκτρονική ψηφοφορία ελεγχόμενης διαδρομής. Σε πάνω από 4.000 εγγεγραμμένους ψηφοφόρους δόθηκε η δυνατότητα να εξετάσουν το σύστημα ηλεκτρονικής ψηφοφορίας που προμηθεύτηκε από την Αμερικάνικη εταιρία AccuPoll.

- **Αγγλία:** Το Μάιο του 2002, τριάντα τοπικές κυβερνήσεις στην Αγγλία δοκίμασαν πολλές διαφορετικές εφαρμογές για ψηφοφορίες ή καταμέτρηση ψήφων.Κάποιοι αρμόδιοι χρησιμοποίησαν τεχνολογίες όπως οθόνες αφής και απομακρυσμένη ψηφοφορία. Εννιά από αυτούς επέτρεψαν στους ψηφοφόρους να δίνουν τη ψήφο τους με ηλεκτρονικές μεθόδους όπως interactive voice response (IVR), συστήματα βασισμένα σε υπολογιστή και συσκευές κινητών τηλεφώνων (SMS). Μερικοί από αυτούς, επέτρεπαν στους ψηφοφόρους τη ρίψη ψήφου μέσω ηλεκτρονικών περιπτέρων (e-kiosk) σε δημόσιους χώρους.Στην αναφορά της Επιτροπής εκλογών που επιθεωρεί τις δοκιμές ηλεκτρονικής ψηφοφορίας, παρατηρήθηκε ότι το λογισμικό και ο εξοπλισμός δούλεψαν σωστά και χωρίς σημαντικά προβλήματα. Τέλος, δεν βρέθηκε καμία απόδειξη απάτης στο πρόγραμμα, αν και εκφράστηκαν ανησυχίες για την ασφάλεια και τις πιθανές παραβιάσεις.

6.1.2 Συγκριτική αξιολόγηση συστημάτων ηλεκτρονικής ψηφοφορίας χωρών

Ας δούμε ορισμένες διαφορές ανάμεσα στα συστήματα ηλεκτρονικής ψηφοφορίας ορισμένων χωρών.

- **Esthoniac voting system vs Norwegian e-voting system**

Το Νορβηγικό σύστημα ηλεκτρονικής ψηφοφορίας είναι διαφανές η Νορβηγική κυβέρνηση έχει δημοσιοποιήσει όλα τα έγγραφα που σχετίζονται με την αρχιτεκτονική του συστήματος όπως επίσης η κυβέρνηση έχει αποφασίσει να προβεί στην δημοσιοποίηση του πηγαίου κώδικα του συστήματος ώστε να είναι διαθέσιμο στο κοινό και να μπορεί να ανακαλύψει τις «τρύπες» στα θέματα ασφάλειας του συστήματος.

Το κρυπτογραφικό πρωτόκολλο που χρησιμοποιεί το σύστημα αυτό είναι σχεδιασμένο από την Scytl μια Ισπανική εταιρία και έχουν προσθέσει 2 μηχανισμούς όπου αυτοί οι μηχανισμοί είναι το sms και το email που λαμβάνει κατά την διαδικασία της ψηφοφορίας. Επίσης ο ψηφοφόρος μπορεί να ψηφίσει όσες φορές θέλει.Ακόμη χρησιμοποιεί τον μηχανισμό mix-net για αποτελεσματικότητα και ασφάλεια.

Η διαδικασία της ψηφοφορίας είναι η εξής ο ψηφοφόρος λαμβάνει ένα email που περιέχει τα ονόματα των υποψηφίων και τον κωδικό επαλήθευσης το email αυτό θα βοηθήσει ώστε να γίνει επαλήθευση της ψηφοφορίας στη συνέχεια με το sms που θα λάβει πιστοποίηση του ψηφοφόρου στον server θα γίνει με το id της εθνικής του ταυτότητας η εφαρμογή λαμβάνει μια λίστα με τους υποψηφίους τότε ο ψηφοφόρος επιλέγει το κόμμα που επιθυμεί και προχωρά στο επόμενο μέρος όπου είναι η επιλογή του ψηφοφόρου σύμφωνα με το κόμμα που επέλεξε στην συνέχεια βλέπει μια περίληψη της ψηφοφορίας του και αν είναι έτοιμος επιλέγει επόμενο όπου σε αυτό το σημείο η ψήφος του κρυπτογραφείτε με ένα δημόσιο κλειδί και στέλνετε στον server και τότε ο ψηφοφόρος θα λάβει με sms στο κινητό του τον κωδικό επαλήθευσης που αναφέραμε πιο πάνω.

Η βασική διαφορά του συστήματος αυτού με το Εσθονικό σύστημα είναι ότι χρησιμοποιεί αυτά τα δύο κανάλια επαλήθευσης κάτι το οποίο το κάνει περισσότερο ασφαλές από το Εσθονικό σύστημα ψηφοφορίας όπως επίσης το Νορβηγικό σύστημα υπερισχύει στο σύστημα ελέγχου. Ακόμη η βασική αρχιτεκτονική και στα δύο συστήματα είναι η ίδια. Επίσης στο Εσθονικό σύστημα δεν υπάρχει η δυνατότητα να συσχετιστεί η ψήφος με τον ψηφοφόρο κάτι το οποίο υπάρχει στο Νορβηγικό σύστημα. Στο Εσθονικό σύστημα ο ψηφοφόρος δεν μπορεί να υποβάλει λευκό ψηφοδέλτιο κάτι το οποίο είναι εφικτό στο Νορβηγικό σύστημα. Ακόμη το Εσθονικό σύστημα

χρησιμοποιεί ομομορφικό μηχανισμό ενώ το Νορβηγικό κάνει χρήση του μηχανισμού mix-net που είναι πιο αποτελεσματικός. Στο Νορβηγικό σύστημα όμως δεν υπάρχει πρόβλεψη για την ψηφοφορία μέσω κινητού κάτι το οποίο έχει καταφέρει με επιτυχία το Εσθονικό σύστημα. Ακόμη το Νορβηγικό σύστημα διαθέτει αυτοματοποιημένο τρόπο διαχείρισης του συστήματος ενώ στο Εσθονικό η διαδικασία αυτή γίνεται από τον administrator χειρονακτικά. Συμπερασματικά το Νορβηγικό σύστημα είναι πιο ασφαλές αν και έχει και αυτό κάποια «τρωτά» σημεία στην ασφάλεια του.

- **Venezuelan 2012 Presidential Election vs United States 2012 Presidential Election**

Τα δύο αυτά συστήματα χρησιμοποιήθηκαν το ίδιο έτος. Η προσέλευση των ψηφοφόρων για το σύστημα της Βενεζουέλας ήταν 75% και για το σύστημα των Ηνωμένων Πολιτειών 61.8%.Όσο αφορά την ασφάλεια της ψηφοφορίας την ευθύνη για το υλικό για την Βενεζουέλα την είχε ο στρατός ενώ για τις Ηνωμένες Πολιτείες η αστυνομία. Ακόμη σε ότι είχε σχέση με την ασφάλεια του υλικού του λογισμικού και των βάσης δεδομένων του συστήματος ηλεκτρονικής ψηφοφορίας για την Βενεζουέλα ο έλεγχος γινόταν από ειδικούς τεχνικούς ενώ για τις Ηνωμένες Πολιτείες οι πληροφορίες αυτές ήταν μυστικές και άνηκαν μόνο στην εταιρία που διαχειριζόταν το λογισμικό του συστήματος.

Το σύστημα της Βενεζουέλας λαμβάνει τις ψήφους κρυπτογραφημένες επίσης οι ειδικοί είναι αυτοί που ελέγχουν τις μηχανές για κακόβουλο λογισμικό η οτιδήποτε άλλο μπορεί να βλάψει το σύστημα κάτι το οποίο δεν βλέπουμε στο σύστημα ηλεκτρονικής ψηφοφορίας των Ηνωμένων Πολιτειών όπου εκεί η κρυπτογράφηση είναι ανύπαρκτη ενώ έλεγχος γίνεται μόνο σε ότι αφορά την λειτουργικότητα του συστήματος. Σε ότι έχει σχέση με την επαλήθευση των ψήφων στο σύστημα της Βενεζουέλας το σύστημα αυτό ενεργοποιείται με το id των ψηφοφόρων και τα δακτυλικά τους αποτυπώματα σε αντίθεση με το σύστημα των Ηνωμένων πολιτειών όπου τα ονόματα των ψηφοφόρων βρίσκονται σε χαρτί τα οποία ελέγχονται από δικαστές.

Η μυστικότητα της ψήφου στο σύστημα της Βενεζουέλας εξασφαλίζεται καθώς το λογισμικό ανακατεύει την ψήφο και το id του ψηφοφόρου και τα ταξινομεί διαφορετικά ώστε να μην είναι δυνατόν να συσχετιστεί η ψήφος με τον ψηφοφόρο κάτι το οποίο δεν συμβαίνει στο σύστημα των Ηνωμένων Πολιτειών. Στο σύστημα της Βενεζουέλας ο ψηφοφόρος λαμβάνει ένα αντίγραφο της εγγραφής του τυπωμένο και μπορεί να συγκρίνει την έντυπη μορφή της

ψηφοφορίας με την ηλεκτρονική αλλά αντίθετα στο σύστημα των Ηνωμένων Πολιτειών δεν υπάρχει κάποια επαλήθευση και η ηλεκτρονική ψηφοφορία λαμβάνεται ως επίσημη χωρίς καμία επαλήθευση.

6.1.3 Παραδείγματα χρήσης ηλεκτρονικής ψηφοφορίας

Κάποια από τα πιο γνωστά παραδείγματα χρήσης συστημάτων ηλεκτρονικής ψηφοφορίας είναι και τα εξής:

- **Voting Over the Internet (VOI)**

  Το 2000, το πρόγραμμα στήριξης της ομοσπονδιακής ψηφοφορίας (FVAP) εφάρμοσε ένα πιλοτικό πρόγραμμα που ονομάζεται «Ψήφος μέσω του Internet» (VOI) για να δει αν θα μπορούσαν οι ψήφοι να καταγραφούν αξιόπιστα και ασφαλή μέσω του Internet. Το πρόγραμμα ήταν μέτριο σε μέγεθος 84 εθελοντές, 21 μέλη και 11 χώρες χρησιμοποίησαν το σύστημα για να ρίξουν ψηφοδέλτια για τις εκλογές στις 7 Νοεμβρίου του 2000.Συμμετείχαν επιλεγμένες κομητείες της Νότιας Καρολίνας, Florida, Texas και Utah.

  Η πρωτοβουλία του VOI σηματοδότησε την πρώτη φορά που στις Ηνωμένες Πολιτείες οι ψηφοφόροι χρησιμοποιούν το Διαδίκτυο σε ομοσπονδιακό, κρατικό και τοπικό εκλογικό αποτέλεσμα. Για να διαβεβαιώσουν τους εθελοντές ότι οι ψήφοι τους θα υπολογίζονται σε περίπτωση ενός αποτυχημένου πειράματος, ο κάθε εθελοντής είχε επίσης τη δυνατότητα να ρίξει μια παραδοσιακή(βασισμένη σε χαρτί) επιστολική ψήφο.Το FVAP σχεδίασε το σύστημα μιμούμενο τα ήδη ιδρυμένα επιστολικά ψηφοδέλτια. Δεν έκαναν όμως το σύστημα σχεδιασμένο για να καταμετρά ψήφους. Κάθε εθελοντής έλαβε ένα CD που είχε ένα browser plug-in που σχεδιάστηκε για να διαβιβάζει τα ψηφοδέλτια στους FVAP servers. Το σύστημα προϋποθέτει ότι οι εθελοντές χρησιμοποιούν το Netscape Navigator 4,05.

  Το Υπουργείο Άμυνας (DOD) εισήγαγε ένα ψηφιακό πρόγραμμα πιστοποίησης για την εξακρίβωση της γνησιότητας της ταυτότητας των ψηφοφόρων. Μόλις ένας ψηφοφόρος διαβίβαζε ένα ψηφοδέλτιο, το DOD θα ενεργοποιούσε την πιστοποίηση για να τον εμποδίσει να ψηφίσει πάλι. Τα κωδικοποιημένα ψηφοδέλτια μεταδίδονται μέσω του Internet στο διακομιστή FVAP. Μόνο ο προορισμός του ψηφοδελτίου παρέμενε μη κρυπτογραφημένος. Ο server ήταν σε ασφαλή θέση, με πολύ περιορισμένη πρόσβαση και αδιάλειπτη παροχή ρεύματος. Δυο συστήματα ανίχνευσης εισβολέων είχαν εγκατασταθεί για την παρακολούθηση για τυχόν απόπειρες δόλιων δραστηριοτήτων. Οι τοπικοί υπάλληλοι των εκλογών (LEOs) χρησιμοποιούσαν

τερματικά στους δικούς τους δικτυακούς τόπους για να αποκτήσουν πρόσβαση στο διακομιστή LEO. Αυτός ο server συνδέεται με του FVAP server, το οποίο διαβιβάζει τα κρυπτογραφημένα ψηφοδέλτια που απευθύνονται στο site του LEO μέσω του Internet. Μόλις φτάσουν τα ψηφοδέλτια, ένας ηλεκτρονικός υπολογιστής από την τοποθεσία LEO τα αποκρυπτογραφεί και οι εκτυπωτές παράγουν αντίγραφα σε χαρτί.

Οι εθελοντές του LEO μεταγράφουν τα εκτυπωμένα αποτελέσματα σε χάρτινα ψηφοδέλτια. Η ασφαλής ηλεκτρονική καταχώρηση και το πείραμα της ψηφοφορίας μετά την επιτυχία του VOI, ζητήθηκε από το Κογκρέσο η σύσταση ενός μεγαλύτερου προγράμματος ψηφοφορίας που να βασίζεται στο Internet. Το 2001, στο DOD άρχισαν να σχεδιάζουν το Secure Electronic Registration and Voting Experiment (SERVE) .Στη DOD εκτιμάται ότι 100000 πολίτες θα συμμετάσχουν στο πείραμα, και οι ψήφοι τους θα συνυπολογίζονται τόσο στις τοπικές όσο και στις γενικές εκλογές του 2004. Αν το πείραμα θεωρηθεί ότι ήταν μια επιτυχία, η ψηφοφορία μέσω Internet πρέπει να επεκταθεί σε όλο το στρατιωτικό προσωπικό και σε άλλους πολίτες.

Στις αρχές του 2004, το πείραμα DOD ακυρώθηκε λόγω ανησυχιών για θέματα ασφαλείας και το πρόγραμμα έληξε πριν από την φάση της υλοποίησης. Συγκεκριμένες ανησυχίες των ψηφοφόρων συμπεριλαμβανομένης της ανωνυμίας έτειναν να υπονομευθούν και ψηφοδέλτια των χακερς στέλνονταν μεθοδευμένα μέσω του Internet.

Το κογκρέσο ζήτησε από την DOD να προσπαθήσει ξανά, αφού το πείραμα της Εκλογικής Επιτροπής Βοηθείας (που θεσπίστηκε από τη HAVA) δημιουργεί νέες κατευθυντήριες γραμμές για τη ψηφοφορία και την καταγραφή του 2007. Τα προγράμματα VOI και SERVE σχεδιάστηκαν για να παρέχουν καλύτερη πρόσβαση στους ψηφοφόρους που βρίσκονται στο εξωτερικό γιατί αλλιώς θα έπρεπε να προσμετρηθούν τα επιστολικά ψηφοδέλτια. Τέτοιοι εκλογείς ανέρχονται σε εκατοντάδες χιλιάδες, και αυτό το μερίδιο συνθέτει μόνο ένα μικρό ποσοστό του συνολικού αριθμού των εγγεγραμμένων ψηφοφόρων. Ψηφοφορίες που βασίζονται στο Internet θα πρέπει να ικανοποιήσουν τους σκεπτικιστές με ασφαλή και αξιόπιστα παραδείγματα καταγραφής και διαβίβασης ψηφοδελτίων. Είναι πιθανόν να περάσουν πολλά χρόνια προτού δούμε το Internet να χρησιμοποιείται ως ένα σημαντικό σύστημα ψηφοφορίας στις Ηνωμένες Πολιτείες.

- **Diebold:**

Η ομάδα αξιολόγησης του Argonne Laboratory ανακάλυψαν ότι οι μηχανές ηλεκτρονικής ψηφοφορίας, με οθόνη αφής Diebold, θα μπορούσαν να δεχθούν απομακρυσμένη επίθεση στο λογισμικό τους. Τα μηχανήματα αυτά ήταν μεγίστης σημασίας διότι προορίζονταν για τις εκλογές τις Αμερικής το 2012. Η απομακρυσμένη επίθεση θα μπορούσε να γίνει ως εξής: καθώς ο ψηφοφόρος πατούσε το κουμπί για να εγγραφεί η ψήφος του, ο απομακρυσμένος επιτιθέμενος θα μπορούσε να χρησιμοποιήσει μια ραδιοσυχνότητα απομακρυσμένα για να υποκλέψει την επικοινωνία αυτή να αλλάξει την ψήφο και στην συνέχεια να την υποβάλει στο σύστημα.

Το ίδιο πρόβλημα αντιμετώπισαν οι ερευνητές και με τα συστήματα ηλεκτρονικής ψηφοφορίας Sequoia το 2009.Η επίθεση αυτή θα μπορούσε να γίνει από κάποιον που δεν διαθέτει εξειδικευμένες γνώσεις πάνω στο αντικείμενο και με κόστος μόνο 29$. Γι' αυτό το λόγο, ερευνητές από το πανεπιστήμιο του Σικάγο απέδειξαν ότι οι δύο τύποι ηλεκτρονικών συσκευών που χρησιμοποιούνται στις σημερινές εκλογές είναι σχεδόν πανεύκολο να "πειραχτούν" από οποιονδήποτε έχει βασικές τεχνικές γνώσεις hacking, με τη μέθοδο "man-in-the-middle".

Η μέθοδος αυτή απαιτεί την τοποθέτηση ενός μικροεπεξεργαστή ή άλλου ηλεκτρονικού μέσου μέσα στην ηλεκτρονική συσκευή ψηφοφορίας (και μάλιστα με κόστος μόλις $10-$26), έτσι ώστε να είναι εφικτή η ενεργοποίηση ή όχι του cheat για την αλλαγή της ψήφου ανάλογα με την επιθυμία του "κλέφτη".Όπως αναφέρει στο παράδειγμα της η ιστοσελίδα Popular Science, απαιτείται η παρουσία κάποιου χειριστή της hackαρισμένης συσκευής για να αλλάζει τις ψήφους (αν χρειάζεται) αμέσως μετά το πάτημα του κουμπιού από τον ψηφοφόρο, κάτι που είναι σχετικά εύκολο από τη στιγμή που οι ηλεκτρονικές συσκευές ψηφοφορίας βρίσκονται συνήθως παρατημένες και απροστάτευτες για τουλάχιστον ένα μήνα σε σχολεία, εκκλησίες και άλλα εκλογικά κέντρα.

Οι ερευνητές "πείραξαν" πιο εύκολα τις συσκευές της Sequoia (μέσα σε μόλις 2 ώρες), οι οποίες διαθέτουν hardware κουμπιά και χρησιμοποιούνται σε 4 πολιτείες για να εξυπηρετήσουν περίπου 9 εκατ. ψηφοφόρους, ενώ δυσκολεύτηκαν ελαφρώς με τις touchscreen συσκευές της Diebold (εξυπηρετούν περίπου 26 εκατ. ψηφοφόρους σε 20

πολιτείες) επειδή δεν είχαν αρκετές γνώσεις για τις οθόνες αφής.Παρόλα αυτά, τα κατάφεραν μέσα σε λίγες ημέρες και το κυριότερο, δε συνάντησαν κανένα εμπόδιο από το λογισμικό των συσκευών για να αλλάζουν τις ψήφους.

- **DS200 optical scanning device**

  Αυτή η συσκευή ηλεκτρονικής ψηφοφορίας οπτικής σάρωσης προοριζόταν να χρησιμοποιηθεί για προεδρικές κατά το έτος 2012 όμως διαπιστώθηκαν κάποιες «ανωμαλίες» σύμφωνα με κυβερνητική έκθεση όπως σφάλματα στην καταγραφή των ψήφων.Η επίσημη όμως έκθεση δόθηκε από την Electronic Assistance Commission (EAC) η οποία πιστοποιεί μηχανές ηλεκτρονικής ψηφοφορίας σύμφωνα με την οποία η συσκευή DS200 optical scanning παρουσιάζει περιοδικά «πάγωμα» της οθόνης,κλείδωμα του συστήματος,<στράβωμα> του ψηφοδελτίου με αποτέλεσμα σημαντικές επιπτώσεις στο αποτέλεσμα,όπως επίσης δεχόταν το ψηφοδέλτιο σε μια γωνία και έκανε αποδεκτό το ψηφοδέλτιο χωρίς να έχει καταγραφεί η ψήφος και τα ειδικά σήματα που απαιτούνταν η έκδοση αυτή χρησιμοποιήθηκε μόνο στο Ohio και Wisconsin,ωστόσο σύμφωνα με ανακοίνωση της ES&S αναφέρεται ότι τα προβλήματα αυτά έχουν και λυθεί και όσες χώρες χρησιμοποιούσαν την έκδοση 3.2.0.0 πρέπει να προχωρήσουν σε αναβάθμιση χρησιμοποιώντας την έκδοση 3.4.0.0.

- **Secure Electronic Registration and Voting Experiment (SERVE)**

  Τα κράτη της States of Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, και Washington συμφώνησαν συμφώνησαν να συμμετάσχουν στο Secure Electronic Registration and Voting Experiment (SERVE) ένα πείραμα το οποίο θα χρησιμοποιούνταν για τις εκλογές του Νοεμβρίου του 2004, 55 νομοί από Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah και Washington συμφώνησαν να συμμετέχουν ωστόσο το πείραμα αυτό ακυρώθηκε λόγω ανησυχίας σε θέματα ασφάλειας διότι η χρήση προσωπικών υπολογιστών μέσω διαδικτύου δεν θα ήταν ασφαλείς.

  Η αρχιτεκτονική του SERVE ήταν ένα κεντρικό περιβάλλον φιλοξενείας όπου η πρόσβαση των ψηφοφόρων θα γινόταν μέσω των προσωπικών τους υπολογιστών και με ελάχιστες απαιτήσεις συμβατότητας.Το σύστημα χρησιμοποιούσε SSL 3.0 με session keys, και κρυπτογράφηση με ψηφιακή υπογραφή (SHA1 with DSA).Το λογισμικό του συστήματος αποτελείται από 8 ολοκληρωμένα υποσυστήματα:

Αναγνώριση και ταυτοποίηση, κοινές υπηρεσίες, εγγραφή ψηφοφόρων, διαχείριση ψηφοφορίας, ορισμός ψηφοδελτίου, ψηφοφορία, λήψη και αποκρυπτογράφηση, και υπολογισμός. Υπήρχε μια SFTP σύνδεση με την βάση δεδομένων εγγραφής του ψηφοφόρου για την λήψη των εφαρμογών εγγραφής στους εκλογικούς καταλόγους που υποβλήθηκαν σύμφωνα με το local election jurisdiction (LEO).Κάθε LEO είχε ένα laptop για την λήψη αποκρυπτογράφηση και καταγραφή των ψήφων από κεντρικό περιβάλλον φιλοξενίας.

Οι δυνατότητες των τοπικών υπαλλήλων των εκλογών περιελάμβαναν την εγγραφή των ψηφοφόρων την αποκρυπτογράφηση και την καταγραφή των ψήφων.Οι ψηφοφόροι έπρεπε να χρησιμοποιούν έναν υπολογιστή που έτρεχε Netscape or Internet Explorer as the web browser ο ψηφοφόρος απαιτούνταν να έχει ένα ψηφιακό πιστοποιητικό SERVE. Οι υπηρεσίες του συστήματος για τους ψηφοφόρους περιελάμβανε online εγγραφή και upload της ψήφου μεταφορά ψηφοδελτίου και συλλογή του ψηφοδελτίου.Μετά την ολοκλήρωση της ψηφοφορίας του ψηφοφόρου οι επιλογές του ψηφοφόρου μεταφέρονταν σε μια προσωρινή μνήμη στην βάση δεδομένων εγγραφής στον κεντρικό servers στην συνέχεια ερχόταν μια επιβεβαίωση στον ψηφοφόρο ότι η ψήφος του καταχωρήθηκε και η ψήφος έμενε εκεί μέχρι να γίνει download από το LEO.

- **Helios σύστημα ηλεκτρονικής ψηφοφορίας**

Το Helios είναι ένα δωρεάν σύστημα ηλεκτρονικής ψηφοφορίας που αναπτύχθηκε από έναν μη κερδοσκοπικό οργανισμό άτομα που έγραψαν τον κώδικα είναι οι :Ben Adida, Olivier de Marneffe, Olivier Pereira.Έχει χρησιμοποιηθεί από αρκετούς οργανισμούς όπως τις προεδρικές εκλογές του ULC university το 2009, στο Princenton university το 2009 καθώς και στο International Association of Cryptographic Research (IACR) το 2010.Μια τυπική ψηφοφορία με το Helios απαιτεί αρχικά την συμπλήρωση ενός online ψηφοδελτίου και μετά κάνοντας click σε ένα κουμπί κάνει την κρυπτογράφηση για να κρύψει το περιεχόμενο του. Τότε αποστέλλονται στους ψηφοφόρους αριθμοί που μπορούν να παρακολουθήσουν τις ψήφους τους τα λεγόμενα ‘fingerprints’. Τέλος υποβάλλουν τις ψήφους τους επαληθεύοντας τις ταυτότητες τους. Στις περισσότερες περιπτώσεις αυτό γίνετε με το να συνδέονται στην εξωτερική πλατφόρμα που απαιτείται.

Οι ψηφοφόροι αν θέλουν να ελέγξουν ότι η ψήφος τους καταμετρήθηκε μπορούν να πάνε στο website της ψηφοφορίας και να ελέγξουν αν ταιριάζει ο αριθμός που τους δόθηκε με το όνομα τους. Ωστόσο υπάρχει και ένα δεύτερο επίπεδο επιβεβαίωσης που επιτρέπει στους ψηφοφόρους να έχουν πρόσβαση στα δεδομένα της ψηφοφορίας κάτι το οποίο προϋποθέτει την γνώση κάποιου επιπέδου μαθηματικών κάτι το οποίο δεν είναι δυνατό για όλους τους ψηφοφόρους αν και όπως παραδέχεται ο Adida αυτή είναι μια από τις σοβαρότερες επικρίσεις του συστήματος αλλά προσδοκά ότι κάθε υποψήφιος θα έχεις τουλάχιστον ένα έμπιστο άτομο με αυτές τις γνώσεις ώστε να έχει πρόσβαση.

Το Helios είναι από τα πιο πολυχρησιμοποιημένα συστήματα και τώρα βρίσκεται στην έκδοση 3.0 . Από διάφορες μελέτες που έχουν γίνει, αρνητικά του συστήματος είναι ότι οι χρήστες που χρειάζονται βοήθεια με κάτι μπορούν να επικοινωνήσουν μόνο με ηλεκτρονικό ταχυδρομείο (μη πρακτικό) και ότι η διαδικασία επαλήθευσης της ψήφου από τον χρήστη είναι αρκετά περίπλοκη. Έχουν γίνει διάφορες επιθέσεις στο παρελθόν που εκμεταλλεύονταν τις αδυναμίες του και γι αυτό για λόγους χρηστικότητας έγιναν οι αναβαθμίσεις. Το σύστημα helios σχεδιάστηκε από ακαδημαϊκούς ερευνητές, παρακολουθείται όμως και συντηρείται από ιδιωτική πλατφόρμα (https://github.com/) κατανεμημένου συστήματος ελέγχου.

Ο δικτυακός αυτός τόπος είναι “τρίτος” προς την διαδικασία εκλογής Συμβουλίων Ιδρύματος.Αλλά και η διαμεσολάβηση του Υπουργείου ή άλλου φορέα στη συλλογή και έκδοση αποτελεσμάτων αποτελεί παραβίαση της αυτοδιοίκησης των ιδρυμάτων. Δεν μπορούμε να συμμετάσχουμε σ' αυτή τη διαδικασία που δεν ελέγχεται από το ίδιο το δημόσιο Πανεπιστήμιο. Πώς να συμμετάσχει κανείς σε μια παρωδία όπου το εκλογικό σύστημα είναι ευάλωτο σε επιθέσεις που μπορεί να οδηγήσουν σε αλλοίωση του αποτελέσματος; Άλλωστε όλοι γνωρίζουμε ότι η διέλευση εμπιστευτικού περιεχομένου από μη ασφαλή μέσα, όπως το διαδίκτυο και οι φυλλομετρητές (browsers), εμπεριέχει μεγάλο κίνδυνο να παραβιαστεί το απόρρητο της ψήφου, με παρέμβαση τρίτων ή με επιθέσεις αλλά και να αλλοιωθεί το αποτέλεσμα.

Τα υπάρχοντα μέτρα προφύλαξης είναι αναποτελεσματικά.Ειδικότερα για το σύστημα Helios στη βιβλιογραφία αναφέρονται εργασίες που αποδεικνύουν ότι εύκολα μπορεί να αλλοιωθεί το αποτέλεσμα και δεν μπορεί να διασφαλιστεί επιστημονικά η μυστικότητα της ψήφου και έτσι δεν είναι σε θέση τουλάχιστον ακόμη να χρησιμοποιηθεί σε εκλογές για κάποιο αξίωμα. Υπάρχουν σενάρια επιθέσεων που αποδεικνύουν ότι μπορεί να αποκαλυφθεί τι θα ψήφιζε κάποιος.

6.2 Υπάρχοντα συστήματα

6.2.1 *Sensus:* A Security-Conscious Electronic Polling System for the Internet.

Το Sensus είναι ένα πρακτικό και ασφαλές σύστημα για διεξαγωγή δημοσκοπήσεων (ακόμη και εκλογών) μέσω δικτύων. Με το Sensus εξασφαλίζεται όχι μόνο ότι οι εγγεγραμμένοι ψηφοφόροι μπορούν να ψηφίσουν μια και μοναδική φορά αλλά ταυτόχρονα να διατηρήσει τη μυστικότητα του ψηφοφόρου. Το συγκεκριμένο σύστημα επιτρέπει στο ψηφοφόρο να επαληθεύσει, ατομικά, ότι η ψήφος του μετρήθηκε σωστά και ανώνυμα να ελέγξει την ορθότητα των αποτελεσμάτων της ψηφοφορίας.

Το Sensus σχεδιάστηκε αρχικά για να αντικαταστήσει τα συστήματα ψηφοφορίας μέσω ταχυδρομείου. Η ευελιξία του όμως το έκανε να εξυπηρετεί και μια ποικιλία άλλων εκλογικών διαδικασιών συμπεριλαμβανομένων και αυτών που δεν είναι δυνατόν να διεξαχθούν με χρήση των παραδοσιακών εκλογικών συστημάτων. Είναι ένα εύκολα προσαρμόσιμο αρθρωτό σύστημα.

