ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΠΡΩΗΝ ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ & ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΠΤΥΞΗ ΠΛΑΤΦΜΟΡΜΑΣ ΔΙΑΔΥΚΤΙΑΚΗΣ ΨΗΦΟΦΟΡΙΑΣ

ΤΟΥ

ΑΘΑΝΑΣΟΠΟΥΛΟΣ ΣΤΥΛΙΑΝΟΣ-ΑΛΕΞΑΝΔΡΟΣ

ΤΖΕΒΕΛΕΚΟΣ ΧΡΗΣΤΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:
ΣΤΑΜΟΣ ΚΩΣΤΑΝΤΙΝΟΣ

ΠΑΤΡΑ-2016

Περίληψη

Η παρούσα πτυχιακήκάνει αναφορά πάνω στην ηλεκτρονική- διαδικτυακή ψηφοφορία, καθώς και στο πώς μπορεί να εφαρμοστεί στην καθημερινότητα μας. Αρχικά αναλύει βασικούς ορισμούς γύρω από τις έννοιες της ψήφου και της ψηφοφορίας. Στη συνέχεια αναφέρει σημαντικές ιστορικές πληροφορίες φτάνοντας μέχρι και την σημερινή εποχή όπου η ψηφιακή ψηφοφορία αρχίζει να εδραιώνεται στην ζωή μας και μας επεξηγεί τα οφέλη της αλλά και τους προβληματισμούς γύρω από αυτήν. Έπειτα παρουσιάζει τις μορφές με τις οποίες εφαρμόζεται, παρουσιάζοντας τα ήδη υπάρχοντα συστήματα και μας πληροφορεί για τα στάδια που την αποτελούν. Μας πληροφορεί επίσης για την αποδοτικότητα των συστημάτων αυτών, τις απαιτήσεις που έχουν, τις μεθόδους άσκησης του εκλογικού δικαιώματος, καθώς και για την εφαρμογή τέτοιου είδους συστημάτων στην χώρα μας αλλά και διεθνώς. Εν συνεχεία ενημερώνει για τα προβλήματα ασφαλείας που μπορούν να υπάρξουν στα συστήματα αυτάκαι αποτυπώνει τις θεμελιώδεις αρχές ασφάλειας που πρέπει να ακολουθούν. Ακόμη μας εισάγει στην κρυπτογράφηση και στους τρόπους κρυπτογραφίας, δίνοντας περισσότερο έμφαση στα ειδικευμένα κρυπτογραφικά μοντέλα πάνω στην ηλεκτρονική ψηφοφορία αλλά και στα βασικά κρυπτογραφικά εργαλεία. Τέλος παρουσιάζεταιη πλατφόρμα Προμηθέας που αποτελεί την προσπάθεια υλοποίησης ενός ηλεκτρονικού συστήματος ψηφοφορίας, αναφέροντας μεθόδους και εργαλεία υλοποίησης παρέχοντας σημαντικές πληροφορίες στους διαχειριστές της για την χρήση και την αξιοποίηση της.

Σκοπός της Πτυχιακής

Σκοπός της πτυχιακής είναι η ανάλυση τωνόρων της Ηλεκτρονικής Ψηφοφορίας, η εξήγηση της διαδικασίας, καθώς και οι μορφές της. Τα προβλήματα που παρουσιάζονται σε θέματα ασφάλειας, ακόμα και η κατασκευή ενός δοκιμαστικού συστήματος Ηλεκτρονικής Ψηφοφορίας.

Συμπέρασμα της Πτυχιακής

Συμπεραίναμε πως η Ηλεκτρονική Ψηφοφορία είναι αναπόσπαστο κομμάτι της ζωής μας.
Όπως δηλαδή, δεν θέλουμε να επεμβαίνουν ξένοι στην ιδιωτικότητα μας έτσι δεν θέλουμε να παρεμβαίνουν και στις προτιμήσεις μας κατά την διάρκειας της εκλογικής διαδικασίας.

Επίσης συμπεραίναμε, κυρίως από την ολοκλήρωση της πτυχιακής, πως η δημιουργία ενός απλού συστήματος Ηλεκτρονικής Ψηφοφορίας απαιτεί προσεκτικό σχεδιασμό όπως και τον καταλογισμό ευθύνης στα μέλη που το απαρτίζουν.
Με λίγα λόγια δεν είναι απλό, θέλει αρκετή προσοχή και φέρειμεγάλη ευθύνη. Ένα λάθος να συμβεί κατά την διάρκεια της ψηφοφορίας ακυρώνεται όλη η διαδικασία αν το σύστημα αδυνατεί να υποστηρίξει τα σφάλματα.

Περιεχόμενα

Πρόλογος

Το δικαίωμα της ψήφου, είναι το θεμέλιο της δημοκρατίας.

Είναι εκείνο μέσω του οποίου οι άνθρωποι, μπορούν να λάβουν πιο αντικειμενικές αλλά και πιο δίκαιες αποφάσεις για σοβαρά θέματα μέσα στην κοινωνία τους, όπως για παράδειγμα γίνεται με τις βουλευτικές εκλογές ή την ψήφιση ενός νόμου μέσα στο κοινοβούλιο.

Ακόμα, μπορούν να θέτουν ερωτήματα μεταξύ ενός συνόλου ατόμων μέσα στην κοινωνία τους, να παίρνουν απαντήσεις και στατιστικά αποτελέσματα για διάφορα θέματα της καθημερινότητας τους και να αντλούν σημαντικές πληροφορίες από αυτά, οι οποίες θα τους βοηθούν να κατανοούν καλύτερα τα προβλήματα που παρουσιάζονται, με αποτέλεσμα να βρίσκουν ευκολότερα τρόπους για να τα περιορίσουν και να βελτιώνουν τον τρόπο ζωής τους.

Αυτό μπορεί να γίνει με την χρήση ενός ερωτηματολογίου το οποίο να θεωρηθεί ένας εναλλακτικός τρόπος ψηφοφορίας.
Συμπεραίνουμε λοιπόν ότι η ψήφος είναι ένα δημιούργημα του ανθρώπου το οποίο αποτελεί χρήσιμο εργαλείο για την επίλυση κρίσιμων ζητημάτων που παρουσιάζονται στην ζωή του.

Σήμερα, καθίσταται δυνατή η βελτιστοποίηση του εργαλείου αυτού, καθώς με την ραγδαία ανάπτυξη της τεχνολογίας είναι δυνατή η υλοποίηση μίας διαδικτυακής πλατφόρμας ψηφοφορίας, η οποία θα κάνει απλούστερη την διαδικασία για τους ψηφοφόρους καθώς βοηθάει στο να παίρνουμε αποτελέσματα γρηγορότερα σε σχέση με το παρελθόν.

Στην συνέχεια θα αναλύσουμε τις μεθόδους υλοποίησης, τις διαδικασίες ψηφοφορίας, καθώς και τα χαρακτηριστικά που πρέπει να περιέχει μια πλατφόρμα τέτοιου τύπου ώστε να ακολουθεί μια συγκεκριμένη δομή που θα έχει οριστεί από εμάς, για την ομαλή διεξαγωγή της ψηφοφορίας.

Ορισμοί

Ορισμός ψήφου
Με τον όρο ψήφο εννοούμε την δυνατότητα έκφρασης του πολίτη μέσω μιας εκλογικής απόφασης.

Ορισμός ψηφοφορίας
Με τον όρο ψηφοφορία χαρακτηρίζουμε την διαδικασία εκλογής της απόφασης των πολιτών.

Ορισμός Ψηφιακής Ψηφοφορίαςή Ηλεκτρονικής Ψηφοφορίας
Με τον όρο ψηφιακής ψηφοφορία χαρακτηρίζουμε την διαδικασία εκλογής της απόφασης των πολιτών, με την χρήση ενός ή περισσότερων δικτύων ηλεκτρονικών συσκευών.

Ορισμός Διαδικτυακής

Με τον όρο δικτυακή ψηφοφορία χαρακτηρίζουμε την διαδικασία εκλογής της απόφασης των πολιτών μέσω ηλεκτρονικών συσκευών με την χρήση του Διαδικτύου(Internet).

Ορισμός Ψηφιακής Πλατφόρμας

Με τον όρο ψηφιακή πλατφόρμα δηλώνουμε ένα ψηφιακό σύστημα καταχώρησης, επεξεργασίας και μεταβολής πληροφοριών.

Σημείωση: Για λόγους ευκολίας και κατανόησης των όρων: Ψηφιακή Ψηφοφορία και Ηλεκτρονικής του;ορίσαμε ίδιας σημασίας με αυτής της Διαδικτυακής Ψηφοφορίας. Μπορεί να είναι διαφορετικοί όροι αλλά συνδέονται άμεσα.

Γιατί;

Γιατί, από την στιγμή που καταργήθηκε η υλική μορφή του ψηφοδελτίου(η ψηφιοποίηση του)δεν γίνεται λόγος σύγχυσης, το μόνο που αλλάζει είναι το μέσο ψηφοφορίας.

Ιστορική αναδρομή

Από την αρχή ο άνθρωπος προσπαθούσε να βρει τρόπους ψηφοφορίας, που δεν βασίζονταν στα ξεπερασμένα πλέον ψηφοδέλτια,δηλαδή η χρήση ενός απλού χαρτιού.

Κατά την διάρκεια του **20ου αιώνα**, αλλά κυρίως μέχρι το 1960 ιδιαίτερα διαδεδομένος ήταν ο μηχανικός τρόπος ψηφοφορίας, που στην πράξη γινόταν με την βοήθεια μια μηχανολογικής εγκατάστασης με μοχλό. Αυτός ο τρόπος αποδείχτηκε μάλλον ανακριβής, ενώ είχε και το επιπρόσθετο μειονέκτημα ότι δεν διατηρούσε κανενός είδους φυσικό αρχείο ψήφων.

Στις αρχές της δεκαετίας του **1960** άρχισε να υιοθετείται η χρήση των διάτρητων καρτών, η οποία διαδόθηκε αρκετά γρήγορα. Η μέθοδος αυτή είχε 2 μορφές την *Votomatic*και *Datavote***.** Πρέπει να αναφερθεί ότι παράλληλα το **1962** εμφανίστηκε μία μέθοδος η οποία αντί για διάτρητες κάρτες χρησιμοποιούσε ένα είδος <<οπτικών>> ψηφοδελτίων τα οποία στην συνέχεια σαρώνονταν.

Το **1975** χρησιμοποιήθηκε η πρώτη **DRE** μηχανή ψηφοφορίας σε πραγματικές εκλογές στο Streamwood και WoodstockIllinois των Η.Π.Α.

Η εξέλιξη της τεχνολογίας και η χρήση της **DRE** μηχανής στην παραδοσιακή διαδικασία της ψηφοφορίας οδήγησε στην αντικατάσταση της χρήσης του χάρτινου ψηφοδελτίου από ένα ηλεκτρονικό ψηφοδέλτιο.

Το **2000** μέθοδοι όπως η *Votomatic* και *Datavote* άρχισαν να εγκαταλείπονται λόγω προβλημάτων που παρατηρήθηκαν στις προεδρικές εκλογές της Florida στις Ηνωμένες πολιτείες Αμερικής, όπως επίσης εγκαταλείφθηκε και ή μέθοδος των << οπτικών>> ψηφοδελτίων. Αξιοσημείωτο είναι ότι το 2000 η Βραζιλία έγινε η πρώτη χώρα που χρησιμοποίησε σύστημα ψηφοφορίας πλήρως βασισμένο σε υπολογιστές.

Έπειτα το **2002** η Georgia των Ηνωμένων Πολιτειών Αμερικής ήταν η πρώτη Πολιτεία που υιοθέτησε μια ενιαία **DRE** τεχνολογία για ψηφοφορία. Χρησιμοποιήθηκαν διάφοροι τύποι ψηφοφορίας, το ποσοστό των των ψηφοδελτίων όπου δεν είχαν συμπληρωθεί όλα τα απαιτούμενα στοιχεία εκλογής μειώθηκε από 4,4% σε λιγότερο από 1%, κάτι που αποτελεί ποιοτικό δείκτη ακεραιότητας ενός εκλογικού συστήματος.

Μεγάλης κλίμακας προσπάθεια έγινε από το Ηνωμένο Βασίλειο κατά τα έτη **2002**, **2003**, **2004** και **2006** στα πλαίσια ενός πιλοτικού προγράμματος με απώτερο σκοπό τη διεξαγωγή ηλεκτρονικών εκλογών μετά το 2006, κάτι που προέκυψε από την ανάγκη για εκσυγχρονισμό της διαδικασίας και της μεγαλύτερης προσέλευσης των ψηφοφόρων.

Η προσπάθεια συντονίστηκε από κοινού από την κεντρική διοίκηση και τις τοπικές αρχές. Οι ανεπάρκειες του συστήματος, που θα αποτελέσουν σημαντική βοήθεια για το μέλλον, εντοπίστηκαν κυρίως σε θέματα οργανωτικά, εσωτερικής επικοινωνίας και συνεργασίας των συντελεστών της διαδικασίας.

Επίσης φάνηκε ότι αν δεν ήταν διαθέσιμα και χάρτινα ψηφοδέλτια ως back-up διαδικασία, θα υπήρχε πρόβλημα. Πιθανώς αυτό αποτελεί απαραίτητο μέτρο έως ότου εξασφαλιστεί η τελειοποίηση της ηλεκτρονικής ψηφοφορίας.

Με λίγα λόγια

Η παραδοσιακή εκλογική διαδικασία είτε συμπληρώθηκε είτε αντικαταστάθηκαν τμήματά της από ηλεκτρονικές τεχνολογίες.
Οιτεχνολογίεςπουχρησιμοποιήθηκανήταν*: Internet voting, telephone voting, Direct Recording e-voting machines (DRE) / Kiosk voting, SMS text message voting, Interactive Digital Television voting.*

Μηχανήψηφοφορίας DRE

(Direct Recording Election)

Οι τεχνολογίες πληροφορικής έχουν δημιουργήσει το πλέον πιο αποδοτικό σύστημα ψηφοφορίας «DirectRecordingSystem». Το σύστημα αυτό καταγράφει τα αποτελέσματα πλήρως και με ακρίβεια. Πρόκειται για ένα δίκτυο ηλεκτρονικών συσκευών μέσω των οποίων οι ψηφοφόροι επιλέγουν τις προτιμήσεις τους. Στην συνέχεια αυτές καταγράφονται σε μια κάρτα μνήμης. Αυτές οι μνήμες μεταφέρονται σε έναν κεντρικό υπολογιστή όπου οι ψήφοι παίρνουν την μορφή ενός πίνακα.Στον υπολογιστή αυτό εκτυπώνονται οι ψήφοι και σε φυσική μορφή.

Οφέλη των αυτοματοποιημένων μηχανών ψηφοφορίας

Ένα φυσικό ψηφοδέλτιο δεν διασφαλίζει ότι μια ψηφοφορία θα μετρηθεί σωστά. Τα φυσικά ψηφοδέλτια μπορούν να χαθούν ή να καταστραφούν πριν από την καταμέτρηση.

Πολλοί παράγοντες μπορούν να συμβάλλουν σε μια εσφαλμένη εφαρμογή ψηφοφορίας χωρίς την χρήση των DRE. Όπως το 2000 στις εκλογές της Φλόριντα όπου οι τρύπες στις κάρτες δεν μπορούσαν να ευθυγραμμισθούν πλήρως στην μεμβράνη, με αποτέλεσμα να μετρηθούν λανθασμένα. Ακόμα όπως 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 σήματα στις κάρτες. Μπορεί επίσης ένας ψηφοφόρο να ψηφίσει δυο ή περισσότερες φορές, που είναι γνωστό ως **overvoting**.

Όλα αυτά έρχεται να λύσει το DRE.

Άμεση καταγραφή των ηλεκτρονικών συστημάτων

Ένα DirectRecordingElectronicSystem είναι ουσιαστικά ένας υπολογιστής. Οι ψηφοφόροι βλέπουν τα ψηφοδέλτια σε μια οθόνη και κάνουν τις επιλογές τους με μια σειρά κουμπιών ή με touchscreen οθόνη ανάλογα. Ορισμένα συστήματα DRE χρησιμοποιούν επίσης ένα σύστημα προσωπικών καρτών που ενεργοποιούντο μηχάνημα. Οι ψήφοι αποθηκεύονται σε μια κάρτα μνήμης, ή άλλη μνήμη της συσκευής. Οι υπάλληλοι των εκλογών μεταφέρουν αυτές τις συσκευές μνήμης σε μια κεντρική τοποθεσία για πινακοποίηση, όπως ακριβώς θα έκαναν και με τα χάρτινα ψηφοδέλτια. Ορισμένα μηχανήματα έχουν τη δυνατότητα να μεταδίδουν τα αποτελέσματα ασύρματα, δηλαδή, μέσω modem, αν και λόγω ανησυχιών για την ασφάλεια των δεδομένων, τα αποτελέσματα αυτά κρίνονται ανεπίσημα μέχρι που να μπορούν να επαληθευθούν από την πινακοποίηση των στοιχείων που αποθηκεύονται στη μνήμη των συσκευών. Πολλές συσκευές DRE έχουν επίσης την ικανότητα να εκτυπώνουν ένα έγγραφο που καταγράφει τη ψηφοφορία.

Ένα σύστημα DRE μπορεί να έχει σημαντικά πλεονεκτήματα έναντι συστημάτων που βασίζονται σε χαρτί, με την προϋπόθεση ότι είναι ασφαλές και αξιόπιστο. Επειδή η ψηφοφορία απεικονίζεται ηλεκτρονικά, δεν υπάρχουν περιορισμοί σχετικά με την εμφάνιση ενός ψηφοδελτίου. Οι προγραμματιστές μπορούν να δημιουργήσουν ψηφοδέλτια σε οποιαδήποτε γλώσσα. Μπορούν να σχεδιάζουν μεγάλες εκτυπώσεις για τους ψηφοφόρους με περιορισμένη όραση ή ακόμη και να ενσωματώσουν αρχεία ήχου για τυφλούς ψηφοφόρους. Επειδή οι ψήφοι καταγράφονται σε μνήμη της συσκευής, η πινακοποίηση παίρνει λιγότερο χρόνο. Δεν βασίζονται σε ψηφοφορίες που πρέπει να σαρωθούν σε χαρτί, με αποτέλεσμα να μειωθούν οι κίνδυνοι μηχανικών σφαλμάτων. Το ανθρώπινο λάθος είναι ακόμη ένας παράγοντας και πάντα υπάρχει μια ανησυχία σχετικά με τα σφάλματα στο λογισμικό, ενώ σε ένα ιδανικό σύστημα, η πινακοποίηση είναι στιγμιαία χωρίς καμία ανάγκη για επαναληπτικές μετρήσεις.

Σήμερα

Καθώς η τεχνολογία δεν σταματά να αναπτύσσεται προβλέπεται ότι τα συστήματα ηλεκτρονικής ψηφοφορίας μέσα στα επόμενα χρόνια θα εδραιωθούν σε μικρότερης δυναμικής εκλογές, όπως οι δημοτικές και οι σχολικές. Εκλογές τέτοιου βεληνεκούς παρουσιάζουν συνήθως τα μεγαλύτερα ποσοστά αποχής και είναι σχετικά «ελαστικές» από πλευράς ασφάλειας (συνήθως οι ίδιοι οι υποψήφιοι καταμετρούν τελικά τις ψήφους), ενώ επίσης στις περισσότερες περιπτώσεις γίνεται κατασπατάληση ανθρωπίνων και χρηματικών πόρων. Έτσι, τα συστήματα ηλεκτρονικής ψηφοφορίας εισάγονται σταδιακά, με στόχο τη μείωση της αποχής και του κόστους, με παράλληλη αύξηση της ασφάλειας.

Η ψηφιακή ψηφοφορία στην ζωή μας

Η ψηφιακή ψηφοφορία χρησιμοποιείται κατά κόρον στην εποχή μας, ειδικά με την ένταξη της τηλεόρασης στην καθημερινότητα μας. Η συνεχής ανάγκη για γρήγορα αποτελέσματα χωρίς να μετακινηθούμε από τον χώρο που ήδη βρισκόμαστε, οδήγησε στην ευρύτερη χρήση του. Ένα σύνηθες παράδειγμα της ευρύτερης χρήσης της ηλεκτρονικής ψηφοφορίας είναι οι τηλεοπτικές εκπομπές όπου αρκετά συχνά καλείται ο κόσμος να επιλέξει ποιος παίκτης θα πρέπει να παραμείνει στο show ή ποιος θα πρέπει να αποχωρήσει, είτε στέλνοντας κάποιο μήνυμα από το κινητό τους τηλέφωνο, είτε επιλέγοντας την επιλογή τους μέσω κάποιου διαδικτυακού ιστότοπου.

Καταλαβαίνουμε με την χρήση του παραπάνω παραδείγματος πως η ψηφιακή ψηφοφορία δεν είναι κάτι καινούριο, αλλά κάτι που ήδη χρησιμοποιείται αποτελεσματικά από πολλούς για διάφορους τομείς.

Προβληματισμοί

Τεχνολογία και δημοκρατία είναι δύο ζητήματα κάθε άλλο παρά ασύνδετα.

Το ζήτημα δεν είναι αν πρέπει να επιχειρήσουμε να χρησιμοποιήσουμε την τεχνολογία, αλλά με ποιο τρόπο και σε ποιο βαθμό θα εξασφαλίσουμε ότι οι νέες μέθοδοι δεν θα θέτουν σε κίνδυνο ή ενδεχομένως, δεν θα παραβιάζουν ισχύουσες νομικές και ηθικές αρχές.

Το ενδιαφέρον που δείχνουν (ή δεν δείχνουν) οι πολίτες στην πολιτική δεν έχει (και δεν θα έπρεπε να έχει) τόσο σχέση με το μέσο εκλογικής έκφρασης, όσο με τον τρόπο αντιστοίχισης του πολιτικού και εκλογικού ανταγωνισμού στα ενδιαφέροντα και τις απαιτήσεις της κοινωνίας.

Κανένα σύστημα, όσο καινοτόμο και να είναι, δεν είναι σε θέση να μετατρέψει τον αδιάφορο πολίτη σε ενεργό.
Ή, αν το κάνει, ο πολίτης αυτός δεν θα είναι πραγματικά ενεργός.

Γιατί ηλεκτρονική ψηφοφορία;

Η ανάγκη για πιο αποτελεσματική, ασφαλή ψηφοφορία χωρίς να μετακινηθούμε από τον χώρο μας με όσον δυνατόν λιγότερο κόστος και απώλειες είναι οι βασικοί λόγοι που δίνουν την απάντηση.

Πλεονεκτήματα

Τα εκλογικά συστήματα με την χρήση του Internet και τα συστήματα DRE έχουν κάποια έμφυτα πλεονεκτήματα σε σύγκριση με τα παραδοσιακά συστήματα ψηφοφορίας, συμπεριλαμβανομένης της μείωσης του λάθους του ψηφοφόρου. Αν το περιβάλλον του συστήματος είναι κατάλληλα σχεδιασμένο ειδοποιεί για παράδειγμα για μια ενδεχόμενη παράλειψη ψήφου ή και για μη έγκυρη ψηφοφορία. Από την άλλη καθίσταται δυνατή η εξυπηρέτηση ψηφοφόρων με αδυναμίες όπως τα άτομα με ειδικές ανάγκες, χωρίς να είναι απαραίτητη η ανθρώπινη βοήθεια μειώνοντας την πιθανότητα ανθρώπινης παρέμβασης.

Άλλοι παράγοντες που καθιστούν αναγκαία τα συστήματα ηλεκτρονικής ψηφοφορίας και πιθανά οφέλη που πρέπει να ληφθούν υπόψη είναι τα εξής:

1)Μείωση της αποχής με αύξηση της προσέλευσης, συμμετοχή των ψηφοφόρων και η προώθηση με αυτό τον τρόπο της δημοκρατικής διαδικασίας.
2)Παρουσία νέων δυνατοτήτων για τις εκλογές (παρέχοντας ψηφοδέλτια σε διάφορες γλώσσες, υποστηρίζοντας μακροσκελή ψηφοδέλτια κλπ).
3)Το άνοιγμα μιας νέας αγοράς, με συνακόλουθες συνέπειες για το εμπόριο και την απασχόληση.
4)Η σαφής διευκόλυνση του ψηφοφόρου.
5)Ο περιορισμός της επέμβασης του ανθρώπινου παράγοντα και συνεπώς της δυνατότητας για νοθεία
6)Η μεγαλύτερη ταχύτητα στην έκδοση και επεξεργασία των αποτελεσμάτων.

Οι παραπάνω λόγοι έχουν οδηγήσει αρκετές χώρες στο να εκδηλώσουν ενδιαφέρον για τη χρήση τέτοιων συστημάτων σε μικρότερη ή μεγαλύτερη κλίμακα αλλά και την αισιοδοξία ότι η ηλεκτρονική ψηφοφορία σταδιακά θα κυριαρχήσει.

Μειονεκτήματα

Εκτός από τα πλεονεκτήματα δεν γίνεται να λείπουν και τα μειονεκτήματα. Όσο και προσοδοφόρα μπορεί να αποτελούν τα συστήματα ηλεκτρονικής ψηφοφορίας για τον άνθρωπο τόσους κινδύνους μπορεί να ελλοχεύουν, καθώς είναι ευρέως γνωστό ότι τα ηλεκτρονικά δεδομένα αλλοιώνονται, αντιγράφονται ή ακόμα και καταστρέφονται πολύ πιο εύκολα από ότι φυσικοί ψήφοι, κάτι που τα κάνει ευάλωτα σε επιθέσεις. Ενώ παράλληλα έχουν και τα εξής αρνητικά χαρακτηριστικά :

1) Ανεπαρκή στοιχεία ελέγχου και ασυνέπεια παροχής οικουμενικής επαληθευσιμότητας,κάτι που κάνει τα αποτελέσματα της εκάστοτε ψηφοφορίας να τίθενται υπό αμφισβήτηση.
2) Αυξημένη πιθανότητα επίθεσης από εσωτερικούς εχθρούς, καθώς και σε επιθέσεις άρνησης εξυπηρέτησης που έχουν ως στόχο τους υπολογιστικούς πόρους ενός ηλεκτρονικού υπολογιστή.
3) Ανεπάρκεια ασφαλών συστημάτων παρά το γεγονός ότι υπάρχουν ασφαλείς κρυπτογραφικοί αλγόριθμοι.
4) Αυξημένο κόστος κατασκευής της πλατφόρμας για την διεξαγωγή της ψηφοφορίας .
5) Μεγάλος χρόνος υλοποίησης.
6) Απαιτούμενη εξειδικευμένη γνώση για την δημιουργία ενός interface που θα είναι ικανό να εξυπηρετεί τους ψηφοφόρους.

Σημείωση: οικουμενική επαληθευσιμότητα, άρνηση εξυπηρέησης αναφέρονται αναλυτικότερα στο κεφάλαιο Προβλήματα ασφάλειας.

Πέρα από αυτά όμως πρέπει να ληφθεί υπόψη και η πιθανότητα αποτυχίας του δικτύου κατά την διάρκεια της ψηφοφορίας, όπου σε αυτή την περίπτωση θα πρέπει να προϋπάρχει εναλλακτικό δίκτυο για την ολοκλήρωση της ψηφοφορίας ή στην χειρότερη περίπτωση η ψηφοφορία να ολοκληρωθεί με τον παραδοσιακό τρόπο.

Μορφές ηλεκτρονικής ψηφοφορίας

Η ηλεκτρονική ψηφοφορία μπορεί να λάβει τη μορφή:

«Ανοικτής» διαδικασίας: Διενεργείται από οποιοδήποτε στοιχειωδώς εξοπλισμένο ηλεκτρονικό μηχάνημα, σε δημόσιο χώρο (βιβλιοθήκες, τόπους συγκέντρωσης) ή ιδιωτικό (σπίτι, γραφείο) και μέσω του ανέλεγκτου λογισμικού που διαθέτει το κάθε χρησιμοποιούμενο μηχάνημα.

«Κλειστής» διαδικασίας: Υλοποιείται βάσει ελεγμένου και ομοιόμορφου λογισμικού, τοποθετημένου σε επίσημα εκλογικά τμήματα (αναλόγως της υποδομής, ο εκλογέας μπορεί να ψηφίζει στην περιοχή που διαμένει ή σε όλη τη χώρα).

Είδη ηλεκτρονικής ψηφοφορίας

Υπάρχουν δυο είδη ηλεκτρονικής ψηφοφορίας:

α. Η "**εκ του σύνεγγυς**" (σε εκλογικά σημεία)

β. Η "**εξ αποστάσεως**" (μέσω διαδικτύου)

“Εκ του σύνεγγυς” ηλεκτρονική ψηφοφορία
Μπορεί να υποστηριχθεί από:

α. Περίπτερα (κιόσκια) ηλεκτρονικής ψηφοφορίας.
Συνήθως περιλαμβάνει τη χρήση ενός υπολογιστή σε μια συγκεκριμένη τοποθεσία η οποία ελέγχεται από την εκλογική επιτροπή. Αυτό διαφέρει από το μηχάνημα(τερματικό) ηλεκτρονικής ψηφοφορίας, διότι μεταξύ άλλων, η ψήφος στέλνεται μέσω διαδικτύου.

β. Ηλεκτρονικά εκλογικά κέντρα.
Είναι συνηθισμένα κέντρα τα οποία όμως διαθέτουν ειδικά τερματικά για την υποβολή της ψήφου.

Η Υποβολή της ψήφου στα εκλογικά σημεία γίνεται ηλεκτρονικά μέσω:

- Προσωπικών υπολογιστών
- Ειδικών συσκευών με οθόνες αφής (DRE) .

Τόσο τα τερματικά που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένα πρόσωπα, οντότητες (π.χ. εκλογικοί αντιπρόσωποι, αστυνομία).

Ανάλογα με το είδος του εκλογικού σημείου, το στάδιο της Επικύρωσης μπορεί να γίνει είτε με φυσικές διαδικασίες (έλεγχος απ’ ευθείας από τους εκλογικούς αντιπροσώπους) είτε με ηλεκτρονικές (π.χ. κωδικός PIN).

Οι ηλεκτρονικές ψήφοι αποθηκεύονται τοπικά σε αποσπώμενες περιφερειακές μονάδες.

Η καταμέτρηση των ψήφων γίνεται επίσης ηλεκτρονικά. Οι ψήφοι καταμετρούνται τοπικά στο εκλογικό κέντρο ή αποστέλλονται στον κεντρικό εξυπηρετητή (server) των εκλογών για τον υπολογισμό των συγκεντρωτικών αποτελεσμάτων.

Η μεταφορά στον κεντρικό server μπορεί να γίνει επίσης ηλεκτρονικά, με «ασφαλείς» συνδέσεις (π.χ. μισθωμένεςγραμμές οπτικών ινών ή μέσω Internet με τεχνικές IPSEC - Εικονικά Ιδιωτικά ΔίκτυαVPNs). Εναλλακτικά, έχει προταθεί η χρήση των δικτύων ATM. (AutomatedTellerMachines) Την ημέρα των εκλογών τα δίκτυα ATM έχουν ορισμέναεπιθυμητά χαρακτηριστικά ασφάλειας (μυστικότητα του καναλιού επικοινωνίας, αξιόπιστος εξοπλισμός, ανθεκτικά τερματικά, υψηλό ποσοστό διείσδυσης). Ωστόσο συχνά διατυπώνονται αντιρρήσεις σχετικά με την καταλληλότητα τους για τη διενέργεια ηλεκτρονικών εκλογών.

Μειονεκτήματα της “εκ του σύνεγγυς” ηλεκτρονικής ψηφοφορίας

Η ψηφοφορία μέσω ειδικών μηχανημάτων ηλεκτρονικής ψηφοφορίας, που είτε βρίσκονται σε εκλογικό κέντρο ή άλλη κεντρική τοποθεσία εξακολουθούν να απαιτούν από τους εκλογείς να μετακινηθούν από την κατοικία τους στα εκλογικά σημεία.

Ενώ σε ορισμένες περιπτώσεις η επίσκεψη σε ένα κεντρικό σημείο ψηφοφορίας, όπως ένα εμπορικό κέντρο ή ένα σούπερ μάρκετ μπορεί να είναι βολική, η χρήση τους εξακολουθεί να απαιτεί επιπλέον προσπάθεια την οποία δεν απαιτεί η ψηφοφορία από το σπίτι ή τον τόπο εργασίας.

"Εξ αποστάσεως" ηλεκτρονική Ψηφοφορία (I-Voting).

Η ψήφος υποβάλλεται μέσω Internet και τα μέσα υποβολής ψήφου(τερματικά) βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (στο σπίτι, στον χώρο εργασίας, σε βιβλιοθήκες, σχολεία, πανεπιστήμια).

Η Εγγραφή στους εκλογικούς καταλόγους μπορεί να γίνει με φυσικές (π.χ. σε εκλογικά γραφεία) ή με ηλεκτρονικές διαδικασίες (π.χ. ψηφιακή υπογραφή).

Τα στάδια της Ταυτοποίησης, της Υποβολής και της Καταμέτρησης γίνονται εξ ολοκλήρου ηλεκτρονικά.

Υπάρχοντα Συστήματα

Το σύστημα Sensus

Το σύστημα Sensus είναι ένα πρακτικό και ασφαλές σύστημα για διεξαγωγή δημοσκοπήσεων (ακόμη και εκλογών) μέσω δικτύων. Το Sensus επιτρέπει στο ψηφοφόρο να επαληθεύσει(ατομικά) ότι η ψήφος του μετρήθηκε σωστά και ανώνυμα καθώς και να ελέγξει την ορθότητα των αποτελεσμάτων της ψηφοφορίας.Το Sensus είναι ένα εύκολα προσαρμόσιμο αρθρωτό σύστημα. Το πρωτόκολλο ψηφοφορίας του απαιτεί την ύπαρξη ενός συστήματος επιβεβαίωση (validator), ενός συστήματος καταμετρητή (tallier) και ενός συστήματος διεξαγωγής της δημοσκόπησης (pollster). Άλλα επιπρόσθετα συστήματα μπορούν να αυξήσουν την λειτουργικότητα του Sensus.

Το σύστημα E-Vox

Το σύστημα αυτό, που ονομάζεται E-Vox συνδυάζει την ευελιξία ενός συστήματος VBM (VoteByMail) 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.

Το σύστημα DirectRecordingElection

Οι τεχνολογίες πληροφορικής έχουν δημιουργήσει το απόλυτο σύστημα ψηφοφορίας «DirectRecordingSystem». 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.

Το σύστημαInfoPoll

InfoPoll Software

Η συλλογή δεδομένων είναι τις περισσότερες φορές χρονοβόρα και δαπανηρή διαδικασία. Η εταιρία InfoPoll βοηθάει στη συγκέντρωση των δεδομένων που έχετε ανάγκη γρήγορα, οικονομικά και αξιόπιστα. Είτε διεξάγεται μία έρευνα σε μερικές χιλιάδες άτομα, είτε γίνεται έρευνα αγοράς σχετικά με ευκαιρίες για νέα προϊόντα, είτε πραγματοποιείται αξιολόγηση ενός Web site, η InfoPoll, επιτρέπει να γίνει εύκολα, γρήγορα και επαγγελματικά.

Τι είναι η InfoPoll;

InfoPoll είναι το όνομα της εταιρίας, καθώς και το όνομα της σειράς των προϊόντων, που επιτρέπουν στους χρήστες να σχεδιάσουν HTML φόρμες για οποιοδήποτε είδος έρευνας και τύπο δεδομένων. Σε αυτές συμπεριλαμβάνονται ερωτηματολόγια, απλά ή σύνθετα, οι λίστες ταχυδρομείου και άλλα. Η σειρά λογισμικού InfoPoll «τρέχει» σε πλατφόρμα που χρησιμοποιεί Microsoft Windows. Οι χρήστες μπορούν να προσπελάσουν τις δημοσιευμένες φόρμες με χρήση ενός webbrowser, από οποιαδήποτε υπολογιστική πλατφόρμα. Η σειρά λογισμικού InfoPoll περιλαμβάνει δύο κύρια συστατικά στοιχεία: τον InfoPoll Σχεδιαστή – Designer και τον InfoPoll Εξυπηρετητή – Server. Τα δύο στοιχεία συνεργάζονται προκειμένου να συλλέξουν τα απαραίτητα δεδομένα, ενώ ταυτόχρονα εξοικονομούν χρόνο, αυξάνουν την απόκριση του συστήματος και παρέχουν λεπτομερείς αναλύσεις των δεδομένων.

Ο InfoPoll Σχεδιαστής

Ο InfoPoll Σχεδιαστής είναι ένα εύκολο στη χρήση εργαλείο, το οποίο μας επιτρέπει να δημιουργούμε φόρμες. Ο Σχεδιαστής παρέχει μια σειρά δυνατοτήτων, όπως ενσωματωμένους οδηγούς χρήσης του προγράμματος, έτοιμα για χρήση πρότυπα ερωτήσεων, καθώς και παραδείγματα ερωτηματολογίων τα οποία βοηθούν στο σχεδιασμό HTML φορμών. Με τη χρήση του Σχεδιαστή μπορεί κανείς να σχεδιάσει και να δημοσιεύσει φόρμες στο Internet, στο εσωτερικό δίκτυο μια εταιρίας ή σε ένα τοπικό δίκτυο, με το πάτημα ενός κουμπιού. Οι δημοσιευμένες φόρμες είναι εύκολα προσβάσιμες από οποιοδήποτε σημείο, οποιαδήποτε στιγμή, με χρήση ενός webbrowser (NetscapeNavigator ή Windows Explorer) και ενός κωδικού πρόσβασης – userid.

Ο InfoPoll Εξυπηρετητής. Ο InfoPoll εξυπηρετητής, είναι η πρώτη web-based πραγματικού χρόνου on-line μηχανή συλλογής, ανάλυσης και παραγωγής αποτελεσμάτων. Αφού χρησιμοποιηθεί πρώτα ο Σχεδιαστής για τη δημοσίευση των φορμών, ο Εξυπηρετητής αυτόματα δημιουργεί έναν ειδικό πίνακα βάσης δεδομένων, στον οποίο συλλέγονται και αποθηκεύονται τα δεδομένα μας. Ο Εξυπηρετητής επιτρέπει τη διεξαγωγή μίας έρευνας ή μιας δημοσκόπησης με απεριόριστο αριθμό χρηστών κάθε στιγμή. Όταν οι χρήστες τελειώσουν με την αποστολή των ψήφων τους , ο εξυπηρετητής αναλαμβάνει να επιβεβαιώσει και να επικυρώσει τα αποτελέσματα. Τα αποτελέσματα δημοσιεύονται με τη μορφή μιας εύκολης στην κατανόηση αναφοράς, η οποία συμπληρώνεται από λεπτομερή στατιστική ανάλυση. Ένα από τα ισχυρά γνωρίσματα του InfoPoll Εξυπηρετητή είναι το εργαλείο στατιστικής ανάλυσης που διαθέτει. Το on-line αυτό εργαλείο επιτρέπει στους χρήστες να κάνουν διεξοδικές αναλύσεις, με την εισαγωγή επιπλέον μεταβλητών στις ερωτήσεις που κάνουν προς τη βάση δεδομένων. Δίνεται επίσης η δυνατότητα για εξαγωγή των δεδομένων ή των αποτελεσμάτων σε άλλα πακέτα λογισμικού όπως τα Microsoft Excel και Microsoft Access. Τέλος, τα αποτελέσματα μπορούν να εξαχθούν και σε άλλα προγράμματα στατιστικής ανάλυσης, για περαιτέρω επεξεργασία. Για καλύτερη απόδοση, συστήνεται το λογισμικό InfoPoll να εγκατασταθεί σε ένα Microsoft Windows NT Server, ο οποίος να έχει εγκατεστημένο και σε λειτουργία έναν MS Internet Information Server IIS, έκδοσης 3.0, 4.0 ή νεώτερης.

Το σύστημαPericles (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 PaulKirby. 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.

Το σύστημαTrueBallot

Άλλο ένα σύστημα που σήμερα είναι διαθέσιμο για ψηφοφορία μέσο Internet είναι αυτό που προσφέρει η TrueBallot, Inc. DemocraticGovernance Systems. Είναι ένα πρότυπο on line σύστημα ψηφοφορίας το οποίο σχεδιάστηκε από την εταιρία με βάση την εμπειρία που απέκτησε από τη 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.

Στάδια ηλεκτρονικής ψηφοφορίας

Η διαδικασία είναι σχεδόν ίδια με εκείνη των παραδοσιακών εκλογών. Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα (4) στάδια:

1. **Εγγραφή.** Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του δικαιώματός τους να ψηφίσουν (π.χ. όριο ηλικίας). Όσοι έχουν δικαίωμα συμμετοχής προστίθενται στον εκλογικό κατάλογο.

2. **Ταυτοποίηση**. Κατά τη διάρκεια των εκλογών, και πριν υποβάλλουν τη ψήφο τους, οι ψηφοφόροι ταυτοποιούνται, δηλαδή επιβεβαιώνεται η ταυτότητα τους τη δεδομένη χρονική στιγμή.

3. **Υποβολή ψήφου.** Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο. Αυτό εξαρτάται με την πολιτική που έχει ορισθεί. Αλλά για λόγους λογικής και ασφάλειας, τις περισσότερες φορές, ένας και μόνο ένας ψηφοφόρος επιτρέπεται να ψηφίσει μία και μόνο μία φορά.

4. **Καταμέτρηση ψήφων.** Μόλις λήξη η προθεσμία υποβολής ψήφων, οι ψήφοι καταμετρούνται και στη συνέχεια ανακοινώνεται το αποτέλεσμα των εκλογών.

Κάθε ένα από τα παραπάνω στάδια λαμβάνει χώρα με χρήση ηλεκτρονικών διαδικασιών.

Αποδοτικότητα συστήματος ηλεκτρονικής ψηφοφορίας

Για να είναι ένα σύστημα αποδοτικό θα πρέπει να είναι:

- Εύκολα υλοποιήσιμο.
- Συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Webκ.λπ).
- Λειτουργικό (Στις εκλογές του 2000 στη Florida των Η.Π.Α ένας μεγάλος αριθμός άκυρων ψήφων υποβλήθηκε λόγω ελλιπούς σχεδίασης των ψηφοδελτίων).
- Να καλύπτει όλες τις απαιτήσεις του πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet κ.λπ.
- Να υποστηρίζει μια ποικιλία από format ψηφοδελτίων, συμπεριλαμβανομένων των «λευκών» ή άκυρων.
- Να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητά του να μην επηρεάζεται δραστικά από το μέγεθος του εκλογικού σώματος ή των αριθμό των υποψηφίων (scalability).
- Να προσφέρει διαφανείς υπηρεσίες ασφάλειας (transparent) στον χρήστη.

Σύσταση και απαιτήσεις ηλεκτρονικής ψηφοφορίας

Απαιτήσεις σε υλικό

Ένα από τα κυριότερα ζητήματα είναι η σωστή επιλογή και συντήρηση υλικού εξοπλισμού (hardware). Στην υπάρχουσα εκλογική διαδικασία το πιο συνηθισμένο, αν όχι το μοναδικό υλικό, που χρησιμοποιείται είναι οι κάλπες και τα παραβάν. Όπως είναι αυτονόητο δεν έχει νόημα να τονίσουμε το θέμα ως απαίτηση ασφαλείας της συμβατικής εκλογικής διαδικασίας. Στην ηλεκτρονική ψηφοφορία, όμως, το θέμα του υλικού εξοπλισμού είναι εξαιρετικής σημασίας. Ο τρόπος λειτουργίας του, καθώς και η ποιότητα των τμημάτων που το συνθέτουν, πρέπει να είναι όσο το δυνατόν καλύτερης ποιότητας. Οι κίνδυνοι που μπορεί να προκύψουν από ανεπαρκές 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 εκτελούνται συστηματικοί έλεγχοι κατά την κατασκευή του, καθώς και κατά το χρονικό διάστημα που θα επέλθει μέχρι να χρησιμοποιηθούν. Πιθανή επιχείρηση τροποποίησης των μηχανημάτων, που χρησιμοποιούνται σε οποιαδήποτε εκλογική διαδικασία, πρέπει να καταλήγει είτε σε αποτυχία της προσπάθειας είτε σε ολοσχερή καταστροφή του μηχανήματος, με αποτέλεσμα όταν ένα μηχάνημα λειτουργεί να είναι βέβαιο πως δεν έχει υποστεί τροποποίηση. Όσον αφορά κάποια τυχαία βλάβη κατά την εκλογική διαδικασία, πρέπει να υπάρχει αυστηρώς κατάλληλα 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 στιγμής έχουν γίνει πάρα πολλές προτάσεις για ειδικά μηχανήματα που μπορούν να χρησιμοποιηθούν για μια εκλογική διαδικασία με επικρατέστερα μέχρι ώρας τα DREs. Να επισημάνουμε πως στις ανάγκες για κατάλληλο υλικό μπορεί να αναφερθεί τυχόν χρήση έξυπνων καρτών (smartcards) για αυθεντικοποίηση των χρηστών.

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.).

Τρόποι άσκησης εκλογικού δικαιώματος

Παραδοσιακή μορφή ψηφοφορίας (χωρίς την χρήση τερματικών)

Είναι η ψηφοφορία στα εκλογικά τμήματα με τη χρήση ενός έντυπου ψηφοδελτίου. Οι εγγεγραμμένοι στους εκλογικούς καταλόγους πολίτες, εισέρχονται στους ειδικά διαμορφωμένους χώρους και με τη μορφή του σταυρού ή της δεσμευμένης επιλογής (λίστα), επιλέγουν τις προτιμήσεις τους. Η μορφή αυτή ψηφοφορίας, παρέχει αρκετές εγγυήσεις για τη διασφάλιση του μυστικού χαρακτήρα της διαδικασίας.

Επιστολική ψήφος (χωρίς την χρήση τερματικών)

Ασκείται με την αποστολή στις αρμόδιες διοικητικές αρχές, μέσω ταχυδρομείου, του έντυπου ψηφοδελτίου που καταγράφει τη βούληση του εκλογέα. Η επιστολική ψήφος εξυπηρετεί ψηφοφόρους, οι οποίοι λόγω της συνδρομής συγκεκριμένων γεγονότων, αδυνατούν να προσέλθουν στα εκλογικά τμήματα, κατά την ημέρα διεξαγωγής των εκλογών για να ασκήσουν το εκλογικό τους δικαίωμα. Σήμερα η εκλογική νομοθεσία των περισσότερων κρατών επιτρέπει την άσκηση της επιστολικής ψήφου μετά από αίτηση του, χωρίς να απαιτεί την επίκληση του. Τελευταία γίνεται λόγος για τη λεγόμενη καθολική επιστολική ψήφο (αναλυτικότερα στην ενότητα Θεμελιώδεις Αρχές Ασφάλειας), όπου τα εκλογικά τμήματα θα καταργηθούν και η ψηφοφορία θα ασκείται αποκλειστικά μέσω ταχυδρομείου.

Ηλεκτρονική ψηφοφορία

Όπως έχει προαναφερθεί περιλαμβάνει μία μεγάλη κλίμακα από καινοτόμες εξελίξεις στον τρόπο οργάνωσης και διεξαγωγής των εκλογικών διαδικασιών. Τις αλλαγές αυτές προκάλεσε, μεταξύ άλλων, η ανάγκη για επιτάχυνση στον τρόπο με τον οποίο καταμετρούνταν τα ψηφοδέλτια, ο οποίος, ιδιαίτερα στα κράτη με μεγάληδημογραφική συγκέντρωση, μπορούσε να αναστείλει για ημέρες την ανακοίνωση του εκλογικού αποτελέσματος, καθώς και η ανάγκη για μείωση του κόστους της εκλογικής διαδικασίας, μέσω της απασχόλησης οικονομικών και ανθρωπίνων πόρων. Οι αλλαγές αυτές αρχικά συνίστατο στην εισαγωγή ηλεκτρονικών μηχανημάτων, τα οποία στόχευαν στην απλοποίηση της διαδικασίας μέτρησης των ψήφων, την οποία αυτοματοποίησαν, και κατά συνέπεια στην επιτάχυνση στην ανακοίνωση των εκλογικών αποτελεσμάτων.