Το πρωτόκολλο ψηφοφορίας του απαιτεί την ύπαρξη ενός συστήματος επιβεβαιωτή (validator), ενός συστήματος καταμετρητή (tallier) και ενός συστήματος διεξαγωγής της δημοσκόπησης (pollster). Άλλα επιπρόσθετα συστήματα μπορούν να αυξήσουν την λειτουργικότητα του Sensus. Τα υποσυστήματα του Sensus ανταποκρίνονται στα χαρακτηριστικά ενός καλού συστήματος ψηφοφορίας. Το πρωτόκολλο Sensus χρησιμοποιεί blindsignatures προκειμένου να παρέχει ασφάλεια ενώ ταυτόχρονα προστατεύει την μυστικότητα του χρήστη. Ο χρήστης πρέπει να ετοιμάσει την ψήφο του, να την κρυπτογραφήσει με ένα μυστικό κλειδί και να την αποκρύψει (blind). Στη συνέχεια ο ψηφοφόρος υπογράφει την ψήφο και την αποστέλλει στον επιβεβαιωτή (validator) [12]. Ο επιβεβαιωτής επικυρώνει ότι η υπογραφή (signature) ανήκει σε εξουσιοδοτημένο χρήστη ο οποίος δεν έχει ψηφίσει ακόμη. Εάν η ψήφος είναι έγκυρη, ο επιβεβαιωτής υπογράφει την ψήφο και την επιστρέφει στον ψηφοφόρο. Ο ψηφοφόρος αφαιρεί το στρώμα απόκρυψης (blinding layer) και αποκαλύπτει ένα κρυπτογραφημένο μήνυμα υπογεγραμμένο από τον επιβεβαιωτή, το οποίο αποστέλλει στον καταμετρητή (tallier). Ο καταμετρητής ελέγχει την υπογραφή πάνω στο κρυπτογραφημένο ψηφοδέλτιο.

Εάν η ψήφος είναι έγκυρη ο καταμετρητής την τοποθετεί σε μια λίστα με έγκυρες ψήφους, η οποίο θα δημοσιευτεί μετά το τέλος της ψηφοφορίας. Στη συνέχεια ο καταμετρητής υπογράφει την κρυπτογραφημένη ψήφο και την επιστρέφει σαν απόδειξη στον ψηφοφόρο. Μόλις ο ψηφοφόρος λάβει την απόδειξη αποστέλλει στον καταμετρητή το κλειδί κρυπτογράφησης. Ο

καταμετρητής χρησιμοποιεί το κλειδί για να αποκρυπτογραφήσει την ψήφο και να προσθέσει την ψήφο στο τελικό αποτέλεσμα.

6.2.2 Το σύστημα E-Vox

Χάρη στις τελευταίες εξελίξεις στον τομέα της κρυπτογραφίας μπορούμε να δημιουργήσουμε ένα ασφαλές ηλεκτρονικό σύστημα ψηφοφορίας. Το σύστημα αυτό, που ονομάζεται E-Vox συνδυάζει την ευελιξία ενός συστήματος VBM (Vote By Mail) με την ταχύτητα και την ισχύ των σύγχρονων υπολογιστών. Το σύστημα σχεδιάστηκε να είναι στο σύνολο του φιλικό προς το χρήστη. Με τον όρο φιλικό προς το χρήστη εννοούμε ότι ο εκάστοτε ψηφοφόρος χρειάζεται να εκτελέσει τον ελάχιστο αριθμό βημάτων που απαιτεί η εκλογική διαδικασία και τίποτα άλλο. Τα δύο απαραίτητα βήματα στην όλη διαδικασία είναι η εγγραφή και η ψηφοφορία. Από τη μεριά του ψηφοφόρου και τα δύο βήματα εκτελούνται εύκολα και γρήγορα.

Η εγγραφή απαιτεί την προσέλευση του ψηφοφόρου στο κατάλληλο γραφείο εγγραφών, μαζί με τα απαραίτητα δικαιολογητικά. Η διαδικασία της ψηφοφορίας απαιτεί την ύπαρξη ενός υπολογιστή, την εισαγωγή των προσωπικών στοιχείων πρόσβασης και την επιλογή των απαντήσεων. Ο ψηφοφόρος μπορεί να φύγει όντας σίγουρος ότι η διαδικασία ολοκληρώθηκε με ασφάλεια και αξιοπιστία, όπως στα παραδοσιακά συστήματα.

Το E-Vox μπορεί να υποστηρίξει εκλογές στις οποίες συμμετέχουν εκατοντάδες ή μερικές χιλιάδες άνθρωποι. Με έναν ικανοποιητικά γρήγορο server το μέγεθος αυτό μπορεί να αυξηθεί σε μερικές δεκάδες χιλιάδες. Στην πραγματικότητα τα όρια περιορίζονται από την ταχύτητα και το μέγεθος του server και το εύρος των συνδέσεων που μπορούμε να επιτύχουμε.Το σύστημα E-Vox σχεδιάστηκε σαν βελτίωση άλλων παλαιότερων και κάνει πολύ λίγες υποθέσεις σχετικά με το περιβάλλον στο οποίο λειτουργεί. Έτσι δεν χρειάζεται να υποθέσουμε ότι προϋπάρχει οποιοδήποτε σύστημα δημοσίου κλειδιού ή άλλο στοιχειώδες κρυπτογραφικό σύστημα στον τόπο λειτουργίας. Ωστόσο πρέπει να κάνουμε κάποιες υποθέσεις:

- Τα κρυπτογραφικά συστήματα που χρησιμοποιούνται είναι δύσκολο να σπάσουν
- Κάθε ένα από τα εμπλεκόμενα μέρη: ψηφοφόρος, διαχειριστής, σύστημα διατήρησης ανωνυμίας και καταμετρητής δεν έρχονται σε σύγκρουση μεταξύ τους.

6.2.3 Η λειτουργία του E-vox

Ο ψηφοφόρος επιλέγει τις απαντήσεις που επιθυμεί και δημιουργεί ένα «αντικείμενο», το οποίο περιέχει το ψηφοδέλτιο με τις επιλογές του.Στη συνέχεια κρυπτογραφείται με χρήση μιας hash συναρτήσεως. Συγκεκριμένα χρησιμοποιείται η HMAC-SHA [13], η οποία απαιτεί δύο κλειδιά. Η συνάρτηση αυτή εκτός από την κρυπτογράφηση επιτρέπει τη χρήση μικρότερων σε μέγεθος μηνυμάτων, τα οποία στη συνέχεια υπογράφονται. Τα hash μηνύματα στη συνέχεια αποκρύπτονται (blinded) και αποστέλλονται στο διαχειριστή προκειμένου να υπογραφούν. Ο διαχειριστής επιβεβαιώνει την εγκυρότητα του ψηφοφόρου να συμμετάσχει στη διαδικασία, ελέγχει το κωδικό πρόσβασης του (password) και ελέγχει αν ο χρήστης έχει ήδη ψηφίσει. Εάν όλοι οι έλεγχοι είναι επιτυχείς ο διαχειριστής υπογράφει την ψήφο του και την επιστρέφει στον αποστολέα.

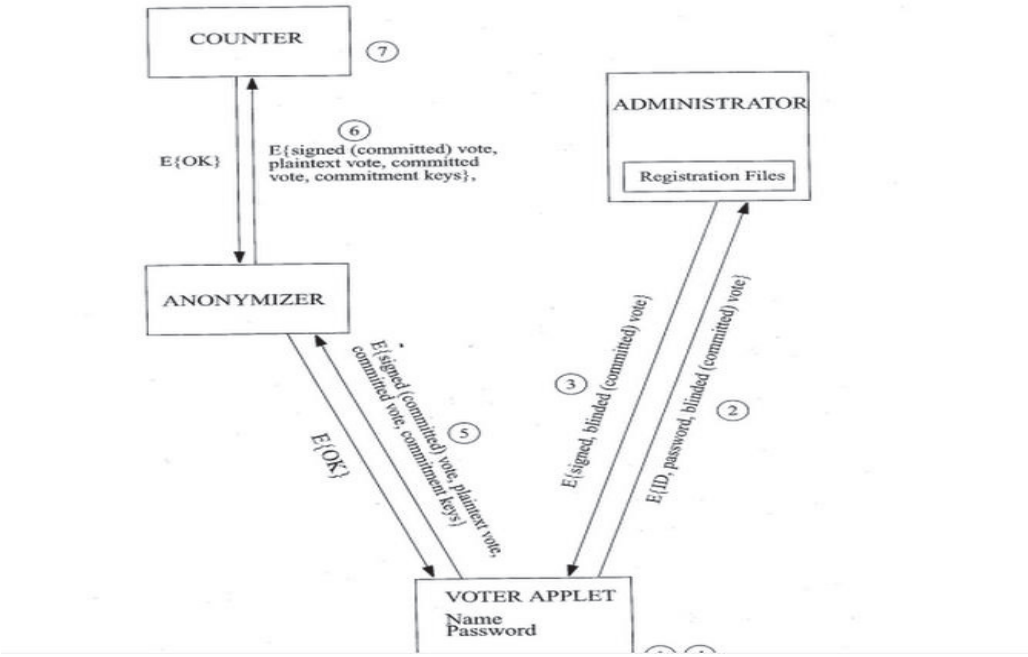
Μετά το πέρας της δημοσκόπησης ο διαχειριστής δημοσιεύει τα ονόματα των ψηφοφόρων, τις αποκρυμμένες ψήφους τους και τις αντίστοιχες υπογραφές που ο ίδιος τοποθετεί. Μόλις ο ψηφοφόρος λάβει την υπογεγραμμένη ψήφο, η εφαρμογή (το κατάλληλο λογισμικό δηλαδή) επιβεβαιώνει την υπογραφή του διαχειριστή και αποκαλύπτει (unblinds) το ψηφοδέλτιο. Η υπογραφή συνεχίζει να ισχύει για το κρυπτογραφημένο, αλλά όχι πλέον αποκρυμμένο ψηφοδέλτιο. Στη συνέχεια δημιουργείται μια ασφαλής σύνδεση με τον καταμετρητή. Πάνω από αυτή τη σύνδεση υπάρχει μια ασφαλής σύνδεση με τον ανώνυμο εξυπηρετητή. Η εφαρμογή αποστέλλει το απλό κείμενο της ψήφου, τα κλειδιά που χρησιμοποιεί για την κρυπτογράφηση, την κρυπτογραφημένη ψήφο και την υπογεγραμμένη κρυπτογραφημένη ψήφο.

Ο πλεονασμός αυτός είναι πολύ χρήσιμος προκειμένου να γίνουν όλοι οι απαραίτητοι έλεγχοι ενάντια σε κάθε λάθος. Τόσο ο ανώνυμος χρήστης, όσο και ο καταμετρητής αποστέλλουν απαντήσεις. Κάτω από φυσιολογικές περιστάσεις και οι δύο θα απαντήσουν με ένα OK. Εάν κάτι πάει στραβά, κάθε ένας μπορεί να απαντήσει με ένα μήνυμα «διαμαρτυρίας» στον εκάστοτε χρήστη. Αυτή η απάντηση δεν είναι απαραίτητη στο πρωτόκολλο και για το λόγο αυτό δεν αναφέρεται ρητά. Εν τούτοις οι απαντήσεις αυτές είναι ένας καλός μηχανισμός ελέγχου.

Οι απαντήσεις κρυπτογραφούνται με χρήση του session key που επιλέγει ο χρήστης. Το session key κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη κατά τη διάρκεια της μετάδοσης από τον αποστολέα στον παραλήπτη. Μόνο ο σωστός παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα προκειμένου να πάρει το session key με το οποίο θα δημιουργήσει τη σωστή απάντηση. Ο ανώνυμος εξυπηρετητής «σώζει» κάθε ψηφοδέλτιο σε ξεχωριστό αρχείο, στο οποίο δεν περιέχεται καμία πληροφορία σχετικά με την πηγή του. Μετά

το πέρας της ψηφοφορίας, ο ανώνυμος εξυπηρετητής αποστέλλει τις ψήφους με χρήση ενός κανονικού καναλιού, με τυχαία σειρά στον καταμετρητή.

Οι ψήφοι είναι ακόμη κρυπτογραφημένες με το δημόσιο κλειδί του καταμετρητή επειδή το χαμηλότερο επίπεδο της ασφαλούς σύνδεσης είναι ενεργό. Μόλις τελειώσει η μετάδοση, ο ανώνυμος εξυπηρετητής δημοσιεύει μια λίστα με τα μηνύματα που έστειλε. Η λίστα που δημοσιεύεται είναι ανακατεμένη για λόγους ασφαλείας. Ο καταμετρητής αρχικά απομακρύνει οποιοδήποτε διπλότυπο ψήφου. Στη συνέχεια επιβεβαιώνει τις υπογραφές που έχει τοποθετήσει ο διαχειριστής και παράγει μια λίστα με το απλό κείμενο των ψήφων, τα κρυπτογραφημένα κλειδιά και τις υπογεγραμμένες ψήφους.Όλες οι λίστες δημοσιεύονται μετά το πέρας κάθε ψηφοφορίας. Οποιοσδήποτε μπορεί να επιβεβαιώσει ότι οι υπογραφές του διαχειριστή είναι έγκυρες, ότι καμία επιπλέον ψήφος δεν καταμετρήθηκε και ότι το τελικό αποτέλεσμα είναι σωστό.



Εικόνα 7: Η διαδικασία λειτουργίας του E-VOX

6.2.4 Το απόλυτο σύστημα ψηφοφορίας "Direct Recording Election"

Οι τεχνολογίες πληροφορικής έχουν δημιουργήσει το απόλυτο σύστημα ψηφοφορίας «Direct Recording System». Το σύστημα αυτό καταγράφει τα αποτελέσματα πλήρως και με ακρίβεια.Με ένα σύστημα που βασίζεται σε έντυπα, το ηλεκτρονικό εξάρτημα είναι συνήθως μια συσκευή πινακοποίησης. Αυτό σημαίνει ότι οι ψήφοι μετριούνται από ένα ηλεκτρονικό σύστημα, το οποίο είναι πολύ πιο γρήγορο από την καταμέτρηση με το χέρι. Ορισμένα συστήματα εκτύπωσης ψηφοδελτίων μοιάζουν με τα DRE συστήματα. Οι ψηφοφόροι χρησιμοποιούν μια οθόνη touchscreen ή παρόμοια ηλεκτρονική συσκευή για να κάνουν τις επιλογές τους. Όταν ο εκλογέας καταθέσει τη ψήφο του, ένας εκτυπωτής συνδεδεμένος με τη συσκευή παράγει ένα χάρτινο ψηφοδέλτιο. Ένας εκλογικός υπάλληλος ή ένας επίσημος εθελοντής λαμβάνει όλα τα ψηφοδέλτια σε χαρτί, που παράγονται σε μια κεντρική τοποθεσία, για να τα καταμετρήσουν μόλις κλείσουν οι κάλπες.

Μια ξεχωριστή ηλεκτρονική συσκευή σαρώνει οπτικά αυτά τα ψηφοδέλτια και εκδίδει τα αποτελέσματα. Ένα από τα πλεονεκτήματα ενός συστήματος που βασίζεται σε χαρτί είναι ότι η ψηφοφορία αντιπροσωπεύεται φυσικά από ένα κομμάτι χαρτί. Αυτό διαβεβαιώνει ότι οι επιλογές των ψηφοφόρων συνυπολογίζονται. Ακόμη, ένα φυσικό ψηφοδέλτιο δεν διασφαλίζει ότι μια ψηφοφορία θα μετρηθεί σωστά. Πολλοί παράγοντες μπορούν να συμβάλλουν σε μια εσφαλμένη εφαρμογή ψηφοφορίας.Οι τρύπες στις κάρτες δεν μπορούν να ευθυγραμμισθούν πλήρως στην μεμβράνη, με αποτέλεσμα να μετρηθούν λανθασμένα, όπως έγινε το 2000 στις κακόφημες εκλογές στη Φλόριντα.

Σχετικά με τις κάρτες οπτικής σάρωσης, μερικά σήματα ή ελλιπείς σημάνσεις μπορούν να παρερμηνευθούν, όταν μετριούνται. Στους εκτυπωτές οπτικού σήματος, που μπορούν να σαρώσουν κάρτες, εξαντλείται συχνά το μελάνι, με αποτέλεσμα τα ελλιπή εύληπτα σήματα στις κάρτες. Μπορεί επίσης να είναι δυνατό για έναν ψηφοφόρο να ψηφίσει δυο ή περισσότερους υποψηφίους για μια ενιαία θέση, που είναι γνωστό ως overvoting, αυτές οι επιλογές, δεν μετριούνται από τις συσκευές.Τα φυσικά ψηφοδέλτια μπορούν να χαθούν ή να καταστραφούν πριν από την καταμέτρηση. Ακόμη, είναι πολύ πιο δύσκολο να χαθούν χάρτινα ψηφοδέλτια από ο, τι είναι να χάσουμε μια ηλεκτρονική καταγραφή των άυλων.

6.2.5 Pericles (MIT)

Στο MIT οι φοιτητικές εκλογές διεξάγονται τόσο ηλεκτρονικά όσο και με την παραδοσιακή τους μορφή (χάρτινα ψηφοδέλτια), σε διαφορετικές περιόδους. Το ηλεκτρονικό σύστημα ψηφοφορίας, γνωστό ως Pericles, αναπτύχθηκε από τον Paul Kirby. Παρά το ότι είναι ένα σύστημα που βασίζεται στη γλώσσα C «τρέχει» μέσω Mosaic. Υπάρχουν όμως δύο μειονεκτήματα σε αυτό το σύστημα. Πρώτον, βασίζεται στο σύστημα Kerberos για πιστοποίηση ταυτοτήτων και κρυπτογράφηση μηνυμάτων, πράγμα το οποίο καθιστά την χρήση του στο ευρύ κοινό περιορισμένη. Δεύτερον, είναι ένα σύστημα με ένα μόνο εξυπηρετητή server. Έχει σχεδιαστεί ώστε να προστατεύει τη μυστικότητα των φοιτητών και να διασφαλίζει μια δίκαιη εκλογική διαδικασία, όμως οποιοσδήποτε έχει πρόσβαση στον εξυπηρετητή μπορεί να «νικήσει» το σύστημα.

6.2.6 Το ηλεκτρονικό σύστημα ψηφοφορίας της Ιταλικής Ακαδημαϊκής Κοινότητας

Η Ιταλική ακαδημαϊκή κοινότητα υλοποίησε ένα σύστημα ψηφοφορίας το οποίο αποτελείται από τα επόμενα συστατικά:

- Την αρχή έκδοσης πιστοποιητικών Δημοσίου Κλειδιού,
- Το κεντρικό εκλογικό γραφείο,
- Την κεντρική κάλπη,
- Το σταθμό ψηφοφορίας,
- Το δίκτυο επικοινωνίας.

Πολλά διαφορετικά στάδια πρέπει να ακολουθηθούν συμπεριλαμβανομένης της έκδοσης έξυπνων καρτών, της έκδοσης λίστας έγκυρων ψηφοφόρων, την παραγωγή προσωπικών κωδικών και κλειδιών αναγνώρισης για κάθε χρήστη, τη διανομή σταθμών ψηφοφορίας και τερματικών, τη στράτευση ανθρώπινου δυναμικού, προκειμένου να γίνει δυνατή η χρήση του συστήματος. Η εκλογική διαδικασία αποτελείται από συνολικά 16 διαφορετικές φάσεις.

6.2.7 TrueBallot, Inc. Democratic Governance Systems

Άλλο ένα σύστημα που σήμερα είναι διαθέσιμο για ψηφοφορία μέσο Internet είναι αυτό που προσφέρει η TrueBallot, Inc. Democratic Governance Systems . Είναι ένα πρότυπο on line σύστημα ψηφοφορίας το οποίο σχεδιάστηκε από την εταιρία με βάση την εμπειρία που απέκτησε από την διαχείριση ψηφοφοριών για οργανισμούς, σωματεία εργαζομένων και εταιρίες.Είναι μια ευέλικτη, ασφαλής και οικονομικά συμφέρουσα προσέγγιση, στην προσπάθεια που γίνεται να εμπλακεί το Internet στην εκλογική διαδικασία. Η βάση δεδομένων της TrueBallot παρέχει πολλαπλά επίπεδα ασφάλειας και μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να ψηφίσουν. Κάθε χρήστης ψηφίζει μόνο μια φορά. Η TrueBallot προσφέρει μια νέα προσέγγιση στην εκλογική διαδικασία, η οποία μπορεί να χρησιμοποιηθεί είτε ανεξάρτητα είτε σε συνδυασμό με τον παραδοσιακό τρόπο ψηφοφορίας.

6.2.8 Vivarto Voting Systems

Το σύστημα που παρέχει η εταιρία Vivarto (http://www.vivarto.com/) προσφέρει μια νέα δυνατότητα στον τομέα της πληροφορικής και των νέων τεχνολογιών επικοινωνίας. Η εφαρμογή μπορεί να χρησιμοποιηθεί από εταιρίες, πανεπιστήμια, πιθανόν κυβερνήσεις και κάθε είδους σωματείο ή ομάδα ατόμων. Σκοπός του συστήματος είναι να βοηθήσει στην επικοινωνία και τη λήψη αποφάσεων και εγγυάται αποτελεσματικότητα, δημιουργικότητα και εξασφάλιση των δημοκρατικών διαδικασιών.

6.2.9 Clear vote

Όταν οι πολίτες των Ηνωμένων Πολιτειών της Αμερικής αντικατέστησαν της μηχανές ηλεκτρονικής ψηφοφορίας με μηχανές οπτικής σάρωσης που χρησιμοποιούσαν χαρτί μερικοί πίστευαν ότι οι εκλογές θα γίνουν περισσότερο διαφανής και επαληθεύσιμες.Ένα νέο εκλογικό σύστημα υποσχόταν να λύσει τα προβλήματα της ψηφοφορίας δίνοντας στους εκπροσώπους των ψηφοφοριών την ικανότητα να ελέγχουν γρήγορα τις μηχανές οπτική σάρωσης, το όνομα του ήταν clear vote το σύστημα αυτό σχεδιάστηκε μετά από έλεγχο σε συστήματα που χρησιμοποιούνταν στην Καλιφόρνια το 2008.

Το Clear vote χρησιμοποιεί υψηλές ταχύτητες στους σαρωτές και είχε δημιουργηθεί από την Fjitsu το λογισμικό του αναπτύχθηκε από την ομάδα Clear Ballot μέσα στην ομάδα αυτή ήταν και ένας πρώην προγραμματιστής που εργαζόταν για την δημιουργία του Lotus Notes.Το σύστημα δοκιμάστηκε σε διάφορες χώρες της Florida το προηγούμενο έτος. Αλλά

δοκιμάστηκε ακόμη περισσότερο στις επερχόμενες προεδρικές εκλογές που έγιναν σε επτά νομούς της Florida όπου χρησιμοποιήθηκε για τον έλεγχο των εκλογικών αποτελεσμάτων. Είναι η πρώτη μεγάλης κλίμακας ψηφοφορία όπου ψηφοφόρος μπορεί να ψηφίζει παντού.
Η σάρωση των ψηφοδελτίων γίνεται πρώτα από τους πωλητές πριν σαρωθούν για δεύτερη φορά από τους σαρωτές της Fujitsu στο clear ballot.Η καταμέτρηση γινόταν συνδέοντας ένα φορητό υπολογιστή με τους σαρωτές της Fujitsu μέσω ενός usb καλωδίου. Στη συνέχεια επεξεργάζεται τις εικόνες των ψηφοδελτίων για να παραχθούν κοιτάξουν γρήγορα τα ψηφοδέλτια για να δουν αν υπάρχει κάποια διαφορά και αναλόγως κρίνουν αν θα αποδεχτούν ως έγκυρη την ψήφο. Η Καλιφόρνια καθώς και άλλα κράτη απαιτούν μετεκλογικούς ελέγχους επιλέγοντας τυχαία 1% των ψήφων σαν ένα τρόπο για να εντοπιστούν οι δυσλειτουργίες του συστήματος.Στόχος των clear vote είναι να παραχθεί ένα γρήγορο αποτέλεσμα μετά την λήξη της ψηφοφορίας.
Το clear vote ωστόσο χρησιμοποιήθηκε για τον έλεγχο αρχειοθετημένων ψηφοδελτίων από τις προεδρικές εκλογές του 2008 στο Ion Sancho όπου αποκάλυψε 40 ψηφοδέλτια τα οποία δεν είχαν καταμετρηθεί λόγω κάποιου λάθους των εκλογικών εκπροσώπων το σύστημα επίσης βρήκε και 9 ψηφοδέλτια τα οποία είχαν διπλή ψήφο και δεν είχαν ανιχνευθεί από τα scanners της ψηφοφορίας.Στις επερχόμενες προεδρικές εκλογές το clear ballot θα χρησιμοποιηθεί σε έξι νομούς Leon,Bay, Okaloosa, Indian River, Madison και Duval County η δοκιμή θα περιλαμβάνει περίπου 900.000 ψηφοδέλτια. Το clear vote είναι ένα εξελιγμένο σύστημα όπου δημιουργεί ένα αρχείο ψηφοφορίας για κάθε τύπο ψηφοφορίας το σύστημα δεν στηρίζεται σε ένα αρχείο που δημιουργήθηκε από τους εκπροσώπους της ψηφοφορίας για τις μηχανές σάρωσης συσκευή σάρωσης ψηφοφορίας χρησιμεύει ως μηχανισμός ελέγχου για την κωδικοποίηση τους συστήματος ενώ το clear vote είναι ένας μηχανισμός ελέγχου για την συσκευή σάρωσης.

6.2.10 Premier/Diebold AccuVote TS

Το Accuvote TS είναι μια μηχανή ηλεκτρονικής ψηφοφορίας με οθόνη αφής με VVPAT (voter-verified paper audit trail) στις εκλογές του 2012 το Accuvote TS χρησιμοποιήθηκε σε τέσσερα κράτη (AL, GA, MD, και UT) και σε ορισμένες δικαιοδοσίες σε 18 πολιτείες (Αριζόνα, Καλιφόρνια, Κολοράντο, Φλόριντα, Ιλινόις, Ιντιάνα, Κάνσας, Κεντάκι, MS, MO, OH, PA, TN, Τέξας, Βιρτζίνια, Ουάσιγκτον, WI, και WY).Η λειτουργία του είναι ως εξής: Τοποθετείτε η κάρτα πρόσβασης των ψηφοφόρων στην υποδοχή στα δεξιά της οθόνης η κάρτα θα πρέπει να έρθει στην ίδια ευθεία με το αριστερό βέλος ώστε να εφαρμοστεί κατάλληλα στην υποδοχή

μέχρι να ασφαλίσει. Πριν ξεκινήσει ο ψηφοφόρος την ψηφοφορία μπορεί να μεγεθύνει την εικόνα ώστε να είναι πιο εύκολη η αναγνωσιμότητα.Για να ξεκινήσει η ψηφοφορία ο ψηφοφόρος πρέπει να πατήσει στο κουμπί next το κουμπί αυτό θα χρησιμοποιείτε σε κάθε σελίδα της ψηφοφορίας ώσπου να φτάσει στο τέλος.

Για την επιλογή του υποψηφίου ο ψηφοφόρος πρέπει να αγγίξει το πλαίσιο που βρίσκεται δίπλα στην επιλογή του και για να αλλάξει την επιλογή του πρέπει να πατήσει ξανά στο ίδιο πλαίσιο αν υπάρχει write-in τότε μπορεί κάποιος να επιλέξει και ένα πληκτρολόγιο και να πληκτρολογήσει το όνομα που θέλει στην συνέχεια πρέπει να επιλεχθεί το Record Write-In το σύστημα θα συλλέξει το όνομα που καταχωρήθηκε και να επανεξεταστούν οι προηγούμενες σελίδες πρέπει να επιλεγεί το κουμπί back όπως επίσης ο ψηφοφόρος μπορεί να επιλέξει το print ballot και να εκτυπώσει το αντίγραφο των επιλογών του μετά από την εκτύπωση μπορεί να καταχωρήσει την ψήφο του αγγίζοντας την επιλογή cast ballot και μόλις ολοκληρωθεί αυτή η διαδικασία πρέπει να επιλέξει το remove card και στη συνέχεια να επιστραφεί η κάρτα στον εκπρόσωπο της ψηφοφορίας.

Εικόνα 8: Εφαρμογή συστημάτων ηλεκτρονικής ψηφοφορίας στην Ελλάδα και τα προβλήματα που παρουσιαστήκαν κατά την εφαρμογή του.

6.3.1 Ζευς

Η «Ψηφιακή Κάλπη Ζευς» είναι ένα πληροφοριακό σύστημα για την αδιάβλητη διεξαγωγή απόρρητων ψηφοφοριών με αμιγώς ηλεκτρονικό τρόπο. Τόσο η προετοιμασία της ψηφοφορίας από τη διεξάγουσα αρχή, όσο και η υποβολή της ψήφου από τους ψηφοφόρους, γίνονται απομακρυσμένα μέσω Διαδικτύου. Το σύστημα Ζευς βασίζεται στην υλοποίηση ηλεκτρονικής ψηφοφορίας όπως περιγράφηκε στην αρχική δημοσίευση του συστήματος Helios. Στο σύστημα αυτό οι ψηφοφόροι λαμβάνουν στην ηλεκτρονική τους διεύθυνση μήνυμα με το οποίο καλούνται να ψηφίσουν. Το μήνυμα περιέχει σύνδεσμο (link) που οδηγεί στο ψηφιακό παραπέτασμα μέσα στο οποίο προετοιμάζεται η ψήφος. Το παραπέτασμα θα ενεργοποιηθεί όταν η εφορευτική επιτροπή εκκινήσει την ψηφοφορία.

Η εφορευτική επιτροπή δίνει τους χρόνους έναρξης και λήξης της ψηφοφορίας.Οι ψηφοφόροι ψηφίζουν εντός του ορισμένου χρονικού διαστήματος,και λαμβάνουν ψηφιακή απόδειξη της συμμετοχής τους. Με το πέρας της ψηφοφορίας, η εφορευτική επιτροπή δίνει την εντολή για την αυτόματη καταμέτρηση των ψηφοδελτίων. Οι ψηφοφόροι υποβάλλουν κρυπτογραφημένα ψηφοδέλτια τα οποία ανακατεύονται ώστε να διατηρείται η ανωνυμία των ψηφοφόρων, αλληλουχία που αποτελεί τη βάση του συστήματος Ζευς.

Σε μεταγενέστερες υλοποιήσεις του Helios, όπως και στη σημερινή υλοποίησή του, εγκαταλήφθηκε αυτή η προσέγγιση και παραλήφθηκε το στάδιο της ανάμιξης των ψηφοδελτίων, καθώς αυτό δεν είναι απαραίτητο σε περιπτώσεις όπου δεν απαιτείται καν η αποκρυπτογράφηση των ψηφοδελτίων για την εξαγωγή των αποτελεσμάτων. Τέτοιες περιπτώσεις είναι οι εκλογικές αναμετρήσεις όπου οι ψηφοφόροι επιλέγουν υποψήφιους (για παράδειγμα με σταυρό) και εκλέγονται οι υποψήφιοι με το μεγαλύτερο αριθμό σταυρών (approval voting). Τότε η εξαγωγή των αποτελεσμάτων μπορεί να γίνει με κρυπτογραφικές (ομομορφικές) πράξεις πάνω στα κρυπτογραφημένα ψηφοδέλτια. Αυτό δεν είναι δυνατόν στις περιπτώσεις που απαιτείται γνώση της πλήρους δομής του ψηφοδελτίου και όχι των ανεξάρτητων επιλογών σε αυτό, όπως για παράδειγμα στο σύστημα της ταξινομικής ψήφου (Single Transferable Vote).