Παρουσία συστήματος ηλεκτρονικής ψηφοφορίας στην Ελλάδα

Στον Ελληνικό χώρο έχουν γίνει βήματα προς την ηλεκτρονική ψηφοφορία, αλλά δεν υπάρχουν ακόμα ούτε οι υποδομές για χρήση της ηλεκτρονικής υπογραγής, παρόλο που με προεδρικό διάταγμα, η ηλεκτρονική υπογραφή ισχύει από το 2001. Ωστόσο, η ηλεκτρονική ψηφοφορία στη χώρα μας έχει χρησιμοποιηθεί πολλές φορές (πάνω από 300 έως τον Μάιο του 2015 μέσω του συστήματος <<ΖΕΥΣ>>). Από πολιτικό φορέα, η ηλεκτρονική ψηφοφορία χρησιμοποιήθηκε για πρώτη φορά στην εκλογή των θεσμικών οργάνων του κόμματος <<Δημιουργία Ξανά>> (Φεβρουάριος 2013).

Πληροφοριακό σύστημα «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. Υποστηρίζονται πολλαπλά είδη ψηφοδελτίων και εκλογικών συστημάτων, όπως ερωτήσεις πολλαπλών επιλογών, ψηφοφορίες με διαφορετικό ψηφοδέλτιο ανά συνδυασμό, και ψηφοδέλτια για ταξινομική ψήφο (STV). Το «Ζευς» αρχικά βασίστηκε στο Helios, και διατηρεί τη γενική προσέγγιση, αλλά έχει έκτοτε ακολουθήσει τη δική του πορεία. Έχει εξυπηρετήσει πάνω από 250 ηλεκτρονικές κάλπες και 35000 ψηφοφόρους για τα Ελληνικά Πανεπιστήμια και άλλους φορείς.

Εφαρμοφή ηλεκτρονικής ψηφοφορίας στην Βουλή

Τα παρακάτω κείμενα πρόκειται για αποσπάσματα ειδήσεων. Περιγράφουν την εφαρμογή ενός συστήματος ψηφιακής ψηφοφορίας μέσα στην Βουλή των Ελλήνων κατά την διάρκεια ψήφησης ενός νόμου.

Απόσπασμα 1

"*Το σύστημα εφαρμόστηκε στη σημερινή συνεδρίαση του Α' Θερινού Τμήματος για πρώτη φορά, ωστόσο θα επαναληφθούν άλλες δύο πιλοτικές εφαρμογές, στο Β' και στο Γ' Θερινά Τμήματα, προκειμένου να τεθεί σε πλήρη εφαρμογή τον Οκτώβριο, με το άνοιγμα των εργασιών της νέας Συνόδου.Της ηλεκτρονικής ψηφοφορίας ακολούθησε και ο παραδοσιακός τρόπος ανάγνωσης του καταλόγου των βουλευτών, προκειμένου να αποφευχθούν οι αστοχίες της πρώτη φοράς.*

Στην πρώτη φάση της ηλεκτρονικής ψηφοφορίας, που αντικατέστησε την παραδοσιακή πρώτη ανάγνωση του καταλόγου, απαιτήθηκε 1 λεπτό και 10 δευτερόλεπτα. Στη δεύτερη επαναληπτική φάση, που αντικατέστησε την παραδοσιακή δεύτερη ανάγνωση του καταλόγου, απαιτήθηκε περίπου 1 λεπτό και 35 δευτερόλεπτα. Έτσι, όπως προκύπτει από τα έγγραφα της νομοθετικής υπηρεσίας για το αυτοματοποιημένο σύστημα ανοιχτής κοινοβουλευτικής ψηφοφορίας, τυπικά η έναρξη έγινε στις 13:27:23 και η λήξη της στις 13:28:00.

Οι συμμετέχοντες ήταν 84, επιλογή «ναι» έκαναν 49 βουλευτές, επιλογή «όχι» 35 βουλευτές και 0 βουλευτές στο «παρών». Το σύστημα αυτόματα καταγράφει το ονοματεπώνυμο του κάθε βουλευτή, την εκλογική παράταξη, την εκλογική περιφέρεια, την επιλογή της ψήφου και την ώρα καταχώρησης της ψήφου."

Απόσπασμα 2

"Πρεμιέρα κάνει την Τρίτη το μεσημέρι το σύστημα ηλεκτρονικής ψηφοφορίας στη Βουλή. Το νέο σύστημα, που αναμένεται να οδηγήσει σε σημαντική οικονομία χρόνου, θα τεθεί σε λειτουργία κατά τη συζήτηση του νομοσχεδίου του υπουργείου Δικαιοσύνης, στο οποίο, μεταξύ άλλων, προβλέπεται και η δημιουργία φυλακών τύπου Γ'.

Ο ΣΥΡΙΖΑ έχει ήδη προαναγγείλει ονομαστικές ψηφοφορίες, όχι μόνο επί της αρχής αλλά και επί των άρθρων του νομοσχεδίου, και αύριο Τρίτη θα δοθεί για πρώτη φορά η ευκαιρία εφαρμογής του, έστω κι αν χρειαστεί να γίνει η ονομαστική ψηφοφορία και με τον παραδοσιακό τρόπο, προκειμένου οι υπάλληλοι να ξεπεράσουν τις δυσκολίες της... πρώτης φοράς.

Πάντως, η τεχνική προετοιμασία της ηλεκτρονικής ψηφοφορίας έχει ολοκληρωθεί και

οι βουλευτές που θα συμμετάσχουν στο πρώτο θερινό τμήμα της Βουλής θα ψηφίζουν με την ατομική κάρτα τους «ναι», «όχι» ή «παρών» στις ονομαστικές ψηφοφορίες.

Από τα στατιστικά στοιχεία που διαθέτουν οι αρμόδιες υπηρεσίες της Βουλής μέχρι σήμερα, μία ονομαστική ψηφοφορία απαιτούσε σχεδόν δύο ώρες για τη ανακοίνωση του αποτελέσματος.

Σχεδόν μία ώρα απαιτούσε η ανάγνωση του καταλόγου και άλλη μία ώρα η καταμέτρηση των ψήφων.

Πλέον, ο χρόνος που θα απαιτείται θα είναι δέκα λεπτά, δεν θα προηγείται ανάγνωση του καταλόγου, ενώ οι βουλευτές που δεν πρόλαβαν να ψηφίσουν κατά την πρώτη ανάγνωση θα έχουν μία ακόμη ευκαιρία, όπως άλλωστε γίνεται και σήμερα αλλά με την επίσης χρονοβόρα διαδικασία της δεύτερης ανάγνωσης.

Στο σύστημα της ηλεκτρονικής ψηφοφορίας θα καταχωρούνται και οι επιστολικές ψήφοι. ”

Αναφορές επιχειρηματία

Ένας επιχειρηματίας με ελληνικές ρίζες, ο πρόεδρος και διευθύνων σύμβουλος της καναδέζικης εταιρείας DominionVoting, Γιάννης Πούλος, σε αντίθεση με τα ελληνικά δεδομένα, προχώρησε στην υλοποίηση ενός προγράμματος, με στόχο να βελτιστοποιήσει την εκλογική διαδικασία με τη συμβολή της τεχνολογίας. Παρείχε τεχνογνωσία και τεχνολογική υποστήριξη στα περισσότερα εκλογικά τμήματα του Οντάριο κατά τις εκλογές του 2010 αλλά και σε πολλά εκλογικά τμήματα των ΗΠΑ.Ο ίδιος περιγράφει τα πρώτα του βήματα, όταν η σκέψη για τη δημιουργία της DominionVoting προέκυψε μετά τις εκλογές του 2000 στις ΗΠΑ. Ειδικά αναφέρει εκείνο που τον ενέπνευσε:

«*Αυτό που είδα στις εκλογές του 2000 στην Αμερική ανάμεσα στον Μπους και τον Αλγκόρ ήταν ότι υπήρχαν προβλήματα κατά την ψηφοφορία, ιδίως στη Φλόριντα. Χρειάστηκε μάλιστα να παρέμβει το Ανώτατο Δικαστήριο για να δώσει τη λύση. Τότε, μαζί με τους συνεργάτες μου είδαμε μία ευκαιρία να εφαρμόσουμε την ηλεκτρονική ψηφοφορία όχι μόνο στις Ηνωμένες Πολιτείες αλλά σε ολόκληρο τον κόσμο, κάνοντας πιο αποτελεσματική την εφαρμογή της Δημοκρατίας*».

Ο καθένας μπορεί να ψηφίσει απ’ οπουδήποτε

«*Ξεκίνησα την εταιρεία το 2002 από το Τορόντο του Καναδά. Στόχος μας ήταν να δημιουργήσουμε ένα σύστημα ψηφοφορίας, το οποίο θα ήταν απόλυτα αξιόπιστο. Έτσι, θα μπορούσε ο καθένας να συμμετάσχει στις εκλογές, καθώς θα ήταν ευκολότερο να ψηφίσει. Ουσιαστικά αυτό που θέλαμε να πετύχουμε ήταν να δώσουμε προσβασιμότητα σε όλους όσους αντιμετώπιζαν διάφορα κινητικά προβλήματα. Άτομα με κάθε μορφής αναπηρία. Το κλειδί της Δημοκρατίας είναι η όσο το δυνατόν μεγαλύτερη συμμετοχή των πολιτών στις διαδικασίες της πολιτείας*», λέει ο ίδιος .

Ποιο είναι το μέλλον της διαδικτυακής ψηφοφορίας;

Η διείσδυση του Internet στις σύγχρονες κοινωνίες καθιστά επωφελή την υιοθέτηση ηλεκτρονικών μεθόδων για την εξ αποστάσεως συμμετοχή του πολίτη στις δημοκρατικές.

Τα συστήματα εξ αποστάσεως ψηφοφορίας μέσω Internet, μαζί με άλλες διαδικασίες που εφαρμόζονταισήμερα σε δημοκρατικά καθεστώτα (π.χ. ψηφοφορία μέσω ταχυδρομείου στην Ελβετία) αναμένεται να απλοποιήσουν την υποβολή της ψήφου και να αυξήσουν τη συμμετοχή των πολιτών στις εκλογές. Σε κάθε περίπτωση, η υποβολή ψήφου μέσω Internet θα πρέπει να αποτελέσει μια εναλλακτική και όχι τη μοναδική δυνατότητα συμμετοχής του πολίτη στις εκλογές. Σε αντίθετη περίπτωση, προκύπτουν ζητήματα κοινωνικού αποκλεισμού και συνταγματικότητας των εκλογών.

Προβλήματα ασφάλειας

Είναι γεγονός ότι υπάρχουν ισχυρά κίνητρα για πραγματοποίηση επίθεσης στην ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας, ιδιαίτερα αυτές που αφορούν εθνικές εκλογές (πολιτικές επιδιώξεις, χρηματική αμοιβή, διεκδίκηση εξουσίας, εμπλοκή μυστικών υπηρεσιών, τρομοκρατικές οργανώσεις). Το είδος και η μορφή των επιθέσεων ποικίλουν. Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πιο εύκολα από ό,τι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις εσωτερικών εχθρών (InsiderAttacks), καθώς και σε επιθέσεις άρνησης εξυπηρέτησης (Denial Of Service/DOS). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας διαθέτουν ανεπαρκή στοιχεία ελέγχου και δεν παρέχουν **οικουμενική επαληθευσιμότητα**[1], με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση. Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω διαδικτύου είναι περισσότερο ευάλωτες σε επιθέσεις καταναγκασμού (Coercion), κατά τις οποίες οι χρήστες αναγκάζονται από ή συναλλάσσονται με κάποιον τρίτο να υποβάλουν προσυμφωνημένη ψήφο (Burmester κ.ά., 2003). Επιπρόσθετα, σε ένα σύστημα εξ αποστάσεως ψηφοφορίας οι ίδοι οι ψηφοφόροι θα πρέπει ενδεχομένως να δημιουργήσουν ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), π.χ. προτού υποβάλλουν την ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω διαδικτύου παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web.

Τα συστήματα ψηφοφορίας μέσω δαδικτύου είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

• **Στα συστήματα-πελάτες:** Ιοί τύπου «σκουλήκια» (Worms) ή «δούρειοι ίπποι» (TrojanHorses) μπορούν να αλλοιώσουν την ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί. Επίσης, ο εισβολέας μπορεί εξ αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web.Παραβίαση δικαιωμάτωνπνευματικής ιδιοκτησίας. Αντιγραφή, αναπαραγωγή, παραποίηση ή/και αναδιανομήδεδομένων, πληροφοριών που προστατεύονται από τους νόμους περί πνευματικής ιδιοκτησίας, χωρίς τη συγκατάθεση του δημιουργού τους.

•Στο επίπεδο της επικοινωνίας: Οι κυριότερες επιθέσεις σε αυτό το επίπεδο είναι οι επιθέσεις πλαστοπροσωπίας (Spoofing) DNS ονομάτων ή IP διευθύνσεων και οι

[1] **Καθολική οικουμενική επαληθευσιμότητα**: Από τις αρχές της δεκαετίας του 1990, έχουν προταθεί πολλά κρυπτογραφικά πρωτόκολλα ψηφοφορίας για την παροχή καθολικής επαληθευσιμότητας. Σε αυτά τα σχήματα, κάθε παρατηρητής μπορεί να επαληθεύσει ότι μόνο οι εγγεγραμμένοι ψηφοφόροι υποβάλλουν ψηφοδέλτια και ότι μόνο τα υποβεβλημένα ψηφοδέλτια καταμετρούνται σωστά. Η καθολική επαληθευσιμότητα χρησιμοποιεί την κρυπτογραφία για να επαναφέρει τον πίνακα ανακοινώσεων του παρελθόντος. Τα ψηφοδέλτια είναι κρυπτογραφημένα και αναρτημένα μαζί με την ταυτότητα του ψηφοφόρου σε απλό κείμενο. Η καθολική επαληθευσιμότητα αποτελεί συνεπώς μία δημόσια καταμέτρηση, επιδιορθώνοντας ένα μεγάλο τμήμα από την τρύπα της δυνατότητας ελέγχου που προκαλείται από την μυστική ψηφοφορία.

επιθέσεις ενδιάμεσης οντότητας (Man in the Middle). Η επικοινωνία μεταξύ πελάτη και εξυπηρετητή μπορεί επίσης να απειληθεί από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κτλ.Ακόμα μη ζητηθείσα επικοινωνία (spam),δηλαδήμηνύματα ηλεκτρονική αλληλογραφίας που αποστέλλονται χωρίς τη συγκατάθεση του παραλήπτη, ενώ συχνά η ταυτότητα του αποστολέα είναι πλαστογραφημένη ή απλά αδύνατον να εντοπιστεί.

• **Στα συστήματα-εξυπηρετητές:** Διακοπή ή υποβάθμιση των παρεχομένων υπηρεσιών ενός συστήματος. 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 (BufferOverflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία. Το πρόβλημα της συμφόρησης (Bottleneck) είναι παρόμοιο, ως προς τις συνέπειές του, με αυτό της επίθεσης 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.

Απειλές στην ασφάλεια ενός συστήματος

Κακόβουλο λογισμικό

Μια από τις πιο επικίνδυνες μορφές επιθέσεων είναι ένας ιός (virus), δούρειος ίππος (TrojanHorse) ή σκουλήκι (Worm) που εξαπλώνεται και περιέχει ένα κακόβουλο ωφέλιμο φορτίο σχεδιασμένο να πάρει τον έλεγχο των υπολογιστών και να δημιουργήσει σημαντικά προβλήματα ή ακόμα και διακοπή της εκλογικής διαδικασίας. Μια τέτοια επίθεση θα μπορούσε να βλάψει την εμπιστευτικότητα και την ακεραιότητα της ψήφου ενός ατόμου, με το να μεταβιβάσει σε κάποιον τρίτο πληροφορίες για τον τρόπο με τον οποίο ψήφισε ο νόμιμος χρήστης, ή με την αλλαγή της ψήφου πριν από τη καταχώρηση της χωρίς ο χρήστης να το γνωρίζει. Οι γνωστές εφαρμογές προστασίας από**ιομορφικό λογισμικό**[2]είναι ανίκανες συχνά να συμβαδίσουν με τη διάδοση των νέων ιών και σκουληκιών. Τα σύγχρονα σκουλήκια είναι ακόμα πιο ισχυρά, διαδίδονται συχνά με πολλαπλές μεθόδους, είναι σε θέση να παρακάμψουν τα firewall και άλλους μηχανισμούς ασφαλείας και μπορεί να είναι δύσκολο να αναλυθούν. Οι επιτιθέμενοι μπορούν να δημιουργήσουν νέους ιούς, ή να τροποποιήσουν αποτελεσματικά τους υπάρχοντες ιούς για να αποφύγουν την ανίχνευση. Αρκετά εργαλεία κατασκευής ιών είναι διαθέσιμα στο διαδίκτυο.

Εσωτερικές απειλές

Οι νόμιμοι χρήστες του συστήματος ηλεκτρονικής ψηφοφορίας εκμεταλλευόμενοι την θέση τους μπορεί να επιδιώξουν να κάνουν κακή χρήση ή να βλάψουν το σύστημα εκλογών. Κατά κανόνα έχουν προνομιούχα δικαιώματα πρόσβασης, καθώς και σημαντικούς τεχνικούς πόρους και δεξιότητες στη διάθεσή τους και συνήθως είτε για οικονομικό κέρδος είτε την προσωπική ικανοποίηση αποκτούν ένα ισχυρό κίνητρο για να υπονομεύσουν την υπηρεσία. Για αυτούς τους χρήστες μπορεί να δημιουργηθεί ένα ειδικό νομικό πλαίσιο, ώστε να υπόκεινται στις απαραίτητες κυρώσεις σε περίπτωση που αποκαλυφθούν παραβιάσεις ασφάλειας που διαπράχθηκαν από αυτούς.

[2]Στο **ιομορφικό λογισμικό** ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο **μη ιομορφικό λογισμικό** τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα.

Εξωτερικές απειλές

Κάποιοι χάκερ μπορεί να επιδιώξουν να προκαλέσουν διάρρηξη στα συστήματα λόγω προσωπικών οφελειών, για την πρόκληση να επιτεθούν σε ένα κυβερνητικό σύστημα ή ως διαμαρτυρία ενάντια στις κυβερνητικές πολιτικές. Μπορούν επίσης να επιθυμήσουν να έχουν πρόσβαση, να αλλοιώσουν ή να κλέψουν δεδομένα, είτε για προσωπικό κέρδος, είτε για λόγους δημοσιότητας. Η διείσδυση στο σύστημα ηλεκτρονικής ψηφοφορίας θα είχε πολύ σοβαρές επιπτώσεις για την εμπιστοσύνη του κοινού στην δικτυακή ψηφοφορία και επιπτώσεις σε σχέση με νόμους και ψηφίσματα όπως αυτά της αρχής προστασίας δεδομένων. Πίσω από τέτοιες επιθέσεις πέρα από μεμονωμένους χάκερ μπορεί να κρύβονται εγκληματικές οργανώσεις, ομάδες διαμαρτυρίας ή ακτιβιστές, ξένες υπηρεσίες πληροφοριών, ή τρομοκρατικές οργανώσεις.

Ακούσια ζημία

Οι νόμιμοι χρήστες μπορούν ακούσια να κάνουν κακή χρήση του συστήματος ηλεκτρονικής ψηφοφορίας και ενδεχομένως να προκαλέσουν ζημία στο σύστημα. Σε περίπτωση που μεγάλος αριθμός ψηφοφόρων χρησιμοποιούσαν το σύστημα λανθασμένα θα μπορούσε να προκληθεί περιττή απώλεια στην απόδοση του συστήματος ή ακόμα και κατάρρευση του.

Η Αρχή της Μυστικότητας της Ψήφου

Η αρχή της μυστικότητας της ψήφου γενικά έχει ως στόχο να προστατεύσει την γνησιότητα της ψηφοφορίας, διασφαλίζοντας το απόρρητο ειδικά σε θέματα όπως των πολιτικών επιλογών του εκλογέα. Κάθε παράβαση της μυστικότητας προκαλέι νόθευση της λαικής βούλησης. Για αυτό οι εκλογικές νομοθεσίες των αρκετών κρατών μεριμνούν για τη διασφαλισή της. Στη χώρα μας ο ελληνικός εκλογικός νόμος προβλέπει παράδοση στον εκλογέα φακέλου με ειδικό γνώρισμα, μονογραμμένο από τον δικαστικό αντιπρόσωπο, απόσυρση του εκλογέα σε ειδικά διαμορφωμένο χώρο και ρίψη του φακέλου στην κάλπη από τον ψηφοφόρο.

ΘεμελιώδειςΑρχέςΑσφάλειας

- **Καθολικότητα:** Η ενσυνείδητη εκ μέρους της Πολιτείας ελαχιστοποίηση των προσόντων που απαιτούνται για να μπορεί ένα πρόσωπο να συμμετάσχει ως ψηφοφόρος σε εκλογές.
- **Αμεσότητα:** Η μη παρεμβολή ενδιάμεσης βούλησης ή οργάνου ανάμεσα στην έκφραση της επιλογής του ψηφοφόρου και στην αποτύπωσή της στο εκλογικό αποτέλεσμα.
- **Μυστικότητα:** Η εξασφάλιση μη γνωστοποίησης του περιεχομένου της ψήφου σε άλλο πρόσωπο εκτός του ψηφίζοντος.
- **Ταυτόχρονη διεξαγωγή:**Η έκφραση της ατομικής εκλογικής προτίμησης διατυπώνεται χωρίς να υπάρχει δυνατότητα γνώσης άλλων αποτελεσμάτων στην ίδια εκλογή.
- **Ισότητα της ψήφου και των ψηφοφόρων:** Κάθε πολίτης δικαιούνται μια ψήφο και όλες οι ψήφοι είναι μεταξύ τους ισοδύναμες.

- **Ελευθερία της ψήφου και της ψηφοφορίας:**Ο ψηφοφόρος έχει το δικαίωμα να εκφράσει τη βούλησή του ελεύθερα και χωρίς κανένα εξαναγκασμό ή άσκηση πίεσης.

Αναλυτικότερα:

Καθολικότητα

Η καθολικότητα είναι δυνατόν να θεωρεί ότι πλήττεται λόγω της απαίτησης ειδικών γνώσεων ή δεξιοτήτων από τα άτομα που πρόκειται να ψηφίσουν ηλεκτρονικώς. Όσο υφίσταται το λεγόμενο «ψηφιακό χάσμα», ο διαχωρισμός δηλαδή του κοινωνικού σώματος σε ψηφιακώς «εγγράμματους» και «αναλφάβητους», η ηλεκτρονική ψηφοφορία δεν μπορεί να θεωρηθεί ότι πληροί τα κριτήρια της καθολικότητας, στην πράξη δε, σε ένα πρώτο τουλάχιστον στάδιο, θα έχει ως συνέπεια να επιτείνει τη διάκριση ανάμεσα σε «δυναμένους» και μη.

Αμεσότητα

Προσκρούει στη (θεωρητική αλλά δύσκολα αποκλειόμενη) δυνατότητα των χειριστών του συστήματος να αλλάξουν το περιεχόμενο της δοθείσας ψήφου, καθώς και στην (επίσης πιθανή σύμφωνα με την ως τώρα εμπειρία) ικανότητα κάποιων «εκτός συστήματος» να εισέλθουν εντός και να επηρεάσουν το αποτέλεσμα.

Μυστικότητα

Κινδυνεύει με δύο τουλάχιστον τρόπους:
Λόγω της πιθανής ύπαρξης άλλου προσώπου που να βλέπει (ακόμα και να επηρεάζει) την ψήφο τη στιγμή που δίνεται από τον ψηφοφόρο.
Λόγω της πιθανής αντιστοίχισης της δοθείσας ψήφου με συγκεκριμένο ψηφοφόρο από χειριστή του συστήματος.

Ταυτόχρονη διεξαγωγή

Παραβιάζεται αν η καταμέτρηση των ηλεκτρονικών ψήφων γίνει σε ύστερο από της «κλασικής» ψηφοφορίας χρόνο, ενώ υπάρχει πάντα και ο κίνδυνος ο χειριστής του συστήματος να ψηφίσει γνωρίζοντας τα αποτελέσματα της «κάλπης» που επιβλέπει.

Στο άρθρο 51 (παρ. 3-5) του ισχύοντος ελληνικού Συντάγματος προβλέπονται ρητά οι **σχετικοί κανόνες και αρχές**.

Θεσμικό και νομικό πλαίσιο

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 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. Τέλος στην προστασία των δικαιωμάτων του πολίτη συμπεριλαμβάνεται και η προστασία του από καταναγκασμό.

Προστασία Από Καταναγκασμό

Στις παραδοσιακές εκλογές, ο ρόλος του εκλογικού παραβάν (votingbooth) δεν περιορίζεται απλώς στο να επιτρέπει στους ψηφοφόρους να επιλέξουν μεαπόλυτη μυστικότητα τη ψήφο τους. Ουσιαστικά η ύπαρξη του παραβάν αποτρέπει γεγονότα όπως η πώληση της ψήφου (voteselling) και ο καταναγκασμός (coercion) των ψηφοφόρων, η αποτροπή τέτοιων επιθέσεων αποτελεί σημαντικόκομμάτι της έρευνας για ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας μέσω Διαδικτύου.Αυτή επιτυγχάνεται εφόσον υποθέσουμε ότι ο Καταναγκαστής δεν μπορεί να ελέγξει από κοινού τον ψηφοφόρο και την Κάρτα (είναι μοναδική για τον καθένα και επιτρέπει την συμμετοχή στην ψηφοφορία). Ισχύει αφού για να αποκαλυφθεί η ψήφος είναι απαραίτητες τόσο η τυχαιότητα του ψηφοφόρου, όσο και η τυχαιότητα της Κάρτας. Επίσης, χάρη στην ιδιότητα των σχημάτων τύπου threshold, ο Καταναγκαστής θα πρέπει να διαφθείρει τουλάχιστον t από Αρχές για να καταφέρει να λάβει γνώση της αποκρυπτογραφημένης ψήφου. Στο βασικό αυτό σχήμα δεν γίνεται καμία υπόθεση φυσικής προστασίας του καναλιού επικοινωνίας μεταξύ του ψηφοφόρου και των Αρχών του συστήματος. Συμπεραίνουμε λοιπόν ότι είναι δύσκολο ο ψηφοφόρος να πέσει θύμα καταναγκασμού και αν για τον οποιοδήποτε λόγο γίνει είναι πολύ πιο δύσκολο να γίνει γνώση το τι ψήφισε.

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 αυτορύθμιση, 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.

Το Πρόβλημα των Απεχόντων Ψηφοφόρων

Ένα μειονέκτημα των συστημάτων ψηφοφορίας που βασίζονται στο μοντέλο των «τυφλών» υπογραφών, είναι ότι εάν ένας ψηφοφόρος εγγράφεται στο σύστημα αλλά

στη συνέχεια αποφασίζει (δικαιωματικά) να απέχει από τις εκλογές, δηλαδή να μην υποβάλλει ψήφο, τότε η Αρχή μπορεί να υποβάλλει μια πλαστή ψήφο για λογαριασμό του ψηφοφόρου, χωρίς μάλιστα αυτό να γίνει αντιληπτό από εξωτερικούς παρατηρητές ή/και από τους υπόλοιπους ψηφοφόρους. Προφανώς το γεγονός αυτό συνιστά άμεση παραβίαση και των δύο ιδιοτήτων της Δημοκρατικότητας του εκλογικού συστήματος. (α) Μόνο εξουσιοδοτημένοι ψηφοφόροι μπορούν να υποβάλλουν ψήφους, και β) Κανένας ψηφοφόρος δε μπορεί να υποβάλει περισσότερες από μια ψήφους.) Στη συνέχεια θα δείξουμε ότι το πρόβλημα των απεχόντων ψηφοφόρων μπορεί να οδηγήσει και σε παραβίαση της Ακρίβειας ($3^{η}$ ιδιότητα:γ)Καμιά ψήφος δε μπορεί να διαγραφεί, χωρίς κάτι τέτοιο να γίνει αντιληπτό) του συστήματος. Εφεξής, ως δέσμευση ψήφου (vote-tag) θα αποκαλούμε την κρυπτογραφημένη ψήφο σε συστήματα που βασίζονται στο μοντέλο των «τυφλών» υπογραφών. Όταν η δέσμευση ψήφου υπογραφεί «τυφλά» από την Αρχή κατά την περίοδο Εγγραφής, τότε και μόνον τότε θεωρείται ως έγκυρη. Πρόσφατα, για την αντιμετώπιση του προβλήματος των ψηφοφόρων που απέχουν, ο Rieraπρότεινε όλοι οι ψηφοφόροι να υποβάλλουν, μετά την εγγραφή τους και πριν υποβάλλουν την έγκυρη δέσμευση ψήφου τους, ένα ψηφιακά υπογεγραμμένο μήνυμα αναγνώρισης Μ το οποίο θα αναφέρει ότι κατέχουν μια έγκυρη δέσμευση ψήφου. Στη συνέχεια, και αφού αρχίσει η περίοδος υποβολής ψήφων, οι χρήστες θα υποβάλλουν ανώνυμα την έγκυρη δέσμευση ψήφου τους στην Αρχή. Η Αρχή θα δημοσιεύσει τη λίστα [έγκυρες δεσμεύσεις, μηνύματα αναγνώρισης] κατά το πρότυπο των δικτύων MIX-net, ώστε να μ ην υπάρχει συνδεσιμότητα των αποτελεσμάτων. Η λύση αυτή έχει το παρακάτω μειονέκτημα: μετά τη δημοσίευση των αποτελεσμάτων, και εάν υπάρχουν περισσότερες ψήφοι από υπογραφές, αυτό μπορεί να σημαίνει:

- Είτε ότι η Αρχή υπέβαλε πλαστές ψήφους,

- Είτε ότι κάποιοι ψηφοφόροι υπέβαλαν (ανώνυμα) την έγκυρη δέσμευση ψήφου χωρίς να έχουν υποβάλλει νωρίτερα (επώνυμα) το μήνυμα αναγνώρισης *M*.

Αν πάλι υπάρχουν περισσότερες υπογραφές από ψήφοι, τότε αυτό μπορεί να σημαίνει:

- Είτε ότι η Αρχή διέγραψε κάποιες ψήφους από την τελική κάλπη,

- Είτε ότι κάποιοι ψηφοφόροι υπέβαλλαν το μήνυμα αναγνώρισης στην Αρχή, αλλά στη συνέχεια αποφάσισαν να απέχουν, δηλαδή δεν υπέβαλαν την έγκυρη δέσμευση της ψήφου τους*M*.

Όλα τα συστήματα που έχουν προταθεί και βασίζονται στο μοντέλο των «τυφλών» υπογραφών πάσχουν από το πρόβλημα της υποβολής πλαστών ψήφων από την Αρχή εκ μέρους των ψηφοφόρων που απέχουν. Σε τέτοια συστήματα, συχνά γίνονται μ η πρακτικές υποθέσεις, π.χ. ότι όλοι οι εγγραφόμενοι ψηφοφόροι που αποφασίζουν να απέχουν θα υποβάλλουν μια λευκή ψήφο.

Προϋποθέσεις για τη διεξαγωγή ασφαλούς εκλογών μέσω Internet

Υπάρχουν αρκετές παράμετροι που πρέπει να ληφθούν σοβαρά υπ' όψιν ώστε να γίνει εφικτή η διεξαγωγή ηλεκτρονικών εκλογών μέσω διαδικτύου,όπως:

Πρωτόκολλα / Λογισμικό.

Για να είναι ασφαλής η ηλεκτρονική ψηφοφορία, το σύστημα θα πρέπει να:

- Υλοποιεί ένα κρυπτογραφικό πρωτόκολλο που ικανοποιεί τις απαιτήσεις ασφάλειας.
- Υποστηρίζεται,για λόγους αξιοπιστίας, με ανοικτό λογισμικό (opensource).
- Συνοδεύεται από τους κατάλληλους μηχανισμούς παρακολούθησης (monitoring) και επαλήθευσης (audit) της λειτουργίας του. Οι ανεξάρτητοι μηχανισμοί επαλήθευσης αυξάνουν την εμπιστοσύνη των πολιτών στο αποτέλεσμα των εκλογών.

Υποδομή Δημόσιου Κλειδιού.

Οι εκλογές μέσω Internet θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής στον ηλεκτρονικό εκλογικό κατάλογο έως και το στάδιο της Καταμέτρησης των ψήφων) μόνον όταν:

- Έχει υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής Υποδομή Δημόσιου Κλειδιού (PublicKeyInfrastructure – PKI), όπου η πιστοποίηση των ψηφοφόρων στο στάδιο της Εγγραφής και της Ταυτοποίησης θα γίνεται με τη χρήση ψηφιακών υπογραφών / ψηφιακών πιστοποιητικών ενώ η ακεραιότητα και η εμπιστευτικότητα των επικοινωνιών θα υποστηρίζονται από κρυπτογραφικούς αλγόριθμουςδημόσιου κλειδιού.
- Παράλληλα,τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο Εφαρμογής του μοντέλουOSI.
- Επιπλέον, τεχνολογίες όπως SSL/TLS (SecureSocketLayer/TransportLayerSecurity) και SSH (SecureShell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.

Ασφάλεια Πληροφοριακού Συστήματος

Εξασφαλίζεται με χρήση εφαρμογών όπως προγράμματαantivirus και εργαλεία firewalls στα τερματικά, καθώς και Συστήματα Ελέγχου Εισβολής (IntrusionDetectionSystems) και firewalls στα συστήματα-εξυπηρετητές(servers).

Παράλληλα επιβάλλεται η χρήση διαδικασιών πλεονασμού (redundancy), ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hotswapping, τεχνικές clustering και loadbalancing για συστοιχίες εξυπηρετητών(servers), αποθηκευτικές μονάδεςDLT) στους servers ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμούδιαμεταγωγής)

καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται.

Ένα συμπληρωματικό μέτρο για τη βελτίωση της διαθεσιμότητας του συστήματος θα ήταν και η παράταση της περιόδου υποβολής ηλεκτρονικών ψήφων, πλέον της μιασημέρας (αρκεί βεβαίως οι ηλεκτρονικές ψήφοι να καταμετρούνται ταυτόχρονα με τις φυσικές, προκειμένου να διατηρηθεί η νομιμότητα των εκλογών).

Νομικά Θέματα

Πέρα από την ολοκλήρωση της θεσμοθέτησης για τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, όπου ήδη έχουν γίνει σημαντικάβήματα, απαραίτητη προϋπόθεση αποτελεί και η ύπαρξη νομολογίας που θα κατοχυρώνει τη **μυστικότητα της ηλεκτρονικής ψήφου** και θα προβλέπει:

Επιθέσεις όπως καταναγκασμός του ψηφοφόρου, ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λπ.

Οι κυριότεροι παράγοντες που αποτρέπουν σήμερα την υιοθέτηση συστημάτων "εξ αποστάσεως" διαδικτυακής ψηφοφορίας είναι:

- Μη ασφαλή συστήματα υπολογιστών
- Έλλειψη Υποδομών ΔημοσίουΚλειδιού
- ΈλλειψηΠροτύπων (Standards)

Η ασφάλεια διεξαγωγής διαδικτυακής ψηφοφορίας εξασφαλίζεται με κρυπτογραφικά μοντέλα ασφάλειας.

Κρυπτογράφηση

Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ.) να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα.

Ορισμοί

Κρυπτογράφηση (encryption)

Ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Αποκρυπτογράφηση (decryption)

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα.

Κρυπτογραφικός αλγόριθμος (cipher)

Είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (plaintext)

Είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (key)

Είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (ciphertext)

Είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

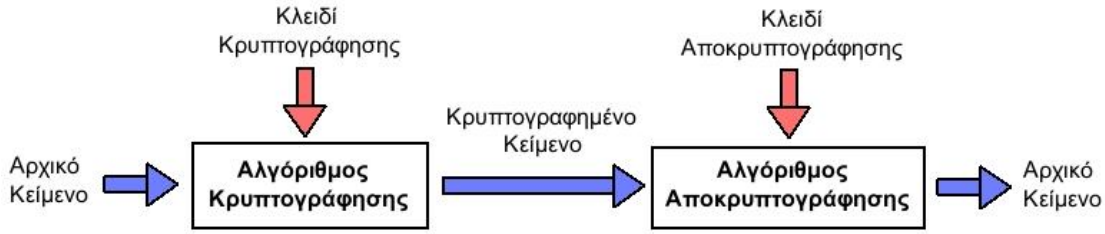
Γενικά

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

Ο αντικειμενικός στόχος της κρυπτογραφίας

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να



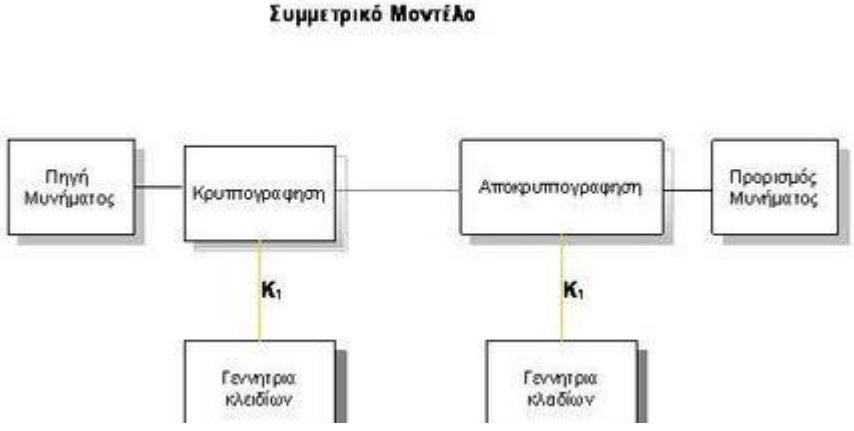
παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Είδη Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα**Συμμετρικά κρυπτοσυστήματα**και **Ασύμμετρα κρυπτοσυστήματα.**

Συμμετρικό κρυπτοσύστημα

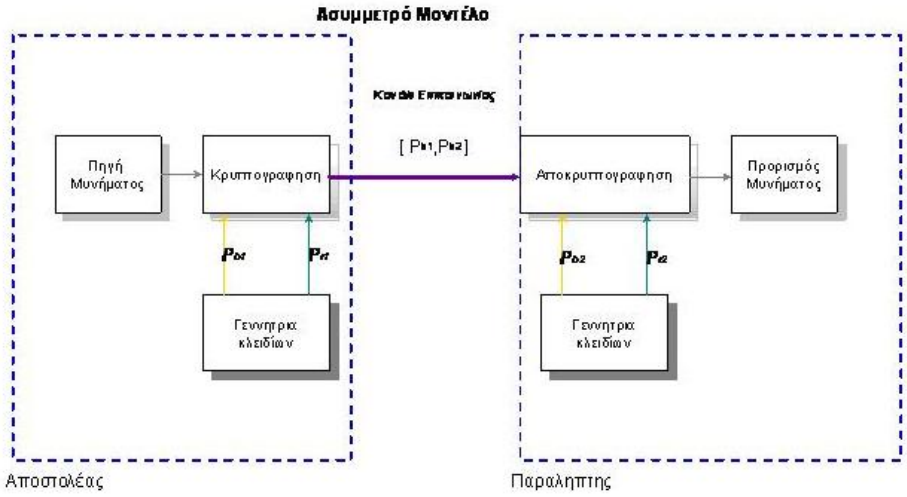
είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά



κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού

(Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο.Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (PublicKeyInfrastructure) και στα Ψηφιακά πιστοποιητικά.



Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" σ το δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής *(non-repudiation)*. Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς *(CertificateAuthority)* ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

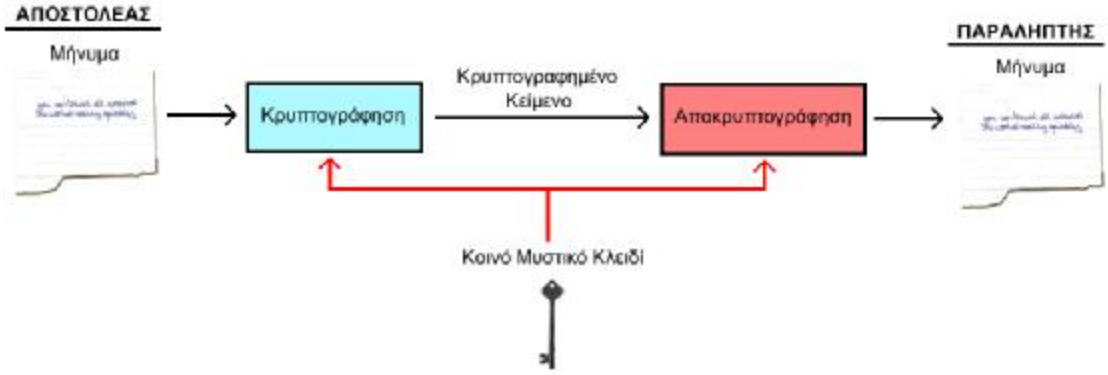
Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι (θα αναλυθούν παρακάτω).

Κρυπτογράφηση συμμετρικού κλειδιού

Η **κρυπτογράφηση συμμετρικού κλειδιού (SymmetricCryptography)** βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί:

Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού



Κρυπτογράφηση δημοσίου κλειδιού

Η **κρυπτογράφηση δημοσίου κλειδιού (PublicKeyCryptography) ή ασύμμετρου κλειδιού (AsymmetricCryptography)** επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους WhitfieldDiffie και MartinHellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφησησυμμετρικού κλειδιού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

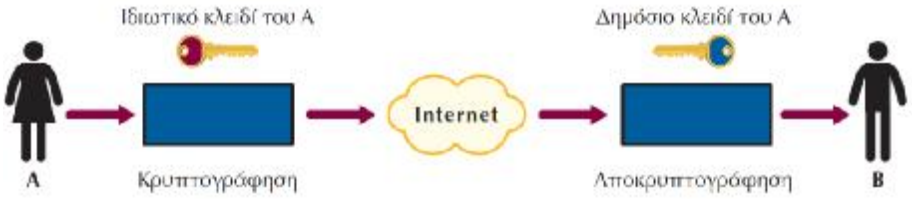
Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (privatekey) και το άλλο δημόσιο κλειδί (publickey). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (publickeyservers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

Δημιουργία κλειδιών

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.



Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού

Πιστοποιητικά

Τα πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν την σχέση μεταξύ μίας δημόσια κλείδας και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι μία συγκεκριμένη δημόσια κλείδα ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικης κλείδας.

Παράδειγμα χρήσης του Πιστοποιητικού

Ας υποθέσουμε ότι ο Α χρειάζεται την δημόσια κλείδα του Β για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον Β να του στείλει την δημόσια κλείδα του μπορεί να θέσει την όλη επικοινωνία σε ρίσκο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης της δημόσιας κλείδα του Β με την δημόσια κλείδα κάποιου άλλου (επίθεση man-in-the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικός με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας μία ψεύτικη δημόσια κλείδα. Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί την δημόσια κλείδα που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

΄Ενα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

1) το όνομα του κατόχου

2) το όνομα της του εκδοτικού οργανισμού – CA (βλέπε παρακάτω),

3) την δημόσια κλείδα του ονόματος που αναγράφεται στο πιστοποιητικό,

4) την ημερομηνία λήξης του πιστοποιητικού,

5) ένα σειριακό αριθμό (serialnumber),

6) την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

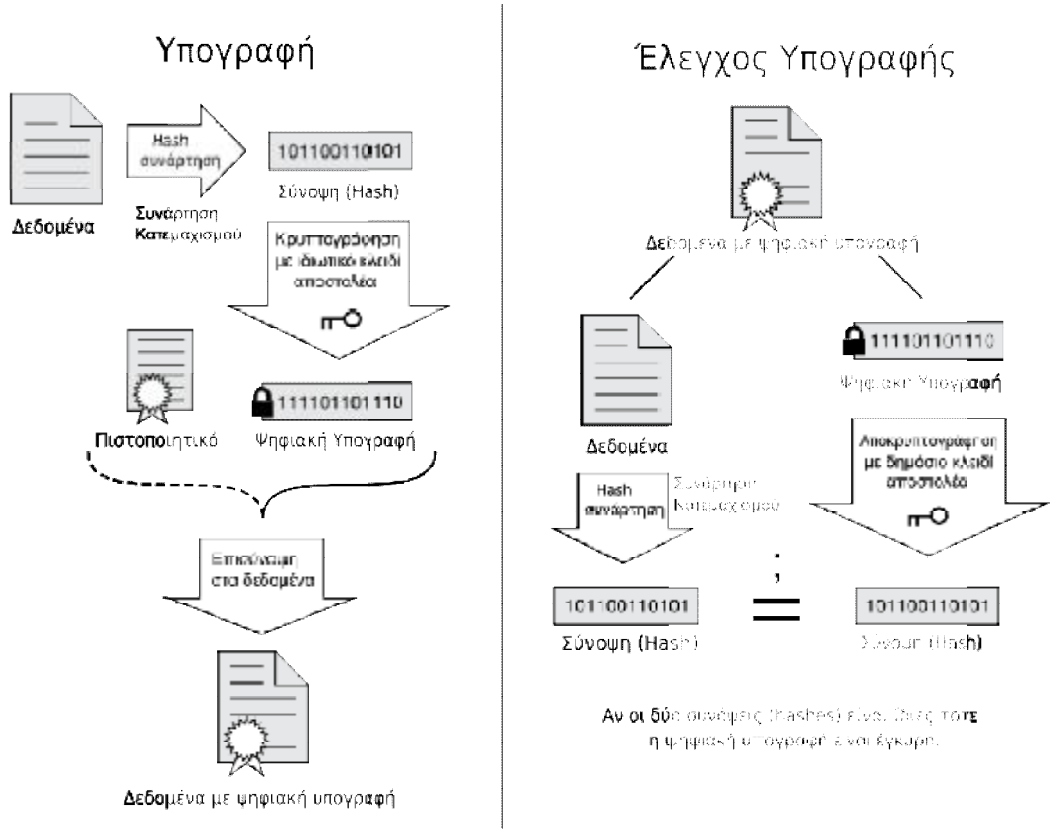
7) Ένα τυπικό παράδειγμα πιστοποιητικού φαίνεται παρακάτω:

8) Η τυποποιημένη μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X.509.

Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει την σωστή δημόσια κλείδα του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση της δημόσιας κλείδας κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι η σύνοψη του μηνύματος η οποία προσκολλάται στο τέλος του ηλεκτρονικού εγγράφου χρησιμοποιώντας ασυμμετρική κρυπτογραφία (ακεραιότητα εγγράφου και απόδειξη ταυτότητας αποστολέα).Οι αλγόριθμοι κατατεμαχισμού δέχονται συνήθως ως είσοδο μηνύματα τυχαίου μεγέθους και παράγουν συνόψεις μηνύματος συγκεκριμένου μήκους. Διαδεδομένοιαλγόριθμοικατατεμαχισμού: Message Digest 4 (MD4), Message Digest 5 (MD5), Secure Hash Algorithm (SHA)



Διάγραμμα χρήσης ψηφιακής υπογραφής.

Παράδειγμα Χρήσης της Ψηφιακής Υπογραφής

Αρχικά πρέπει τα δύο μέρη της επικοινωνίας (π.χ. ο Bob και η Alice) να έχουν συμφωνήσει σε κάποιο αλγόριθμο δημοσίου κλειδιού (ασυμμετρικής κρυπτογράφησης, π.χ. PGP, DigitalSignature Standard κλπ) και κάποιο αλγόριθμο κατατεμαχισμού (π.χ. MD5).

Και τα δύο μέρη πρέπει να έχουν ζευγάρια δημοσίων και ιδιωτικών κλειδιών σύμφωνα με τον αλγόριθμο που επέλεξαν προηγουμένως. Θα πρέπει να ανταλλάξουν μεταξύ τους τα δημόσια κλειδιά τους.