Η πρόσβαση των ψηφοφόρων στο πληροφοριακό σύστημα Ζευς επιτυγχάνεται μέσω ενός απλού προγράμματος περιήγησης στον Παγκόσμιο Ιστό (web browser), ενώ προστατεύεται όπως ακριβώς και οι οικονομικές συναλλαγές μέσω Διαδικτύου. Οι ψηφοφόροι ψηφίζουν εντός του καθορισμένου χρονικού διαστήματος, και λαμβάνουν ψηφιακή απόδειξη της συμμετοχής τους. Η ακεραιότητα της ψηφοφορίας είναι μαθηματικά επαληθεύσιμη μέσω της χρήσης κρυπτογραφίας και χωρίς καμία προσβολή του απορρήτου. Το σύστημα Ζευς,

κληρονομώντας από το σύστημα Helios, απαγορεύει τη μεταβολή των υποψηφίων μετά την οριστικοποίησή της. Ταυτόχρονα, η ενημέρωση των ψηφοφόρων γίνεται μέσω αποστολής ηλεκτρονικών μηνυμάτων που τους προσκαλούν να ψηφίσουν, μπορεί να γίνει μόνο μετά την οριστικοποίηση της ψηφορορίας από την εφορευτική επιτροπή.

Στην πρώτη ψηφοφορία του «Ζευς», για το Χαροκόπειο Πανεπιστήμιο, ένας υποψήφιος παραιτήθηκε μετά την Οριστικοποίηση και πριν την επίσημη έναρξη της ψηφοφορίας, δημιουργώντας έτσι την ανάγκη μεταβολής της λίστας των υποψηφίων. Επειδή τη μεταβολή την απαγόρευε το σύστημα, ακυρώθηκε η ψηφοφορία και δημιουργήθηκε νέα, σε ελάχιστο χρόνο, πριν την προγραμματισμένη επίσημη έναρξη. Για την αποφυγή τέτοιων περιστατικών στο μέλλον, η ομάδα ανάπτυξη διερεύνησε την αλλαγή της διαδικασίας ώστε να επιτρέπεται στην εφορευτική επιτροπή να μεταβάλλει τη λίστα των υποψηφίων πριν τη επίσημη έναρξη της ψηφοφορίας. είναι πρακτικά εξασφαλισμένο καθώς μπορεί να παραβιαστεί μόνο με συνεννόηση όλων των μελών της εφορευτικής επιτροπής και του διαχειριστή του συστήματος Ζευς.Η ανάπτυξη νέων λειτουργιών δεν γίνεται στο σύστημα της παραγωγής. Η ομάδα ανάπτυξης δημιουργεί και ελέγχει το λογισμικό σε ξεχωριστά συστήματα πριν την ενεργοποίηση των νέων εκδόσεων στον εξυπηρετητή παραγωγής του «Ζευς». Παρ' όλα αυτά, κατά τη διάρκεια της διερεύνησης μία γραμμή εκ του συνόλου του κώδικα δοκιμών διέφυγε και εισήλθε στον κώδικα παραγωγής.

Ποια όμως ήταν η ακριβής φύση του σφάλματος; Το σύστημα Helios, και κατ' επέκταση και το «Ζευς», μεταξύ άλλων χρησιμοποιεί 5 μεταβλητές για τη χρονική τοποθέτηση των ψηφοφοριών:

- 1. voting_starts_at -- ο προγραμματισμένος χρόνος έναρξης
- 2. voting_started_at -- ο πραγματικός χρόνος έναρξης
- 3. voting_ends_at -- ο προγραμματισμένος χρόνος λήξης
- 4. voting_extended_until -- ο χρόνος μετά την παράταση
- 5. voting_ended_at -- ο πραγματικός χρόνος λήξης

Οι πραγματικοί χρόνοι μπορούν να διαφέρουν από τους προγραμματισμένους για να μπορεί ο διαχειριστής της ψηφοφορίας να δίνει ρητές εντολές κατά τη δική του κρίση και απόφαση. Στον ακόλουθο σύνδεσμο, στο ιστορικό του δημόσιου αποθετηρίου του συστήματος «Ζευς», φαίνεται η ακριβής γραμμή του αρχείου που δημιουργούσε το σφάλμα, όπως ίσχυε στο σύστημα το πρωί της 24^{ης} Οκτωβρίου και το προηγούμενο διάστημα από τη στιγμή της οριστικοποίησης της συγκεκριμένης ψηφοφορίας. Αναλυτικά:

https://github.com/grnet/zeus/blob/0329f1988894cffe67bc4450da0e81c64c0f14b7/helios/models.py#L747

Η γραμμή αυτή βρίσκεται μέσα στη συνάρτηση freeze(), η οποία πραγματοποιεί την Οριστικοποίηση:

> self.voting_started_at = datetime.datetime.utcnow()

η γραμμή αυτή ρητά---και εσφαλμένα---καταχωρεί την παρούσα στιγμή της Οριστικοποίησης ως τη στιγμή της έναρξης. Η γραμμή αυτή έπρεπε να λείπει εντελώς, αφού η καταγραφή της στιγμής της Οριστικοποίησης έχει γίνει στην προηγούμενη γραμμή, και δεν υπάρχει ανάγκη για παραπέρα καταγραφή χρόνων.

Αμιγώς τεχνικά, το σφάλμα δεν είναι σοβαρό για την ακεραιότητα του συστήματος. Δεν προκύπτει κανένα τεχνικό ζήτημα για την κρυπτογραφική ακεραιότητα της ψηφοφορίας, ούτε για την επαλήθευση, αλλά ούτε και για την ανωνυμία. Ο κρυπτογραφικός πυρήνας του συστήματος είναι ανεξάρτητος και δεν επηρεάστηκε από την αλλαγή που προαναφέρθηκε. Η σοβαρότητα του σφάλματος προκύπτει κυρίως από τη διατάραξη της προδιαγεγραμμένης διαδικασίας των εκλογών. Οι εκλογές θα μπορούσαν και να συνεχιστούν κανονικά, αφού δεν υπάρχει τρόπος να παραβιαστεί η ανωνυμία και το απόρρητο των ψήφων που είχαν καταχωρηθεί. Σε περίπτωση που οι ήδη ψηφίσαντες ψηφοφόροι κατέθεταν νέα ψήφο, δεν θα προέκυπτε διπλή ψήφος, αλλά η καταμέτρηση θα λάμβανε υπόψη μόνο την τελευταία ψήφο τους.

Το σφάλμα διορθώθηκε με απλή αφαίρεση της προσβάλλουσας γραμμής στο λογισμικό, ενώ έχουν προγραμματιστεί αντίστοιχοι έλεγχοι ώστε να μην επανεμφανιστεί.

6.3.2 ΠΝΥΚΑ

Ο τομέας ηλεκτρονικής διακυβέρνησης του Ερευνητικού Ακαδημαϊκού Ινστιτούτου Τεχνολογίας Υπολογιστών (ΕΑΙΤΥ) της Πάτρας σε συνεργασία με την εταιρία EXPERTNET - Προηγμένες Εφαρμογές Α.Ε δημιούργησε το σύστημα υποστήριξης ηλεκτρονικών ψηφοφοριών ΠΝΥΚΑ[19]. Βασικός στόχος του έργου ΠΝΥΚΑ (http://www.pnyka.cti.gr)_ήταν ο καθορισμός και εφαρμογή ενός ολοκληρωμένου πλαισίου (framework) για την ανάπτυξη συστημάτων e-Voting τα οποία βασίζονται σε τυπικές μεθόδους σχεδίασης και διαχείρισης κινδύνων ώστε να αντιμετωπίζονται συστηματικά από την αρχική φάση της σχεδίασης όλες οι κρίσιμες απαιτήσεις ενός τέτοιου συστήματος όπως είναι η εμπιστοσύνη σε αυτό, η ασφάλεια, η αποδοτικότητα, η επεκτασιμότητα κλπ. που αποτελούν μέρος ενός ευρύτερου πλαισίου χρήσης νέων τεχνολογιών για την επίτευξη των στόχων της ηλεκτρονικής διακυβέρνησης.

Το πλαίσιο εστιάζει στην προσέλκυση της εμπιστοσύνης του πολίτη και θα καλύπτει όλο το εύρος εφαρμογής του e-Voting. Η σύγχρονη ΠΝΥΚΑ υποστηρίζει όλα τα στάδια μιας διαδικτυακής ηλεκτρονικής ψηφοφορίας, όπως εγγραφή, πιστοποίηση, υποβολή ψήφου, καταμέτρηση αποτελεσμάτων και επαλήθευση. Ενσωματώνει σημαντικές τεχνολογικές καινοτομίες, όπως πλήρως κατανεμημένη αρχιτεκτονική, ομομορφική κρυπτογράφηση κατωφλίου, συσκευές υλικού για την αποθήκευση των κλειδιών και έχει αναπτυχθεί εξ' ολοκλήρου με εργαλεία ανοικτού κώδικα. Μπορεί δε να παραμετροποιηθεί για να υποστηρίξει διαφορετικές μορφές ψηφοφορίας, από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές και δημοψηφίσματα μεγάλης κλίμακας. Τον Ιούνιο 2008 το σύστημα ΠΝΥΚΑ συμμετείχε στο διαγωνισμό e-voting που διοργάνωσε το Competence Center for Electronic Voting and Participation, με χορηγό τον αυστριακό οργανισμό Internet Foundation Austria (IFA). Ο διαγωνισμός αφορούσε σε μη εμπορικά διαδικτυακά συστήματα ηλεκτρονικής ψηφοφορίας, που έχουν αναπτυχθεί εξ ολοκλήρου με εργαλεία ανοικτού κώδικα και είναι ο 1^{ος} που διενεργείται για συστήματα e-voting στην Ευρώπη.

Τον Ιούλιο 2008 γνωστοποιήθηκαν τα αποτελέσματα της αξιολόγησης από πενταμελή επιτροπή εμπειρογνωμόνων σύμφωνα με το οποία το σύστημα ΠΝΥΚΑ μπήκε στην τελική τριάδα μαζί με δύο άλλα τα οποία αναπτύχθηκαν από μια αυστριακή και μια γερμανική ομάδα αντίστοιχα. Τα τρία συστήματα παρουσιάστηκαν στις 6 Αυγούστου 2008 στο Bregenz της Αυστρίας στο πλαίσιο του 3^{ου} Διεθνούς Συνεδρίου στο e-Voting (http://www.e-voting.cc/topics/conference2008/). Έγινε επίσης επίδειξη μιας ηλεκτρονικής ψηφοφορίας και ακολούθησε ανοικτή συνεδρία ερωτήσεων – απαντήσεων ενώπιον της επιτροπής.

Η διαδικασία της τελικής αξιολόγησης ανέδειξε το σύστημα ΠΝΥΚΑ νικητή του διαγωνισμού και η νίκη συνοδεύτηκε με χρηματικό έπαθλο 3000€.Βασικοί συντελεστές της επιτυχίας αυτής ήταν ο καθηγητής και διευθυντής του ΕΑΙΤΥ κ. Π. Σπυράκης, που ήταν και ο επιστημονικός υπεύθυνος του έργου, τα στελέχη του Τομέα Ηλεκτρονικής Διακυβέρνησης του ΕΑΙΤΥ, κ.κ. Χ. Μανωλόπουλος και Δ. Σοφοτάσιος, καθώς και ο επ. καθηγητής κ. Ι. Σταματίου, στέλεχος του Τομέα Ασφάλειας του ΕΑΙΤΥ, οι μηχανικοί ανάπτυξης του Τομέα Ηλεκτρονικής Διακυβέρνησης κ. Α. Παναγιωτάκη, Π. Νάκου, Δ. Σαλούρος, Γ. Αβραμίδης και ο Α. Τατάκης από την EXPERTNET. Η σπουδαία αυτή διάκριση αποδεικνύει και την ουσιαστική συμβολή του ελληνικού ερευνητικού δυναμικού στην ανάπτυξη καινοτομίας και στην προώθηση της έρευνας που συντελείται σε διεθνές επίπεδο.

Οι επιμέρους στόχοι του έργου ήταν οι εξής:

- Η σχεδίαση και υλοποίηση ενός πληροφοριακού συστήματος ηλεκτρονικών ψηφοφοριών ικανό να υποστηρίξει τεχνικά από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές μεγάλης κλίμακας.
- Η εφαρμογή τυπικών μεθόδων σχεδίασης έτσι ώστε να είναι εφικτός ο συστηματικός έλεγχος όλων των φάσεων ανάπτυξης του συστήματος καθώς και αντίστοιχες παρεμβάσεις, όπου απαιτούνται.
- Η σχεδίαση των συστατικών μερών του συστήματος με τρόπο που να τα καθιστά επαναχρησιμοποιήσιμα, υπό μορφή βιβλιοθηκών.
- Η ενσωμάτωση του απαιτούμενου βαθμού εμπιστοσύνης στο τελικό σύστημα κατά τη φάση σχεδίασής του καθώς και κατά τη διάρκεια λειτουργίας του με βάση ένα μοντέλο εμπιστοσύνης η οποία θεωρεί την εμπιστοσύνη ως μία ιδιότητα που κτίζεται σταδιακά από το φυσικό επίπεδο του συστήματος μέχρι και τον τρόπο παρουσίασής του στους χρήστες.

Το τελικό προϊόν του έργου ήταν ένα πρωτότυπο πλήρους συστήματος υποστήριξης ηλεκτρονικής ψηφοφορίας το οποίο ολοκληρώθηκε σε δύο στάδια. Στο πρώτο στάδιο υλοποιήθηκε ένα βασικό σύστημα που υποστηρίζει δημοσκοπήσεις και διαδικασίες εκλογών περιορισμένης κλίμακας και στο δεύτερο στάδιο ενσωματώθηκε στο βασικό σύστημα ένα σύνολο επιπλέον συστατικών (components) συνθέτοντας ένα πρωτότυπο πλήρους συστήματος για την υποστήριξη δημοψηφισμάτων και εκλογών εθνικής εμβέλειας. Το βασικό σύστημα χρησιμοποιήθηκε σε μια δοκιμαστική ηλεκτρονική ψηφοφορία μεταξύ 200 μελών του ΤΕΕ Δυτικής Ελλάδας και λειτούργησε χωρίς προβλήματα.

Στο πλαίσιο ανάπτυξης του τελικού προϊόντος αναπτύχθηκαν επίσης:

- Η τεκμηρίωση της ορθότητας και ασφάλειας του συστήματος βασισμένη στην εφαρμογή τυπικών μεθοδολογιών,
- Το μοντέλο εμπιστοσύνης του συστήματος,
- Το θεωρητικό (μαθηματικό) μοντέλο για την εκτίμηση της απόδοσης εφαρμογής του συστήματος σε μεγάλη κλίμακα και επαλήθευση του μοντέλου με τη χρήση προσομοιωτικών μεθόδων και τέλος
- Η βιβλιοθήκη με τα συστατικά μέρη του συστήματος (library of components) που αποτελούν διακριτές και εύκολα επαναχρησιμοποιήσιμες λειτουργίες σε διαφορετικές εκδόσεις ενός συστήματος eVoting ή σε άλλα παρόμοια συστήματα

Οι επιμέρους στόχοι του έργου είναι:

- Η σχεδίαση και υλοποίηση ενός πληροφοριακού συστήματος ηλεκτρονικών ψηφοφοριών ικανό να υποστηρίξει τεχνικά από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές μεγάλης κλίμακας
- Η εφαρμογή τυπικών μεθόδων σχεδίασης έτσι ώστε να είναι εφικτός ο συστηματικός έλεγχος όλων των φάσεων ανάπτυξης του συστήματος καθώς και αντίστοιχες παρεμβάσεις ,όπου απαιτούνται
- Η σχεδίαση των συστατικών μερών του συστήματος με τρόπο που να τα καθιστά επαναχρησιμοποιήσιμα υπό μορφή βιβλιοθηκών.
- Η ενσωμάτωση του απαιτούμενου βαθμού εμπιστοσύνης στο τελικό σύστημα κατά τη φάση σχεδίασης του καθώς και κατά την διάρκεια λειτουργίας του με βάση μια αρχιτεκτονική εμπιστοσύνης η οποία θεωρεί την εμπιστοσύνη ως μια ιδιότητα που κτίζεται σταδιακά από το φυσικό επίπεδο του συστήματος μέχρι και τον τρόπο παρουσίασης του στους χρήστες.

Το τελικό προϊόν του έργου θα είναι ένα πρωτότυπο πλήρους συστήματος υποστήριξης ηλεκτρονικής ψηφοφορίας το οποίο θα ολοκληρωθεί σε δύο στάδια.Στο πρώτο στάδιο θα υλοποιηθεί ένα βασικό σύστημα που θα μπορεί να υποστηρίξει δημοσκοπήσεις και διαδικασίες εκλογών περιορισμένης κλίμακας και στο δεύτερο θα ενσωματωθεί στο βασικό σύστημα σε ένα σύνολο επιπλέον συστατικών(components) συνθέτοντας ένα πρωτότυπο πλήρους συστήματος για την υποστήριξη δημοψηφισμάτων και εκλογών εθνικής εμβέλειας.

Στο πλαίσιο ανάπτυξης του τελικού προϊόντος θα αναπτυχθούν επίσης:

- Η τεκμηρίωση της ορθότητας και ασφάλειας του συστήματος βασισμένη στην εφαρμογή τυπικών μεθοδολογιών
  (μοντέλο εμπιστοσύνης του συστήματος βασισμένο στη σχεδίαση του συστήματος με βάση μια ιεραρχική αρχιτεκτονική εμπιστοσύνης όπως έχει προταθεί και εφαρμοστεί από το EAITY.
- Το θεωρητικό (μαθηματικό) μοντέλο για την εκτίμηση της απόδοσης εφαρμογής του συστήματος σε μεγάλη κλίμακα και επαλήθευση του μοντέλου με τη χρήση προσομοιωτικών μεθόδων.
- Η βιβλιοθήκη με τα συστατικά μέρη του συστήματος που μπορούν να αποτελέσουν διακριτές και εύκολα επαναχρησιμοποιήσιμες λειτουργίες σε διαφορετικές εκδόσεις ενός συστήματος evoting είτε σε άλλα παρόμοια συστήματα.

6.3.3 Η εμπειρία του δήμου Αμαρουσίου

Ο δήμος Αμαρουσίου διοργάνωσε το 2004 ηλεκτρονικό «δημοψήφισμα» για να εκφράσουν οι δημότες τις απόψεις τους για κάποια θέματα.Το έργο χρηματοδοτήθηκε κατά 50% από την Ευρωπαϊκή Ένωση μέσα στα πλαίσια του προγράμματος IST(information society technologies).Για το σκοπό αυτό πραγματοποιήθηκαν στο δήμο Αμαρουσίου 5 ψηφοφορίες στις οποίες συμμετείχαν μόνο πολίτες του δήμου και κάτοικοι της περιοχής,οι οποίοι καλούνταν να εκφράσουν τη γνώμη τους σχετικά με διάφορα θέματα που αφορούσαν το δήμο.Το περιεχόμενο των ψηφοφοριών ήταν το εξής:

- Ολυμπιακοί αγώνες και δήμος Αμαρουσίου
- Ποιότητα παρεχομένων υπηρεσιών από το δήμο
- Προβλήματα και υποχρεώσεις του επιχειρηματικού κόσμου
- Πολεοδομικός σχεδιασμός
- Ποιότητα ζωής

Όπως είναι λογικό, η πιο δύσκολη ψηφοφορία ήταν η πρώτη και αυτό διότι θα έπρεπε να γίνουν όλες οι απαραίτητες εκείνες ενέργειες,οι οποίες θα βοηθούσαν στην ομαλή διεξαγωγή της ψηφοφορίας και σχετίζονταν με την ενημέρωση πολιτών,την εγκατάσταση υπολογιστών που ια διευκόλυναν την ψηφοφορία πολιτών που δεν διέθεταν υπολογιστή, η δημιουργία του ψηφοδελτίου και η εγκατάσταση του ίδιου του συστήματος, ώστε να μπορέσει να ανταποκριθεί στις απαιτήσεις πού όριζε η συγκεκριμένη ψηφοφορία. Όσο αφορά την ενημέρωση των πολιτών οι ενέργειες οι οποίες έλαβαν χώρα σχετίζονταν ,κυρίως, με τη διαφημιστική εκστρατεία και ήταν οι εξής:

- Έκδοση φυλλαδίου(6000 αντίτυπα)
- Ιστοσελίδα δήμου
- Ανακοίνωση στον τύπο
- Διανομή φυλλαδίων
- Καταχωρήσεις
- Πανό

Από τα παραπάνω το πιο σημαντικό στοιχείο ήταν το φυλλάδιο και αυτό γιατί περιείχε όλες εκείνες τις πληροφορίες σχετικά με την πρωτοβουλία του δήμου Αμαρουσίου.Το συγκεκριμένο φυλλάδιο περιείχε μεταξύ άλλων ένα σύντομο μήνυμα του δημάρχου Αμαρουσίου μια περιεκτική περιγραφή του έργου e-vote τα θέματα των ψηφοφορίών,διάφορες πληροφορίες σχετικές με τη διαδικασία, τα απαραίτητα βήματα που έπρεπε να ακολουθήσει ένας πολίτης προκειμένου να λάβει μέρος στην ψηφοφορία,καθώς και ένα έντυπο συμμετοχής.

Η προετοιμασία της ψηφοφορίας περιλάμβανε τις εξής σημαντικότερες ενέργειες και διαδικασίες,οι οποίες έπρεπε να λάβουν χώρα:

- Ετοιμασία ψηφοδελτίου/ερωτηματολογίου
- Επιλογή κατάλληλων χωρών που θα λειτουργούσαν ως εκλογικά κέντρα και στα οποία θα μπορούσαν οι πολίτες να ψηφίσουν
- Συναρτήσεις με δημοτικούς οργανισμούς
- Εγγραφή ψηφοφοριών (συμπλήρωση εντύπου)
- Επίδοση κωδικών των ψηφοφόρων από το δημαρχείο,τους χώρους ψηφοφορίας και μέσω ηλεκτρονικού ταχυδρομείου.

ΚΕΦΑΛΑΙΟ 7: ΑΠΑΙΤΗΣΕΙΣ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΨΗΦΟΦΟΡΙΑΣ ΣΕ ΥΛΙΚΟ ΚΑΙ ΛΟΓΙΣΜΙΚΟ

7.1 Απαιτήσεις σε υλικό

Αρχικά πολύ σημαντικό ζήτημα είναι η επιλογή και συντήρηση κατάλληλου υλικού εξοπλισμού (hardware). Στην υπάρχουσα εκλογική διαδικασία το κυριότερο, αν όχι το μοναδικό υλικό, που χρησιμοποιείται είναι οι κάλπες και τα παραβάν. Όπως είναι προφανές δεν έχει νόημα να αναφέρουμε αυτό το θέμα ως απαίτηση ασφαλείας της συμβατικής εκλογικής διαδικασίας. Στην ηλεκτρονική ψηφοφορία, όμως, το θέμα του υλικού εξοπλισμού είναι πολύ σημαντικό. Ο τρόπος λειτουργίας του, καθώς και η ποιότητα των τμημάτων που το αποτελούν, πρέπει να είναι όσο το δυνατόν καλύτερης ποιότητας. Οι κίνδυνοι που μπορεί να προκύψουν από ελλιπές ή ελαττωματικό υλικό δεν προκύπτουν μόνο από ηθελημένη και κακόβουλη τροποποίηση του, αλλά και από ακούσια βλάβη.

Όσον αφορά την κακόβουλη τροποποίηση του υλικού εξοπλισμού πρέπει να υπάρχουν εντατικοί έλεγχοι και κατά την κατασκευή του, αλλά και κατά το χρονικό διάστημα που θα ακολουθήσει μέχρι να χρησιμοποιηθούν. Πιθανή προσπάθεια τροποποίησης των μηχανημάτων, που χρησιμοποιούνται σε μια εκλογική διαδικασία, θα πρέπει να οδηγεί είτε σε αποτυχία της προσπάθειας είτε σε καταστροφή του μηχανήματος, έτσι ώστε ένα μηχάνημα που λειτουργεί να είναι σίγουρο πως δεν έχει υποστεί τροποποίηση. Όσον αφορά τυχόν βλάβη κατά τη διάρκεια της εκλογικής διαδικασίας, πρέπει να υπάρχει ειδικευμένο και εξουσιοδοτημένο προσωπικό σε κάθε εκλογικό κέντρο, ώστε να μπορεί άμεσα να επιδιορθώνει το πρόβλημα και να αποκαθιστά την ορθή λειτουργία του υλικού. Μέχρι τώρα έχουν γίνει διάφορες προτάσεις για ειδικά

μηχανήματα που μπορούν να χρησιμοποιηθούν για μια εκλογική διαδικασία με επικρατέστερα μέχρι στιγμής τα DREs. Να αναφέρουμε πως μέσα στις ανάγκες για κατάλληλο υλικό μπορεί να αναφερθεί τυχόν χρήση έξυπνων καρτών (smart cards) για αυθεντικοποίηση των χρηστών.

7.2 Απαιτήσεις σε λογισμικό

Εξίσου σημαντικό ζήτημα είναι και η ανάπτυξη και ο έλεγχος του λογισμικού που χρησιμοποιείται. Τα σημαντικότερα θέματα που φαίνεται να σχετίζονται με το λογισμικό έχουν να κάνουν με τους κρυπτογραφικούς αλγόριθμους και με τη διαφάνεια του κώδικα. Η κρυπτογραφία είναι, ίσως, το σημαντικότερο εργαλείο για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των ψήφων, αλλά και των μηχανισμών αυθεντικοποίησης των ψηφοφόρων.

Η διαφάνεια του κώδικα είναι, επίσης, πολύ σημαντικό θέμα. Αρχικά, ο κώδικας πρέπει να είναι όσο το δυνατόν πιο απλός και ευκολονόητος, χωρίς βέβαια αυτό να σημαίνει υποβάθμιση της ασφάλειας. Όσο πιο απλός είναι ο κώδικας, τόσο πιο ευκολονόητος θα είναι και τόσο πιο εύκολος θα είναι ο έλεγχός του. Το να είναι ευκολονόητος ο κώδικας είναι βασικό στοιχείο για τη διαφάνεια του. Αυτό δεν σημαίνει βέβαια πως πρέπει οποιοσδήποτε, χωρίς κατάλληλο υπόβαθρο γνώσεων, να μπορεί να τον καταλάβει, αλλά δεν πρέπει ο κώδικας να είναι κατανοητός μόνο στην προγραμματιστική ομάδα που το δημιούργησε, όσο έμπιστη και κοινής αποδοχής και να είναι. Επίσης, ένας απλός και καλά δομημένος κώδικας μπορεί να οδηγήσει στην εύκολη και έγκαιρη ανίχνευση κάποιας προσθήκης μη εξουσιοδοτημένων τμημάτων (δούρειοι ίπποι, ιοί, κ.λπ.).

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 8^{Ο}: ΠΕΡΙΓΡΑΦΗ ΣΥΣΤΗΜΑΤΟΣ ΥΠΟΣΤΗΡΙΞΗΣ e-voting

8.1 Ιστορικά Στοιχεία για το JOOMLA

Το Joomla ανήκει στην κατηγορία των συστημάτων διαχείρισης περιεχομένου (CMS – Content Management System) καθώς και στα λογισμικά ελεύθερου πηγαίου κώδικα (open source) λογισμικά που καλύπτονται από τη δεύτερη έκδοση GNU της γενικής δημόσιας άδειας. Στην ίδια κατηγορία των συστημάτων διαχείρισης περιεχομένου ανήκουν και το Drupal αλλά και το WordPress, όπου και τα τρία αυτά συστήματα χρησιμοποιούνται ως κύριο κορμό μια ιστοσελίδας τόσο για ιδιώτες όσο και για μεγάλες επιχειρήσεις. Το Joomla αντιπροσωπεύει τα δέκα με πενήντα εκατομμύρια ιστοσελίδες παγκοσμίως ενώ αγγίζει τις 750.000 λήψεις από την ιστοσελίδα του συστήματος.

Το Joomla θεωρείται η μετεξέλιξη του λογισμικού Mambo, όπου τον Μάρτιο του 2000 η εταιρεία Miro Construct Pty Ltd ξεκίνησε την ανάπτυξη ενός ιδιόκτητου συστήματος περιεχομένου. Το Mambo παραμένει για καθαρά ιδιωτική χρήση μέχρι τα μέσα του 2002 όπου η εταιρεία παραγωγής του αποφασίζει να δημιουργήσει και μία έκδοση καθαρά εμπορική με την ονομασία Mambo 2002. Σημαντικό στοιχείο στην εξέλιξη του λογισμικού ήταν η απόφαση της εταιρείας Miro να απελευθερώσει τον κώδικα του λογισμικού στις αρχές του 2003 όπου του δόθηκε και το 1^{ο} βραβείο του 2004 για το καλύτερο ελεύθερο λογισμικό εκείνης της χρονιάς. Ωστόσο, από το τέλη του ίδιου έτους και τα τέλη του επόμενου, το λογισμικό Mambo δέχτηκε σοβαρότατες νομικές απειλές σχετικά με τα πνευματικά δικαιώματα ορισμένων κομματιών του πηγαίου του κώδικα κάτι που έκανε όλη την ομάδα των προγραμματιστών να αποχωρήσει από την τεχνική υποστήριξη του project αυτού. Έτσι, παρατηρήθηκε μια στροφή προς τη

δημιουργία ενός νέου συστήματος περιεχομένου ως καθαρή μετεξέλιξη του Mambo με την ονομασία Joomla το οποίο όμως θα έδινε μεγαλύτερη βάση σε θέματα ασφάλειας από την τελευταία έκδοση του Mambo. Με αυτή τη λογική, το Joomla στα πρώτα του χρόνια κατάφερε να αποσπάσει δύο συνεχόμενες χρονιές (2006 , 2007) το βραβείο του καλύτερου ανοιχτού κώδικα δημόσιου πακέτου/συστήματος περιεχομένου ενώ κρίθηκαν αντίστοιχα για τα επόμενα 2 χρόνια ως πιο ικανοί επαγγελματίες δύο προγραμματιστές από την ομάδα υλοποίησης του.