Ας υποθέσουμε ότι η Alice θέλει να στείλει στον Bob ένα υπογεγραμμένο μήνυμα. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού ο οποίος θα παράγει μια σύνοψη (digest).

Θα κρυπτογραφήσει τη σύνοψη με το ιδιωτικό της κλειδί, και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου. Θα αποστείλει στον Bob το τελικό αυτό έγγραφο.

Ο Bob θα εξάγει τη κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα την αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της Alice. Εφόσον η αποκρυπτογράφηση γίνει σωστά, γνωρίζουμε ότι η σύνοψη δεν έχει αλλοιωθεί. Έπειτα, θα πάρει το μήνυμα, θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα συγκρίνει τη σύνοψη που υπολόγισε ο ίδιος με τη σύνοψη που έλαβε από την Alice. Αν οι συνόψεις είναι ίδιες τότε γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί.

Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας

Η ασφάλεια των συστημάτων ψηφοφορίας βασίζεται κυρίως στην υλοποίηση κρυπτογραφικών μοντέλων ασφάλειας. Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι:

- Το μοντέλοMIX-net
- Το μοντέλο των «τυφλών» υπογραφών
- Το μοντέλο του Benaloh
- Το ομομορφικό μοντέλοκρυπτογράφησης

Το μοντέλο MIX-net

Ο D. Chaum (1981) εισήγαγε την έννοια των δικτύων MIX-net (MIX networks), τα οποία αποτελούν έναν κρυπτογραφικό μηχανισμό για την κατασκευή ανώνυμων καναλιών (AnonymousChannels) σε εφαρμογές υψηλής ασφάλειας. Ένα δίκτυο MIX-net αποτελείται από εξυπηρετητές που συνδέονται μεταξύ τους, τους ονομαζόμενους κόμβουςMIX. 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 τέτοιον τρόπο ώστε τα μηνύματα της εξόδου να μην μπορούν να συνδεθούν με τα μηνύματα της εισόδου. Έτσι, καμία συνέργεια οποιουδήποτε αριθμού κόμβων MIX (εκτός από τη συνέργεια όλων των κόμβων) δεν μπορεί να αποφανθεί ποια ψήφος αντιστοιχεί σε ποιον ψηφοφόρο. Στην ηλεκτρονική ψηφοφορία κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη από αυτή 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 καθεμία και αναδιατάσσοντας τη λίστα με τις ψήφους που προκύπτει) και στη συνέχεια την προωθεί στον επόμενο κόμβο. Αυτό το μοντέλο καλείται MIX-net αποκρυπτογράφησης. Σε ένα παραπλήσιο μοντέλο, σε κάθε κόμβο MIX λαμβάνει χώρα μόνον ο μετασχηματισμός των ψήφων, και στη συνέχεια όλοι οι κόμβοισυνεργάζονται για την αποκρυπτογράφηση της τελικής λίστας των ψήφων (Hirt, 2000). 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 ανθεκτικότητά τους έναντι συνεργειών μεταξύ (έως) ενός ορισμένου αριθμού MIX. Γι' αυτούς τους λόγους, τα δίκτυα MIX-net έχουν χρησιμοποιηθεί κατά καιρούς με στόχο την επίτευξη ανωνυμίας σε εφαρμογές ηλεκτρονικού εμπορίου. Έως σήμερα πάντως, κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν έχει υλοποιηθεί με χρήση τεχνικών MIX-net.

Το μοντέλο των «τυφλών» υπογραφών

Η έννοια της «τυφλής» υπογραφής (BlindSignature) παρουσιάστηκε αρχικά ως μια κρυπτογραφική μέθοδος, για την υπογραφή ενός μηνύματος χωρίς τη γνώση του ίδιου του μηνύματος. Θα μπορούσε, χρησιμοποιώντας ένα παράδειγμα από

την καθημερινή ζωή, να αντιστοιχιστεί με την υπογραφή (εξωτερικά) ενός σφραγισμένου φακέλου, που θα περιέχει ένα χαρτί τοποθετημένο κάτω από ένα καρμπόν. Όταν ο φάκελος αργότερα θα ανοιχτεί από τον νόμιμο παραλήπτη, τότε το χαρτί θα έχει αποτυπωμένη την υπογραφή. Αυτή η μέθοδος, αν και υιοθετήθηκε αρχικά σε εφαρμογές ηλεκτρονικού χρήματος (e-Cash), χρησιμοποιήθηκε επίσης για την επίλυση του προβλήματος της επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητάς τους (Fujioka κ.ά., 1993). Έως σήμερα έχουν υλοποιηθεί αρκετά τέτοια συστήματα σε εκλογές μικρής κλίμακας (όπως το SENSUS και το e-EVOX). Πλεονεκτήματα του μοντέλου των «τυφλών» υπογραφών είναι ο χαμηλός επικοινωνιακός φόρτος και το χαμηλό υπολογιστικό κόστος, ακόμα και όταν ο αριθμός των ψηφοφόρων/υποψηφίων είναι μεγάλος (Scalability). Επιπλέον, η μυστικότητα των ψήφων επαφίεται στους ψηφοφόρους, στοιχείο που ευνοεί την εύκολη και ασφαλή διαχείριση του συστήματος από την (συνήθως μια) Αρχή. Ένα σημαντικό μειονέκτημα των συστημάτων «τυφλής» υπογραφής είναι ότι απαιτούν από τον ψηφοφόρο να είναι ενεργός (Online) σε όλα τα στάδια της ψηφοφορίας. Επίσης, προσφέρουν μόνο ατομική επαληθευσιμότητα, δηλαδή οι ψηφοφόροι μπορούν να εντοπίζουν και να διορθώνουν τα λάθη που αφορούν μόνο τη δική τους ψήφο.

Το Μοντέλο του Benaloh

Το μοντέλο αυτό χρησιμοποιεί ένα σχήμαομομορφικούδιαμοιρασμού μυστικών[3] (homomorphicsecretsharing). Σε τέτοια ομομορφικάσχήματα υπάρχει μια πράξη⊕ορισμένη στο σύνολο των μεριδίων, τέτοια ώστε το «άθροισμα» των μεριδίων οποιονδήποτε δυο μυστικώνx1,x2να ισούται με ένα μερίδιο του «αθροίσματος» x1 ⊕ x2. ΣτοσχήματουBenalohκάθεψηφοφόροςδιαμοιράζειτηψήφοτου σε Αρχές, χρησιμοποιώντας ένα (t,n) thresholdσχήμαδιαμοιρασμού 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 οικουμενικάεπαληθεύσιμα. 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.

Το ομομορφικό μοντέλο κρυπτογράφησης

Το μοντέλο αυτό (Cramer κ.ά., 1997) χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγόριθμων κρυπτογράφησης, για να εδραιώσει την οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων. Κατ' αυτόν τον τρόπο, η ταυτότητα του ψηφοφόρου δεν χρειάζεται να προστατευτεί με τεχνικές ανωνυμίας, αφού καμία

[3] Ένα σχήμα Διαμοιρασμού Μυστικού επιτρέπει την κατάτμηση ενός μυστικού σε μερίδια (shares), τα οποία δίδονται σε ένα σύνολο n οντοτήτων, ούτως ώστε η συνεργασία και των n οντοτήτων να είναι απαραίτητη για την ανάκτηση του μυστικού. Σε ένα (t,n) thresholdσχήμα Διαμοιρασμού Μυστικού, η ανάκτηση του μυστικού είναι εφικτή εφόσον συνεργαστεί μιαομάδα από τουλάχιστον t οντότητες, όπου t≤n.

ψήφος δεν αποκρυπτογραφείται μεμονωμένα, αλλά όλες συνδυάζονται και το τελικό κρυπτογράφημα αποκρυπτογραφείται από τις Αρχές του συστήματος. Το σύστημα VoteHere, το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί υλοποίηση του ομομορφικού μοντέλου κρυπτογράφησης. Ένα μειονέκτημα των συστημάτων που βασίζονται στο ομομορφικό μοντέλο είναι η περιορισμένη ευκαμψία τους (Flexibility), καθώς οι ψήφοι περιορίζονται συνήθως σε δίτιμες ψήφους του τύπου «Ναι»/«Όχι» (π.χ. {+1, -1}). Όσον αφορά μεγάλο αριθμό υποψηφίων, οι υλοποιήσεις του μοντέλου συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Ωστόσο, έχουν προταθεί εναλλακτικά κρυπτογραφικά σχήματα, των οποίων η υπολογιστική πολυπλοκότητα είναι είτε γραμμική (Linear) είτε λογαριθμική (Logarithmic) ως προς τον αριθμό των υποψηφίων (Damgard κ.ά., 2003).

Βασικά Κρυπτογραφικά Εργαλεία

Στη συνέχεια παρουσιάζονται τα βασικά εργαλεία που χρησιμοποιούνται από τα περισσότερα κρυπτογραφικά πρωτόκολλα ηλεκτρονικής ψηφοφορίας.

Πίνακες Ανακοινώσεων (BulletinBoards)

Πρόκειται για κανάλια δημόσιαςεκπομπής (publicbroadcastchannels) που επιτρέπουν στους χρήστες (π.χ. ψηφοφόροι) να επικοινωνούν μ ε 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 κατανεμημένοσύστημαRampart.

Ανώνυμα Κανάλια Επικοινωνίας (AnonymousChannels)

Τα κανάλια αυτά εξασφαλίζουν την ανωνυμία των χρηστών του συστήματος. Εκτός από τα δίκτυα MIX-net, υπάρχουν και τα συστήματαανωνυμίας με τη χρήση διαμεσολαβητή (proxysystems), όπως επίσης και τα υβριδικά συστήματα (hybridsystems) ανωνυμίας.

Κρυπτογραφίατύπου Threshold (threshold cryptography). Τα συστήματα κρυπτογράφησης τύπου thresholdκατανέμουν τη λειτουργικότητα των κρυπτογραφικών πρωτοκόλλων ώστε να επιτύχουν ανθεκτικότητα (robustness). Για παράδειγμα, σε μια ψηφοφορία η διαδικασία της καταμέτρησης μπορεί να κατανεμηθεί μεταξύηΑρχών Ψηφοφορίας, με τη χρήση ενός (t,n) threshold κρυπτογραφικού συστήματοςδημοσίου κλειδιού (π.χ. thresholdElGamal). Σε αυτήν την περίπτωση υπάρχει μόνον ένα δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί διαμοιράζεται στιςη 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 μ ε τη συνεργασία τουλάχιστον t Αρχών. Η μυστικότητα της ψήφου και η ακρίβεια των αποτελεσμάτων εξασφαλίζεται εφόσον δεν υπάρχουν περισσότερες από t-1 κακόβουλες ή απλά δυσλειτουργικές Αρχές. Ο αριθμόςt αποτελεί τη τιμήthreshold του κρυπτογραφικού συστήματος. Τα συστήματαthreshold μπορούν να ενισχυθούν, για προστασία από επιθέσεις υποκλοπής κλειδιού (keyconfiscation), με μηχανισμούς όπως προ-ενεργή ασφάλεια[4] (proactivesecurity) καθώς και με τεχνικές ισχυρής χρονικής ασφάλειας (strongforwardsecurity).

Αποδείξεις με Μηδενική Γνώση (ZeroKnowledgeProofs)

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

[4]Στα κατανεμημένασυστήματα με προενεργή ασφάλεια, οι Αρχές ανανεώνουν περιοδικά τα μερίδια τους κατά τρόπο ώστε η γνώση της τιμής ενός μεριδίου να μη μπορεί να οδηγήσει στην γνώση της τιμής που θα έχει το μερίδιο μετά την ανανέωση. Η τεχνική αυτή αυξάνει την ασφάλεια των συστημάτων τύπου threshold έναντι επιθέσεων όπου ο επιτιθέμενος κατορθώνει να ανακτήσει έναν αριθμό μυστικών μεριδίων που είναι μικρότερος από την τιμήthreshold του κρυπτογραφικού συστήματος.

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 χρησιμοποιούνταιπροκειμένου να αποδειχθεί η ορθότητα των μετασχηματισμών στα συστήματα ψηφοφορίας που χρησιμοποιούν δίκτυα MIX-net για την ανωνυμία των ψήφων (π.χ. για να αποδειχτεί η εγκυρότητα των κρυπτογραφημένων ψήφων στις ομομορφικές εκλογές (π.χ. για την ορθότητα των κρυπτογραφήσεων στα πρωτόκολλα προστασίας από καταναγκασμό, καθώς και για την ορθότητα των επικυρωμένων ψήφωνστα 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, επομένωςοικουμενικάεπαληθεύσιμες, με την ευριστική προσέγγιση των Fiat-Shamir. Στην περίπτωση αυτή η ασφάλεια βασίζεται στο μοντέλορandomoracle[5]

[5]Το μοντέλοrandomoracle είναι ένα τυπικό μοντέλο απόδειξης ασφάλειας στο οποίο οι συναρτήσεις κατακερματισμού (hashfunctions) αντιμετωπίζονται ως συναρτήσεις τυχαιότητας.

Εφαρμογή Ηλεκτρονικής ψηφοφορίας διεθνώς

Η εμπειρία της Αυστραλίας

Ενώ εκείνη που ήταν ενάντια της ηλεκτρονικής ψηφοφορίας στις Ηνωμένες Πολιτείες ανησυχούσαν όλο και περισσότερο κάθε ημέρα για την ανασφάλεια των μηχανημάτων ηλεκτρονικής ψηφοφορίας. Αντίθετα οι Αυστραλοί σχεδίασαν πριν από δύο χρόνια ένα σύστημα που χαλάρωσε τις περισσότερες αυτές τις ανησυχίες. Επέλεξαν να κάνουν το λογισμικό λειτουργίας του συστήματός τους εντελώς ανοιχτό στο δημόσιοκοινό. Παρά το γεγονός ότι μια ιδιωτική αυστραλιανή εταιρεία σχεδίασε το σύστημα, ήταν με βάση τις προδιαγραφές που καθορίστηκαν από ανεξάρτητους υπαλλήλους των εκλογών, που τοποθέτησαν τον κώδικα στο Internet για να τον δουν και να τον αξιολογήσουν όλοι. Θα πέραρναγε από μια δοκιμαστική λειτουργία σε κρατικές εκλογές το 2001. Οι επικριτές λένε ότι η αναπτυξιακή διαδικασία αποτελεί ένα υπόδειγμα για το πώς τα μηχανήματα ηλεκτρονικής ψηφοφορίας θα πρέπει να γίνουν στις Ηνωμένες Πολιτείες.Ονομάζεται eVACS, ή Σύστημα Ηλεκτρονικής Ψηφοφορίας και Καταμέτρησης, το σύστημα δημιουργήθηκε από μια εταιρεία που ονομάζεται Software Improvements για να τρέχει σε Linux, ένα opensource λειτουργικό σύστημα διαθέσιμο στο Διαδίκτυο.

Οι υπάλληλοι των εκλογών στο Australian Capital Territory, ένα από τα οκτώ κράτη και τα εδάφη της χώρας, στράφηκε στην ηλεκτρονική ψηφοφορία για τον ίδιο λόγο, που και οι Ηνωμένες Πολιτείες έκαναν στις εκλογές το 1998 σημειώθηκαν λάθη στο σύστημα καταμέτρησης με το χέρι. Δύο υποψήφιοι είχαν διαχωριστεί από μόνο τρεις ή τέσσερις ψήφους, δήλωσε ο PhillipGreen, ο Εκλογικός Επίτροπος των εκλογών. Μετά το μέτρημα ξανά, οι υπάλληλοι ανακάλυψαν ότι από τα 80000 ψηφοδέλτια, είχαν γίνει περίπου 100 λάθη. Αποφάσισαν να εξετάζουν άλλες μεθόδους ψηφοφορίας.

Το 1999, η Αυστραλιανή Εκλογική Επιτροπή προέβη σε δημόσια πρόσκληση για την ηλεκτρονική ψηφοφορία για να δούνε αν μια ηλεκτρονική επιλογή ήταν βιώσιμη. Πάνω από 15 προτάσεις ήρθαν, αλλά μόνο μία προσέφερε μια open-source λύση. Δύο εταιρείες πρότειναν το σχέδιο σε σύμπραξη μετά από εκτενείς διαβουλεύσεις με ακαδημαϊκούς στο Εθνικό Πανεπιστήμιο της Αυστραλίας. Όμως, μία από τις εταιρείες αργότερα εγκατέλειψε το σχέδιο, αφήνοντας την Software Improvements στην οικοδόμηση του συστήματος. Ο Green είπε ότιτο open-source ήταν μια προφανής επιλογή. "Παρακολουθούσαμε τι είχε συμβεί στην Αμερική (το 2000), και ήμασταν επιφυλακτικοί με τη χρήση του ιδιόκτητου λογισμικού που κανείς δεν επιτρέπεται να δει», είπε. "Ήμασταν πολύ επίμονοι για την όλη διαδικασία να είναι διαφανής, ούτως ώστε ο καθένας και ιδιαίτερα τα πολιτικά κόμματα, οι υποψήφιοι, αλλά και ολόκληρος ο κόσμος να πεισθεί ότι το λογισμικό πράγματι κάνει ότι έμελλε να κάνει. "Πήρε άλλον ένα χρόνο για τις αλλαγές στον αυστραλιανό νόμο ώστε να επιτρέψουν την ηλεκτρονική ψηφοφορία να πάει μπροστά. Στη συνέχεια, τον Απρίλιο του 2001, η Software Improvements υπέγραψε σύμβαση για την κατασκευή του συστήματος για τις κρατικές εκλογές τον Οκτώβριο. Η MattQuinn, η επικεφαλής μηχανικός της εταιρείας, δήλωσε ότι η Επιτροπή κάλεσε όλα τα πλάνα. "Πρόκειται, όπως τον πελάτη, που υπαγορεύει τις απαιτήσεις ασφάλειας συμπεριλαμβανομένης και της λειτουργικότητας, (και αυτοί) έχουν εμπλακεί σε κάθε βήμα της διαδικασίας ανάπτυξης, από τις απαιτήσεις μέχρι την δοκιμή," είπε η Quinn. "Ενέκριναν κάθε έγγραφο που παράγαμε." Η Επιτροπή ενέγραψε σχέδια, καθώς και τον τελικό κώδικα λογισμικού για το Internet για να τον επανεξετάσει το κοινό. Η αντίδραση ήταν πολύ θετική. "Το γεγονός ότι ο πηγαίος κώδικας είχε δημοσιευθεί πραγματικά προκάλεσε την κριτική," είπεηQuinn. Λίγα άτομα κατέγραψαν σφάλματα στην έκθεση, συμπεριλαμβανομένου ενός ακαδημαϊκού στο Αυστραλιανό Εθνικό Πανεπιστήμιο

που βρήκε το πιο σοβαρό πρόβλημα.«Δεν ήταν ένα λειτουργικόή ένα θέμα ασφαλείας, αλλά ήταν λάθος, που ήμασταν ευτυχείς που είχε επισημανθεί για εμάς", είπε ηQuinn.

Το παράδειγμα της Ελβετίας

Η Γενεύη είναι ένα από τα λίγα κράτη σε όλο τον κόσμο που ασχολούνται με τη ψηφοφορία μέσω Internet και την οργάνωση επίσημων on-line ψηφοφοριών σε τακτική βάση. Για πρώτη φορά οργανώθηκε τον Ιανουάριο του 2003.

Το έργο του e-voting γεννήθηκε το έτος 2000, όταν άρχισε στη Γενεύη το θέμα της ηλεκτρονικής διακυβέρνησης. Το ίδιο έτος, το ομοσπονδιακό κοινοβούλιο κάλεσε την κεντρική κυβέρνηση να μελετήσει την εφαρμογή των ΤΠΕ στη θεσμική ζωή και στη δημοκρατική διαδικασία.

Το έργο αναπτύχθηκε στη Γενεύη με τρόπο, που εγκρίθηκε από τη συνομοσπονδία, ώστε να επωφελούνται και τα δύο μέρη. Η Γενεύη υποστηρίζεται οικονομικά από τη συνομοσπονδία και επωφελείται από τηντεχνογνωσία και μέσω διαβουλεύσεων επιθυμεί να απαλλαγεί από την εποπτεία της Ομοσπονδιακής Επιτροπής, ενώ η οργάνωση και η ομοσπονδιακή επιτροπή επωφελούνται από τις νέες εξελίξεις που λαμβάνουν χώρα στη Γενεύη.

Η ψηφοφορία μέσω Internet είναι μια μέθοδος ψηφοφορίας δύο φάσεων: είναι τόσο ένας απομακρυσμένος τρόπος ψηφοφορίας όσο και μια ηλεκτρονική ψηφοφορία με κατακερματισμένη διαδικασία. Η απομακρυσμένη ψήφος έχει εφαρμοστεί ήδη από το 1995 και είναι ο πρώτος τρόπος ψηφοφορίας: το 95% των ψηφοδελτίων είναι μέσω ταχυδρομείου και η προσέλευση αυξήθηκε κατά 20 εκατοστιαίες μονάδες από την εισαγωγή της ταχυδρομικής ψήφου. Η ηλεκτρονική πλευρά της ψηφοφορίας μέσω Internet είναι ένα αποτέλεσμα των μηχανημάτων ψηφοφορίας που είναι ευρέως διαδεδομένα στην Ευρώπη.

Σε αντίθεση με τις μηχανές ψηφοφορίας, ωστόσο, και ιδιαίτερα σε αντίθεση με τα μηχανήματα που δεν είναι συνδεδεμένα με ένα δίκτυο, αλλά εργάζονται offline, η εφαρμογή της ηλεκτρονικής ψηφοφορίας στη Γενεύη δεν μπορεί να προσεγγιστεί ούτε σωματικά ούτε λογικά σε χρονικά διαστήματα κατά τη διάρκεια της ψηφοφορίας. Το κλείδωμα και άνοιγμα του κουτιού eBallot λαμβάνει χώρα με την παρουσία των ελεγκτών που διορίζονται από τα πολιτικά κόμματα και ενεργούν όπως μία εκλογική επιτροπή.

Θα μπορούσε να μας εκπλήσσει το γεγονός ότι σε μια χώρα όπου οι πολίτες σε ορισμένα σημεία ακόμα ψηφίζουν στην κεντρική πλατεία της πόλης με ανάταση των χεριών τους αναπτύσσεται μια εφαρμογή ψηφοφορίας μέσω Internet. Ωστόσο, υπάρχουν μια σειρά λόγοι για την υποστήριξη αυτού του έργου:

*Οι Ελβετοί πολίτες ψήφιζαν τέσσερις έως πέντε φορές το χρόνο, μερικές φορές περισσότερο. Άνεση είναι μια λέξη-κλειδί της διαδικασίας της ψηφοφορίας. * Τα λεγόμενα συστήματα "άμεσης δημοκρατίας" είναι κατάλληλα για την ψηφοφορία στο Internet, όχι μόνο επειδή υποστηρίζουν πολλές ψηφοφορίες,αλλά και για τις πολλές αρμοδιότητες που αναλαμβάνουν οι πολίτες και την αντιπροσωπεία της περιορισμένης κυριαρχίας που δόθηκε στην βουλευτές. * Σύμφωνα με την Ομοσπονδιακή Υπηρεσία για τις στατιστικές, το 65% του ελβετικού πληθυσμού είναι συνδεδεμένο στο Internet, είτε από το σπίτι ή το χώρο εργασίας. Ένας στους τρεις Ελβετούς κάνει πλοήγηση στο Διαδίκτυο σε καθημερινή βάση. * 580,000 Ελβετοί πολίτες (περίπου ένας στους δέκα) ζουν στο εξωτερικό. Πρέπει να τους παρέχουν ένα απλό και αποτελεσματικό σύστημα ψηφοφορίας. Το ίδιο ισχύει και για τα άτομα με αναπηρία που ζουν στην Ελβετία. * Η δημόσια υπηρεσία οφείλει να προσαρμοστεί στο νέο τρόπο ζωής και πρέπει να είναι όπου είναι οι άνθρωποι, συμπεριλαμβανομένου και του διαδικτύου.

Η ηλεκτρονική ψηφοφορία δεν θα αντικαταστήσει τους σημερινούς τρόπους ψηφοφορίας, τις ταχυδρομικές υπηρεσίες, τα δικαιώματα ψήφου και το εκλογικό κέντρο, θα είναι μια τρίτη δυνατότητα που δίνεται στους πολίτες.