8.2 Ανάλυση – Δομή JOOMLA

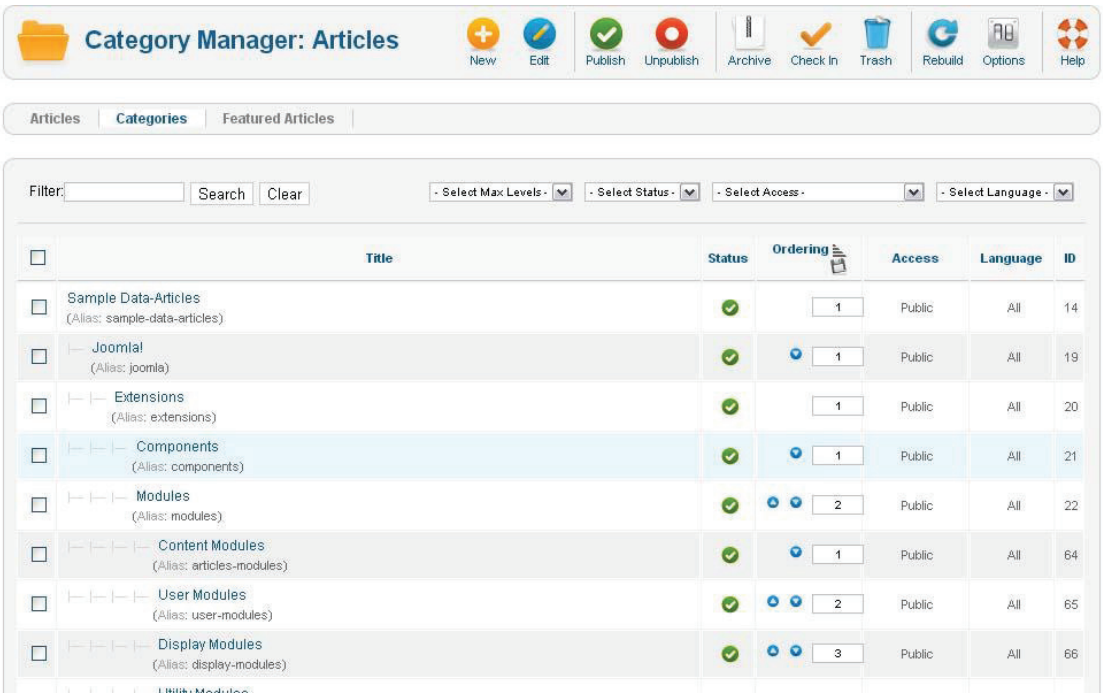
Το Joomla σε γενικές γραμμές χρησιμοποιείται παγκοσμίως για ιστοσελίδες ανεξαρτήτου του πλήθους των δεδομένων αλλά και των τεχνικών σχεδιασμών τους. Για παράδειγμα γίνεται εκτενής χρήση σε:

- On-line περιοδικά, εφημερίδες και γενικότερα εκδόσεις,
- Εταιρικές ιστοσελίδες και portals,
- Ηλεκτρονικό Εμπόριο (e-commerce) και online κρατήσεις,
- Εταιρικά intranets και extranets
- Εφαρμογές κυβερνητικών κρατών
- Οικογενειακές ή προσωπικές ιστοσελίδες
- Οργανωτικές και μη κερδοσκοπικές ιστοσελίδες
- Μικρές ιστοσελίδες επιχειρήσεων
- Portals Κοινοτήτων Χρηστών
- Ιστοσελίδες εκκλησιών και σχολείων

Τα βασικότερα μέρη του Joomla είναι:

- Το περιεχόμενο,
- Η πλοήγηση,
- Η λειτουργικότητα,
- Το χρώμα / σχέδιο του γραφικού περιβάλλοντος (scheme)

Όσο αναφορά το περιεχόμενο, το Joomla διαχειρίζεται τα δεδομένα αυτά μέσω μιας βάσης δεδομένων MySQL και χωρίζεται σε κατηγορίες (categories), Οι κατηγορίες είναι ένα από τα κομμάτια της βάσης δεδομένων που χρησιμοποιεί το Joomla ώστε να δομηθούν τα μενού της σελίδας χωρίς να σχετίζονται με τη διαδικασία της πλοήγησης της. Κάθε άρθρο δηλώνεται κάτω από την γενικότερη ομπρέλα μιας κατηγορίας ώστε να ομαδοποιείται το περιεχόμενο της εκάστοτε ιστοσελίδας για πιο γρήγορη και άμεση αναζήτηση (Εικόνα 9). Το λογισμικό δίνει τη δυνατότητα να οριστούν και υποκατηγορίες σε υφιστάμενες κατηγορίες για καλύτερη ομαδοποίηση των περιεχομένων της ιστοσελίδας.



Εικόνα 9: Ορισμός κατηγοριών του Joomla

Η πλοήγηση στο Joomla σχετίζεται με τη διάταξη των ενοτήτων (modules). Η κυριότερη ενότητα είναι το μενού για το λόγο ότι είναι αυτό που ευθύνεται για την πλοήγηση στην ιστοσελίδα. Στην ουσία, μια ενότητα είναι ένα μπλοκ του περιεχομένου που μπορεί να κινηθεί γύρω από την ιστοσελίδα και να εφαρμοστεί σε διαφορετικές σελίδες . Για παράδειγμα, υπάρχει μια ενότητα που εμφανίζει τυχαία φωτογραφίες, ένα module που επιτρέπει στους χρήστες να αλλάξουν το πρότυπο (template) για την περιοχή, ένα module που εμφανίζει τα πιο δημοφιλή είδη περιεχομένου της ιστοσελίδας, ή τα πιο πρόσφατα ή τα συναφή είδη (με βάση τα metadata). Τέλος, σε κάθε μενού μπορούν να οριστούν ετικέτες (labels) που βοηθούν και αυτές με τη σειρά τους στην πλοήγηση των χρηστών από ένα σύνδεσμο σε ένα άλλο. Χαρακτηριστικό στοιχείο των μενού είναι η δυνατότητα που δίνει το Joomla στην μορφοποίηση της εμφάνισης

του ώστε να μπορεί να ορισθεί σε οριζόντια, σε ευθεία ή σε κατακόρυφη μορφή ανάλογα με τη συνολική μορφοποίηση της σελίδας.

Όσο αναφορά τη λειτουργικότητα του Joomla, το σύστημα αυτό δίνει τη δυνατότητα στο χρήστη να προσθέσει κάποιες επιπλέον λειτουργικές εφαρμογές μέσω των Mambots αλλά και των στοιχείων (components). Τα Mambots είναι ουσιαστικά τμήματα του κώδικα ή μικρά προγράμματα τα οποία όταν καλούνται μέσω διαφόρων παραμέτρων, είτε ενεργοποιούν ένα πρόγραμμα, ένα script, ή εκτελούν μια συγκεκριμένη λειτουργία ενός στοιχείου (component) ή της ίδιας της βάση δεδομένων. Για παράδειγμα: οι προηγμένοι συντάκτες κειμένου WYSIWYG και TinyMCE ή και ένα πρόγραμμα ηλεκτρονικής ψηφοφορίας όπως είναι το jVoteSystem ή και η τεχνολογία των RSS feeds ανήκουν στην κατηγορία των components των συστημάτων Joomla. Αξίζει να αναφερθεί πως για την προσθαφαίρεση αυτών των στοιχείων υπεύθυνοι είναι οι διαχειριστές του συστήματος. Αυτοί αποφασίζουν ποιο component θα εντάξουν μέσα στο σύστημα του Joomla, σύμφωνα πάντα με τις ανάγκες των λειτουργιών της ιστοσελίδας, αλλά ταυτόχρονα τους δίνεται και η δυνατότητα να συντάξουν το δικό τους κώδικα προγραμματισμού καλύπτοντας έτσι τις ιδιαίτερες ανάγκες τους.

Επιπρόσθετα, το χρώμα και το σχέδιο του γραφικού περιβάλλοντος του Joomla σχετίζεται με τα πρότυπα (templates) που μπορούν να χρησιμοποιηθούν από τους διαχειριστές του συστήματος. Ένα template είναι πολλά αρχεία με κώδικα γραμμένα σε PHP όπου καθορίζουν τόσο το σχέδιο όσο και τις χρωματικές αποχρώσεις της ιστοσελίδας. Ο κεντρικός πυρήνας ενός προτύπου είναι ένα αρχείο με κατάληξη .css όπου εκεί μπορεί να γίνει ο όποιος χειρισμός των χρωμάτων, των ευθυγραμμίσεων, αλλά και των γραμματοσειρών των κειμένων. Πέρα από το αρχείο css σημαντικό ρόλο έχει και το αρχείο με κατάληξη html όπου καθορίζει το μέρος που το περιεχόμενό μιας ιστοσελίδας ακολουθεί με γνώμονα την εκάστοτε επιλογή του χρήστη ή του διαχειριστή. Επίσης, στο html αρχείο περιέχονται και μία σειρά από σενάρια που στην ουσία είναι αυτά που πραγματοποιούν τη φόρτωση ποικίλων στοιχείων μιας ιστοσελίδας όπως τα μενού, οι εικόνες κ.α.

Ο ρόλος του προτύπου είναι να ορίζει:

- Το χρώμα του κειμένου που αποτελεί το κύριο σώμα της ιστοσελίδας.
- Το κεντρικό χρώμα του φόντου ή εναλλακτικά την κεντρική εικόνα ως φόντο.
- Το σημείο εμφάνισης όλων των στοιχείων της ιστοσελίδας – π.χ. αριστερά, δεξιά, στο κέντρο αλλά και σε πιο σημείο της ιστοσελίδας.

- Το είδος της γραμματοσειράς και όλα τα χαρακτηριστικά της (π.χ. μέγεθος, εμφάνιση).

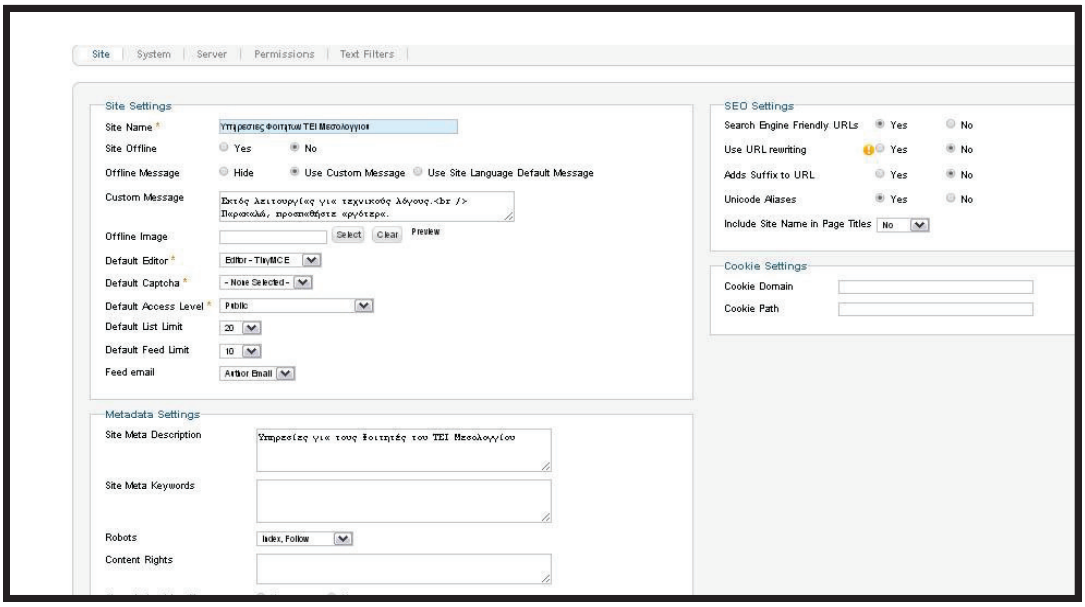
- Τι θα εμφανίζεται και σε ποιόν – π.χ. να αλλάζει τα χρώματα ή τις γραμματοσειρές ανάλογα με τις ομάδες των χρηστών ή να εμφανίζονται συγκεκριμένες επιλογές στο μενού ανάλογα με την ομάδα στην οποία ανήκει ο χρήστης.

Ένα σύστημα Joomla ως προς τη δομή του δε διαφέρει από τις υπόλοιπες ιστοσελίδες που έχουν κατασκευαστεί χωρίς τη χρήση κάποιου συστήματος διαχείρισης περιεχομένων. Τα μέρη και των δύο αυτών κατηγοριών είναι τα ίδια. Η μόνη εξαίρεση που αποτελεί και την κύρια διαφορά του Joomla με τις υπόλοιπες συμβατικές ιστοσελίδες επικεντρώνεται στην ονοματολογία των επιλογών που είναι οργανωμένες σε διαφορετικές κατηγορίες. Επίσης, το Joomla δίνει τη δυνατότητα να καθοριστούν σε όλο το περιεχόμενο της ιστοσελίδας γενικές ρυθμίσεις / παραμετροποιήσεις (global Configuration), πέρα από τις ειδικές ρυθμίσεις σε κάθε ένα από τα περιεχόμενα.

Οι γενικές ρυθμίσεις/παραμετροποιήσεις του Joomla καθορίζονται από τους διαχειριστές του συστήματος και κατόπιν πιστοποίησης της ταυτότητας τους με τη χρήση username και password.

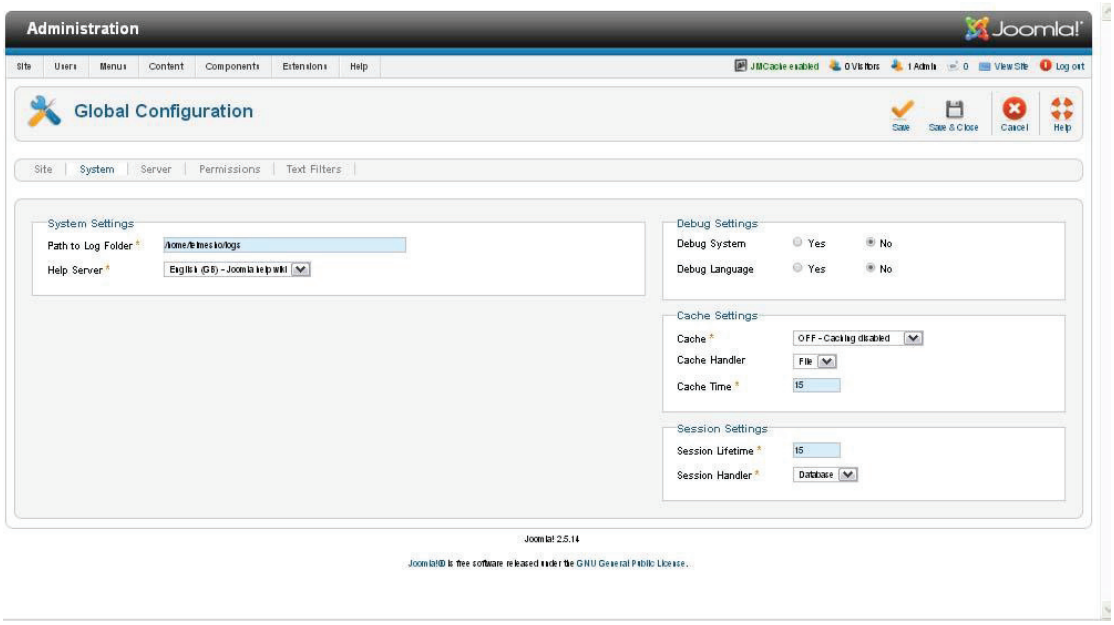
Οι ρυθμίσεις αυτές κατηγοριοποιούνται σύμφωνα με:

- Οτιδήποτε αφορά γενικά την ιστοσελίδα (επιλογή site), π.χ. όνομα της ιστοσελίδας, ρυθμίσεις βελτιστοποίησης αποτελεσμάτων των μηχανών αναζήτησης (SEO), ρυθμίζεις και ορισμό meta λέξεων κλειδιών, ρυθμίσεις cookies (Εικόνα 10).



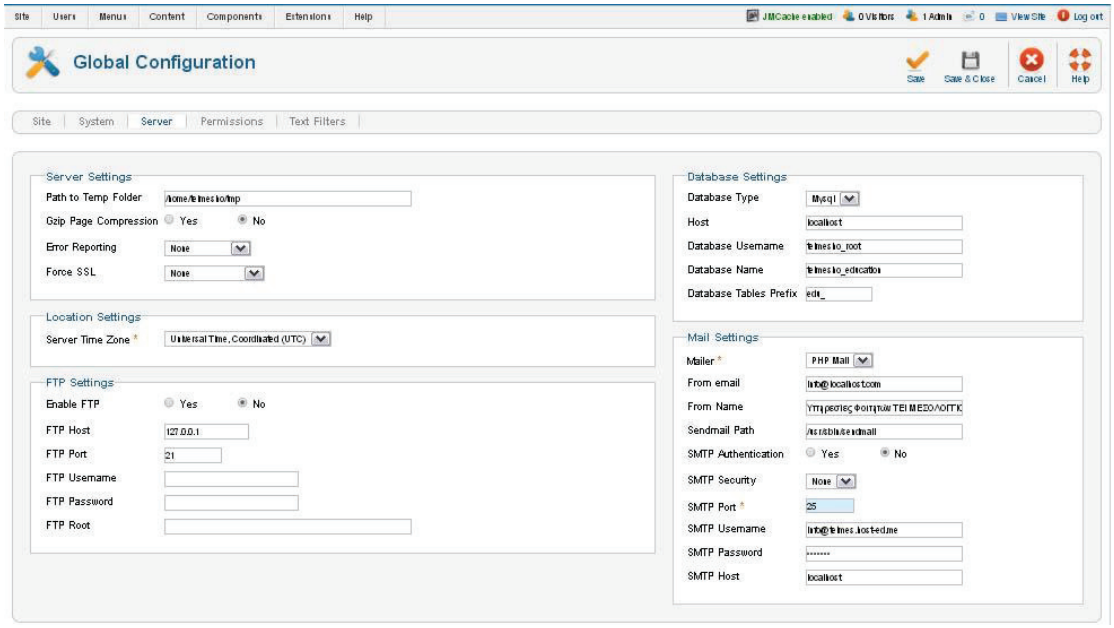
Εικόνα 10: Γενικές ρυθμίσεις Ιστοσελίδας Joomla

- Οτιδήποτε αφορά γενικά το σύστημα του Joomla, π.χ. ορισμός διαδρομής όπου θα αποθηκεύονται τα αρχεία καταγραφής (log files), ρυθμίσεις που σχετίζονται με την διόρθωση των λαθών του προγράμματος, της μνήμης cache του λογισμικού (Εικόνα 11).



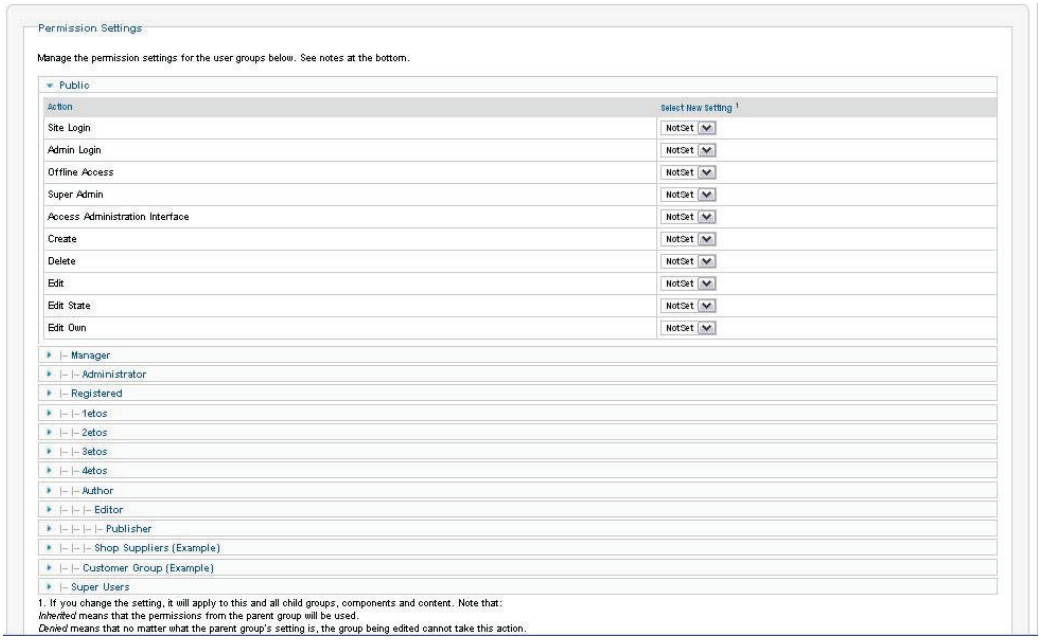
Εικόνα 11: Γενικές ρυθμίσεις συστήματος Joomla

- Οτιδήποτε αφορά τον διακομιστή, π.χ. ζώνη ώρας του διακομιστή, ρυθμίσεις FTP, ρυθμίσεις της βάσης δεδομένων καθώς και ρυθμίσεις του διακομιστή του μαιλ. (Εικόνα 12).



Εικόνα 12: Ρυθμίσεις διακομιστή (server) του Joomla

- Οτιδήποτε αφορά τις άδειες χρήσης και λειτουργίας του συστήματος τόσο στη δημόσια πρόσβαση του όσο και σε πρόσβαση από ποικίλες κατηγορίες χρηστών π.χ. εγγραμμένους χρήστες, διαχειριστές, συντάκτες περιεχομένων κ.α. (Εικόνα 13).



Εικόνα 13: Ρυθμίσεις αδειών χρήσης και λειτουργίας του Joomla

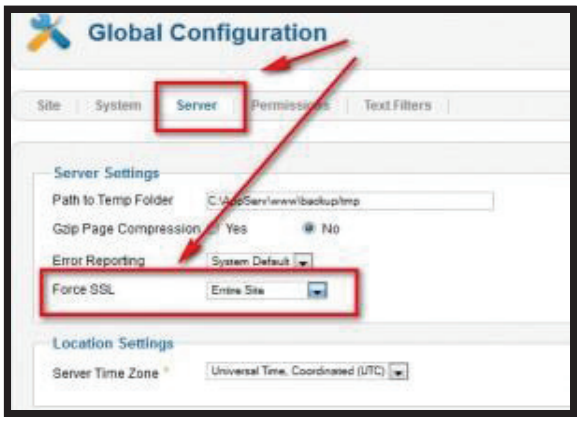
8.3 Ασφάλεια JOOMLA

Για μια ιστοσελίδα απαραίτητο στοιχείο για τους διαχειριστές της είναι και το γεγονός ότι θα πρέπει το περιεχόμενο και οι υπηρεσίες της να διέπονται από την μέγιστη δυνατή ασφάλεια. Η διασφάλιση τόσο του ίδιου του περιεχομένου όσο και των υπηρεσιών μιας ιστοσελίδας θεωρείται από αρκετούς διαχειριστές το πιο δύσκολο στοιχείο μιας ιστοσελίδας ακόμα και από την συνολική υλοποίηση της. Αυτό οφείλεται στο ότι ένα εργαλείο όπως το Joomla διαθέτει πολλούς μηχανισμούς και παραμέτρους, όπως και κάθε ιστοσελίδα, όπου οι διαχειριστές του θα πρέπει να λάβουν υπόψη τους.

Μιλώντας για την ασφάλεια ενός συστήματος εννοούμε την προστασία της λειτουργίας του μέχρι το βαθμό που το ίδιο το σύστημα θα βρίσκεται σε μια ομαλή κατάσταση χωρίς να παρεμποδίζονται ή να δημιουργούνται δυσλειτουργίες από την καθιερωμένη χρήση του. Δηλαδή, ναι μεν οι πληροφορίες να είναι διαθέσιμες στους χρήστες της ιστοσελίδα χωρίς όμως, όταν πρέπει, να παραβιάζονται άλλα στοιχεία όπως το ιδιωτικό απόρρητο καθώς και η απαραίτητη πιστοποίηση των στοιχείων τους για πρόσβαση και υπηρεσίες που απαιτούν κάτι τέτοιο.

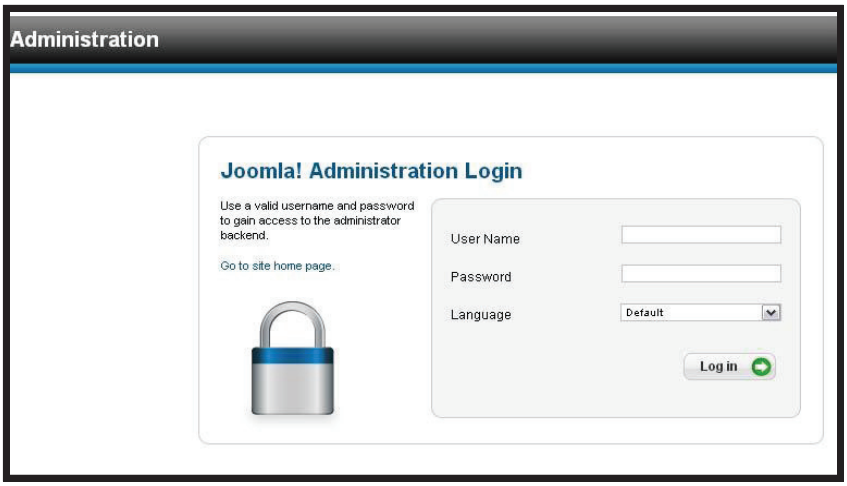
Το Joomla σαν σύστημα διαχείρισης περιεχομένου έχει κατασκευαστεί λαμβάνοντας υπόψη τις βασικές αρχές πιστοποίησης της ταυτότητας των χρηστών της. Πιο συγκεκριμένα, όταν ένας χρήστης ανήκει στην κατηγορία των εγγεγραμμένων (registered) χρηστών τότε απαιτείται η ταυτοποίηση τους με τη χρήση username και password. Οτιδήποτε αποτελεί συστατικό μιας ιστοσελίδας με Joomla αποθηκεύεται μέσα σε μία βάση δεδομένων μαζί και τα στοιχεία των χρηστών. Η διαφορά των στοιχείων των χρηστών σε σχέση με τα υπόλοιπα στοιχεία που περιέχει μια ιστοσελίδα σε Joomla είναι ότι τα στοιχεία που χρησιμοποιούνται για τη διαδικασία της ταυτοποίησης όλων των κατηγοριών των χρηστών αποθηκεύονται κρυπτογραφημένα με 128-bit (16 byte) αλγόριθμο md5. Πέρα από την κρυπτογράφηση αυτή το Joomla χρησιμοποιεί τη τεχνολογία του .htaccess αρχείου ως ένα από τους βασικότερους τρόπους προστασίας των αρχείων του συστήματος από ανεπιθύμητες προσβάσεις. Το αρχείο .htaccess σχετίζεται με τη τεχνολογία SSL την οποία υποστηρίζει το Joomla (Εικόνα 14) σε συνδυασμό με τον server από όπου αντλούνται οι πληροφορίες των αρχείων του συστήματος περιεχομένου. Για να είναι εφικτή η χρήση του SSL του Joomla θα πρέπει να δίνεται η δυνατότητα και από τις λειτουργίες του server μιας τέτοιας υπηρεσίας. Συνήθως, οι δωρεάν servers δίνουν αυτή την υποστήριξη χωρίς όμως να δίνουν και τη δυνατότητα στους δωρεάν

πελάτες τους να έχουν το δικό τους πιστοποιητικό (certificate) το οποίο χρειάζεται ώστε να τεθεί σε πλήρη εφαρμογή η τεχνολογία SSL.



Εικόνα 14: Ρύθμιση ασφάλειας SSL του Joomla

Επιπρόσθετα, το σύστημα διαχείρισης περιεχομένου Joomla προσφέρει αυτόνομη τοποθεσία για την ταυτοποίηση της ταυτότητας των διαχειριστών του συστήματος μέσω της κεντρικής σελίδας εισαγωγής των στοιχείων των διαχειριστών (Εικόνα 15). Η τεχνολογία της ταυτοποίησης στηρίζεται στην κρυπτογράφηση με τον αλγόριθμο md5 128-bit. Η διεύθυνση της εν λόγω φόρμας εισαγωγής ταυτοποίησης των στοιχείων των διαχειριστών του Joomla λειτουργεί κάτω από τη διεύθυνση /administrator της βασικής σελίδας. Με τη χρήση των επεκτάσεων (extensions) του Joomla καθώς και των επιπρόσθετων στοιχείων (components) μπορούμε να βελτιώσουμε από θέμα ασφάλειας το μέσο εισαγωγής των στοιχείων των διαχειριστών μιας ιστοσελίδας.



Εικόνα 15: Φόρμα εισαγωγής στοιχείων ταυτοποίησης Διαχειριστών του Joomla

Το Joomla αναμφισβήτητα έχει κατασκευαστεί ως ένα εργαλείο διαχείρισης περιεχομένων ιστοσελίδων λαμβάνοντας υπόψη τις άκρως απαραίτητες ανάγκες που θα μπορούσε να έχει ο κάθε διαχειριστής καθώς και κάποιες βασικές λειτουργίες που σχετίζονται με τη σωστή και ασφαλή λειτουργία τους. Για παράδειγμα, να μπορούν να κατηγοριοποιούνται οι χρήστες και να δίνεται η δυνατότητα να ξεχωρίζουν οι απλοί επισκέπτες από τους εγγεγραμμένους χρήστες ή οι απλοί διαχειριστές θεματικών ενοτήτων από τους κύριους κατόχους ή/και τους τεχνικούς διαχειριστές του συστήματος. Αντιθέτως, μέσα στο βασικό κορμό δεν έχει ληφθεί υπόψη μια πιθανή επίθεση όπως είναι η Άρνηση των Υπηρεσιών (Denial of Service, DoS) η οποία θα έθετε τις υπηρεσίες και γενικά όλη την ιστοσελίδα εκτός λειτουργίας από μερικά λεπτά μέχρι και αρκετές ώρες. Σε περίπτωση που ένα τέτοιο περιστατικό λάμβανε χώρα σε ώρα αιχμής ή κατά τη διάρκεια ενεργοποίησης μια υπηρεσίας όπως π.χ. μιας ψηφοφορίας, θα ακυρωνόταν πλήρως ο ρόλος και η λειτουργικότητα της σελίδας.

Οι βασικές λεπτομέρειες, όπως οι παραπάνω που αναφέραμε, μπορούν να καλυφθούν ως ένα βαθμό με τα ποικίλα extensions και plug-ins που διατίθενται για το Joomla είτε δωρεάν είτε με πληρωμή κάτι που βοήθησε και την εφαρμογή που δημιουργήσαμε για τις ανάγκες αυτής της πτυχιακής εργασίας.

8.4 Σενάριο Δημιουργίας Ιστοσελίδας σε JOOMLA

Για να μπορέσουμε να αποτυπώσουμε καλύτερα και σε μεγαλύτερο βάθος από πλευράς ασφάλειας τις δυνατότητες που παρέχει το Joomla στους διαχειριστές αλλά και στους χρήστες του, κατασκευάσαμε μια ηλεκτρονική πλατφόρμα που απευθύνεται σε φοιτητές του τμήματος Τηλεπικοινωνιακών Συστημάτων και Δικτύων του ΤΕΙ Μεσολογγίου. Στη πλατφόρμα αυτή παρέχεται δωρεάν πρόσβαση σε όλους τους χρήστες του διαδικτύου σε επιλεγμένες πληροφορίες, όπως για παράδειγμα τα νέα του τμήματος όσον αναφορά εκδηλώσεις ή υπηρεσίες που παρέχονται από το τμήμα προς τους φοιτητές του. Η λειτουργία της πλατφόρμας επικεντρώνεται κυρίως στους εγγεγραμμένους φοιτητές σε κάθε έτος φοίτησης όπου τους ζητείται ειδική πρόσβαση σε πληροφορίες και υπηρεσίες που είναι ενεργές αποκλειστικά και μόνο γι' αυτούς.

Σε γενικές γραμμές, οι υπηρεσίες που παρέχονται στους εγγεγραμμένους φοιτητές μπορούν να ομαδοποιηθούν στις παρακάτω κατηγορίες:

- Ενημέρωση με νέα και ανακοινώσεις που αφορούν τη φοίτηση των φοιτητών,
- Υπηρεσίες ηλεκτρονικής γραμματείας προς τους φοιτητές της σχολής,
- Δικαιώματα και υποχρεώσεις των φοιτητών για τη σωστή λειτουργία του ιδρύματος

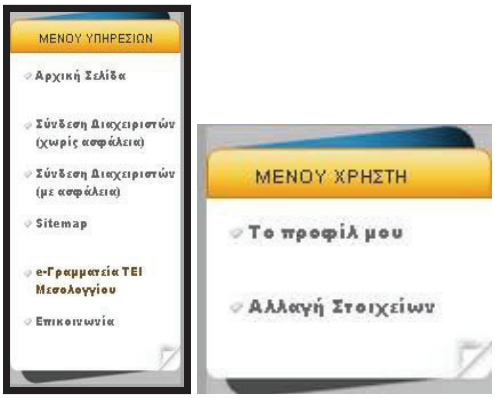
Πιο συγκεκριμένα, η πλατφόρμα αυτή παρέχει στους φοιτητές της σχολής άμεση και έγκυρη ενημέρωση τόσο των ανακοινώσεων όσο και άλλον θεμάτων που σχετίζονται με τη πορεία της φοίτησής τους. Για παράδειγμα, η αναγγελία έναρξης του νέου ακαδημαϊκού έτους ή η έναρξη των εξεταστικών περιόδων κάθε εξαμήνου φοίτησης είναι δυο πολύ βασικές διεργασίες του εκπαιδευτικού προγράμματος της σχολής ώστε να διασφαλιστεί η ομαλή του λειτουργία. Μέσω της ιστοσελίδας του σεναρίου, οι φοιτητές μπορούν να έχουν γραμματειακές υπηρεσίες κάτι που θα διευκολύνει πάρα πολύ ιδιαίτερα τους φοιτητές που είτε δε μένουν κοντά στην ευρύτερη περιοχή του τει είτε δε έχουν το χρόνο να επισκεφτούν τη γραμματεία του τει – όταν αυτό διατηρεί διαφορετικά παραρτήματα από την κύρια έδρα του. Έτσι, οι φοιτητές μέσω της ηλεκτρονικής γραμματείας – ή αλλιώς e-γραμματείας – μπορούν να αιτηθούν την έκδοση αναλυτικής βαθμολογίας για κάθε εξάμηνο φοίτησης τους καθώς και να αιτηθούν την εγγραφή τους σε κάθε εξάμηνο φοίτησης. Εξαίρεση αποτελούν οι νέοι φοιτητές που πρέπει να εγγραφούν στο $1^{ο}$ εξάμηνο φοίτησης μιας και μαζί με τη σχετική τους αίτηση θα πρέπει να προσκομίσουν και τα υπόλοιπα δικαιολογητικά όπως οι ιατρικές εξετάσεις κ.α.. Τέλος, στην πλατφόρμα αυτή οι φοιτητές μπορούν να εκπληρώσουν ορισμένα από τα φοιτητικά τους

δικαιώματα όπως είναι η άμεση και έγκυρη συμμετοχή τους στις φοιτητικές εκλογές του ΤΕΣΥΔ ή στην ατομική αξιολόγηση του εκάστοτε μαθήματος για το οποίο έχουν ήδη επιτυχώς ολοκληρώσει την παρακολούθηση του.

8.5 Ανάλυση Εφαρμογής JOOMLA

Για την υλοποίηση της εφαρμογής του προαναφερθέντος σεναρίου έγινε χρήση του συστήματος διαχείρισης περιεχομένων (CMS) με όνομα Joomla. Η έκδοση που επιλέχτηκε είναι η 2.5.14, η πιο stable έκδοση που ήταν διαθέσιμη κατά την πραγματοποίηση αυτού του project. Φυσικά, αξίζει να αναφέρουμε πως την ίδια περίοδο ήταν διαθέσιμη και η έκδοση 3.2.0 που είναι και η πιο ανανεωμένη από πλευράς του κεντρικού πυρήνα του συστήματος. Για λόγους καθαρά ασφάλειας καθώς και για λόγους που οφείλονται στο είδος των υπηρεσιών που θέλουμε να προσφέρουμε στους φοιτητές μας δε θα μπορούσαμε να χρησιμοποιήσουμε την πιο πρόσφατη έκδοση του Joomla. Σημαντικός παράγοντας για την επιλογή την 2.5.14 έκδοσης ήταν και το γεγονός ότι η 2.5.X έκδοση του Joomla δίνει τη δυνατότητα στους διαχειριστές να επιλέξουν από ένα μεγαλύτερο πλήθος επιπρόσθετων προγραμμάτων και scripts πλήρως δοκιμασμένα και εναρμονισμένα με αυτή την έκδοση κάτι που δεν ισχύει για την 3.2 έκδοση του συστήματος. Μπορεί πολύ διαχειριστές να θεωρούν πως η χρήση ενός συστήματος στην άκρως τελευταία του έκδοση να είναι και κριτήριο μεγαλύτερης ασφάλειας λόγω του ότι ακόμα δεν έχουν ανιχνευτεί πλήρως τα πιθανά τρωτά του σημεία. Παρόλα αυτά κάτι τέτοιο δεν είναι απόλυτα σωστό μιας και έχει παρατηρηθεί πως μια stable έκδοση σαν την 2.5.14 που επιλέξαμε, εφόσον παραμετροποιηθεί σωστά και γίνει προσεκτική επιλογή των επιπρόσθετων εφαρμογών που θα χρησιμοποιηθούν, μπορεί να θεωρηθεί πιο ασφαλής από την τελευταία της έκδοση. Εξάλλου ανεξαρτήτου έκδοσης σημαντικό ρόλο από θέμα ασφάλειας παίζουν το πώς θα ρυθμιστούν τα προγράμματα που το απαρτίζουν καθώς και τους τρόπους που θωρακίζεται ο server που φιλοξενεί τα αρχεία του Joomla.

Στην έκδοση αυτή έχει δημιουργηθεί ένα κεντρικό μενού που δίνει της υπηρεσίες που παρέχονται στους χρήστες της ιστοσελίδας. Αξίζει να αναφέρουμε πως οι υπηρεσίες που παρέχονται στους απλούς επισκέπτες είναι περιορισμένες (Εικόνα 16α) σε σχέση με τους εγγεγραμμένους χρήστες – είτε ως απλοί εγγεγραμμένοι χρήστες είτε ως διαχειριστές (Εικόνα 16β). Τα δύο αυτά μενού υπηρεσιών αναλύονται εκτενέστερα παρακάτω.



Εικόνα 16α: Μενού υπηρεσιών επισκεπτών

Εικόνα 16β: Μενού υπηρεσιών εγγεγραμμένων

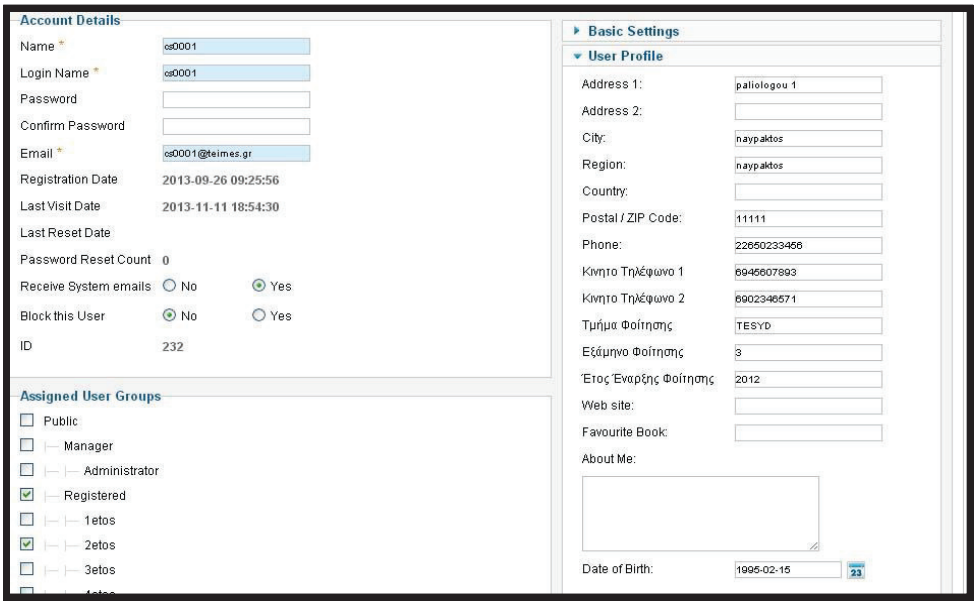
Η κατανομή των χρηστών ανά κατηγορία και με συγκεκριμένα δικαιώματα που έχουμε ακολουθήσει παρουσιάζεται παρακάτω:

- Επισκέπτες, μπορούν απλά να διαβάσουν τα νέα και να κατοχυρώσουν κάποιο ηλεκτρονικό αίτημα επικοινωνίας με το αρμόδιο τμήμα του ιδρύματος κυρίως για διευκρινήσεις σχετικά με τα προγράμματα σπουδών του
- Εγγεγραμμένοι, οι οποίοι είναι: α) φοιτητές που φοιτούν στο ΤΕΣΥΔ ανεξαρτήτου εξαμήνου φοίτησης και β) διαχειριστές οι οποίοι μπορούν να έχουν πρόσβαση στις υπηρεσίες του ΤΕΙ για καθαρά τεχνικούς λόγους
- Διαχειριστές, οι οποίοι έχουν ορισθεί τρία άτομα (με usernames: epan, epan2, epan3) από τη μηχανογράφηση του τει ως υπεύθυνοι για την τεχνική υποστήριξη/αναβάθμιση του συστήματος αλλά και για τον έλεγχο της λειτουργικότητας των υπηρεσιών προς τους φοιτητές του.

Για τους επισκέπτες δεν απαιτείται να προσδιορίσουν ή να επιβεβαιώσουν στοιχεία της ταυτότητας τους παρά μόνο όταν κατοχυρώνουν κάποιο αίτημα για επικοινωνία. Σε αυτή την περίπτωση ζητείται το ονοματεπώνυμο τους, ο αριθμός του τηλεφώνου τους καθώς και η προσωπική τους διεύθυνση ηλεκτρονικής αλληλογραφίας (e-mail) ώστε να μπορεί ο αρμόδιος υπάλληλος τους ιδρύματος να έρθει σε επικοινωνία μαζί τους. Αντίθετα, οι εγγεγραμμένοι

χρήστες, δηλαδή οι φοιτητές που έχουν ήδη κάνει εγγραφή σε κάποιο εξάμηνο φοίτησης έχουν πρόσβαση με προσωπικούς κωδικούς που δηλώνουν την ταυτότητα τους. Η διαδικασία που ακολουθείται για την εγγραφή των φοιτητών και την κατοχύρωση του λογαριασμού του στην πλατφόρμα του Joomla είναι η ακόλουθη:

- Με την αρχική εγγραφή των πρωτοετών μέσω της ειδικής αίτησης των νέων φοιτητών (συμπεριλαμβανομένου και της παράδοσης των ιατρικών εξετάσεων που πρέπει να παραδώσει ο εκάστοτε φοιτητής) καταγράφονται τα στοιχεία τους (διεύθυνση κατοικίας, τηλέφωνα, ημερ/νια γέννησης, έτος εγγραφής και έτος εισαγωγής στην σχολή) από τη γραμματεία της σχολής και δίδονται στον αρμόδιο υπάλληλο της μηχανογράφησης (που έχει οριστεί ως ένας εκ των τριών διαχειριστών του συστήματος) ώστε να μηχανογραφηθούν μέσα στην ηλεκτρονική πλατφόρμα (Εικόνα 17).



Εικόνα 17: Αλλαγή στοιχείων φοιτητή/εγγεγραμμένου χρήστη από τον διαχειριστή

- Με την μηχανογράφηση τους επίσης, εκδίδεται μέσω του πίνακα ελέγχου της εταιρείας hosting και μία προσωπική ηλεκτρονική διεύθυνση αλληλογραφίας (e-mail) της μορφής username@teimes.gr χρησιμοποιώντας ένα μοναδικό username της μορφής csXXXX όπου XXXX αριθμοί με αύξοντα σειρά και ένα προκαθορισμένο password όπου αποστέλλονται στο προσωπικό e-mail που τους έχει δώσει το ίδιο το τει (είναι της μορφής: csXXXX@teimes.gr).

- Ο κάθε φοιτητής θα πρέπει να αλλάξει τον κωδικό πρόσβασης με την πρώτη του είσοδο στο σύστημα ώστε να μη τον γνωρίζει ο διαχειριστής που τον όρισε αρχικά.

- Οι διαχειριστές δεν έχουν πρόσβαση στο περιεχόμενο των κωδικών των χρηστών μιας και είναι κρυπτογραφημένοι (με md5, 128-bit) ενώ μπορούν να ορίσουν νέο κωδικό ανά πάσα στιγμή που ο χρήστης το επιθυμεί (εικόνα 9).

- Τέλος κάθε φοιτητής πέρα από την ομάδα group των registered users εντάσσεται και στην αντίστοιχη ομάδα που υποδηλώνει το πραγματικό έτος στο οποίο έχει ενταχθεί με βάση το επίπεδο ολοκλήρωσης των μαθημάτων του. Για παράδειγμα, οι φοιτητές που έχουν γραφτεί για το 1^{ο} έτος και έχουν ολοκληρώσει επιτυχώς όλα τα μαθήματα του έτους αυτού εντάσσονται και στην ομάδα των χρηστών του 1^{ου} έτους (εικόνα 9).

Προσπάθεια

Επίσης έγινε προσπάθεια ώστε να καταχωρείτε κρυπτογραφημένη η ψήφος στην βάση έτσι στην διαδρομή των αρχείων του joomla:education\components\com_jvotesystem\classes\vote.class.php

Αλλάχθηκε η γραμμή 730 σε: $nV->answer_id = (md5($answerID));

Επίσης μέσα στην βάση πρέπει να αλλαχθεί το answer_id αντί για INT(11) το άλλαξα σε varbinary(11)

Ώστε να αποθηκεύεται η ψήφος κρυπτογραφημένη κάτι και το οποίο έγινε η ψήφος μπορούσε να κρυπτογραφηθεί έτσι αλλα δημιουργήθηκε πρόβλημα στις ψηφοφορίες του συστήματος διότι δεν αποθηκευόταν η ψήφος στην πλατφόρμα του συστήματος αλλα μόνο στην βάση και έτσι δεν το εφαρμόσαμε το αφήσαμε ώς έχει

8.6 Μενού Υπηρεσιών

Όπως έχουμε ήδη αναφέρει, οι υπηρεσίες που παρέχονται στους επισκέπτες της πλατφόρμας είναι διαφορετικές από αυτές των εγγεγραμμένων χρηστών – δηλαδή των φοιτητών του τμήματος. Η διαφορά του ενός μενού υπηρεσιών από το άλλο επικεντρώνεται στις υπηρεσίες της e-γραμματείας καθώς και στο ενδεικτικό σύνδεσμο που οδηγεί στην σύνδεση των διαχειριστών στο Joomla. Ο σύνδεσμος για την σύνδεση των διαχειριστών έχει τοποθετηθεί ενδεικτικά ώστε να μπορέσει να αποτυπωθεί με ακρίβεια η ύπαρξη ή μη της ασφάλειας κατά την είσοδο των διαχειριστών. Επίσης, οι εγγεγραμμένοι χρήστες μετά την είσοδο τους στο σύστημα έχουν πρόσβασή σε 2 επιπλέον μενού πλην του βασικού μενού υπηρεσιών: α) στο μενού των χρηστών και β) στο μενού των ψηφοφοριών. Το μεν μενού των χρηστών

παρέχει στους φοιτητές τη δυνατότητα να ελέγξουν τα προσωπικά τους στοιχεία – π.χ. ονοματεπώνυμο, διεύθυνση κατοικίας ή ακόμα και τα τηλέφωνα επικοινωνίας τους – και να τα επικαιροποιούν ανά πάσα στιγμή. Για το δε μενού των ψηφοφοριών οι φοιτητές έχουν πρόσβαση στις διαθέσιμες ενεργές ψηφοφορίες τις οποίες μπορούν να λάβουν μέρος – για παράδειγμα στις φοιτητικές εκλογές 2013. Και τα δύο αυτά μενού είναι ορατά σε χρήστες που ανήκουν ιεραρχικά σε υψηλότερες κατηγορίες από αυτή των επισκεπτών.

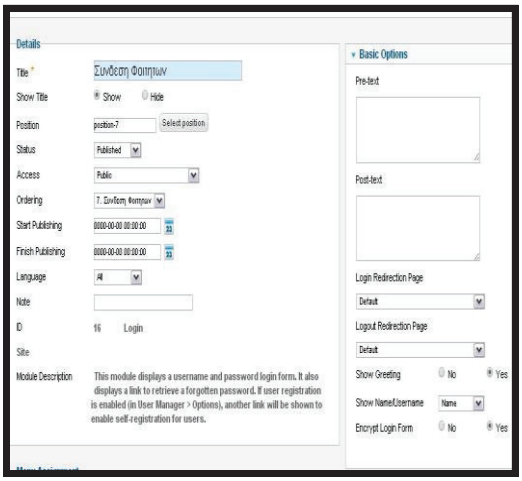
8.7 Επιπρόσθετα Εργαλεία του JOOMLA

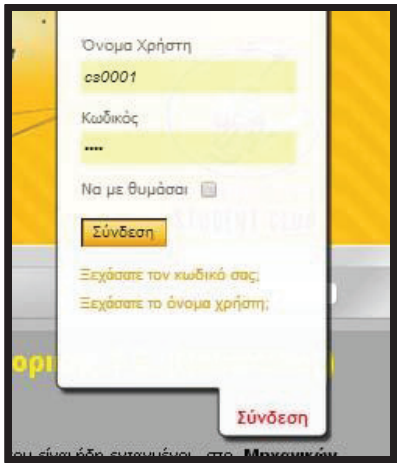
Στην πλατφόρμα που δημιουργήθηκε για τις ανάγκες του σεναρίου αυτού του project οι φοιτητές έχουν πρόσβαση σε 2 βασικές υπηρεσίες:

- Στη διαδικασία σύνδεσης/αποσύνδεσης των χρηστών
- Στην επικοινωνία με την γραμματεία
- Στη συμμετοχή τους σε ποικίλες ψηφοφορίες

8.8 Διαδικασία Σύνδεσης/Αποσύνδεσης Χρηστών

Το Joomla εκ κατασκευής υποστηρίζει ένα πολύ αξιόπιστο σύστημα εισόδου/εξόδου των χρηστών του. Φυσικά αυτό απλά δίνει τη δυνατότητα να συνδέονται/αποσυνδέονται οι χρήστες με την ταύτιση των κρυπτογραφημένων κωδικών που είναι αποθηκευμένοι μέσα στη βάση δεδομένων του ίδιου του συστήματος. Θέλοντας να δώσουμε και μια επιπλέον ιδιαιτερότητα στη διαδικασία αυτή, προσθέσαμε το plug-in με όνομα *Hidden on Top Login* στην 2.5.1 έκδοση του. Το plug-in αυτό στηρίζεται στο module login που διαθέτει ήδη το Joomla και απλά το μετακινεί στην κορυφή υπό τη μορφή κρυφού παραθύρου που μετακινηθείτε προς τα κάτω όταν ο χρήστης πατήσει πάνω στην καρτέλα του (Εικόνα 18β).





Εικόνα 18α: Ρυθμίσεις HOT Login

Εικόνα 18β: Φόρμα Σύνδεσης HOT Login

8.9 Ασφάλεια Σύνδεσης/Αποσύνδεσης Χρηστών

Η δυνατότητα που μας δίνει το module login υποστηρίζει και κωδικοποίηση στη φόρμα της σύνδεσης μέσω της τεχνολογίας SSL που προσφέρει επίσκεψη στη σελίδα μέσο του πρωτοκόλλου https. Ωστόσο, για να μπορέσουμε να πετύχουμε μεγαλύτερη ασφάλεια μεταξύ του τερματικού του χρήστη και του συστήματος μας προσθέσαμε και τα εξής επιπρόσθετα προγράμματα:

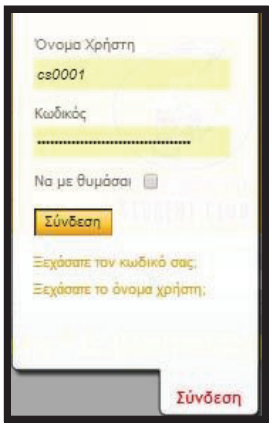
- Το δωρεάν plugin με όνομα SSL Redirection στην 0.9.8 έκδοση
- Το δωρεάν plugin με όνομα Brute Force Stop στην 1.0.0 έκδοση
- Το δωρεάν component Encryption Configuration στην 2.0.6 έκδοση

Το SSL Redirection plug-in δημιουργεί μια ανακατεύθυνση μη ασφαλούς HTTP σελίδας ώστε να εξασφαλιστεί η συνέχιση σε HTTPS σελίδες, με σκοπό τη στιγμιαία διασφάλιση της μεταφοράς ευπαθών δεδομένων όπως είναι ο προσωπικός κωδικός ενός χρήστη. Το plug-in καθολικές ή και μεμονωμένες ενέργειες στις οποίες θα εφαρμόζεται αυτή η διαδικασία. Στο σύστημα έχει ορισθεί η διαδικασία της ψηφοφορίας να υπόκειται σε τέτοιου είδους σύστημα ασφάλειας για μεγαλύτερη διασφάλιση της εγκυρότητας των αποτελεσμάτων της.

Επιπρόσθετα, το Brute Force Stop plug-in παρέχει τα μέσα για την αποτροπή Brute Force επιθέσεων σε συστήματα Joomla. Όταν μιλάμε για Brute Force επιθέσεις εννοούμε τις

αποτυχημένες προσπάθειες σύνδεσης με σκοπό είτε την εύρεση των προσωπικών κωδικών σύνδεσης είτε την υπερφόρτωση της ευρύτερης λειτουργίας του συστήματος. Η λειτουργία του στηρίζεται στην καθαρή από αποθήκευση των αποτυχημένων προσπαθειών σύνδεσης και μόλις το πλήθος τους φθάσει στο ρυθμιζόμενο μέγιστο αριθμό τέτοιων αποτυχιών login από κάθε μία διεύθυνση IP του εισβολέα θέτει σε εφαρμογή το συνολικό μπλοκάρισμα της. Επίσης, ενημερώνει σχετικά με τις αποτυχημένες απόπειρες και τα μπλοκαρίσματα των διευθύνσεων IP.

Τέλος, το component encryption configuration προσφέρει στους χρήστες που επιχειρούν να συνδεθούν στο σύστημα με τα προσωπικά τους στοιχεία – είτε είναι απλοί εγγεγραμμένοι χρήστες είτε διαχειριστές – μια επιπλέον κρυπτογράφηση του κωδικού τους ώστε να μην μπορεί να υποκλαπεί κατά τη διάρκεια των πακέτων μεταφοράς μεταξύ του τερματικού και του συστήματος. Σημαντική παρατήρηση είναι και το γεγονός ότι η προσφερόμενη ασφάλεια παρέχετε καθαρά από την πλευρά του client. Έτσι, κατά το πάτημα του κουμπιού σύνδεσης του χρήστη προσθέτει επιπλέον χαρακτήρες στα ήδη πληκτρολογημένα ψηφία με σκοπό να μη μπορεί να καταγραφεί εύκολα και το πλήθος των χαρακτήρων που απαρτίζουν τον εκάστοτε κωδικό σύνδεσης (Εικόνα 19). Στο σύστημα μας έχουμε ορίσει προσωπικό κωδικό του χρήστη *cs0001* τεσσάρων ψηφίων ενώ το component αυτό τον «αλλοιώνει» σε πολλά περισσότερα ψηφία. Το ίδιο συμβαίνει κατά την είσοδο ενός διαχειριστή είτε στην ίδια φόρμα σύνδεσης είτε στην ειδική φόρμα σύνδεσης των διαχειριστών που τους δίνει πρόσβαση στα εργαλεία διαχείρισης του συστήματος.



Εικόνα 19: Εφαρμογή encryption configuration

8.10 Ασφάλεια Σύνδεσης Διαχειριστών

Το Joomla δίνει τη δυνατότητα στους διαχειριστές να συνδέονται σε ειδική φόρμα με τον πίνακα ελέγχου του συστήματος. Αυτή η διεύθυνση βρίσκεται κάτω από την διαδρομή

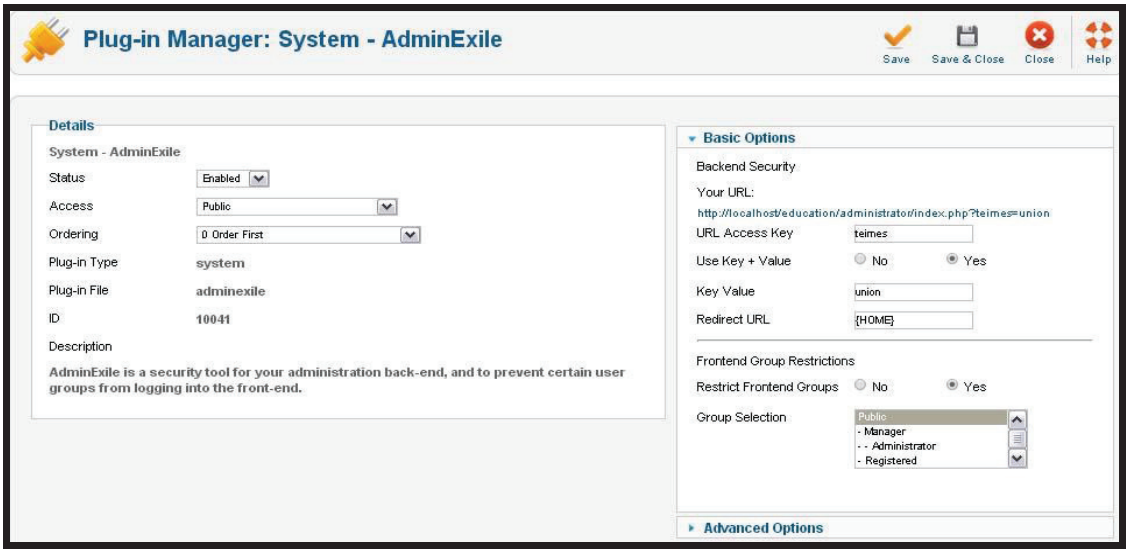
/administrator και είναι προς δημόσια χρήση. Η διαδρομή αυτή θεωρείται από τους προγραμματιστές ένα χαρακτηριστικό στοιχείο από το οποίο μπορούν πολύ εύκολα να προσδιορίσουν το είδος αλλά και την έκδοση της πλατφόρμας που χρησιμοποιείται σε μια ιστοσελίδα. Το γεγονός αυτό, καθιστά κάθε ιστοσελίδα πιθανό στόχο επιθέσεων και μάλιστα τον πιο εύκολο σε σχέση με τις υπόλοιπες. Δεδομένου ότι ένα τέτοιο στοιχείο αυξάνει τις πιθανότητες το να τεθεί το σύστημα μας στόχος επιθέσεων, αναζητήσαμε μία αξιόπιστη και αποτελεσματική λύση.

Για να μπορέσουμε να απαλλαγούμε από αυτή την πιθανότητα χρησιμοποιήσαμε το plug-in με όνομα AdminExile στην 2.1.3 έκδοση του. Το AdminExile λειτουργεί κατά κύριο λόγο ως ένα πρόγραμμα που θέτει εκτός λειτουργίας την παραδοσιακή διεύθυνση σύνδεσης στον πίνακα ελέγχου των διαχειριστών και την οποία διαθέτει το Joomla εκ κατασκευής. Όσοι ασχολούνται με το Joomla, αλλά ιδίως οι hackers, γνωρίζουν πως το εν λόγω σύστημα διαχείρισης περιεχομένου χρησιμοποιεί τη διαδρομή "*/administrator*" για τη σύνδεση των διαχειριστών στα εργαλεία παραμετροποίησης του. Μία τέτοια πληροφορία είναι χρήσιμη στους hackers μιας και επιβεβαιώνουν τη χρήση του Joomla και εκμεταλλεύονται πιθανές λάθος παραμετροποιήσεις ή ακόμα και τρύπες του ίδιου του συστήματος ή των επιπρόσθετων προγραμμάτων του. Το AdminExile ακυρώνει την παραδοσιακή διαδρομή σύνδεσης των διαχειριστών και προσφέρει μία νέα διαδρομή η οποία περιέχει μία ή και δύο λέξεις κλειδιά για μεγαλύτερη ασφάλεια. Οι λέξεις αυτές είναι επιλογή των διαχειριστών του συστήματος. Επιπλέον, έχει την ικανότητα να ελέγχει κατά πόσο ο κάθε λογαριασμό είναι ενεργός μόνο για back-end χρήση. Αυτός ο έλεγχος περιορίζει την χρήση λογαριασμών ως front-end ενώ έχουν δηλωθεί ως back-end. Πέρα από την ανάκτηση των χαμένων κλειδιών, αυτό το plug-in έχει τη δυνατότητα να παρέχει κυρώσεις στους χρήστες που κάνουν κατάχρηση των υπηρεσιών ή/και των λειτουργιών του συστήματος (το λεγόμενο Brute Force Protection). Η black/white λίστα είναι ένα επιπλέον δυνατό σημείο του plug-in αυτού. Επιτρέπει τον άμεσο αποκλεισμό ή την άμεση πρόσβαση του αντίστοιχα στο σύστημα παρέχοντας ενημέρωση σχετικά με την ενέργεια στους διαχειριστές μέσω mail. Σημαντικό χαρακτηριστικό του AdminExile είναι και η μη χρήση των cookies στους διαχειριστές μέσω της λειτουργίας Stealth που διαθέτει.

Έτσι λοιπόν, στο σύστημα που κατασκευάσαμε η παραδοσιακή διεύθυνση σύνδεσης των διαχειριστών έχει μετασχηματιστεί σε: "/ administrator/index.php?teimes=union" (Εικόνα 20). Για να κατανοήσουμε πλήρως τη λειτουργία της παραδοσιακής διεύθυνσης και τις μετασχηματισμένης λόγω του AdminExile, έχουμε προσθέσει στο κεντρικό μενού της ιστοσελίδας μας δύο δημόσιους συνδέσμους:

- Σύνδεση Διαχειριστών (χωρίς ασφάλεια)
- Σύνδεση Διαχειριστών (με ασφάλεια)

Η σύνδεση διαχειριστών (χωρίς ασφάλεια) εμφανίζεται δημόσια ακόμα και στους επισκέπτες. Αντιθέτως, η σύνδεση διαχειριστών (με ασφάλεια) εμφανίζεται μόνο στους εγγεγραμμένους χρήστες και άνω. Εξετάζοντας καθαρά την αλλαγή αυτή από πλευράς ασφάλειας, διαπιστώνουμε πως σε ένα σύστημα που γνωστοποιείται είτε δημόσια είτε ιδιωτικά κατά κάποιο τρόπο αποτελεί μείζον θέμα. Θέτοντας την πλατφόρμα αυτή που κατασκευάστηκε σε πλήρη δημόσια λειτουργία και τα δύο ήδη σύνδεσης των διαχειριστών δε θα πρέπει να υφίσταντο. Οι διαχειριστές οφείλουν να απομνημονεύουν τη διαδρομή αυτή χωρίς να την αποθηκεύουν στον κατάλογο με τα αγαπημένα του φυλλομετρητή τους.