Ο ρυθμός των τεχνολογικών εξελίξεων και οι αλλαγές που αυτό συνεπάγεται στην καθημερινή μας ζωή επιβάλλει ότι οι δημόσιες υπηρεσίες μένουν μπροστά από τις επικείμενες προσδοκίες των ανθρώπων. Αναμένοντας την "κατάλληλη στιγμή" για να επιβιβαστεί στο τρένο των νέων τεχνολογιών, θα περιμένουν πάρα πολύ καιρό. Πρέπει να προλάβουμε τις προσδοκίες του πληθυσμού, πρέπει ήδη να εργαστούμε πάνω στις νέες μορφές σχέσεων κράτους-πολίτη. Είναι αυτό που επέλεξε να κάνει η Γενεύη, με τη στήριξη της Συνομοσπονδίας.

Το παράδειγμα της Εσθονίας

Η Εσθονία είναι η πρώτη χώρα στην οποία οι πολίτες είχαν τη δυνατότητα να ψηφίσουν μέσω του διαδικτύου για τις εθνικές εκλογές πουπραγματοποιήθηκαν στις 4 Μαρτίου 2007. Ο ψηφοφόρος που επιθυμούσε να ψηφίσει μέσω διαδικτύου προμηθευόταν μια ειδική κάρτα και ένα PIN, και με αυτά μπορούσε να ψηφίσει σε διάστημα τριών ημερών πριν από την τελική μέρα των εκλογών. Την ημέρα των εκλογών η «ηλεκτρονική κάλπη» έκλεινε και οι πολίτες μπορούσαν να ψηφίσουν μόνο ρίχνοντας την ψήφο τους στα εκλογικά κέντρα με τον καθιερωμένο τρόπο. Οι πολίτες που χρησιμοποίησαν το εν λόγω σύστημα και ψήφισαν μέσω διαδικτύου ήταν μόλις 9.500 (μικρότερο από το 1% του εκλογικού σώματος), άλλα οι υπεύθυνοι του πληροφοριακού συστήματος της ηλεκτρονικής ψηφοφορίας εκτιμούν πως ο αριθμός αυτός θα αυξηθεί κατά πολύ σε μελλοντικές εκλογικές αναμετρήσεις. Το σύστημα ψηφοφορίας της Εσθονίας, για να εξασφαλίσει περισσότερη ασφάλεια, ήταν σχεδιασμένο με τέτοιο τρόπο, ώστε ο χρήστης να έχει τη δυνατότητα ν' ακυρώσει την ψήφο του και να ξαναψηφίσει.

Η εμπειρία της Αμερικής

Όσοι από εμάς έχουν χρησιμοποιήσει μία τραπεζική ATM δεν μπορούν παρά να δεχθούν ότι η οθόνη αφής είναι εξυπηρετική: διαβάζουμε τις προβαλλόμενες στην οθόνη επιλογές, διαλέγουμε την επιθυμητή, τη δείχνουμε αγγίζοντάς την και... το «σουσάμι ανοίγει», εφόσον βεβαίως έχει αναγνωρίσει την ταυτότητά μας μέσω μιας μαγνητικής κάρτας με κωδικό. Εντελώς αντίστοιχη είναι και η διαδικασία ψήφισης που θα ακολουθήσουν 50 εκατομμύρια Αμερικανοί στις 2 Νοεμβρίου, στα εκλογικά κέντρα που έχουν προικισθεί με αυτή τη νέα τεχνολογία. Η κύρια διαφορά με τις γνωστές μας ATM είναι ότι η μαγνητική κάρτα παραδίδεται στον αντίστοιχο ψηφοφόρο μόνο όταν είναι η σειρά του να ψηφίσει και μπορεί να χρησιμοποιηθεί μόνο μία φορά. Τα πλεονεκτήματα είναι εξίσου προφανή: η ουρά κινείται ταχύτερα από ό,τι όταν έχουμε να παραλάβουμε ένα πακέτο ψηφοδέλτια και... τα «σημαδεμένα χαρτιά» ή τα «κρυπτογραφημένα μηνύματα προς κομματάρχες» αποκλείονται. Λογικά λοιπόν αυτός ο νέος τρόπος ψηφοφορίας δεν έχει παρά να επεκταθεί και να κυριαρχήσει παντού τα επόμενα χρόνια. Έχει ήδη δοκιμαστεί σε τοπικές εκλογές στη Βρετανία και στην Αυστραλία, σε δημοψηφίσματα στην Ελβετία και στη Βενεζουέλα ή και σε πανεθνική κλίμακα κατά τις τελευταίες εκλογές της Ινδίας. Τα μηχανήματα και η τεχνολογία τους ποικίλλουν. Στην Ινδία προτίμησαν φθηνές συσκευές με πλήκτρα, καθώς έπρεπε να καλύψουν ένα εκλογικό πολυάριθμο σώμα. Στην Αυστραλία πρωτοπόρησαν στη «διαφάνεια»: το λογισμικό των συσκευών ήταν ανοιχτό στο κοινό και αναπτύχθηκε με τηλεσυνεργασία μέσω Διαδικτύου. Έτσι όλοι οι πολίτες είχαν τη δυνατότητα να γνωρίζουν πώς ακριβώς δουλεύουν οι συσκευές, οπότε και η αξιοπιστία τους ήταν η μέγιστη δυνατή. Στην Ελβετία όπου η άμεση δημοκρατία λατρεύεται σχεδόν όσο και στην Αρχαία Αθήναέφθασαν στο σημείο να δεχθούν ως

νόμιμη την ψηφοφορία μέσω Internet! Η πρώτη φορά ήταν τον Ιανουάριο του 2003, όταν σε ένα προάστιο της Γενεύης οι δημότες ψήφισαν για το αν θα χρηματοδοτούσαν την... αναπαλαίωση ενός εστιατορίου. Το σχετικό λογισμικό αναπτύχθηκε από τις τοπικές αρχές σε συνεργασία με δύο ιδιωτικές εταιρείες. Εφέτος, στις 26 Σεπτεμβρίου, οι Ελβετοί πρωτοτύπησαν ξανά παγκοσμίως, αποδεχόμενοι την ψηφοφορία μέσω Διαδικτύου σε εθνικό δημοψήφισμα. Αυτή τη φορά οι πολίτες κλήθηκαν να πουν τη γνώμη τους για το αν αποδέχονταν να χαλαρώσει η νομοθεσία παροχής ελβετικής υπηκοότητας σε ξένους, για το αν γινόταν αποδεκτή η περικοπή των ταχυδρομικών γραφείων ανά την χώρα και για το αν δέχονταν να χορηγείται άδεια μητρότητας 14 εβδομάδων. Για την ιστορία, στα δύο πρώτα κυριάρχησε το «όχι», ενώ στο τρίτο το «ναι».Η προσπάθεια διεύρυνσης της συμμετοχής των πολιτών στη λήψη αποφάσεων είναι σαφές ότι προάγει την έννοια της δημοκρατίας. Αυτός άλλωστε είναι και ο στόχος της λεγόμενης «ηλεκτρονικής δημοκρατίας» (edemocracy), για την οποία τόσα έχουν γραφεί από τα χρόνια που το δίδυμο Κλίντον - Γκορ εξήγγειλε την «υπερλεωφόρο της πληροφορίας» στις ΗΠΑ και η Ευρωπαϊκή Ένωση έκανε σκοπό της την «Κοινωνία της Πληροφορίας». Ειδικά όμως στις ΗΠΑ η αμφισβήτηση του αδιάβλητου των ψηφιακών εκλογών κινδυνεύει να καταστήσει τη δημοκρατία κυριολεκτικά «εικονική». Ας δούμε γιατί.Οι εκλογικές οθόνες αφής που κυριαρχούν στις ΗΠΑ είναι καθαρά ψηφιακές συσκευές, που διαχειρίζονται την πληροφορία ψήφου σε κλειστό κύκλωμα. Ακόμη και αν κάποιες από αυτές εκδίδουν χάρτινες αποδείξεις για τους ψηφοφόρους, κανείς δεν μπορεί να διασταυρώσει τα αποτελέσματα της εκλογικής διαδικασίας με κάποια καταγραφή σε χαρτί. Όλες οι ψήφοι αποθηκεύονται σε ηλεκτρονικές μνήμες και, μέσω ειδικού δικτύου,καταχωρίζονται σε κεντρικές βάσεις δεδομένων. Τον έλεγχο λειτουργίας τής κάθε συσκευής και διαχείρισης των πληροφοριών-εκλογικών αποτελεσμάτων τον έχουν οι δύο - τρεις κατασκευάστριες εταιρείες, υπό την υψηλή εποπτεία των αρχών διεξαγωγής των εκλογών. Ο κώδικας του λογισμικού των συσκευών και των βάσεων δεδομένων είναι «κλειδωμένος» και κανείς εκτός του προσωπικού των εταιρειών δεν επιτρέπεται να δει τι περιέχει το εκλογικό «μαύρο κουτί». Στο καθεστώς αυτό αντέδρασε πρώτη η RebeccaMercuri, μια εμπειρογνώμων της ηλεκτρονικής ψηφοφορίας από τη Σχολή Δημόσιας Διοίκησης Κένεντι του Πανεπιστημίου Χάρβαρντ, όταν η εκλογική της περιφέρεια στην Πενσυλβανία θέλησε το 1989 να προμηθευθεί σχετικό εξοπλισμό. Έπειτα από έρευνα, η Mercuri κατέληξε στο ότι οι εν λόγω συσκευές επιδέχονταν αλλοίωση αποτελεσμάτων με πολύ μικρή προσπάθεια, οπότε ζήτησε να υπάρχει υποχρεωτικά και εκτύπωση της ψήφου σε χαρτί, που θα μπορούσε να το δει αλλά όχι να το αγγίξει ο ψηφοφόρος και θα αποθηκευόταν σε ερμητικά κλειστή κάλπη. Αυτός κατά τη Mercuri ήταν και είναι ο μόνος τρόπος για να διασφαλιστεί η διασταύρωση των αποτελεσμάτων. Ελάχιστοι τότε έδωσαν όμως σημασία στις ενστάσεις της. Τα χρόνια κύλησαν και οι εκλογικές συσκευές αφής κέρδιζαν έδαφος, παρά το ότι κόστιζαν 3.000 δολάρια η μία. Το 1997 η Πολιτεία της Αϊόβας συνέστησε μια ειδική επιτροπή για να γνωμοδοτήσει αν οι συσκευές της εταιρείας Diebold ήταν κατάλληλες για να εισαχθούν στην εκλογική διαδικασία. Ένα από τα μέλη της επιτροπής, ο καθηγητής Πληροφορικής του Πανεπιστημίου της Αϊόβας DougJones, ανακάλυψε με τρόμο ότι το κλειδί κρυπτογράφησης ήταν το ίδιο για όλες τις συσκευές, και μάλιστα ήταν καταχωρισμένο στο λογισμικό του συστήματος! Ένα κολοσσιαίο λάθος που διδάσκεται προς αποφυγήν στο πρώτο έτος της κρυπτογραφίας. Ο Τζόουνς ενημέρωσε την Diebold για το πρόβλημα, η εταιρεία τον διαβεβαίωσε ότι θα το έλυνε και του έκλεισε το στόμα με ένα συμβόλαιο μη αποκάλυψης στοιχείων.

Η εμπειρία του Βελγίου

Το Βέλγιο πειραματίστηκε με την ηλεκτρονική ψηφοφορία από το 1991, όταν πραγματοποιήθηκαν δοκιμές για την αντιμετώπιση μια σειράς πο-λύπλοκων διαδικασιών και περιορισμών εκλογικού συστήματος. Στο παραδοσιακό σύστημα ψηφοφορίας, οι πολυπλοκότητες οδηγούν σε μια δύσκολη διαδικασία, η οποία υπόκειται συχνά σε λάθη. Η ηλεκτρον-ική ψηφοφορία εγκρίθηκε με νόμο το έτος 1994 , ενώ αξίζει να σημειωθεί ότι χρησιμοποιήθηκε το 1999 και το 2000 στις εθνικές και τις δημοτικές εκλογές. Οι βελγικές αρχές έχουν επεκτείνει σταδιακά τις εκλογικές περιφέρειες που χρησιμοποιούν ηλεκτρονική ψηφοφορία, και το σύστημα αναμενόταν να τεθεί σε εφαρμογή σε ολόκληρη την επικράτεια μέχρι το 2006. Στις εθνικές εκλογές του 2003, 3,2 εκατομμύρια Βέλγοι πολίτες ήταν σε θέση να ψηφίσουν ηλεκτρονικά.

Η προσέγγιση του Βελγίου ήταν παρόμοια με της Ιρλανδίας υπό την έννοια ότι δεν τροποποιεί την διαδικασία ψηφοφορίας αλλά αντικαθιστά το ψηφοδέλτοπ με μηχανή στο εκλογικό τμήμα και στην συνέχεια χρησιμοποιεί ένα ηλεκτρονικό σύστημα καταμέτρησης.

Η ασφάλεια των συστημάτων ηλεκτρονικής ψηφοφορίας που βρισκόταν σε χρήση επικρίθηκε κατά το παρελθόν τόσο από ομάδες πολιτών όσο και από ορισμένα πολιτικά κόμματα. Για να αντιμετωπίσουν αυτές τις επικρήσεις, ο νόμος επιβάλει πλέον ανεξάρτητο έλεγχο των συστημάτων πριν από τις εκλογές. Το 2003 η έκθεση ελέγχου που εκδόθηκε από την Ομοσπονδιακή Δημόσια Υπηρεσία Εσωτερικών, ενέκρινε τα συστήματα μετά από μια προσομοίωση που πραγματοποιήθηκε με βάσει 1 εκατομμύριο περίπου ψήφους.

Για να ενισχύσει τη δημόσια εμπιστοσύνη στο σύστημα, η Ομοσπονδιακή κυβέρνηση αποφάσισε επίσης να δημοσιεύει τον πηγαίο κώδικα των τριών συστημάτων λογισμικού της ηλεκτρονικής ψηφοφορίας που χρησιμοποιήθηκαν(Digivoteπου παρέχονται από την steria ,το Jitesπου παρέχεται από τη Philipsκαι τη stesud) και να εκτελέσημοα προσομοίωση ηλεκτρονικής ψηφοφορίας στην πύλη της ηλεκτρονικής διακυβέρνησης,http://Belgium.b3.

Ορισμένα προβλήματα καταγράφηκαν στις Βελγικές κοινότητες κατά τη διάρκει της ψηφοφορίας το 2003 όπου η ηλεκτρονική κάλπη ήταν σε χρήση για τις εθνικές εκλογές. Στις εκλογές αυτές ανανεώνονταν και οι δύο βουλές της χώρας. Οι καθυστερήσεις που σημειώθηκαν κατά την ψηφοφορία σε μερικές περιοχές ανάγκασαν κάποια εκλογικά τμήματα να παραμείνουν ανοιχτά και μετά την επίσημη ώρα του κλεισίματος στις 3 μ.μ . Οι ψηφοφόροι ως εκ τούτου έπρεπε να περιμένουν μεγάλο χρονικό διάστημα μέχρι να ψηφήσουν. Οι περισσότεροι περίμενα λόγο της υποχρεωτικής ψηφοφορίας που επικρατεί στο Βέλγιο, η παράλειψη της οποίας επιφέρει κυρώσεις. Παρόλα αυτά στατιστικές έδειξαν ότι το 10 % περίπου των ψηφοφόρων απείχαν από την ψηφοφορία.

Σύμφωνα με πρόσφατη έρευνα οι αιτίες της καθυστέρησης ήταν οι εξής:

- Περιορισμένος αριθμός υπολογιστών σε κέντα που είχε οριστεί να γίνει ηλεκτρονική ψηφοφορία
- Πολυπλοκότητα των συστημάτων ηλεκτρονικής ψηφοφορίας και έλλειψη πληροφόρησης και γνώσεις των ψηφοφόρων για την διαδικασία.
- Μεγάλος αριθμός σφαλμάτων των υπολογιστών, με περισσότερες από 500 εργασίες συντήρησης και επισκευής.

Ωστόσο καθυστερήσεις παρουσιάστηκαν και σε εκλογικά τμήματα με τις παραδοσιακές μεθόδους ψηφοφορίας λόγω προβλημάτων όπως έλλειψη δελτίων, έλλειψη επιθεωρητών ψηφοφορίας ή ανεπαρκούς αριθμού εκλογικών τμημάτων.

Αξιοσημείωτο είναι ότι η χρήση της ηλεκτρονικής ψηφοφορίας στο Βέλγιο σταθερά εξαπλώνεται. Μάλιστα από το 2006 είχε προγραμματιστεί η εξολοκλήρου εγκατάσταση συστημάτων ηλεκτρονικής ψηφοφορίας. Ο λόγος για την αντικατάσταση της παραδοσιακής ψηφοφορίας με την ηλεκτρονική βρίσκεται στην μείωση χρηματοοικονομικών εξόδων.

Η εμπειρία της Γαλλίας

Πιλοτικά προγράμματα οργανώθηκαν με την συμμετοχή 4000 ψηφοφόρων στο Στρασβούργο κατά την διάρκεια των εκλογών του Ευρωπαϊκού κοινοβουλίου το 1994 και στην Issy-les-Moulineauxκατά την διάρκεια των προεδρικών εκλογών το 1995. Το 2000,η πόλη της Λυών οργάνωσε μια δοκιμαστική ηλεκτρονική ψηφοφορία. Η Γαλλία έχει επίσης πειραματιστεί με το ολοκληρωμένο σύστημα ψηφοφορίας που χρησιμοποιήθηκε στη Ιρλανδία, την Γερμανία και τις κάτω χώρες. Παρά την θετική διάθεση που υπάρχει, η ευρεία χρήση της ηλεκτρονικής ψηφοφορίας δεν προβλέπεται προς το παρόν στην Γαλλία.

Η εμπειρία της Ισπανίας

Αν και δεν έχει χρησιμοποιήσει ακόμη την ηλεκτρονική ψηφοφορία σε εθνικό επίπεδο, η Ισπανία έχει πειραματιστεί με διάφορες μορφές της ηλεκτρονικής ψηφοφορίας. Στις 14 Μαρτίου 2004 σε διεξαγωγή εθνικών εκλογών, μικρής κλίμακας, μη δεσμευτική ηλεκτρονικής ψηφοφορίας, δοκιμάστηκε με επιτυχία. Η διαδικασία περιλάμβανε την χρήση απομακρυσμένης μεθόδου ψηφοφορίας , όπως το Ίντερνετ και τα SMSπου χρησιμοποιεί αυστηρά η Ιρλανδία.

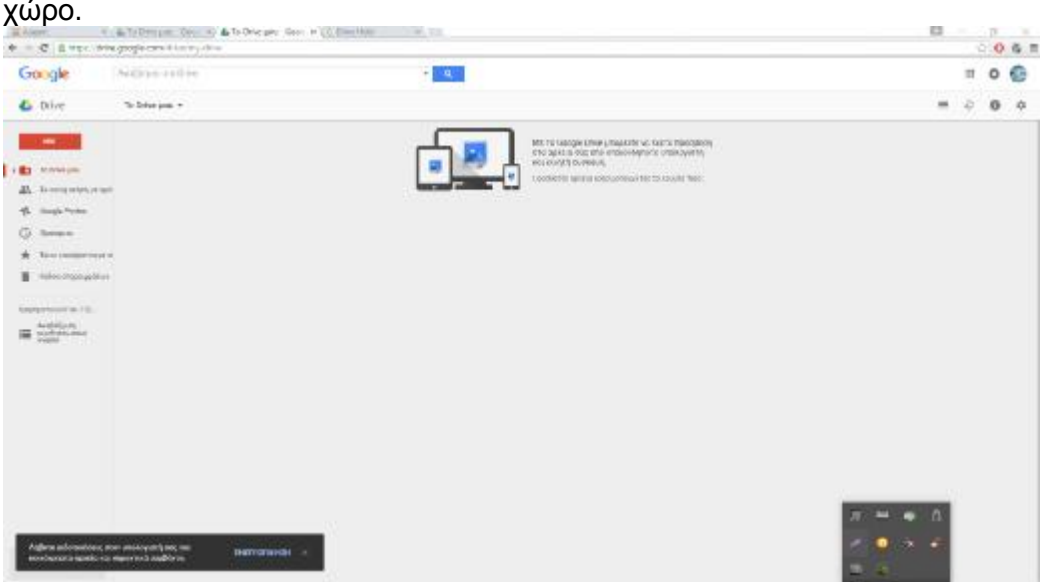
Στις 16 Νοεμβρίου 2003,τρεις ηλεκτρονικές πιλοτικές δοκιμές διεξήχθηκαν με επιτυχία κατά την διάρκεια των βουλευτικών εκλογών της Καταλονίας.Όσοι είχαν το δικαίωμα ψήφου και ζούσαν στο εξωτερικό, μπορούσαν να ψηφίσουν μέσω του διαδικτύου, ενώ ταυτόχρονα υπήρχαν οθόνες αφής σε πέντε δήμους σε συνδυασμό με ένα ηλεκτρονικό σύστημα καταμέτρησης (που αναπτύχθηκε από την Demotek). Παρά το σχετικά χαμηλό επίπεδο συμμετοχής στις εκλογές, κυβερνητικές υπηρεσίες δήλωσαν ότι είναι ευχαριστημένες με την αντίδραση των ψηφοφόρων προς τα καινοτόμα δοκιμαστικά εγχειρήματα. Οι δοκιμαστικές εφαρμογές δεν είχαν νομική αξία και οι πολίτες που συμμετείχαν έπρεπε να ψηφίσουν μέσω παραδοσιακών μεθόδων. Η εγκαθίδρυση ενός ηλεκτρονικού συστήματος ψηφοφορίας και η αλλαγή ουσιαστικά του παραδοσιακού μοντέλου στην Καταλονία, θα απαιτούσε από το κοινοβούλιο να ψηφίσει ένα νέο εκλογικό νόμο.

Υλοποίηση

GoogleDrive

Η Google μας προσφέρει ποικίλες υπηρεσίες(Apps) για την εξυπηρέτηση διάφορων σκοπών. Μια από αυτές τις εφαρμογές- υπηρεσίες είναι το GoogleDrive. Το GoogleDrive είναι υπηρεσία αποθήκευσης και συγχρονισμού αρχείων που παρέχεται από την Google, κυκλοφόρησε στις 24 Απριλίου του 2012, και επιτρέπει την χρήση αποθηκευτικού νέφους, τον διαμοιρασμό αρχείων και την συνεργατική επεξεργασία από τον χρήστη. Τα αρχεία που μοιράζονται δημόσια στο GoogleDrive μπορούν να αναζητηθούν με μηχανές αναζήτησης.

Το GoogleDriveμε λίγα λόγια είναι το "σπίτι" των GoogleDocs, μίας σουίτας γραφείου με εφαρμογές παραγωγικότητας, που προσφέρει την συνεργατική επεξεργασία εγγράφων, υπολογιστικών φύλλων, παρουσιάσεων και άλλων.
Το GoogleDrive προσφέρει σε όλους τους χρήστες του έναν αρχικό online χώρο αποθήκευσης 15 GB (αρχικά ήταν 5GB), που μπορεί να χρησιμοποιηθεί από τις τρεις πιο διαδεδομένες υπηρεσίες: το GoogleDrive, το Gmail και της Φωτογραφίες του Google+. Ο χρήστης μπορεί να λάβει επιπλέον χώρο αποθήκευσης, ο οποίος μοιράζεται μεταξύ Picasa και GoogleDrive, από 100 GB μέχρι και 16TB μέσω της καταβολής μηνιαίας συνδρομής (US4.99$ το μήνα για 100GB). Ο χρήστης με τον πληρωμένο αποθηκευτικό χώρο δεν λαμβάνει δωρεάν χώρο μαζί με τον πληρωμένο χώρο.



Η εικόνα αυτή μας δείχνει πώς είναι το περιβάλλον του GoogleDrive, ενώ πρέπει να σημειωθεί ότι απαραίτητη προϋπόθεσηγια την δημιουργία φόρμας είναι η ύπαρξη λογαριασμού στην Google (Gmail).

Δυνατότητες που προσφέρει το GoogleDrive

- Δυνατότητα αποθήκευσης αρχείων
- Δυνατότητα προβολής των αρχείων οποιαδήποτε στιγμή από οποιονδήποτε υπολογιστή.
- Δυνατότητα λήψης των αρχείων από οποιονδήποτε υπολογιστή.
- Κοινή χρήση αρχείων ώστε να μπορούν να τα δούνε , να τα επεξεργαστούν και να τα κατεβάσουν στον υπολογιστή τους άλλοι χρήστες.

- Δυνατότητα επεξεργασίας αρχείων εκτός σύνδεσης και αυτόματη ενημέρωση του Drive (συγχρονισμός) όταν υπάρξει σύνδεση στο internet.
- Αναγνώριση υπολογιστικών φύλλων ή αρχείων κειμένων, από το Micrososft Office.

Google Forms

Ένα είδος αρχείου που μας επιτρέπει να δημιουργήσουμε η υπηρεσία GoogleDriveείναι οι διαδικτυακές φόρμες(GoogleForms) μέσω των οποίων μπορούμε να αναπτύξουμε ερωτηματολόγια με σκοπό να πάρουμε απαντήσεις που θα βοηθήσουν στην βελτιστοποίηση της λήψη αποφάσεων για τα διάφορα θέματα που περιγράφουν.
Μέσω αυτής της υπηρεσίας(GoogleDrive-GoogleForms) θα μπορέσουμε να εξάγουμε αποτέλεσμα από τις διάφορες ψηφοφορίες στην σελίδα μας.

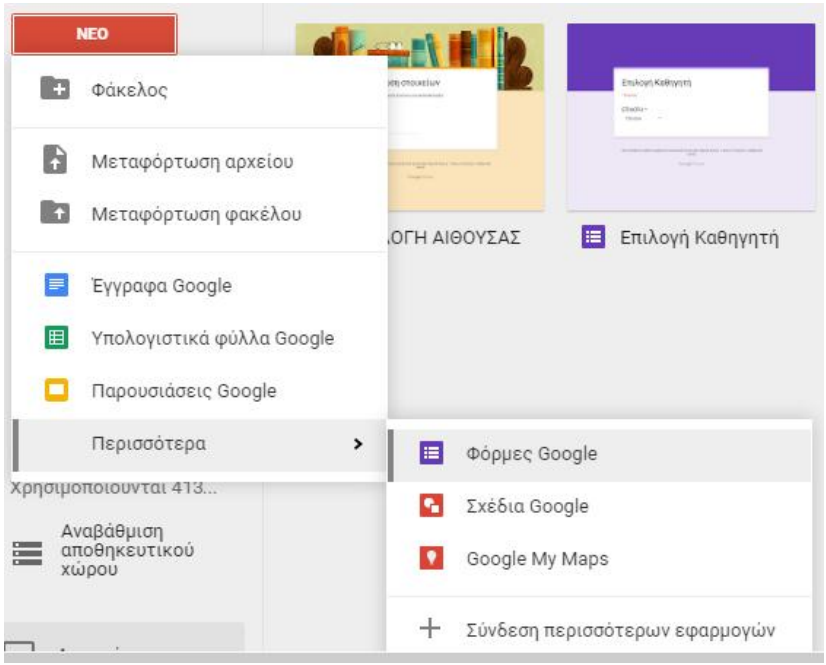
Πρόσθετα Φόρμας

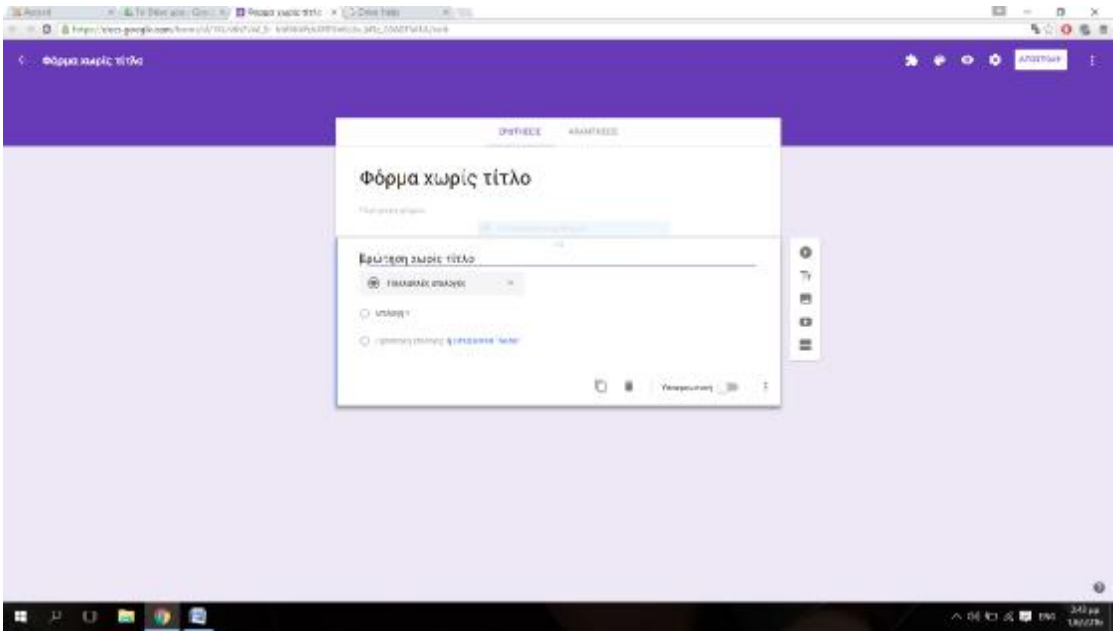
Δυνατότητα λήψης μεγάλης ποικιλίας προσθέτων τα οποία είναι δωρεάν, επεκτείνουν την λειτουργικότητα της φόρμας και είναι εύκολα στην χρήση. Για παράδειγμα το formLimiterμε το οποίο μπορούμε να ορίσουμε τον αριθμό των απαντήσεων που δέχεται η φόρμα, να θέσουμε όρια στο χρόνο απάντησης με βάση την επιθυμητή ημερομηνία που θέλουμε να κλείνει η φόρμα.

Διαδικασία δημιουργίας φόρμας

Αρχικά πρέπει να συνδεθούμε στο λογαριασμό μας στην Google. Έπειτα από τις εφαρμογές πατάμε στο GoogleDrivekαι στην συνέχεια επιλέγουμε *Νέο* **à** *Περισσότερα* **à** *Φόρμες*Googleόπως φαίνεται και στην παρακάτω εικόνα.

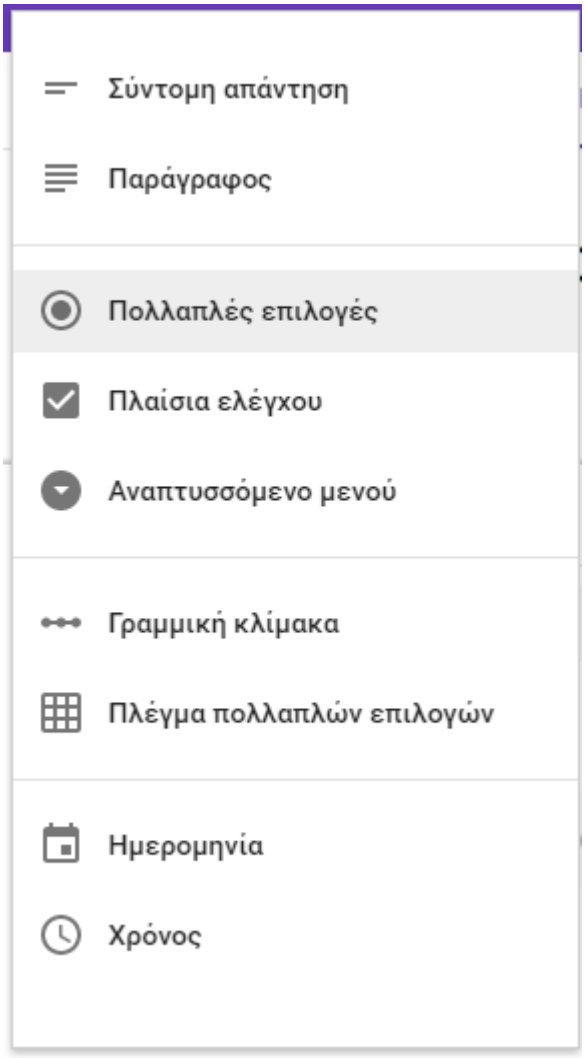
Περιβάλλον δημιουργίας φόρμας





Τρόποι Ερώτησης

Οι φόρμες μας προσφέρουν πολλές εναλλακτικές επιλογές για τον τρόπο με τον οποίο μπορούμε να απαντήσουμε.



Σύντομη απάντηση:Ο ερωτούμενος-η κλείνεται να απαντήσει κάτι σύντομο, ενώ συνήθως τέτοιου είδους απαντήσεις αφορούν συγκεκριμένες πληροφορίες. Για παράδειγμα όνομα, επίθετο,ηλεκτρονική διεύθυνση και τα λοιπά.

Παράγραφος:Ο ερωτούμενος-η καλείται να απαντήσει περιγραφικά για το εκάστοτε θέμα. Για παράδειγμα το πεδίο άλλη απάντηση οπού μπορεί ο ερωτούμενος να προσθέσει την δικιά του απάντηση εφόσον δεν τον καλύπτουν οι υπάρχοντες απαντήσεις.

Πολλαπλές επιλογές:Ο ερωτούμενος-η πρέπει να επιλέξει μια εκ των διαθέσιμων επιλογών.

Για παράδειγμα:

Ερώτηση: Ποια αίθουσα διδασκαλίας θα θέλατε;

Διαθέσιμες απαντήσεις : Αίθουσα Α ή Αίθουσα Β ή Αίθουσα Γ

Πλαίσια ελέγχου:Ο ερωτούμενος-η έχει την δυνατότητα να επιλέξει περισσότερες από μία επιλογές ανάλογα με το πόσες του έχουν οριστεί.

Για παράδειγμα:

Ερώτηση: ποιους καθηγητές θεωρείτε καταλληλότερους για το μάθημα γλώσσας c;

Διαθέσιμες απαντήσεις : καθηγητής Α , Καθηγητής Β, καθηγητής γ, καθηγητής δ.

Αναπτυσσόμενο μενού:Οι διαθέσιμες επιλογές του ερωτούμενου-ης εμφανίζονται σε μορφή αναπτυσσόμενου πλαισίου.

Γραμμική κλίμακα:Ο ερωτούμενος-η καλείται να απαντήσει μέσω μιας κλίμακας η οποία συνήθως χρησιμοποιείται για να δηλώσει το βαθμό της αρεσκείας του.

Για παράδειγμα:

Ερώτηση**:** Πόσο ικανοποιημένοι είστε από την εξυπηρέτηση της γραμματείας του τμήματος σας;

Κλίμακα απαντήσεων :

1 (πολύ λίγο)

2(λίγο)

3(μέτρια)

4(πολύ)

5(πάρα πολύ)

Πλέγμα πολλαπλών επιλογών:Ουσιαστικά ο ερωτούμενο-η αντιστοιχεί μια χρήση επιλογών με μία άλλη.

Για παράδειγμα:

Ερώτηση: Ποιον καθηγητή πιστεύετε ότι είναι καταλληλότερος για το κάθε μάθημα;

	Καθηγητής 1	Καθηγητής 2
Μάθημα 1	√	
Μάθημα 2		√

Ημερομηνία:Οερωτούμενος-η καλείται να απαντήσει μία συγκεκριμένη ημερομηνία.

Χρόνος: Ο ερωτούμενος-η συμπληρώνει μια χρονική στιγμή η μια χρονική διάρκεια.

Υπάρχουν όμως και άλλες σημαντικές λειτουργίες με τις οποίες μπορούμε να βελτιώσουμε τις φόρμες αλλά και να τις επεξεργαστούμε όπως φαίνεται στην παρακάτω εικόνα.

Μπάρα Μενού

Αναλυτικότερα :

Μια λειτουργία με την οποία μπορούμε να δούμε τα πρόσθετα που έχουμε προσθέσει.

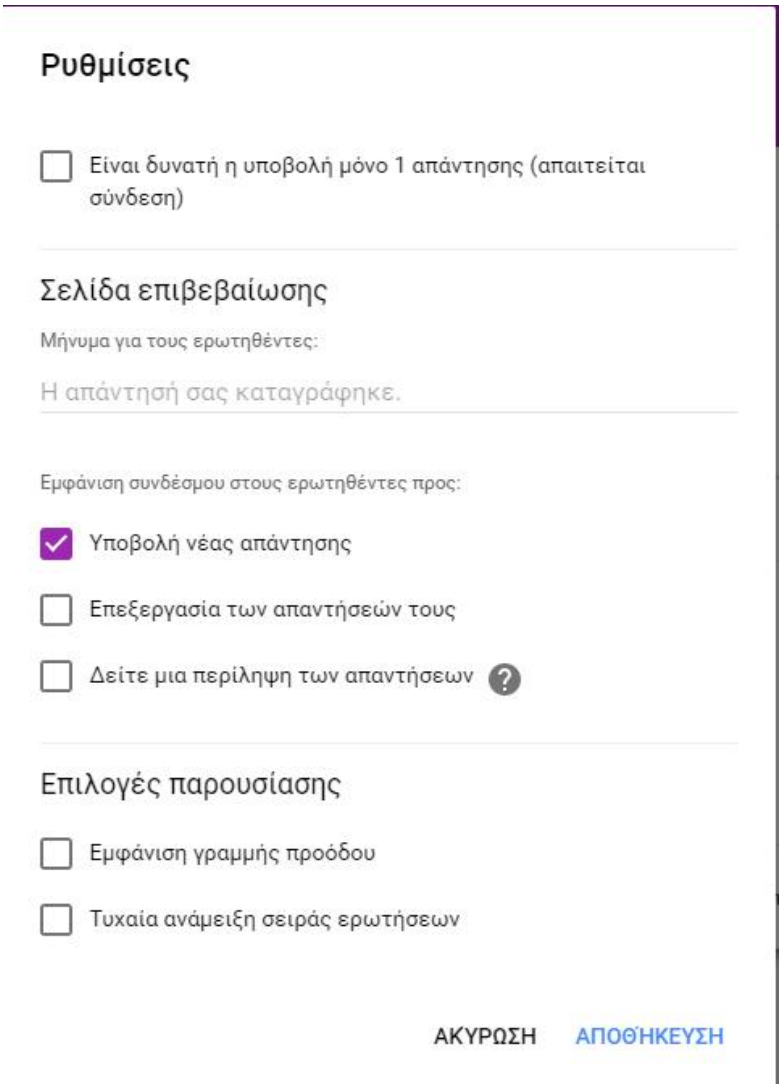
Μία μπορεί

κυρίως οπτική επιλογή καθώς ο διαχειριστής της φόρμας να την τροποποιήσει ανάλογα με το χρώμα της αρεσκείας του.

Μία χρήσιμη επιλογή με την οποία ο διαχειριστής μπορεί να κάνει προεπισκόπηση την φόρμα του και έτσι να ελέγξει το πώς φαίνεται στους χρήστες πριν την δημοσιοποιήσει οπουδήποτε.

Μια επιλογή με την οποία μπορούμε να κάνουμε σημαντικές ρυθμίσεις στην φόρμα μας όπως φαίνεται στην παρακάτω εικόνα.

Με την πρώτη επιλογή ουσιαστικά δεχόμαστε μία απάντηση από κάθε ερωτηθέντα, ο



οποίος για να απαντήσει θα πρέπει να είναι συνδεδεμένος για να απαντήσει.

Στην ***Σελίδα επιβεβαίωσης*** μπορούμε να γράψουμε το μήνυμα το οποίο επιθυμούμαι να εμφανίζεται στον ερωτηθέντα μετά την υποβολή της απάντησης του.

Με την επιλογή ***Υποβολή νέα απάντησης*** δίνουμε την δυνατότητα στο ερωτηθέντα να ξανά απαντήσει την φόρμα μας.

Με την επιλογή ***Επεξεργασία των απαντήσεων τους*** δίνουμε την δυνατότητα στον ερωτηθέντα να επεξεργαστεί τις είδη υποβεβλημένες απαντήσεις του.

Με την επιλογή ***Δείτε μια περίληψη των απαντήσεων*** ο ερωτηθέντας μπορεί να δει συνοπτικά τι έχει απαντήσει.

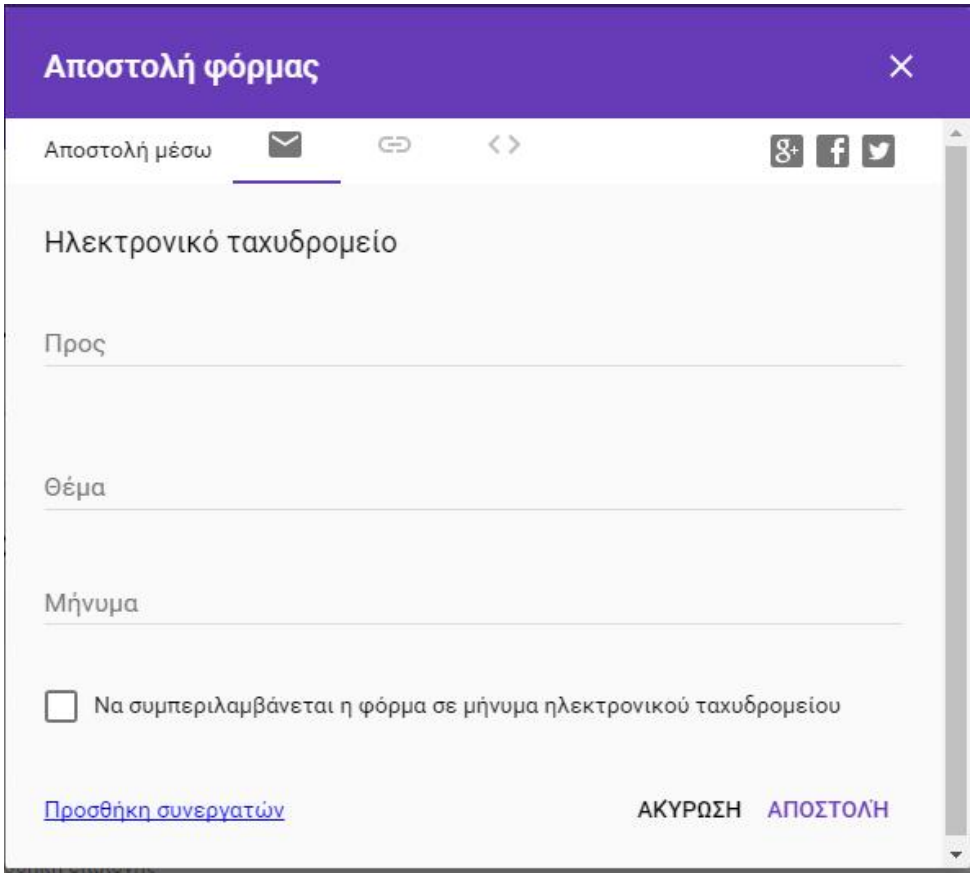
Με την ***Εμφάνιση γραμμής προόδου***, κατά την διάρκεια συμπλήρωσης της φόρμας εμφανίζεται μια μπάρα στου ερωτηθέντες η οποία τους πληροφορεί κατά πόσο της εκατό έχουν τελειώσει την διαδικασία συμπλήρωσης.

Με την επιλογή ***Τυχαία ανάμειξη σειράς ερωτήσεων*** ουσιαστικά οι ερωτήσεις εμφανίζονται με τυχαία σειρά στους ερωτηθέντες και όχι με την σειρά που τις έγραψε ο διαχειριστής της φόρμας.

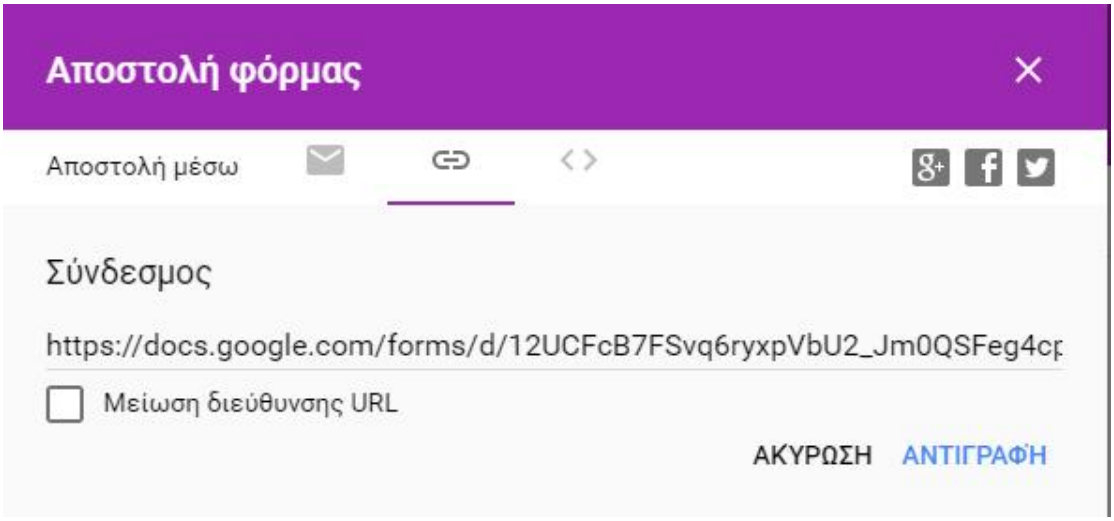
Πατώντας την επιλογή αποστολή εμφανίζονται οι δυνατοί τρόποι με τους οποίους μπορούμε να στείλουμε την φόρμα μας.

Ο πρώτος τρόπος είναι μέσω ***Ηλεκτρονικού ταχυδρομείου*** όπως φαίνεται στην παρακάτω εικόνα.

Επιλογές Αποστολής



Ο δεύτερος τρόπος είναι μέσω ***συνδέσμου***, δηλαδή μπορούμε να στείλουμε το σύνδεσμο(link) στους ερωτηθέντες, να το ανοίξουν και να συμπληρώσουν την φόρμα.

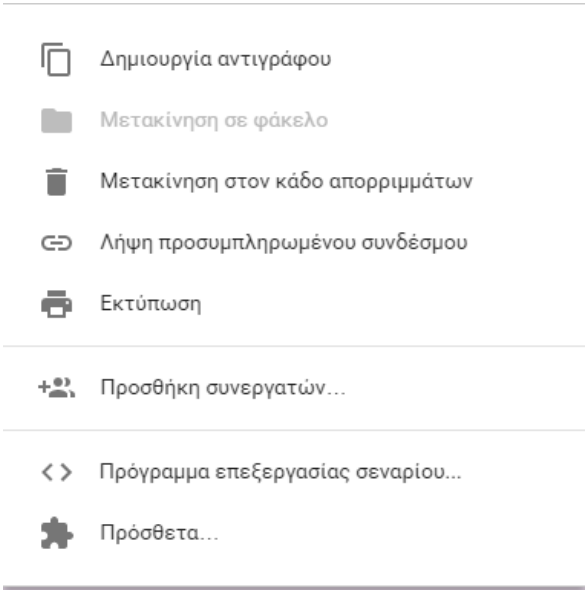


Ο τρίτος τρόπος είναι με ***ενσωμάτωση HTML*** όπου στην συγκεκριμένη περίπτωση μας εμφανίζει ένα πηγαίο κώδικα τον οποίο μπορούμε να τον χρησιμοποιήσουμε και

να τον ενσωματώσουμε μέσα σε μία άλλη ιστοσελίδα με σκοπό η φόρμα να εμφανίζεται μέσα σε αυτή.

Υπομενού (3 τελείες)

Σε αυτή την επιλογή εμφανίζονται ακόμα περισσότερες δυνατότητες.



Με την επιλογή ***δημιουργία αντιγράφου*** μπορούμε να δημιουργήσουμε ένα αντίγραφο της φόρμας μας.