Εικόνα 20: Ρυθμίσεις του plug-in AdminExile

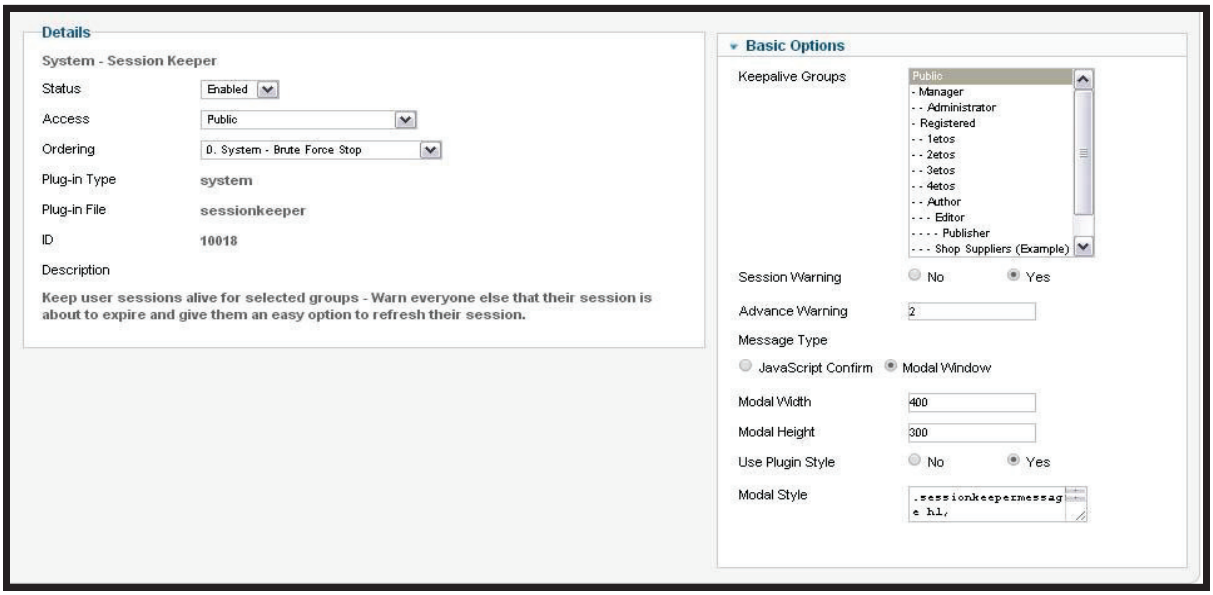
Επιπρόσθετος παράγοντας για τη διασφάλιση της ασφάλειας κατά τη διαδικασία της σύνδεσης των διαχειριστών στον πίνακα ελέγχου της πλατφόρμας είναι και το γεγονός ότι δε θα πρέπει να χρησιμοποιούν την απομνημόνευση των στοιχείων σύνδεση τους μέσω της τεχνολογίας των cookies. Το Joomla, όπως και όλες οι ιστοσελίδες ανεξαρτήτου την ύπαρξης ή όχι ενός συστήματος διαχείρισης περιεχομένου, χρησιμοποιεί την τεχνολογία των http cookies, όπου στην ουσία είναι ένα μικρό κομμάτι δεδομένων που αποστέλλονται από μια ιστοσελίδα και αποθηκεύεται στο φυλλομετρητή του χρήστη κατά τη διάρκεια της περιήγησης του. Το cookie έχει ως ρόλο να στέλνετε πίσω στο server κάθε φορά που ο χρήστης φορτώνει την ιστοσελίδα,

ενημερώνοντας με αυτό τον τρόπο τον δικτυακό τόπο για προηγούμενες δραστηριότητες του, όπως για παράδειγμα εάν ήταν συνδεδεμένος με προσωπικά στοιχεία (usrename/password) και ποια είναι αυτά.

Λαμβάνοντας υπόψη αυτή τη τεχνολογία οι διαχειριστές, για καθαρά λόγους ασφάλειας δεν θα πρέπει να αποθηκεύουν τα στοιχεία της σύνδεσης τους ούτε στον τοπικό τους υπολογιστή αλλά ούτε σε φορητές συσκευές όπως laptops ή smartphones.

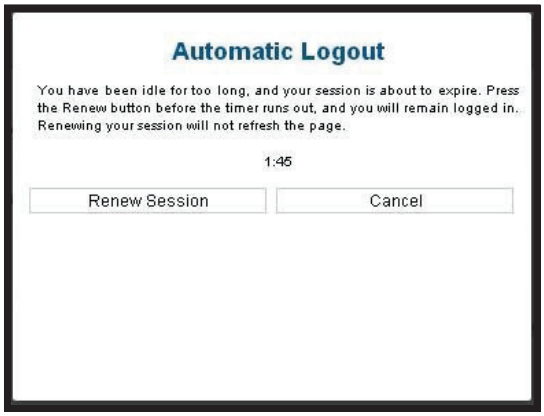
Δε θα πρέπει να παραλείψουμε να αναφέρουμε ότι πέρα από την αποφυγή αποθήκευσης των στοιχείων σύνδεσης των διαχειριστών σε οποιοδήποτε είδος συσκευής, σημαντικός παράγοντας είναι και ο χρόνος αδράνειας της σύνδεσης των διαχειριστών. Με τον όρο χρόνο αδράνειας εννοούμε το χρόνο που έχει περάσει από τη τελευταία κίνηση του διαχειριστή κατά τη διάρκεια της ενεργής σύνδεσης του. Συχνά, οι διαχειριστές συνδέονται στα πληροφοριακά συστήματα που εποπτεύουν και ενώ έχουν ολοκληρώσει τις ενέργειες και τις αλλαγές που ήθελαν να κάνουν, για παράδειγμα στις ρυθμίσεις του συστήματος, αφήνουν τον φυλλομετρητή τους συνδεδεμένο με τα προσωπικά τους στοιχεία. Από την κατασκευή του το Joomla δεν έχει την προγραμματιστική μέριμνα να αποσυνδέει τους διαχειριστές όταν αυτοί βρίσκονται σε αποδεδειγμένη αδράνεια. Αυτό έχει σαν αποτέλεσμα να υπάρχει πάντα ο κίνδυνος μια κακόβουλης επίθεσης εξαιτίας της συνεχιζόμενης σύνδεσης των διαχειριστών χωρίς μάλιστα να κρίνεται και αναγκαία.

Γι’ αυτό το λόγο, χρησιμοποιήσαμε το plug-in με όνομα Session Keeper στην έκδοση 1.1. Το Session Keeper μπορεί να τροποποιεί τη διάρκεια σύνδεσης όλων των χρηστών μια ιστοσελίδας με βάση την κατηγορία στην οποία ανήκουν. Ο ρόλος του plug-in αυτού είναι διπλός: α) επεκτείνει τη διάρκεια της συνεδρίας των διαχειριστών εφόσον αυτό κριθεί απαραίτητο και β) περιορίζει τη διάρκεια της συνεδρίας των χρηστών και των διαχειριστών (Εικόνα 21a).



Εικόνα 21a: Ρυθμίσεις του plug-in Session Keeper

Μια επιπλέον επιλογή του plug-in, είναι ένα προειδοποιητικό μήνυμα – με τη χρήση ενός Javascript ή Modal παράθυρου που περιλαμβάνει ένα χρονόμετρο αντίστροφης μέτρησης – δίνει τη δυνατότητα να προσδιοριστεί το χρονικό διάστημα πριν από τη λήξη της σύνδεσης/συνεδρίας (Εικόνα 21b).



Εικόνα 21b: Μήνυμα ανανέωσης συνεδρία χρήστη

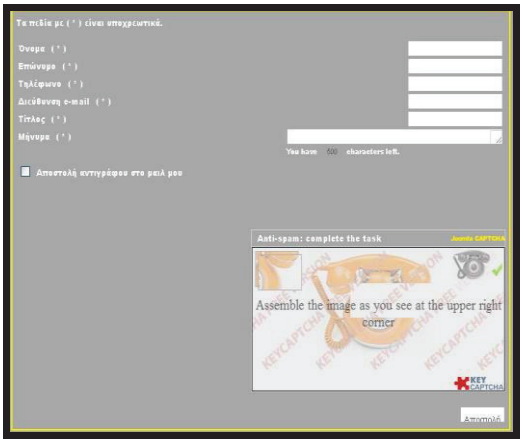
Εικόνα 21c: Μήνυμα λήξης συνεδρίας

Το μήνυμα αυτό αφήνει στο χρήστη χρόνο για επανασύνδεση χωρίς να χρειάζεται να ανανεώσει τη σελίδα. Φυσικά ο χρήστης μπορεί επίσης να επιλέξει να απορρίψει το μήνυμα είτε ακυρώνοντας το είτε αγνοώντας το κάτι που δε θα παρεμβάλει τη διάρκεια της λήξης της συνεδρίας. Εφόσον ο χρόνος λήξης παρέλθει ο χρήστης λαμβάνει ένα μήνυμα ειδοποίησης για τη λήξη της σύνδεσης του (Εικόνα 21c).

8.11 Υπηρεσία Επικοινωνίας

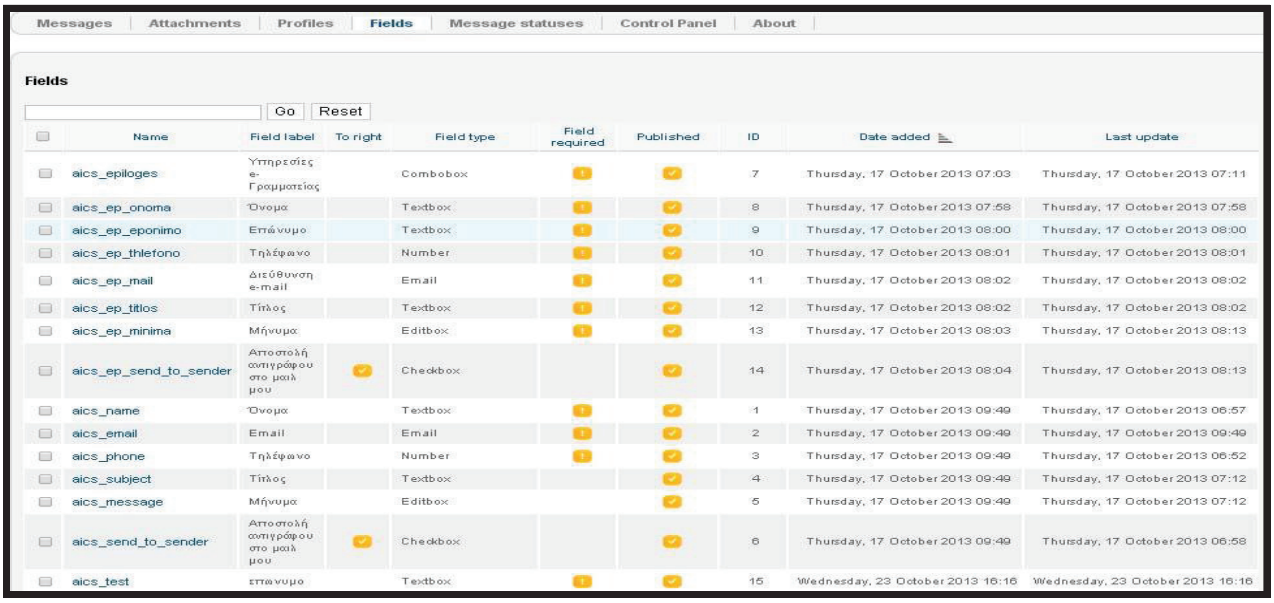
Για τις ανάγκες αυτής της λειτουργίας έχει χρησιμοποιηθεί το component aiContactSafe στην έκδοση 2.0.21c.stable. Πρόκειται για μια εφαρμογή που εντάσσεται στο Joomla και παρέχεται δωρεάν στους χρήστες του συστήματος. Η εφαρμογή αυτή δίνει τη δυνατότητα στους διαχειριστές να δημιουργήσουν εύκολα, γρήγορα, και αξιόπιστα μια ή περισσότερες φόρμες επικοινωνίας. Αυτό επιτυγχάνεται με τη δυνατότητα που παρέχει η εφαρμογή στο να

δημιουργηθούν παραπάνω από ένα προφίλ. Το προφίλ έχει την ιδιότητα να κατηγοριοποιεί τις φόρμες κάτω από μία ονομασία. Για παράδειγμα, για τις ανάγκες του συστήματος που δημιουργήσαμε έπρεπε να κατασκευαστούν δύο διαφορετικές φόρμες επικοινωνίας: α) μία για τους επισκέπτες του συστήματος απλά για να αποστέλλουν τα ερωτήματα ή τα όποια αιτήματα έχουν από το πανεπιστήμιο (Εικόνα 22α), και β) μια για τους εγγεγραμμένους χρήστες, δηλαδή τους φοιτητές, όπου θα τους δίνει την υπηρεσία είτε να αποστείλουν ηλεκτρονικά αιτήματα στην γραμματεία για έκδοση αναλυτικής βαθμολογίας είτε να αιτηθούν την εγγραφή τους στο επόμενο έτος φοίτησης (Εικόνα 22β).



Εικόνα 22α: Φόρμα Επικοινωνίας Επισκεπτών **Εικόνα 22β:** Φόρμα Επικοινωνίας Φοιτητών

Αξίζει να σημειωθεί πως η εφαρμογή αυτή προσφέρει τη δυνατότητα να εντάξουμε τα πεδία που επιθυμούμε σε κάθε προφίλ δηλαδή σε κάθε φόρμα ξεχωριστά όπως φαίνεται και στην εικόνα 17. Επίσης, μπορούν όλοι οι διαχειριστές να παρακολουθούν τα αιτήματα μαζικά όλων των φορμών μέσα από την ίδια την εφαρμογή ως καθαρά συμπληρωματική υπηρεσία ενημέρωσης (Εικόνα 23).



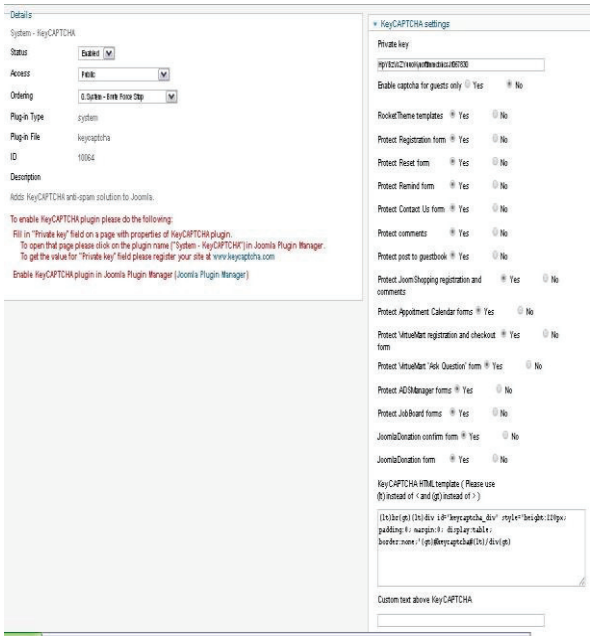
Εικόνα 23: Πεδία φορμών επικοινωνίας aiContactSafe

Αναφέρουμε ότι είναι καθαρά συμπληρωματική υπηρεσία μιας και η εφαρμογή aiContactSafe υποστηρίζει και την αποστολή e-mail σε διευθύνσεις που έχουν ορισθεί από τους διαχειριστές. Έτσι με τον τρόπο αυτό μπορούν για παράδειγμα να ενημερώνονται για τα αιτήματα ταυτόχρονα και η γραμματεία αλλά και οι διαχειριστές του συστήματος.

Εικόνα 24: Λίστα μηνυμάτων μέσω των φορμών επικοινωνίας της εφαρμογής aiContactSafe

8.12 Ασφάλεια Υπηρεσίας Επικοινωνίας

Το πρόγραμμα aiContactSafe προσφέρει τη δημιουργία φορμών στο σύστημα Joomla. Ωστόσο δεν είναι σε θέση να προστατέψει συνολικά το σύστημα μας από πιθανές επιθέσεις όπως για παράδειγμα από μια μαζικά ταυτόχρονη υποβολή αιτημάτων επικοινωνίας από τη δημόσια φόρμα των επισκεπτών. Η εν λόγω επίθεση στηρίζεται στο γεγονός ότι πολλοί υπολογιστές-κλώνοι του βασικού υπολογιστή προσθέτουν αιτήματα επικοινωνίας άνευ ουσιαστικού περιεχομένου – τα ονομαζόμενα και ως σκουπίδια – με σκοπό την στιγμιαία υπερφόρτωση των υπηρεσιών της ιστοσελίδας αλλά και την αύξηση του μεγέθους των δεδομένων της βάσης με σκοπό την επιβράδυνση της λειτουργίας της. Γι' αυτό το λόγο, κρίθηκε επιτακτική ανάγκη η χρήση του keycaptcha ενός δωρεάν επιπρόσθετου προγράμματος anti-spam captcha λειτουργίας. Με αυτό το plug-in προστίθεται ένα υποτυπώδες πάζλ σε κάθε φόρμα που ζητά από τον χρήστη να το λύσει (Εικόνα 25). Έτσι, διασφαλίζεται πως ο χρήστης είναι υπαρκτός και όχι κάποιο robot- δηλαδή πρόγραμμα – που συμπεριφέρεται σαν να είναι χρήστης. Όπως και κάθε plug-in η ρύθμιση του είναι απλή ενώ για την ενεργοποίηση του απαιτείται η έκδοση ενός private key από την επίσημη ιστοσελίδα του keycaptcha (Εικόνα 26).



Εικόνα 25: Πάζλ keycaptcha plug-in **Εικόνα 26:** Ρυθμίσεις keycaptcha plug-in

Με τον τρόπο που περιγράψαμε παραπάνω μπορούμε να διασφαλίσουμε την πραγματική υπόσταση του χρήστη και να την ξεχωρίσουμε από αυτή μιας οργανωμένης επίθεσης που στόχο έχει να πλήξει τη σωστή λειτουργία των υπηρεσιών. Εναλλακτικός τρόπος για αυτή την υπηρεσία ο οποίος συνηθίζεται να χρησιμοποιείται είναι και η πληκτρολόγηση από τον χρήστη

μιας τυχαίας σειράς γραμμάτων ή/και αριθμών ή ακόμα και το αποτέλεσμα από μία απλή δοθείσας μαθηματικής πράξης.

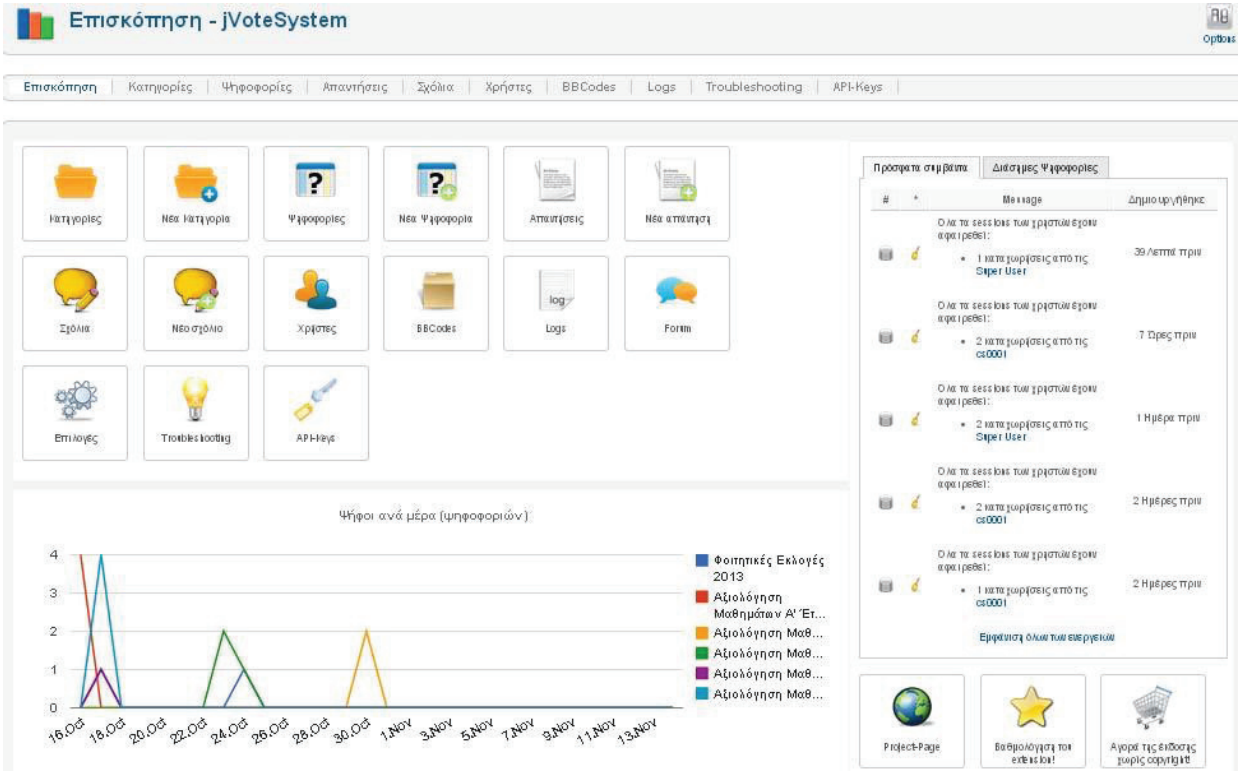
Σημαντικό στοιχείο για την φόρμα επικοινωνίας των εγγεγραμμένων χρηστών που δε θα πρέπει να παραλείψουμε είναι και το γεγονός πως δεν ζητείται εκ νέου ο χρήστης να πληκτρολογήσει τα προσωπικά του στοιχεία – όπως τον κωδικό του, το username του αλλά και το e-mail του – μιας και εμφανίζονται από μόνα τους. Με αυτό τον τρόπο κάθε αίτημα προς την e-γραμματεία θα είναι πλήρως συμπληρωμένο ώστε να διασφαλίζεται και η εγκυρότητα του.

8.13 Σύστημα Ηλεκτρονικής Ψηφοφορίας

Για τις ανάγκες της ηλεκτρονικής ψηφοφορίας έχει χρησιμοποιηθεί το component jVoteSystem στην 2.56 έκδοση του. Το πακέτο αυτό προσφέρει στην πλατφόρμα μας την υπηρεσία των ψηφοφοριών με τρόπο οργανωμένο, αξιόπιστο, έγκυρο και αποτελεσματικό. Οι λειτουργική του διαχείριση συνοψίζεται στις παρακάτω καρτέλες διαχείρισης:

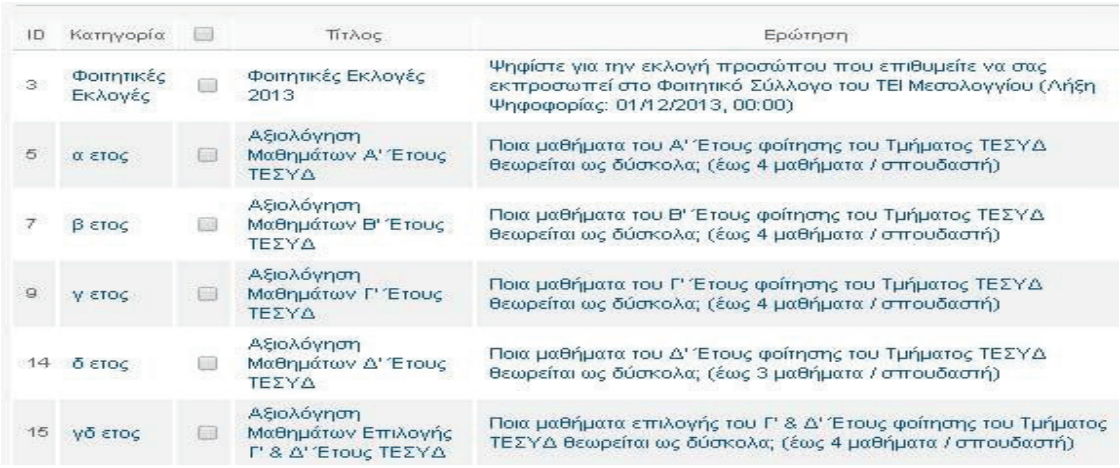
- Επισκόπηση
- Κατηγορίες
- Ψηφοφορίες
- Απαντήσεις
- Σχόλια
- Χρήστες
- BBCodes
- Logs
- Troubleshooting
- API-keys

Όλες οι δυνατότητες του προγράμματος είναι οργανωμένες στην καρτέλα της επισκόπησης, η οποία αποτελεί τη γενική διαχειριστική κονσόλα του προγράμματος jVoteSystem δίνοντας στους διαχειριστές την ικανότητα της άμεσης εποπτείας τόσο από πλευράς λειτουργίας όσο και από πλευράς σφαλμάτων κατά τη διάρκεια των ψηφοφοριών. Οι διαχειριστές μπορούν να επεξεργαστούν ή να προσθέσουν είτε μια κατηγορία, είτε μια ψηφοφορία, είτε μια απάντηση, είτε ένα σχόλιο, ενώ μπορούν να διαγράψουν έναν ή και περισσότερους χρήστες από την υπηρεσία της ψηφοφορίας (Εικόνα 27). Σημαντικό στοιχείο για την άμεση εποπτεία των διαχειριστών αποτελεί και το κομμάτι που αναφέρει άμεσα και περιληπτικά τόσο τα πιο πρόσφατα συμβάντα όσο και τη λίστα με τις ψηφοφορίες που έχουν προστεθεί στο σύστημα συνολικά.



Εικόνα 27: Πίνακας Διαχείρισης jVoteSystem

Αξίζει να σημειωθεί πως ο ρόλος των κατηγοριών των ψηφοφοριών αποτελεί τον βασικό παράγοντα ώστε η κάθε ψηφοφορία να είναι ενεργή προς συμμετοχή μόνο στους φοιτητές που έχουν δικαίωμα να καταχωρήσουν τη ψήφο τους. Για παράδειγμα, έχουμε δημιουργήσει τις κατηγορίες της Εικόνας 28 οι οποίες αντιστοιχούν σε κάθε μια ψηφοφορία ξεχωριστά.

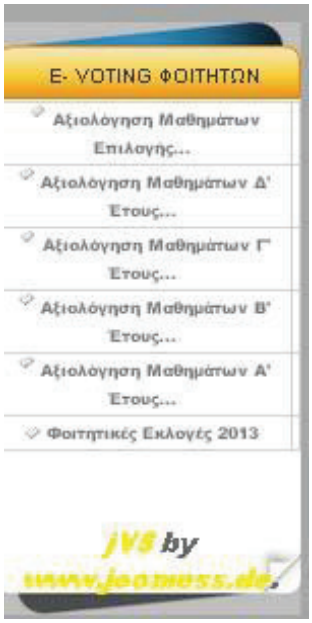


ID	Κατηγορία		Τίτλος	Ερώτηση
3	Φοιτητικές Εκλογές		Φοιτητικές Εκλογές 2013	Ψηφίστε για την εκλογή προσώπου που επιθυμείτε να σας εκπροσωπεί στο Φοιτητικό Σύλλογο του ΤΕΙ Μεσολογγίου (Λήξη Ψηφοφορίας: 01/12/2013, 00:00)
5	α ετος		Αξιολόγηση Μαθημάτων Α' Έτους ΤΕΣΥΔ	Ποια μαθήματα του Α' Έτους φοίτησης του Τμήματος ΤΕΣΥΔ θεωρείται ως δύσκολα; (έως 4 μαθήματα / σπουδαστή)
7	β ετος		Αξιολόγηση Μαθημάτων Β' Έτους ΤΕΣΥΔ	Ποια μαθήματα του Β' Έτους φοίτησης του Τμήματος ΤΕΣΥΔ θεωρείται ως δύσκολα; (έως 4 μαθήματα / σπουδαστή)
9	γ ετος		Αξιολόγηση Μαθημάτων Γ' Έτους ΤΕΣΥΔ	Ποια μαθήματα του Γ' Έτους φοίτησης του Τμήματος ΤΕΣΥΔ θεωρείται ως δύσκολα; (έως 4 μαθήματα / σπουδαστή)
14	δ ετος		Αξιολόγηση Μαθημάτων Δ' Έτους ΤΕΣΥΔ	Ποια μαθήματα του Δ' Έτους φοίτησης του Τμήματος ΤΕΣΥΔ θεωρείται ως δύσκολα; (έως 3 μαθήματα / σπουδαστή)
15	γδ ετος		Αξιολόγηση Μαθημάτων Επιλογής Γ' & Δ' Έτους ΤΕΣΥΔ	Ποια μαθήματα επιλογής του Γ' & Δ' Έτους φοίτησης του Τμήματος ΤΕΣΥΔ θεωρείται ως δύσκολα; (έως 4 μαθήματα / σπουδαστή)

Εικόνα 28: Πίνακας Διαχείρισης jVoteSystem

Για να μπορέσουμε να δημιουργήσουμε στο σύστημα τα απαραίτητα δικαιώματα σε κάθε έναν χρήστη μεμονωμένα κατηγοριοποιήσαμε καταρχήν τους φοιτητές ανά εξάμηνο φοίτησης. Έτσι λοιπόν στην κατηγορία «α' Έτος» εντάξαμε όλους τους πρωτοετής φοιτητές. Ομοίως αντίστοιχα και τις κατηγορίες των υπόλοιπων ετών φοίτησης. Με αυτό τον τρόπο διασφαλίσαμε ότι ο κάθε φοιτητής θα μπορεί να ψηφίσει μόνο εφόσον είναι εγγεγραμμένος επίσημα στο συγκεκριμένο έτος φοίτησης που απαιτεί η ψηφοφορία και για το τρέχων μόνο ακαδημαϊκό έτος. Υπενθυμίζουμε πως τα στοιχεία των εγγραφών ανά έτος των φοιτητών ανανεώνονται κάθε χρόνο στο σύστημα του Joomla με βάση τις ετήσιες αιτήσεις όλων των φοιτητών για την εγγραφή τους στο επόμενο έτος. Όσο αναφορά για την κατηγορία με τίτλο «Φοιτητικές Εκλογές» σε αυτή είναι ενταγμένοι όλοι οι φοιτητές ανεξαρτήτου έτους φοίτησης μιας και έχουν δικαίωμα βάση του νόμου να συμμετέχουν στην ετήσια ψηφοφορία των φοιτητικών αντιπροσώπων της σχολής τους.

Επομένως, όταν ένας χρήστης εισέλθει στο σύστημα με τα προσωπικά του στοιχεία κάτω από το μενού του χρήστη του εμφανίζεται και το μενού των ψηφοφοριών (e-voting Φοιτητών), είτε έχει δικαίωμα να ψηφίσει είτε έχει μόνο δικαίωμα να έχει γνώση για την εξέλιξη της ψηφοφορίας και τα αποτελέσματα της (Εικόνα 28).

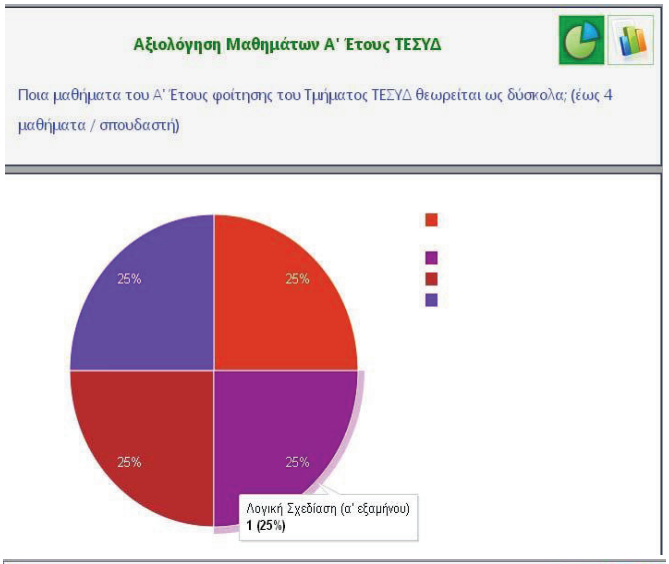


Εικόνα 29: Μενού e-voting φοιτητών με τη χρήση του jVoteSystem

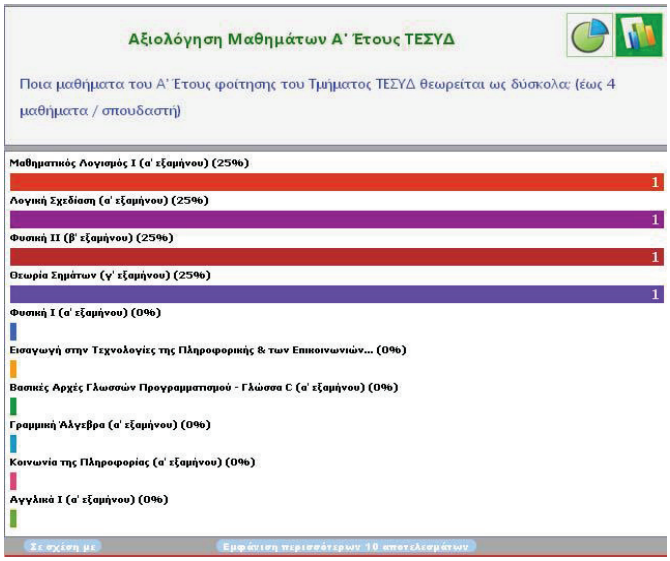
Με πρόγραμμα jVoteSystem είμαστε σε θέση να ορίσουμε το πλήθος των ψήφων που μπορεί να υποβάλει ο κάθε χρήστης ενώ μπορούμε να ορίσουμε και άλλες παραμέτρους, όπως για παράδειγμα την ημερομηνία έναρξης και λήξης για την κάθε ψηφοφορία καθώς και το εάν θα μπορούν οι ψηφοφόροι θα μπορούν να προσθέσουν το δικό τους σχόλιο σε κάθε μία ψηφοφορία. Χαρακτηριστικό στοιχείο των ετήσιων φοιτητικών εκλογών είναι η διάρκεια – μιας μέρας – που μπορεί κάποιος να υποβάλει τη ψήφο του. Έτσι ορίσαμε μια συγκεκριμένη περίοδο διάρκειας 3 μηνών ιδανική για να προσδιοριστεί και ο τρόπος που αναφέρετε μέσα στην ίδια την ερώτηση της ψηφοφορίας. Με τον ίδιο τρόπο εμφανίζεται και το υπόλοιπο πλήθος των ψήφων που απομένουν σε κάθε χρήστη αλλά και το κατά πόσο έχει δικαίωμα συμμετοχής (Εικόνα 29).

Εικόνα 30: Υπολειπόμενες ψήφοι ανά χρήστη

Επίσης, μία σημαντική παράμετρος των ψηφοφοριών είναι να εμφανίζει τα αποτελέσματα υπό τη μορφή είτε διαγράμματος πίτας είτε ραβδοειδούς διαγράμματος (Εικόνες 31, 32). Αυτή η επιλογή μπορεί να απενεργοποιηθεί όπως έχουμε κάνει με τις «Φοιτητικές Εκλογές 2013» όπου κάθε είδους στατιστικά έχουν απενεργοποιηθεί μέχρι να ολοκληρωθεί πλήρως η ψηφοφορία όπως ορίζει και ο νόμος διεξαγωγής των εκλογών (Εικόνα 33).



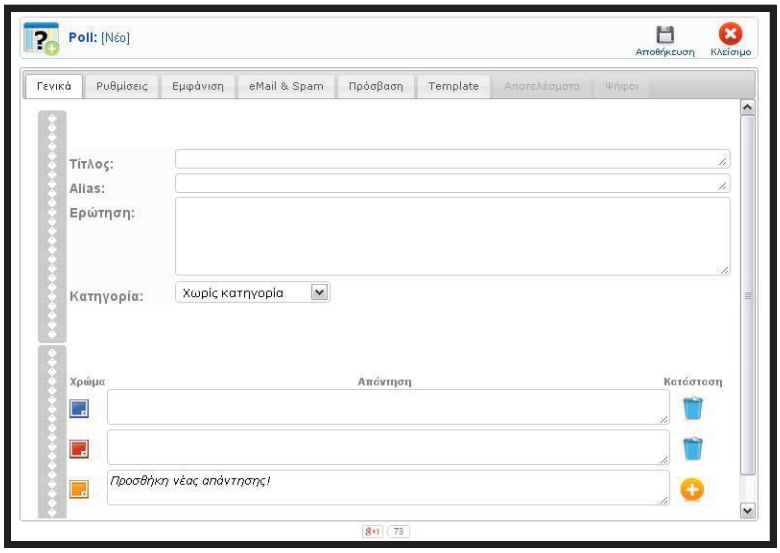
Εικόνα 31: Προβολή αποτελεσμάτων μορφής πίτας



Εικόνα 32: Προβολή αποτελεσμάτων ραβδοειδούς μορφής

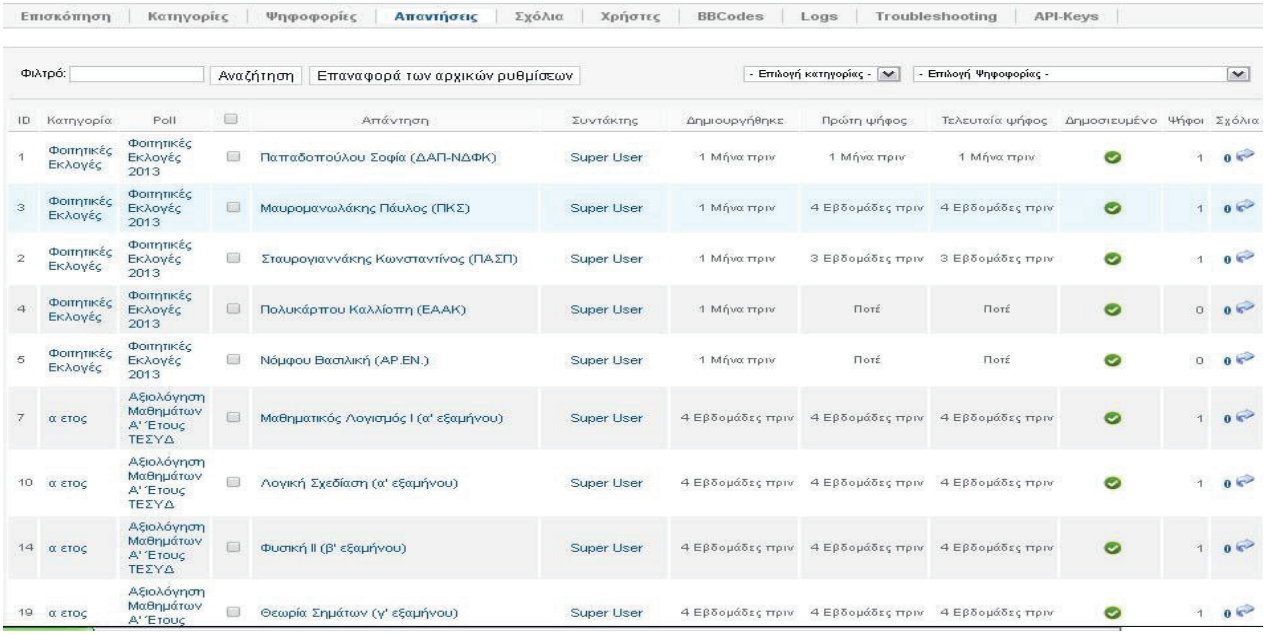
Εικόνα 32: Προβολή απενεργοποιημένων αποτελεσμάτων

Επιπλέον, όπως αναφέραμε και παραπάνω οι διαχειριστές μπορούν να δημιουργήσουν νέες ψηφοφορίες όπως φαίνεται και στην εικόνα 28 ορίζοντας τόσο την ερώτηση αλλά και τις επιλογές που καλούνται να επιλέξουν οι φοιτητές.

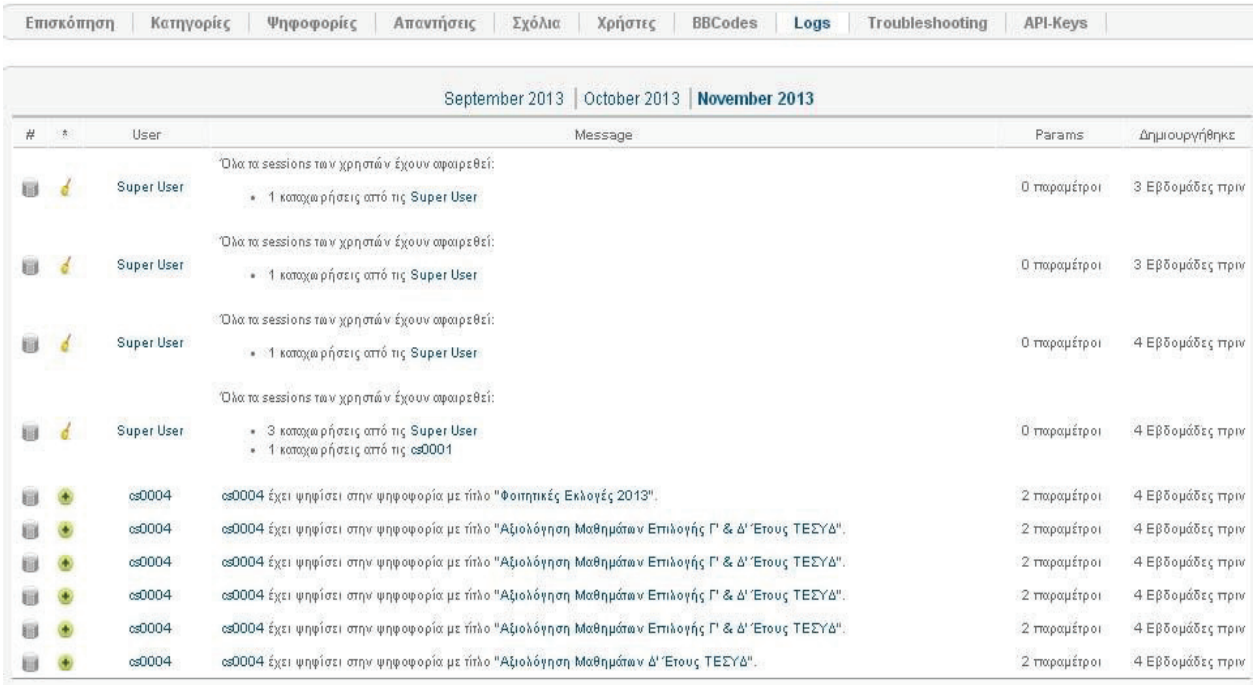


Εικόνα 33: Δημιουργία νέας ψηφοφορίας

Οι διαχειριστές μπορούν να επιβλέπουν όλες τις ενέργειες που πραγματοποιούνται σε όλο το σύστημα ψηφοφορία έχοντας ιεραρχημένες μία προς μία όλες τις κινήσεις ακόμα και αυτές των υπολοίπων διαχειριστών (Εικόνα 34, 35).



Εικόνα 34: Απαντήσεις ψηφοφοριών



Εικόνα 35: Καταγραφή ενεργειών όλων των χρηστών

8.14 Ασφάλεια Συστήματος Ψηφοφορίας

Το jVoteSystem εκ κατασκευής παρουσίαζε ανόμοια χαρακτηριστικά σε σχέση με τη χρήση που εμείς επιθυμούσαμε. Για να γίνουμε πιο συγκεκριμένοι, το component αυτό έχει κατασκευαστεί χωρίς να λαμβάνει υπόψη το δικαίωμα της κρυφής ψήφου του κάθε ψηφοφόρου. Τα περισσότερα λογισμικά που ασχολούνται με ψηφοφορίες στο διαδίκτυο διαθέτουν μεν το απόρρητο της ψήφου μεταξύ των ψηφοφόρων. Δεν ισχύει όμως το ίδιο και για τους διαχειριστές των συστημάτων που έχουν εντάξει τα λογισμικά αυτά. Ο παράγοντας αυτός σε μία επίσημη ψηφοφορία ενός δημόσιου ιδρύματος που διέπεται εκ των πραγμάτων από αυστηρούς δημοκρατικούς περιορισμούς θεωρείται μείζονος σημασίας και σπουδαιότητας.

Για να μπορέσουμε να προσαρμόσουμε τις υπηρεσίες του jVoteSystem σύμφωνα με τις ανάγκες και προδιαγραφές του ΤΕΣΥΔ, χρειάστηκε να παρέμβουμε στον κώδικά του. Οι παρεμβάσεις που κάναμε ήταν κυρίως δύο μορφών: α) στα στοιχεία της βάσης δεδομένων που αποθήκευε το λογισμικό, και β) στον πηγαίο κώδικα του λογισμικού όπου αντλούσε τα στοιχεία από τη βάση δεδομένων. Έτσι, με τις αλλαγές στον κώδικα του λογισμικού, καταφέραμε να απομακρύνουμε την όποια αναφορά στη λίστα των ενεργειών των διαχειριστών που είχε να κάνει με το περιεχόμενο της ψήφου του κάθε φοιτητή καθώς και την ικανότητα των διαχειριστών στην αλλαγή των ψήφων. Φυσικά, στην περίπτωση της αλλαγής των ψήφων από τους ίδιους τους διαχειριστές είναι μια ενέργεια πολύ σπάνια μιας και θεωρούνται άτομα απολύτου εμπιστοσύνης του ιδρύματος. Ακολουθήθηκε αυτή η ασφαλιστική δικλίδα ώστε να είναι πλήρως προστατευμένο και έγκυρο το σύνολο των ψήφων από άτομα που ενδεχομένως θα έχουν αποκτήσει δικαιώματα όμοια με αυτά των διαχειριστών.

Επιπρόσθετα, το jVoteSystem χρησιμοποιεί την επικύρωση μέσω των cookies, προκειμένου να αποτρέψει τους χρήστες από πολλαπλές ψήφους. Κάθε cookie έχει μια ιδιαίτερη διαδρομή που ορίζεται από το κεντρικό μενού παραμετροποίησης του Joomla. Κάθε φοιτητής όταν επισκέπτεται ξανά την ιστοσελίδα μιας ψηφοφορίας που έχει ήδη συμμετάσχει σε αυτή, του εμφανίζεται μήνυμα ότι έχει ήδη ψηφίσει και δεν επιτρέπεται να ξαναψηφίσει. Έτσι διασφαλίστηκε η μοναδικότητα αλλά και η εγκυρότητα κάθε ψήφου.

Αξίζει να σημειωθεί πως το περιεχόμενο των ψήφων, πλην των σχολίων που κατοχυρώνουν οι φοιτητές δημόσια, καταγράφονται μέσα στη βάση δεδομένων του

συστήματος διαχείρισης περιεχομένου κρυπτογραφημένα ώστε να μην είναι ορατό ακόμα και από τους ίδιους τους διαχειριστές. Η διαδικασία της κρυπτογράφησης είναι η ίδια με αυτή που ακολουθείται και για τα προσωπικά στοιχεία των εγγεγραμμένων χρηστών (δηλαδή αλγόριθμο md5 με 128-bit).

Επιπρόσθετα, έχει επιλεχτεί ως βασικός τρόπος σύνδεσης όλων των συνδέσεων καθώς και η διεξαγωγή των ψηφοφοριών με τη χρήση της τεχνολογίας https. Ωστόσο, η χρήση της απαιτεί την έκδοση ενός πιστοποιητικού ασφαλείας (security certificate) κάτι που το παρέχουν αποκλειστικά οι providers. Εξαιτίας του ότι η πλατφόρμα μας έχει τεθεί σε λειτουργία κάτω από την εποπτεία δωρεάν provider, δε μας δίνει τη δυνατότητα ορθής χρήσης του πρωτοκόλλου https παρά μόνο εφόσον γίνει η απαραίτητη αγορά αυτής της υπηρεσίας. Γι' αυτό το λόγο όλες μας οι συνδέσεις γίνονται χωρίς τη χρήση του πρωτοκόλλου https.

Υπό κανονικές συνθήκες, η εταιρεία που θα μας παρείχε την αποθήκευση των αρχείων μας – συμπεριλαμβανομένης και της βάσης δεδομένων – με πληρωμή θα εξέδιδε και ένα επίσημο πιστοποιητικό με την επωνυμία του ιδρύματος του ΤΕΣΥΔ. Έτσι, κάθε χρήστης θα γνώριζε ότι το πιστοποιητικό αυτό φέρει επίσημα την επωνυμία της σχολής του, θα αποδεχόταν τη χρήση του, άρα και τις υπηρεσίες που του προσφέρονται, και θα μπορούσε να συνδεθεί σε ένα ασφαλές περιβάλλον.

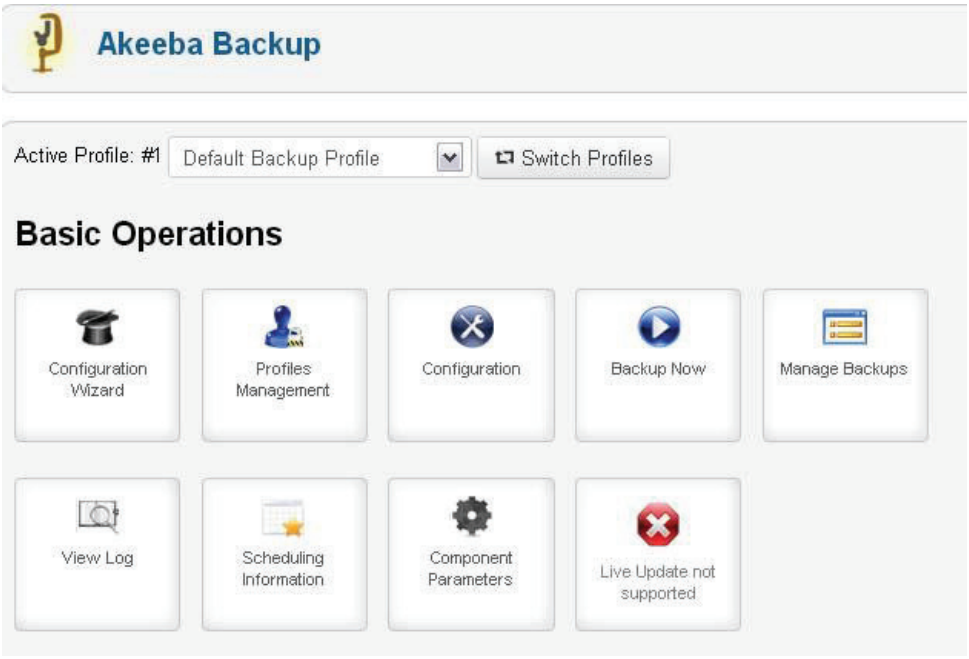
8.15 Χρήση Αντιγράφων Πλατφόρμας

Σημαντικός παράγοντας τόσο για τη διαδικασία της ψηφοφορίας όσο και για την ίδια την πλατφόρμα συνολικά είναι η συλλογή των απαραίτητων αντιγράφων. Τα αντίγραφα αυτά αφορούν ναι μεν τα αρχεία που γίνονται χρήση για τη δημιουργία κάθε ιστοσελίδας μας αλλά και τη βάση δεδομένων στην οποία αποθηκεύονται όλο το περιεχόμενο των σελίδων. Κάθε ιστοσελίδα είναι αναγκαίο να διαθέτει ένα σύστημα συλλογής αντιγράφων των αρχείων και του περιεχομένου της ιστοσελίδα ώστε ανά πάσα στιγμή να είναι διαθέσιμο στους διαχειριστές. Ο ρόλος των αντιγράφων είναι να διασφαλίζουν το περιεχόμενο και τις όποιες αλλαγές έχουν πραγματοποιηθεί σε αυτό με σκοπό την άμεση αντικατάσταση τους σε περίπτωση δυσλειτουργίας τους μερικώς ή ολικώς. Για παράδειγμα, συχνά παρατηρείται οι εισβολείς να αποκτούν πρόσβαση με σκοπό να αλλοιώσουν στοιχεία ή και όλο το περιεχόμενο μιας ιστοσελίδας καθαρά

για λόγους γοήτρου ή προσωπικής αναγνώρισης στο άμεσο περιβάλλον τους. Στη περίπτωση αυτή, η δυσλειτουργία που εμφανίζεται μπορεί να πλήττει μόνο την κεντρική σελίδα ή ακόμα και πλήθος αυτών.

Υπεύθυνοι για τη δημιουργία και οργάνωση αυτών των αντιγράφων είναι αποκλειστικά και μόνο οι διαχειριστές της πλατφόρμας. Τα αντίγραφα αυτά κατασκευάζονται μέσω του δωρεάν component με όνομα Akeeba Backup στην 3.8.2 έκδοση του. Το Akeeba Backup είναι ένα ανοιχτού κώδικα (open source) επιπρόσθετο πρόγραμμα δημιουργίας αντιγράφων ασφαλείας για το Joomla. Δηλαδή, δημιουργεί ένα αντίγραφο ασφαλείας που μπορεί να χρησιμοποιηθεί ως μέσω αποκατάστασης του server που φιλοξενεί το σύστημα διαχείρισης περιεχομενών του Joomla. Βασική του δυνατότητα είναι ότι μπορεί και δημιουργεί ένα αντίγραφο ασφαλείας της ιστοσελίδας σε ένα ενιαίο αρχείο. Το αρχείο αυτό περιέχει όλα τα επιμέρους αρχεία, ένα στιγμιότυπο της βάσης δεδομένων και ένα πρόγραμμα εγκατάστασης που μοιάζει λειτουργικά με αυτό του ίδιου του Joomla. Θα πρέπει να αναφέρουμε πως η δημιουργία αντιγράφων ασφαλείας και διαδικασία επαναφοράς AJAX είναι δυο στοιχεία που μας βοηθούν στο να αποφύγουμε πιθανά λάθη υπέρβασης χρόνου του διακομιστή. Η ιδιότητα της υπέρβασης χρόνου του διακομιστή είναι ένα στοιχείο ασφάλειας προκειμένου ο ίδιος ο διακομιστής να μπορεί να προσφέρει το καλύτερο των δυνατοτήτων του.

Το Akeeba Backup μας δίνει τη δυνατότητα να συλλέγουμε στιγμιαία αντίγραφα ολόκληρης της ιστοσελίδας ενώ μπορούμε να το χρησιμοποιήσουμε και ως μέσο για να φορτώσουμε το αντίγραφο μας στον διακομιστή. Επιπλέον, διαθέτει αναλυτικές ρυθμίσεις για τη σωστή λειτουργία του ώστε να μπορεί να χρησιμοποιείται και για μεγάλο όγκο αρχείων και δεδομένων στη βάση χωρίς να τίθεται ο διακομιστής εκτός επικοινωνίας. Επίσης, στην επί πληρωμή έκδοση παρέχει μία βασική λειτουργία στους διαχειριστές της ιστοσελίδας: τη δημιουργία αυτόματων αντιγράφων πλήρους περιεχομένου ανά χρονικές περιόδους που ορίζονται από τους διαχειριστές. (Εικόνα 36)



Εικόνα 36: Ρυθμίσεις Akeeba Backu

ΚΕΦΑΛΑΙΟ 9^{ο}: ΣΥΓΚΡΙΣΗ & ΑΞΙΟΛΟΓΗΣΗ ΣΥΣΤΗΜΑΤΩΝ e-VOTING

Όπως έχουμε αναφέρει ήδη, έγιναν ποικίλες προσπάθειες υιοθέτησης συστημάτων ηλεκτρονικής ψηφοφορίας από διάφορα κράτη της υφηλίου. Αξιολογώντας τα πιο σημαντικά διαπιστώνουμε τα ακόλουθα πλεονεκτήματα και μειονεκτήματα:

9.1 Πλεονεκτήματα Συστημάτων e-VOTING

- Καλύπτεται η ανάγκη για μείωση του κόστους διεξαγωγής των εκλογών με τον παραδοσιακό τρόπο μέσω της χρήσης ειδικών συστημάτων ηλεκτρονικής ψηφοφορίας,
- Επιτυγχάνεται η συμμετοχή των απόδημων ψηφοφόρων στις εθνικές εκλογές του κράτους τους λαμβάνοντας υπόψη και τη δικιά τους γνώμη-ψήφο,
- Παρέχετε σε ορισμένα συστήματα – π.χ. στο σύστημα της Εσθονίας – η δυνατότητα αλλαγής της ψήφου από τον κάτοχο του μέσα στα χρονικά πλαίσια διεξαγωγής της ψηφοφορίας,

- Αυτοματοποιούνται οι διαδικασίες ψηφοφορίας με αποτέλεσμα να αυξάνεται και η συμμετοχή των ψηφοφόρων σε αυτές,

- Ακολουθείται κυρίως ο τρόπος πιστοποίησης των ψηφοφόρων που εφαρμόζεται στις τραπεζικές συναλλαγές μέσω των ATM και των καρτών ανάληψης χρημάτων, κάτι που προσδίδει μεγαλύτερη ασφάλεια στον ψηφοφόρο για τη διεξαγωγή και τα αποτελέσματα των ψηφοφοριών,

- Γίνεται η χρήση νέων τεχνολογιών και προηγμένων συσκευών όπως ένα έξυπνο κινητό (smartphone) ως μέσω πιστοποίησης του ψηφοφόρου λόγω της αντιστοίχισης της κάρτας SIM του τηλεφώνου του με τα στοιχεία της ταυτότητας του,

9.2 Μειονεκτήματα Συστημάτων e-VOTING

- Ορισμένα συστήματα ηλεκτρονικής ψηφοφορίας όπως αυτό της Εσθονίας ενεργοποιούνται 2-4 ημέρες πριν την ημέρα των εκλογών ώστε να μπορεί να γίνει έγκαιρη καταγραφή και προσμέτρηση των ηλεκτρονικών ψήφων κατά την ημέρα των εκλογών.

- Η έλλειψη εγγύησης των συστημάτων για τη μη εξουσιοδοτημένη παρέμβαση τρίτων ατόμων στη διαδικασία της ψηφοφορίας, όπως για παράδειγμα την άρνηση της αποθήκευσης ή και της εκτύπωσης ενός εγγράφου ή μιας φόρμας αλλοιωμένης σε σχέση με αυτή που συμπληρώνει ηλεκτρονικά ο ψηφοφόρος.

- Πιο δύσκολη η ανίχνευση και ο εντοπισμός της πηγής των σφαλμάτων καθώς και των τεχνικών δυσλειτουργιών σε σχέση με τις παραδοσιακές/συμβατικές ψηφοφορίες.

- Υπάρχει πάντα η πιθανότητα ενός πλήρους ψηφιοποιημένου συστήματος να μη εξάγονται αποτελέσματα ή/και οι μηχανισμοί δημιουργίας αντιγράφων να μην τεθούν σε λειτουργία κάτι που θα δυσκολέψει ή και θα αποτρέψει την έγκαιρη και αξιόπιστη καταμέτρηση των ψήφων.

- Οι τεχνολογικές τους προδιαγραφές βασίζονται σε τεχνικές προστασίας που έχουν ήδη υιοθετηθεί από άλλα πληροφοριακά συστήματα κατόπιν σχετικών επιθέσεων ή/και ζημιών σε αυτά κάτι που απαιτούν συνεχή χρηματική

υποστήριξή βελτίωσης τους σύμφωνα με τα τρωτά σημεία που παρουσιάζονται παγκοσμίως.

Συγκρίνοντας δύο ή περισσότερα συστήματα e-voting μεταξύ τους, θα πρέπει να λάβουμε υπόψη μας τόσο στις τεχνολογίες που έχουν χρησιμοποιηθεί όσο και τις παρεχόμενες δυνατότητες/υπηρεσίες που προσφέρει το κάθε ένα. Αξίζει να επισημάνουμε πως τα περισσότερα συστήματα e-voting δεν ανήκουν στην κατηγορία των open-source προγραμμάτων αλλά υποστηρίζονται αποκλειστικά από τις εταιρείες που τα εμπορεύονται. Αυτό το στοιχείο προσδίδει από μόνο του μια επιπλέον ασφάλεια αλλά συνήθως δε μπορεί να καλύψει 100% της ανάγκες μιας ψηφοφορίας συνδυάζοντας ταυτόχρονα και το χαμηλό κόστος του. Το πλέον δωρεάν και πιο γνωστό προς χρήση συστήματος ηλεκτρονικής ψηφοφορίας είναι το Helios Voting. Οι υπηρεσίες του Helios Voting είναι αποκλειστικά μέσω διαδικτύου και δίνει τη δυνατότητα της ελεύθερη δημιουργία και διαχείριση μιας ψηφοφορίας από κάθε χρήστη του internet.

Το σύστημα αυτό υποστηρίζεται τεχνικά από την ίδια την εταιρεία παρέχοντας τις βασικές λειτουργίες και δυνατότητες που μπορεί να ζητά ένας κάτοχος μιας ψηφοφορίας. Χαρακτηριστικό του στοιχείο είναι ότι μπορεί ο διαχειριστής να θέσει μία ψηφοφορία είτε υπό δημόσια είτε υπό περιορισμένη δημοσίευση. Τα πλεονεκτήματα και τα μειονεκτήματα του μπορούν να επικεντρωθούν ως εξής:

9.3 Πλεονεκτήματα Helios Voting System

- Παρέχει στους χρήστες του διαδικτύου μια άμεση και απλή διαχείριση/λειτουργία μιας ψηφοφορίας χωρίς να απαιτούνται τεχνικές γνώσεις από τη μεριά και του διαχειριστή και του απλού ψηφοφόρου.

- Δίνει τη δυνατότητα να επιλέξουν εάν οι ψηφοφορίες θα είναι δημόσια δημοσιευμένες ή σε περιορισμένο αριθμό χρηστών. Στη δεύτερη περίπτωση, ο διαχειριστής μπορεί να ορίσει συγκεκριμένους χρήστες του Helios Voting που έχουν δικαίωμα ανάγνωσης και ψήφου.

- Γίνεται χρήση του πρωτοκόλλου https ώστε να μπορεί να διασφαλιστεί η εγκυρότητα και η σωστή λειτουργία της ψηφοφορίας.

- Ως κύρια τεχνική κάλυψη του Helios Voting είναι η εταιρεία δημιουργίας και εκμετάλλευσης του συστήματος και όχι ο ίδιος ο διαχειριστής μιας ψηφοφορίας. Αυτό διευκολύνει τον αρχάριο διαχειριστή στην άμεση λειτουργία μιας ψηφοφορίας.

9.4 Μειονεκτήματα Helios Voting System

- Το σύστημα ηλεκτρονικής ψηφοφορίας Helios Voting δε δίνει τη δυνατότητα να μη δημοσιοποιείται η ψήφος του κάθε χρήστη ακόμα και στον ίδιο τον διαχειριστή της.

- Δε μπορεί ο διαχειριστής να παρέμβει στον βασικό κορμό του κώδικα λειτουργίας μιας ψηφοφορίας αφού δεν πρόκειται για open-source σύστημα.

- Το γεγονός ότι δεν μπορεί ο διαχειριστής να παρέμβει στον βασικό κορμό του κώδικα του συστήματος Helios Voting το καθιστά και αναξιόπιστο όσο αναφορά την εγκυρότητα μιας ψηφοφορίας

- Η χρήση του https είναι γεγονός όμως ο κάθε διαχειριστής δε μπορεί να είναι σίγουρος ότι η ψηφοφορία του θα έχει την ασφάλεια που πρέπει μιας και δεν ορίζει ο ίδιος τις όποιες αναβαθμίσεις στο σύστημα της δικιάς του ψηφοφορίας.

- Το γεγονός της έλλειψης της αίσθησης της ασφάλειας καθορίζει και το κατά πόσο το σύστημα μπορεί να χρησιμοποιηθεί για πιο μείζονος σημασίας ψηφοφορίες όπως είναι για παράδειγμα οι εκλογές ενός κράτους ή ενός πανεπιστημιακού ιδρύματος. Επομένως, η χρήση του συστήματος Helios Voting περιορίζεται σε απλές ψηφοφορίες μεταξύ κοινωνικών ομάδων για καθαρά ψυχαγωγικούς ή στατιστικούς λόγους.

- Το Helios Voting δε διασφαλίζει την απόκρυψη της ψήφους του κάθε χρήστη ακόμα και από τον διαχειριστή της ψηφοφορίας με αποτέλεσμα να μπορεί να ταυτιστεί το περιεχόμενο των ψήφων με τον κάθε συμμετέχοντα.

- Το σύστημα αυτό δίνει τη δυνατότητα στους χρήστες που αντλούν παραπάνω από μία ψηφοφορία από τον server του συστήματος να έχουν πρόσβαση σε μία λίστα που εμφανίζει τα ονόματα χρηστών με κρυπτογραφημένα τα περιεχόμενα των ψήφων τους. Κάτι τέτοιο δε θα έπρεπε να είναι ορατό, ειδικά σε περιπτώσεις υψηλούς κύρους ψηφοφοριών όπως οι εθνικές εκλογές.

- Δε δίνεται η δυνατότητα πλήρους προσαρμογής του συστήματος ψηφοφορίας μέσα στην επίσημη σελίδα ενός ιδρύματος όπως το ΤΕΣΥΔ κάτι που μπορεί να θεωρηθεί και ως δείγμα έλλειψης αξιοπιστίας της ίδιας της λειτουργίας των ψηφοφοριών του.

- Ένα σύστημα ελευθέρας χρήσης όπως το Helios Voting μπορεί να θεωρηθεί ότι δε διασφαλίζει την εγκυρότητα, την ακεραιότητα και την αξιοπιστία των λειτουργιών του εξαιτίας του ότι δεν γνωστοποιούνται τεχνικά χαρακτηριστικά του στους διαχειριστές του. Αυτό έχει σαν αποτέλεσμα οι ίδιοι οι διαχειριστές να μην είναι σε θέση πλήρους βεβαιότητας για την ύπαρξη των παραπάνω χαρακτηριστικών που αναφέραμε. Το γεγονός επίσης της μη πρόσβασης και προσαρμογής στον προγραμματιστικό κώδικα λειτουργίας του συστήματος δημιουργεί επιπλέον αβεβαιότητα από τη μεριά των διαχειριστών του.

- Παρατηρούνται σύμφωνα με την αρχική δημοσίευση του συστήματος του Helios τρωτά σημεία, δηλαδή: «Ομάδες όπως οι διοικήσεις των σπουδαστών, των τοπικών συλλόγων, οι κοινότητες λογισμικού ανοιχτού κώδικα κ.α. … χρειάζονται επιπλέον προφύλαξη για να διασφαλιστεί το απόρρητο και η αξιοπιστία στα εκλογικά τους αποτελέσματα, κάτι που δεν μπορεί να επιτευχθεί επί του παρόντος. Γι' αυτό το Helios καλύπτει μόνο τις εκλογές χαμηλού εξαναγκασμου (low-coercion elections)».

ΚΕΦΑΛΑΙΟ 10^{ο}: ΣΥΓΚΡΙΣΗ HELIOS VOTING SYSTEM ΜΕ JOOMLA (jVoteSystem)

Το Helios Voting System παρέχει τις βασικές λειτουργίες στους χρήστες του διαδικτύου για τη δημιουργία μιας ψηφοφορίας με γρήγορο, άμεσο, και ανέξοδο τρόπο παρέχοντας τα βασικά στοιχεία από θέμα διασφάλισης της ομαλής λειτουργίας του. Ωστόσο, από την άλλη μεριά μια εφαρμογή όπως το Joomla μπορεί να αποφέρει ενδεχομένως καλύτερα αποτελέσματα σε σχέση με το Helios Voting System. Για να μπορέσουμε να εξετάσουμε κατά πόσο μια υλοποίηση ενός συστήματος όπως του Joomla – με τη βοήθεια του jVoteSystem – μπορεί να μας δώσει καλύτερα ή χειρότερα δείγματα στην ίδια τη λειτουργία μιας ψηφοφορίας, θα πρέπει να αποτυπώσουμε τα πλεονεκτήματα και τα μειονεκτήματα του ίδιου του Joomla.

10.1 Πλεονεκτήματα Joomla σε σχέση με το Helios Voting System

Τα σημαντικότερα πλεονεκτήματα του Joomla σε σχέση με το Helios Voting System είναι τα εξής:

- Δίνεται η δυνατότητα παρέμβασης του κώδικα του προγράμματος κάτι που καθιστά τον χρόνο προσαρμογής και παραμετροποίησης σύντομο
- Η παραμετροποίηση του κώδικα από τους διαχειριστές παρέχει ποιοτικό αποτέλεσμα πλήρως προσαρμοσμένο στις ανάγκες και τις λειτουργίες των διαχειριστών
- Η δυνατότητα ελεύθερων προς χρήση επιπρόσθετων προγραμμάτων καθιστά το κόστος λειτουργίας ενός συστήματος Joomla ως ο πιο οικονομικότερος τρόπος παροχής των υπηρεσιών μιας ψηφοφορίας.
- Η μεγάλη ποικιλία από μη ελεύθερα λογισμικά ανοίγει ακόμα τους ορίζοντες σε μια πιο λεπτομερής υλοποίηση των υπηρεσιών με επιπρόσθετη ασφάλεια, ειδικά όταν οι διαχειριστές είναι σε αρχάριο επίπεδο γνώσεων.
- Τα περισσότερα πανεπιστημιακά ιδρύματα κάνουν χρήση ήδη του πακέτου οργάνωσης δεδομένων Joomla για λόγους οικονομίας και κέρδος χρόνου στη διάρκεια της υλοποίησης, Έτσι, μπορούν με το υπάρχον σύστημα να

προσαρμόσουν και τις ειδικές υπηρεσίες όπως είναι μια ψηφοφορία προσδίδοντας στην ιστοσελίδα τους περισσότερο κύρος αλλά και μεγαλύτερο εύρος πληροφοριών.

- Με το επιπρόσθετο λογισμικό του jVoteSystem ο διαχειριστής μπορεί να προσαρμόσει ποικίλες διαφορετικές ιδιότητες και ρυθμίσεις για κάθε μία ψηφοφορία ξεχωριστά ενώ παράλληλα μπορεί να διασφαλίσει το απόρρητο των ψήφων μέσω των ειδικών αλλαγών που υλοποιήσαμε γι' αυτή μας την ανάγκη.

- Το jVoteSystem μπορεί να συνεργαστεί χωρίς κανένα πρόβλημα με τον mail server οποιασδήποτε εταιρείας ή οργανισμού ώστε να παρέχει άμεσες και έγκυρες ενημερώσεις κατά κύριο λόγο στους διαχειριστές του συστήματος αλλά και στους ίδιους τους ψηφοφόρους εφόσον αυτό κριθεί σκόπιμο.

- Διαθέτει αναλυτική καταγραφή των κινήσεων τόσο των διαχειριστών όσο και όλων των ψηφοφόρων χωρίς όμως να καταγράφει το περιεχόμενο των ψήφων κάτι που στο Helios Voting System παρατηρείται σε ελλιπή βαθμό.

- Γίνεται χρήση ειδικού λογισμικού για άμεσο backup – Akeeba backup – διασφαλίζοντας τα περιεχόμενα τόσο των ψηφοφοριών όσο και των αποτελεσμάτων τους κάτι που δεν προσδιορίζεται από την εταιρεία που παρέχει το Helios Voting System.

- Με τη χρήση του ίδιου συστήματος για την παροχή των πληροφοριών ενός ιδρύματος σαν το ΤΕΣΥΔ με τη μορφή ιστοσελίδας και με την λειτουργία ειδικών ψηφοφοριών, αυτοματοποιείται και η λίστα των χρηστών/φοιτητών σύμφωνα με τα προσωπικά του στοιχεία φοίτησης. Αντίθετα στο Helios, οι χρήστες πρέπει να δημιουργηθούν επιπλέον σε ένα άλλο ανεξάρτητο σύστημα το οποίο δε θα συνεργάζεται με τις ειδικές υπηρεσίες όπως είναι αυτή της ηλεκτρονικής γραμματείας.

- Παρέχεται η δυνατότητα από το Joomla επιπρόσθετων μεθόδων ασφάλειας, πέρα από τη τεχνολογία του https που διαθέτει το Helios, όπως είναι η χρήση του captcha κατά τη διάρκεια ενός ηλεκτρονικούς αιτήματος προς τη γραμματεία της σχολής.

10.2 Μειονεκτήματα Joomla σε σχέση με το Helios Voting System

Τα σημαντικότερα μειονεκτήματα του Joomla σε σχέση με το Helios Voting System είναι τα εξής:

- Απαιτείται συστηματικός έλεγχος για πιθανές νέες αναβαθμίσεις του ίδιου του Joomla αλλά και των επιπρόσθετων προγραμμάτων ώστε να μπορεί το σύστημα να είναι θωρακισμένο από κάθε είδους νέες απειλής. Αυτό απαιτεί από τους διαχειριστές επιπλέον γνώσεις λόγω του ανοιχτού κώδικα του Joomla κάτι που στο Helios αναλαμβάνει η ίδια η εταιρεία υποστήριξης.

- Είναι πιο εύκολος ο εντοπισμός και η εκμετάλλευση των τρωτών σημείων του Joomla σε σύγκριση με ένα σύστημα κλειστού κώδικα.

- Μπορεί να θεωρηθεί ευκολότερα αναξιόπιστο όσο αναφορά τις υπηρεσίες που παρέχει λόγω του ότι ανήκει στην κατηγορία των συστημάτων ανοικτού κώδικα.

- Θεωρείται το Joomla από ορισμένους διαχειριστές ιδιαίτερα πολύπλοκο ώστε να ληφθούν υπόψη όλες οι παραμέτρους για τη σωστή λειτουργία του που κάνει το Helios να φαίνεται πιο εύκολο και άμεσο.

- Εξαιτίας του ότι αρκετά επιπρόσθετα προγράμματα παρέχουν πιο εξειδικευμένες υπηρεσίες μόνο στις επί πληρωμή εκδόσεις τους, προσδίδει στη δωρεάν έκδοση τους μια εικόνα που καλύπτει μόνο τα βασικά στοιχεία. Έτσι, αναγκαστικά από θέμα ασφάλειας και διαχείρισης ενός συστήματος απαιτείται και κάποια μικρή οικονομική επιβάρυνση, η οποία όμως σε σύγκριση με την πλήρως δωρεάν παροχή του Helios φαίνεται πολύ μεγαλύτερη.

10.3 Βελτιώσεις του Συστήματος JOOMLA (jVoteSystem)

Αναμφισβήτητα το σύστημα διαχείρισης των πληροφοριών και των ψηφοφοριών του Joomla χρήζει βελτιώσεις ώστε οι υπηρεσίες αλλά και η λειτουργία του να παραμένει στο ίδιο υψηλό επίπεδο όπως και κατά την αρχική του υλοποίηση. Οι βελτιώσεις αυτές επικεντρώνονται κυρίως στα παρακάτω:

- Αναβαθμίσεις των τελευταίων εκδόσεων τόσο του Joomla όσο και των επιπρόσθετων προγραμμάτων (plug-ins, components, extentions). Για παράδειγμα, η έκδοση που χρησιμοποιήσαμε είναι η 2.5.14 ενώ σήμερα που συντάσσεται αυτή η έκθεση έχει δημοσιευτεί η 2.5.16 έκδοση της ή ίσως θα έπρεπε να γίνει η χρήση μίας από την 3 έκδοση του.

- Χρήση άλλης επιπρόσθετης εφαρμογής ψηφοφορίας όπως το Community Polls επί πληρωμή όπου τα θέματα ασφάλειας θα ήταν πιο περιορισμένα λόγω του κλειστού κώδικα τους αλλά και της τεχνικής τους υποστήριξης. Όμως πάλι η ανάγκη της παραμετροποίησης τους κρίνεται επιβεβλημένη λόγω των ιδιαιτεροτήτων που έχει μια ψηφοφορία σαν τις φοιτητικές εκλογές ενός πανεπιστημιακού ιδρύματος.

- Θα πρέπει να γίνει χρήση μιας εταιρείας παροχής υπηρεσιών hosting επί πληρωμή ώστε να μπορεί να ενεργοποιηθεί κανονικά και το https με την έκδοση μιας προσωπικής και μοναδικής ηλεκτρονικής υπογραφής. Η ηλεκτρονική υπογραφή θα διασφαλίσει πλήρως την ακεραιότητα και την εγκυρότητα των ψήφων των σπουδαστών.

- Να δημιουργηθεί ένα ειδικά προσαρμοσμένο πρόγραμμα συλλογής αντιγράφου για να δίνει τη δυνατότητα να αποθηκεύεται και σε διαφορετικό μέρος το εν λόγω αντίγραφο. Έτσι θα πραγματοποιηθεί η ανεξαρτησία μεταξύ των αντιγράφων αυτών καθώς και η άμεση πρόσβαση της ανάκτησης των λειτουργιών της ιστοσελίδας μας μετά από το πέρας μιας επίθεσης.

- Για να εμπλουτίσουμε το προφίλ των σπουδαστών παρέχοντας τους ένα περιβάλλον πιο φιλικό με περισσότερες πληροφορίες για τα ενδιαφέροντα τους θα μπορούσαμε να χρησιμοποιήσουμε μία πιο λεπτομερή εφαρμογή όπως το Community Builder Pro. Με αυτή την εφαρμογή θα μπορούσαμε να προσθέσουμε πολύ πιο εύκολα νέα πεδία στο προφίλ των σπουδαστών, θα μπορούσαμε να διαχειριστούμε καλύτερα τις λίστες όλων των φοιτητών όλων των ετών φοίτησης καθώς και να εντάξουμε και τις συμμετοχές τους στις ψηφοφορίες στο προφίλ τους – χωρίς να εμφανίζεται το τι ψήφισαν σε κάθε ψηφοφορία. Η χρήση αυτής της εφαρμογής θα μας επέτρεπε να εντάξουμε στο σύστημα μας και επιπρόσθετα κομμάτια της κύριας εφαρμογής, όπως το να

μπορούμε να στείλουμε ενημερωτικά μαιλ ή sms αυτοματοποιημένα σε όλους τους φοιτητές π.χ. με περιεχόμενα μια επείγουσα ανακοίνωση του ιδρύματος ή ακόμα και να συνδέσουμε μελλοντικά νέες υπηρεσίες με τις διάφορες σελίδες κοινωνικής δικτύωσης.

- Ως μελλοντική επέκταση των λειτουργιών του συστήματος θα μπορούσε να είναι η υιοθέτηση μιας επέκτασης του Joomla σαν το Password Reminder SMS η οποία θα μπορούσε να διασφαλίσει και να αυτοματοποιήσει ακόμα περισσότερο την διαδικασία ανάκτησης του κωδικού πρόσβασης των σπουδαστών με τη χρήση των κινητών τους τηλεφώνων. Η επέκταση αυτή αποστέλλει με SMS στο προσωπικό τηλέφωνο του φοιτητή ένα νέο προσωρινό κωδικό πρόσβασης του λογαριασμού του σε περίπτωση που δεν θυμάται το σωστό κωδικό πρόσβασης. Η υπηρεσία αυτή μπορεί να χρησιμοποιηθεί και να αποδώσει τόσο από πλευράς ασφάλειας όσο και από πλευράς λειτουργικότητας της ανάκτησης των κωδικών πρόσβασης εφόσον το σύστημα έχει τους επικαιροποιημένους τηλεφωνικούς αριθμούς όλων των φοιτητών/μελών του.

- Για να καλυφθούν και οι ανάγκες χρήσης των υπηρεσιών του ιδρύματος και από τα κινητά τηλέφωνα με ασφάλεια, χρήσιμο θα ήταν να κατασκευαστεί μία εφαρμογή που θα επέτρεπε την εμφάνιση της πλατφόρμας του Joomla και σε «έξυπνα κινητά» ώστε να μην αγνοείται και η ασφάλεια των υπηρεσιών. Μπορεί για το Joomla να υπάρχουν ήδη επί πληρωμή εφαρμογές που παρέχουν την αυτόματη μετατροπή της ιστοσελίδας σε προβολή για κινητά τηλέφωνα, τις περισσότερες φορές χρειάζεται εξειδικευμένα λογισμικά τα οποία θα συνεργάζονται απόλυτα με όλες τις λειτουργίες της πλατφόρμας μας. Γι' αυτό και η υλοποίηση μιας τέτοια εφαρμογής που θα παντρεύει την τεχνολογία των SMS με την ασφάλεια και την χρήση της πλατφόρμας μέσω κινητών τηλεφώνων θεωρείται επιτακτική να γίνει από μία ομάδα επαγγελματιών προγραμματιστών.

SCRIPT ΣΕ PYTHON

Επίσης για να αποστέλλονται κρυπτογραφημένα password στους ψηφοφόρους εκτός απο τον τρόπο που αναφέραμε πιο πάνω ώς βασικό σενάριο για την υλοποιήση του συστήματος δημιουργήσαμε και ένα δεύτερο τρόπο χρησιμοποιώντας την γλώσσα python.Το script που ακολουθεί ανακτά τα email απο την βάση δεδομένων της σχολής και ενώ μέσα στην ηλεκρονική πλατφόρμα κάποιος εξουσιοδοτημένος υπάλληλος της γραμματείας ο οποίος θα είναι και ένας απο τους 3 administrator έχει καταχωρήσει απλά το username και το email του φοιτητή αυτό το script θα ανακτά αυτό το email θα παράγει ένα τυχαίο password και θα το αποστέλει στο φοιτητή στο email αυτό και στην συνέχεια το password που έστειλε θα το καταχωρεί κρυπτογραφημένο στην βάση.Ο κώδικας είναι ο ακόλουθος:

```
#!/usr/bin/python

# -*- coding: utf-8 -*-


import MySQLdb as mdb

import smtplib

import string

from random import sample, choice

"""

This method is type void and it takes two arguments.

The mail of the recipient and the random generated password.

"""


def sendMail(reciever, password):
```

```
        SMTP_SERVER = 'smtp.gmail.com'

        SMTP_PORT = 587


        sender = 'evotingtesyd@gmail.com'

        recipient = reciever

        subject = 'kwdikos'

        body = 'Your password for tesyd e-voting system http://www.teimes.host-ed.me  is: ' + password

        password = 'teimestesyd123'

        "Sends an e-mail to the specified recipient."


        body = "" + body + ""


        headers = ["From: " + sender,
    "Subject: " + subject,
    "To: " + recipient,
    "MIME-Version: 1.0",
    "Content-Type: text/html"]

        headers = "\r\n".join(headers)


        session = smtplib.SMTP(SMTP_SERVER, SMTP_PORT)


        session.ehlo()
```

```
                session.starttls()
                session.ehlo
                session.login(sender, password)

                session.sendmail(sender, recipient, headers + "\r\n\r\n" + body)
                session.quit()



con = mdb.connect('127.0.0.1', 'root', '', 'education');

"""
This method returns a random generated string for use as a code.
It takes no arguments.
"""

def passwordGenerator():
                chars = string.letters + string.digits
                length = 8
                password = ''.join(sample(chars,length)) # way 1
                return password

with con:
```

```
    cur = con.cursor()
    cur.execute("SELECT email FROM edu_users")
    list = cur.fetchall()
    for i in list:
                print i
                password = passwordGenerator()
                sendMail(str(i[0]), password)
                cur.execute("UPDATE test SET pass='" + password + "' WHERE email='" + str(i[0]) + "'")
```

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα μελέτη ερευνήσαμε τα συστήματα που επικεντρώνονται στην ηλεκτρονική ψηφοφορία τόσο από την πλευρά των υπηρεσιών που παρέχουν όσο και από θέμα κατασκευής και ασφάλειας της λειτουργίας τους. Αναφερθήκαμε στα ποικίλα συστήματα ηλεκτρονικής ψηφοφορίας που έχουν χρησιμοποιηθεί τα τελευταία είκοσι χρόνια παγκοσμίως ενώ επικεντρωθήκαμε στο δωρεάν σύστημα ψηφοφοριών Helios Voting όπου και χρησιμοποιήσαμε ως μέτρο σύγκρισης με το σύστημα που υλοποιήσαμε σε τεχνολογία Joomla.

Λαμβάνοντας υπόψη τα πλεονεκτήματα και τα μειονεκτήματα του ενός και του άλλου συστήματος καταλήγουμε στα εξής συμπεράσματα:

- Η ηλεκτρονική ψηφοφορία δεν είναι κάτι το απλό για να διασφαλιστεί η εγκυρότητα, η αξιοπιστία, η ακεραιότητα καθώς και η πιστοποίηση των ψηφοφόρων χωρίς να καταπατούνται τα ατομικά και θεσμικά δικαιώματα των ψηφοφοριών. Γι' αυτό το λόγο, ορισμένα κράτη ανά την υφήλιο σταμάτησαν την εφαρμογή τέτοιων συστημάτων ενώ άλλα τα περιόρισαν σε έκταση και χρήση. Αντίθετα άλλα κράτη όπως η Ινδία προχώρησαν στην επέκταση της εφαρμογής τους έστω και ας μην εφαρμόζουν την πλήρη ηλεκτρονική ψηφοφορία μέσω διαδικτύου όπως η εφαρμογή που κατασκευάσαμε.

- Για να επιτύχουμε την μέγιστη ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας θα πρέπει να υπάρχει λεπτομερής επιμόρφωση των διαχειριστών του σχετικά με τις νέες μεθόδους επίθεσης, τις ενέργειες που θα πρέπει να προβούν σε περίπτωση επίθεσης καθώς και σε τρόπους και μεθόδους αναβάθμισης και ανίχνευσης μιας εισβολής αντίστοιχα.

- Τα περισσότερα πανεπιστημιακά ιδρύματα και ιδιαίτερα τα ΤΕΙ έχουν ήδη θέσει σε χρήση την πλατφόρμα του Joomla ως σύστημα λειτουργίας των ιστοσελίδων τους. Ωστόσο, τα περισσότερα ιδρύματα δεν έχουν εκμεταλλευτεί τις δυνατότητες του Joomla καθώς και τη σωστή παραμετροποίηση τους με αποτέλεσμα να είναι ένας εύκολος στόχος επίθεσης από hackers.

- Το Joomla είναι σε γενικές γραμμές εύκολο στην παραμετροποίηση του καθώς παρέχονται και βοηθητικές οδηγίες στην εγκατάσταση του όπως και στην υποστήριξη των επιπρόσθετων εφαρμογών – είτε των δωρεάν (non-commercial) είτε των επί πληρωμή (commercial). Ωστόσο είναι απαραίτητες οι γνώσεις PHP, Javascript και https τεχνολογιών για να παραμετροποιηθεί με ασφαλή τρόπο. Σαν ένα μη-δομημένο σύστημα όπως είναι η αρχική του μορφή, δεν περιέχει ουσιαστικά στοιχεία που να σχετίζονται με την ασφάλεια και να διατηρούν σε βάθος την ακεραιότητα και τη γνησιότητα των δεδομένων του. Για το λόγο αυτό, κρίνεται επιβεβλημένη η διασφάλισει της ασφαλής λειτουργίας του και της ακεραιότητας των υπηρεσιών του μέσω είτε των επιπρόσθετων προγραμμάτων – δωρεάν ή μη – είτε μέσω της υλοποίησης αποκλειστικής χρήσης προγραμμάτων υλοποιημένα από προγραμματιστές που θα ορίσει το ίδιο το ίδρυμα. Η αποκλειστική δημιουργία και χρήση ενός προγράμματος έχει ως στόχο τη περαιτέρω θωράκιση της πλατφόρμας με μεθόδους και πρακτικές που δεν χρησιμοποιούνται ευρέως.

- Η διαδικασία και η λειτουργία μιας ηλεκτρονικής ψηφοφορίας μπορεί σε μεγάλο βαθμό να καλυφθεί από τα διάφορα επιπρόσθετα προγράμματα του Joomla όπως το jVoteSystem που χρησιμοποιήσαμε. Ωστόσο, θα ήταν καλύτερο από πλευράς εγκυρότητας να συνδυαζόταν είτε με άλλα επιπρόσθετα προγράμματα επί πληρωμή είτε να προσαρμόζονταν τμήματα τους στο ίδιο το jVoteSystem. Με τον τρόπο αυτό, θα μετασχηματιζόταν το πρόγραμμα ψηφοφορίας και σε μορφολογικό επίπεδο όσο και σε επίπεδο ασφάλειας.

  Με τις παρεμβάσεις που κάναμε στο κύριο κορμό του προγράμματος ψηφοφορίας καταφέραμε: α) να αποκρύψουμε τις εμφανίσεις των username των ψηφοφόρων σε παραπάνω του ενός σημεία, β) να αποκρύψουμε από τους ίδιους τους διαχειριστές το περιεχόμενο της κάθε ψήφους του φοιτητή ώστε να μην μπορεί να προκληθεί η παραμικρή νοθεία στα αποτελέσματα τους, γ) να ενισχύσουμε την ασφάλεια σύνδεσης των φοιτητών μέσα στο σύστημα με επιπλέον εργαλεία ασφάλειας και κρυπτογράφησης, π.χ. το πρωτόκολλο https, η κρυπτογράφηση των προσωπικών στοιχείων σύνδεσης τους κ.α., δ) να οριοθετήσουμε τα ακριβή δικαιώματα κάθε φοιτητή ανάλογα με το έτος φοίτησης ώστε να μην αλλοιώνονται τα αποτελέσματα των ψηφοφοριών από

ψήφους που ενδεχομένως να είναι άνευ σημασίας, και ε) πραγματοποιήσαμε τη δυνατότητα στους διαχειριστές να λαμβάνουν αντίγραφα όλων των αρχείων της ιστοσελίδας χωρίς να επηρεάζεται η μυστικότητα των ψήφων των φοιτητών.

Αξίζει να αναφερθεί πως το σύστημα που δημιουργήσαμε χρήση επιπλέον βελτιώσεις και αναβαθμίσεις ώστε να συνεχίσει να είναι αυξητικό το επίπεδο ασφάλειας του. Οι βελτιώσεις επικεντρώνονται είτε στη δημιουργία νέων προγραμμάτων που θα είναι σε αποκλειστική χρήση για το ΤΕΣΥΔ είτε στην αναπροσαρμογή των ήδη υπαρχόντων προγραμμάτων σύμφωνα με τις ανάγκες των νέων υπηρεσιών. Τέλος, σημαντικό παράγοντα αποτελούν και οι αναβαθμίσεις του συστήματος συνολικά – του κύριου κορμού του Joomla και των plug-ins, των extensions και των module – με σκοπό την καλύτερη θωράκιση του συστήματος από επιθέσεις όπως η DDoS αλλά και άλλες. Ο συνδυασμός των βελτιώσεων και των αναβαθμίσεων είναι ο πιο αποτελεσματικός τρόπος άμυνας και κύρους ώστε και οι επιθέσεις να αποτρέπονται σε μεγάλο βαθμό αλλά και η αξιοπιστία των υπηρεσιών του συστήματος ολοένα και να μεγαλώνει αντίστοιχα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Brenton C. & Hunt C. (2003). *Ασφάλεια Δικτύων*. Αθήνα: Γκιούρδας

Γκλαβά Μ. (2009). *Ασφάλεια Δικτύων*. Αθήνα: Γκιούρδας

Οικονόμου Ε.(2004) *Ασφάλεια δικτύων και η διαχείριση της*. Αθήνα: Γκιούρδας

Stalling W. (2011). *Κρυπτογραφία και ασφάλεια δικτύων*. Αθήνα: Ίων

Strebe M. (2005). *Ασφάλεια δικτύων*. Αθήνα: Γκίουρδας

Χαριτούδη Γ. & Σαπαλίδης Κ. (2010). *Δυνατότητες και εφαρμογές του παγκόσμιου ιστού.* Αθήνα: Δίσιγμα

Διευθύνσεις Ιντερνετ

- http://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B1

- http://el.wikipedia.org/wiki/%CE%95%CE%BA%CE%BB%CE%BF%CE%B3%CE%AD%CF%82

- http://wikipedia.qwika.com/en2el/Electorate

- *Local government association implementing electronic voting in the UK.*

- *http://www.edssurvey.com/images/File/ve2006_nrpt.pdf*

- *http://electionresources.org/europe.htm*

- http://www.edemocracy.gov.uk/

- http://en.wikipedia.org/wiki/Elections_in_Brazil

- http://en.wikipedia.org/wiki/Electronic_voting_examples

- Kenneth Benoit, 'Experience of Electronic Voting Overseas',

- http://gigaom.com/2013/07/12/estonia-releases-e-voting-system-to-open-source-community/

- http://lorrie.cranor.org/pubs/hicss/hicss.html
- https://dspace.ist.utl.pt/bitstream/2295/153049/1/dissertacaoFinal.pdf
- http://en.wikipedia.org/wiki/DRE_voting_machine
- *Kenneth Benoit, 'Experience of Electronic Voting Overseas',*
- https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf
- https://zeus.minedu.gov.gr/
- http://www.ntua.gr/announcements/dty/uploads/2012-12-04_135303_ZEUS-Voter_Manual_v2.pdf
- http://www.pnyka.cti.gr/indexEn.php
- http://avirubin.com/vote.pdf
- http://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Ekloges/
- http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections2011/fr/presentation/bevoting-1_gb.pdf
- http://cgi.csc.liv.ac.uk/~alexei/COMP522_10/COMP522-E-VOTING-06.pdf
- http://www.icsd.aegean.gr/website_files/metaptyxiako/215363813.ppt%E2%80%8E

- http://newagebd.com/newspaper1/archive_details.php?date=2011-06-04&nid=21203

- http://dspace.lib.uom.gr/bitstream/2159/15561/3/PatsaliaEumorphiaMsc2012.pdf

- http://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf

- http://catedras.fsoc.uba.ar/rusailh/Unidad%204/Moynihan%202004%20Building%20secure%20elections%20y%20e%20voting.pdf

- http://www.ijstr.org/final-print/mar2013/Implementation-And-Analysis-Of-Secure-Electronic-Voting-System.pdf

- http://dspace.lib.uom.gr/dspace/bitstream/2159/14887/5/SaridisChristosMsc2011.pdf

- http://www.ionio.gr/~emagos/web_psifofories.pdf

- http://www.engr.uconn.edu/~sad06005/pubs/Conference/sac12.pdf

- http://www.ceid.upatras.gr/tech_news/brabeio_PNYKAdeltio_typou_Patrwn.pdf

- http://www.wired.com/threatlevel/2012/10/clear-ballot/

- http://votingmachines.procon.org/view.resource.php?resourceID=000276#IV

- http://www.vvk.ee/voting-methods-in-estonia/engindex/
- http://www.computingreviews.com/hottopic/hottopic_essay_10.cfm
- http://ballot-integrity.org/Venezuelan-vs-US-election-systems.pdf
- http://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-final.pdf
- http://www.edri.org/edrigram/number10.13/e-voting-france-problems-2012
- http://news.cnet.com/8301-27080_3-20113063-245/e-voting-machines-vulnerable-to-remote-vote-changing/
- http://eprint.iacr.org/2012/116.pdf
- http://harvardmagazine.com/2010/05/secret-ballots-verifiable-votes
- http://news.cnet.com/8301-27080_3-57354354-245/e-ballot-device-for-presidential-vote-has-bugs-report-confirms/
- http://www.oregonvotes.gov/pages/voterresources/voter_assistance/index.html
- http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf
- Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner, “A Security

- Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)",January 21, 2004
- http://expertwebprofessionals.com/news/articles-about-joomla/joomla-background/103-history-of-joomla.html
- HTTP State Management Mechanism – Overview". *IETF*. April 2011.
- http://static.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf
- http://extensions.joomla.org/extensions/contacts-and-feedback/polls/21726?qh=YTozOntpOjA7czo0OiJwb2xsIjtpOjE7czo1OiJwb2xscyI7aToyO3M6NzoicG9sbGluZyI7fQ%3D%3D
- http://extensions.joomla.org/extensions/contacts-and-feedback/surveys/11301?qh=YTozOntpOjA7czo0OiJwb2xsIjtpOjE7czo1OiJwb2xscyI7aToyO3M6NzoicG9sbGluZyI7fQ%3D%3D
- http://www.joomlapolis.com/community-builder/cb-quickstart-pro
- http://extensions.joomla.org/extensions/access-a-security/site-access/authentication-management/23509?qh=YTOxOntpOjA7czozOiJzbXMiO30%3D