Με την επιλογή ***μετακίνηση στον κάδο απορριμμάτων*** μπορούμε να σβήσουμε την φόρμα μας αλλά όχι οριστικά. Για να σβηστή οριστικά θα πρέπει να σβήσουμε την φόρμα και από τον κάδο απορριμμάτων.

Με την επιλογή ***Λήψη συμπληρωματικού συνδέσμου***εμφανίζεται στον ερωτηθέντα μία είδη προεπιλεγμένη απάντηση. την οποία όμως μπορεί και να αλλάξει.

Με την επιλογή ***Εκτύπωση*** μπορούμε να φωτοτυπήσουμε την φόρμα μας.

Με την επιλογή ***Προσθήκη συνεργατών*** μπορούμε να προσθέσουμε συνεργάτες μας μέσω Gmail(ή οποιαδήποτε άλλη ηλεκτρονική υπηρεσία ταχυδρομείου) , Facebook ,Google+ και Twitter.

Με την επιλογή ***Πρόγραμμα επεξεργασία σεναρίου*** εμφανίζεται ένα παράθυρο στο οποίο μπορούμε να γράψουμε και ενσωματώσουμε κώδικα.

Με την επιλογή ***Πρόσθετα*** μία πάρα πολύ σημαντική επιλογή μέσω της οποίας μπορούμε βελτιώσουμε τις φόρμες μας.

Μας δίνει την δυνατότητα να ενσωματώσουμε πάνω σε αυτές πρόσθετες λειτουργίες οι οποίες μπορούν να κάνουν σημαντική δουλειά για μας. Χαρακτηριστικό παράδειγμα είναι το FormLimiterτο οποίο το αναλύσαμε παραπάνω όταν αναφερθήκαμε στα πρόσθετα φόρμας ως δυνατότητα του GoogleForms.

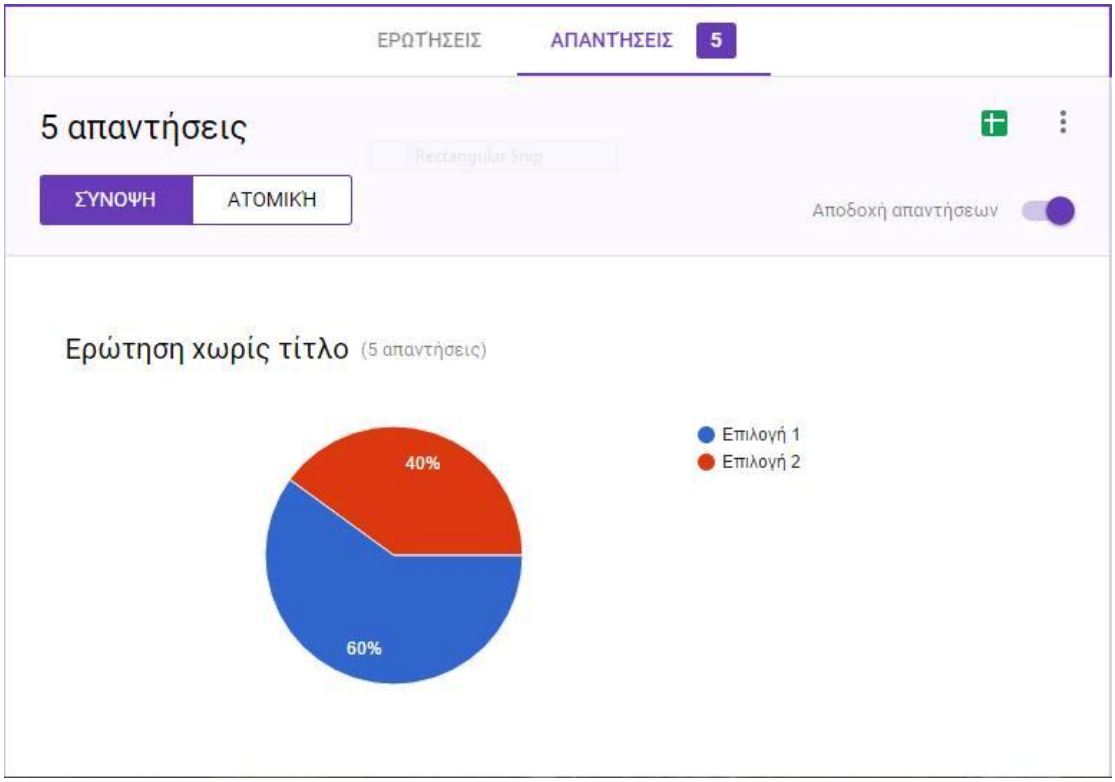
Στατιστικά

Το Googleformsόμως πέρα από την δυνατότητα που μας δίνει να φτιάχνουμε φόρμες ερωτήσεων μας δίνει και την δυνατότητα να αντλήσουμε και κάποια στατιστικά στοιχεία πάνω στις ερωτήσεις αυτές.

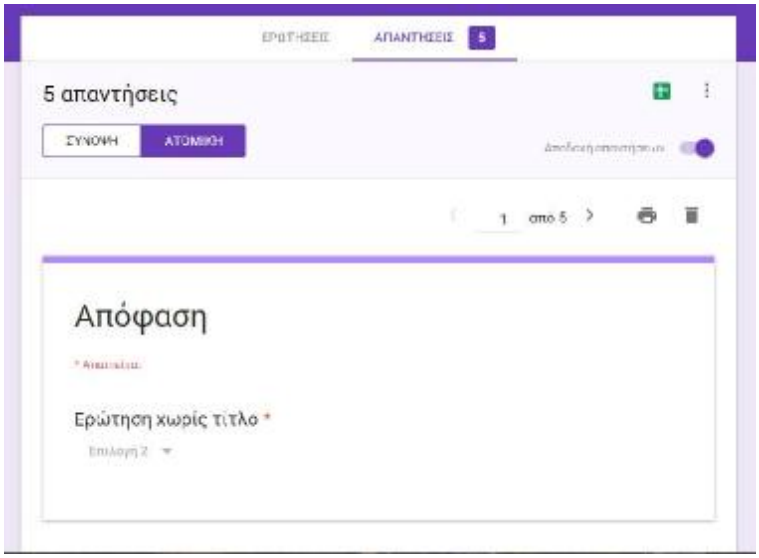
Πιο αναλυτικά :

Μπορούμε να δούμε τον αριθμό των απαντήσεων , δηλαδή των αριθμό των ατόμων που έχουν απαντήσει όπως φαίνεται στην παρακάτω εικόνα :

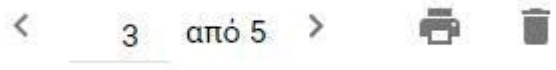
Μπορούμε να δούμε στατιστικά διαγράμματα τα οποία μας δείχνουν σε ποσοστά στην επικρατέστερη επιλογή :



Ακόμα έχουμε την δυνατότητα να μπορέσουμε να δούμε τις απαντήσεις ατομικά, δηλαδή να δούμε ξεχωριστά την κάθε απάντηση



Επίσης πρέπει να αναφέρουμε ότι έχουμε την δυνατότητα εκτύπωσης όχι μόνο της ίδιας της απάντησηςξεχωριστά αλλά και το σύνολο των απαντήσεων:



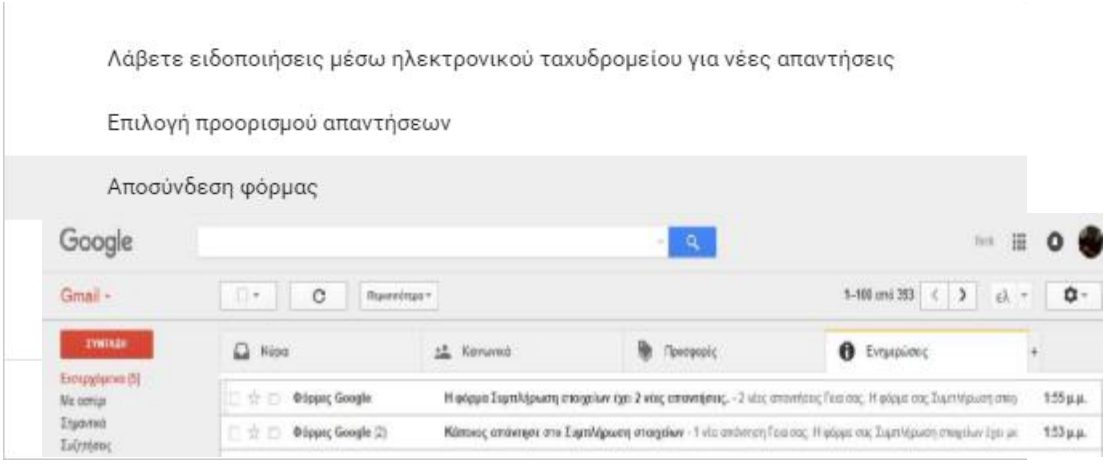
Ορισμένες επιπρόσθετες δυνατότητες.

Οι φόρμες μας δίνουν την δυνατότητα να τις εξάγουμε και να τις αποθηκεύσουμε στον υπολογιστή μας σε υπολογιστικά φύλλα (αρχεία του Microsoft Excel).

Αυτό μπορεί να γίνει πατώντας το πράσινο εικονίδιο όπως φαίνεται στην παρακάτω εικόνα.

Μενού (3 τελείες)

Εάν επιλέξουμε το εικονίδιο με τις τελίτσες μας εμφανίζει ένα ακόμα μενού επιλογών όπως φαίνεται στην εικόνα.



Με την **επιλογή λάβετε ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου** κάθε φορά που ένας ερωτηθέντας απαντάει θα λαμβάνουμε αντίστοιχα ενημερωτικό e-mail. Όπως φαίνεται στην παρακάτω εικόνα :

Με την **επιλογή προορισμού απαντήσεων** μπορούμε να συνδέσουμε την φόρμα με ένα νέο ή ένα ήδη υπάρχον υπολογιστικό φύλλο (αρχείο excel) με σκοπό να αποθηκεύονται εκεί οι απαντήσεις των ερωτηθέντων.

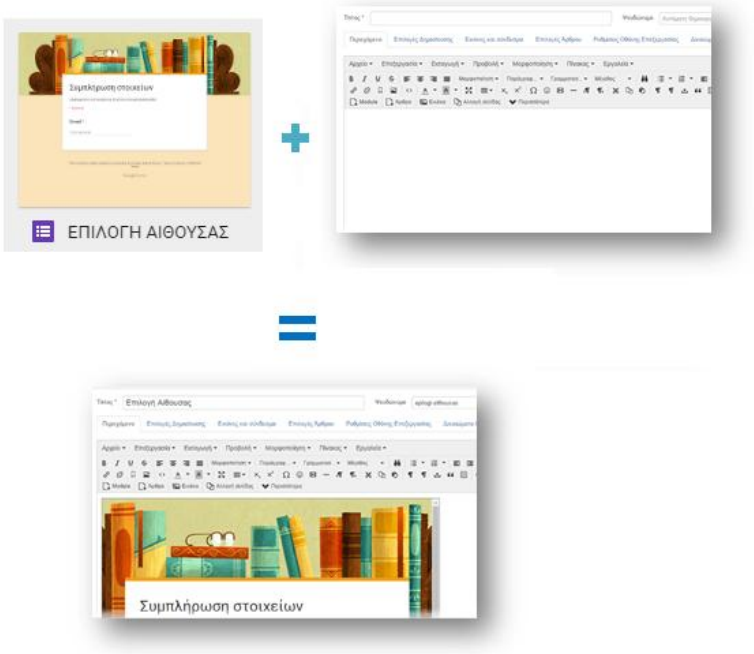
Με την επιλογή **αποσύνδεση φόρμας** μπορούμε να απενεργοποιήσουμε την διαδικασία ψηφοφορίας δηλαδή οι ερωτηθέντες δεν θα μπορούν να ψηφίσουν.

Με την επιλογή **λήψη απαντήσεων(.csv)** μπορούμε να εξάγουμε σε υπολογιστικό φύλλο (αρχείο excel) τις ήδη υποβεβλημένες απαντήσεις και να τις έχουμε στον υπολογιστή μας.

Με την επιλογή **εκτύπωση όλων των απαντήσεων** μπορούμε να φωτοτυπήσουμε όλες τις υποβεβλημένες απαντήσεις των ερωτηθέντων.

Με την επιλογή **διαγραφή όλων των απαντήσεων** μπορούμε να διαγράψουμε όλες τις υποβεβλημένες απαντήσεις της φόρμας μας

Σύνδεση GoogleForms μετην πλατφόρμα του Προμηθέα



Όπως παρουσιάζεται και στην παραπάνω εικόνα η φόρμα που έχει δημιουργηθεί με την χρήση της υπηρεσίας GoogleForm που είναι κυριολεκτικά το ψηφοδέλτιο, αποτυπώνεται μέσα σε ένα άρθρο στην Joomla. Η ακριβής επίτευξη αυτού αναφέρεται στην ενότητα Εισαγωγή φορμών(ψηφοφοριών).

Υλοποίηση-Περιβάλλον

Πριν γίνει αναφορά είναι σημαντικό να πούμε ότι η λέξη άρθρο συνδέεται άμεσα με την λέξη ψηφοφορία, ο λόγος γιατί όπως προαναφέραμε η ψηφοφορία δημοσιεύεται με μορφή άρθρου.

Η υλοποίηση της ιντερνετικής ψηφοφορίας πραγματοποιήθηκε με την εφαρμογή δημιουργίας ιστοσελίδων Joomla.

E-Prometheus πρόκειται για την προσπάθεια υλοποίησης ενός συστήματος ιντερνετικής ψηφοφορίας, από εμάς, για την πραγματοποίση του σκοπού της πτυχιακής.

Γενική εικόνα της αρχικής σελίδας του συστήματος **E-Prometheus**.

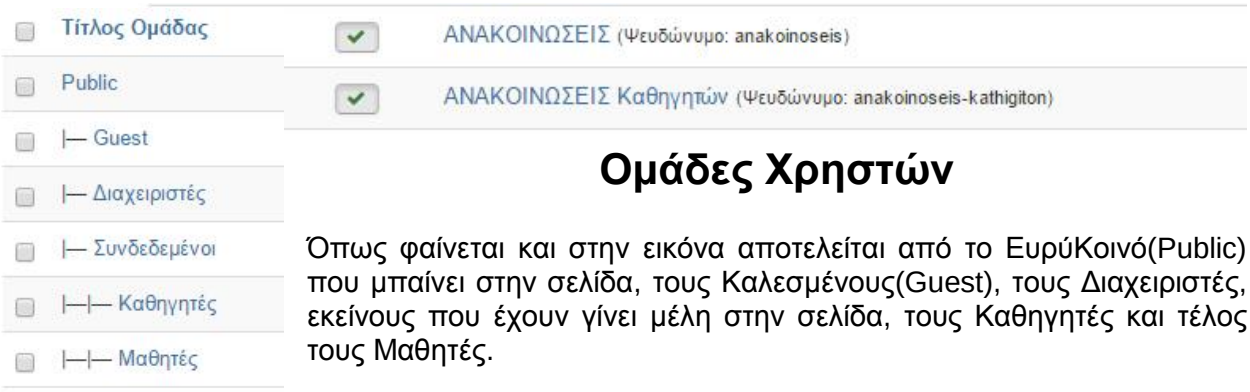
Μπορείτε να περιηγηθείτε στην σελίδα πατώντας το ακόλουθο link: http://e-prometheus.esy.es

Κατηγορίες Άρθρων

Για την υλοποίηση του συστήματος ψηφοφορίας ορίσαμετις εξής κατηγορίες άρθρων.

ΚΕΙΜΕΝΑ όπου σαν υποκατηγορία έχει τα **ΕΙΣΑΓΩΓΙΚΑ**, δηλαδή περιλαμβάνει όλα τα κείμενα τα οποία εμφανίζονται στην σελίδα και έχουν σχέση με την περιγραφή της. Την **ΨΗΦΟΦΟΡΙΑ** που αποτελεί σημαντικό κομμάτι για την σωστή ροή της πλατφόρμας. Αποτελείται από το **Ψηφίζω** και το**Ιστορικό**. Στα οποία εμφανίζονται οι ψηφοφορίες, εκείνες που βρίσκονται σε εξέλιξη και εκείνες που έχουν σταματήσει αντίστοιχα. Τα**ΣΧΟΛΙΑ** όπου περιέχονται όλα τα σχόλια των μελών που έχουν γράψει για τον Προμηθέα.

Οι **ΑΝΑΚΟΙΝΩΣΕΙΣ** που περιέχουν τις γενικές ανακοινώσεις που εμφανίζονται στους Χρήστες. Τέλος οι **ΑΝΑΚΟΙΝΩΣΕΙΣ Καθηγητών** που απαρτίζουν τις ανακοινώσεις των Καθηγητών μόνο



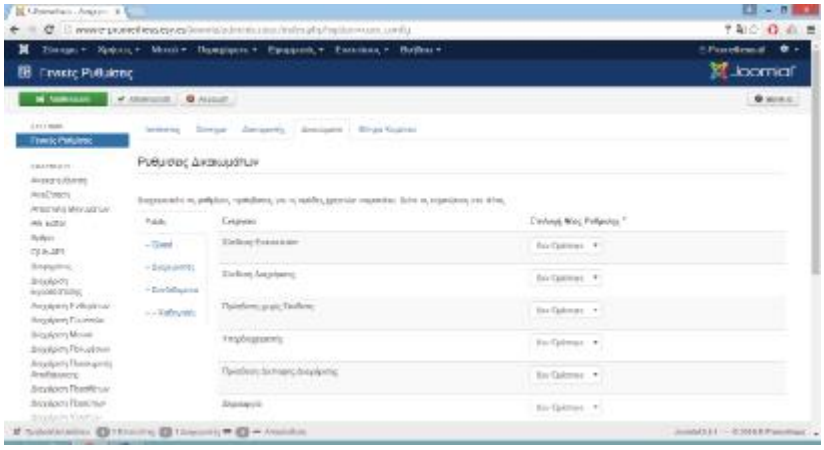
Ομάδες Χρηστών

Όπως φαίνεται και στην εικόνα αποτελείται από το ΕυρύΚοινό(Public) που μπαίνει στην σελίδα, τους Καλεσμένους(Guest), τους Διαχειριστές, εκείνους που έχουν γίνει μέλη στην σελίδα, τους Καθηγητές και τέλος τους Μαθητές.

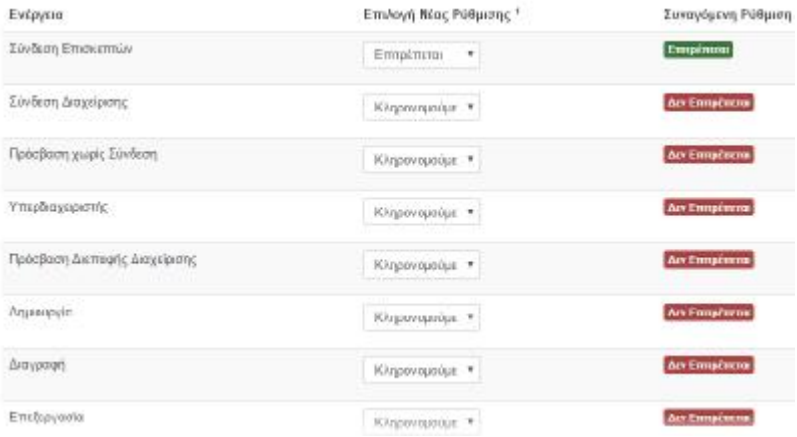
Ακόμα στην εικόνα φαίνονται οι υποκατηγορίες των κατηγοριών, οι Καλεσμένοι, Διαχειριστές, Συνδεδεμένοι αποτελούν υποκατηγορία του Ευρύ Κοινού. Δεν σημαίνει ότι όμως ότι έχουν τις ίδιες ιδιότητες. Τέλος οι Καθηγητές και οι Μαθητές αποτελούν υποκατηγορία των Συνδεδεμένων, που σημαίνει ότι για να είναι Καθηγητές, Μαθητής πρέπει πρώτα να είναι μέλος στην πλατφόρμα.

Δικαιώματα Μελών

Στις Γενικές Ρυθμίσεις από τον Πίνακα Ελέγχου του Συστήματος και στην καρτέλα Δικαιώματα φαίνονται τα εξής.



Σε αυτήν την καρτέλα βλέπουμε τα δικαιώματα που έχουν οριστεί για τον καθένα μέλος της σελίδας.



Στην καρτέλα των **Συνδεδεμένων, Μαθητών** βλέπουμε τα δικαιώματα του.

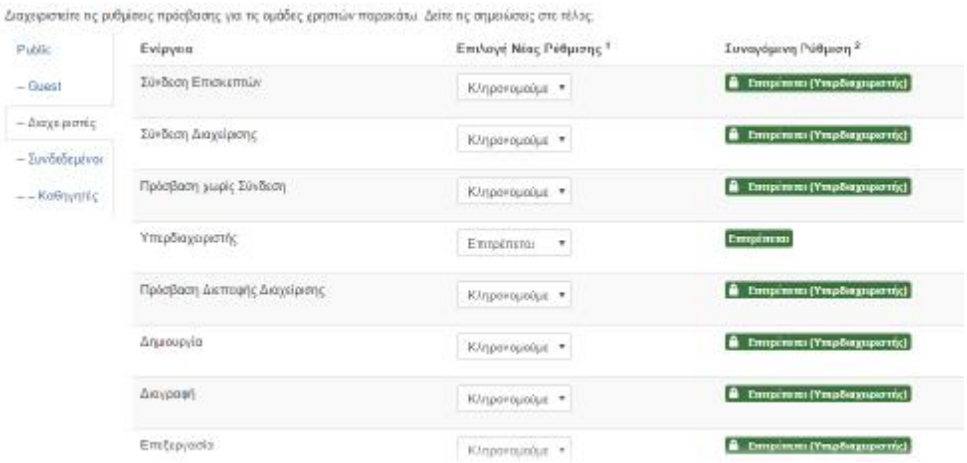
Με πράσινο βλέπουμε τα δικαιώματα που έχει και με κόκκινο εκείνα που δεν έχει. Στην συγκεκριμένη βλέπουμε ότι επιτρέπεται η σύνδεση-εγγραφή με λογαριασμό. Δηλαδή αμέσως αποκτάνε την ιδιότητα πρόσβασης της ψηφοφορίας στην σελίδας. Οι **Συνδεδεμένοι** έρχονται από το **Ευρύ Κοινό** που σαν δυνατότητα έχει την περιήγηση-εξερεύνηση της πλατφόρμας.

Στην καρτέλα του **Διαχειριστή** όπως είναι λογικό έχει πλήρη πρόσβαση σε ό,τι αφορά την σελίδα.

Σύνδεση Επισκεπτών	Κληρονομούμε	Επιτρέπεται
Σύνδεση Διαχείρισης	Επιτρέπεται	Επιτρέπεται
Πρόσβαση χωρίς Σύνδεση	Κληρονομούμε	Δεν Επιτρέπεται
Υπερδιαχειριστής	Κληρονομούμε	Δεν Επιτρέπεται
Πρόσβαση Διεπαφής Διαχείρισης	Επιτρέπεται	Επιτρέπεται
Δημιουργία	Επιτρέπεται	Επιτρέπεται
Διαγραφή	Κληρονομούμε	Δεν Επιτρέπεται
Επεξεργασία	Απαγορεύεται	Δεν Επιτρέπεται
Επεξεργασία Κατάστασης	Επιτρέπεται	Επιτρέπεται
Επεξεργασία Ιδιοκτησίας	Επιτρέπεται	Επιτρέπεται

Στην καρτέλα δικαιωμάτων των **Καθηγητών** έχει οριστεί η δυνατότητα εγγραφής-σύνδεσης με λογαριασμό στο Προμηθέα, η πρόσβαση στον Πίνακα Ελέγχου με περιορισμένη πρόσβαση, η δημιουργία άρθρων, η επεξεργασία κατάστασης δηλαδή αν θα συνεχίζει να φαίνεται στην σελίδα ένα άρθρο ή όχι και τέλος και σημαντικότερο η επεξεργασία ιδιοκτησίας όπου περιορίζει στον κάθε Καθηγητή να επεξεργάζεται μόνο και μόνο τα δικά του άρθρα.

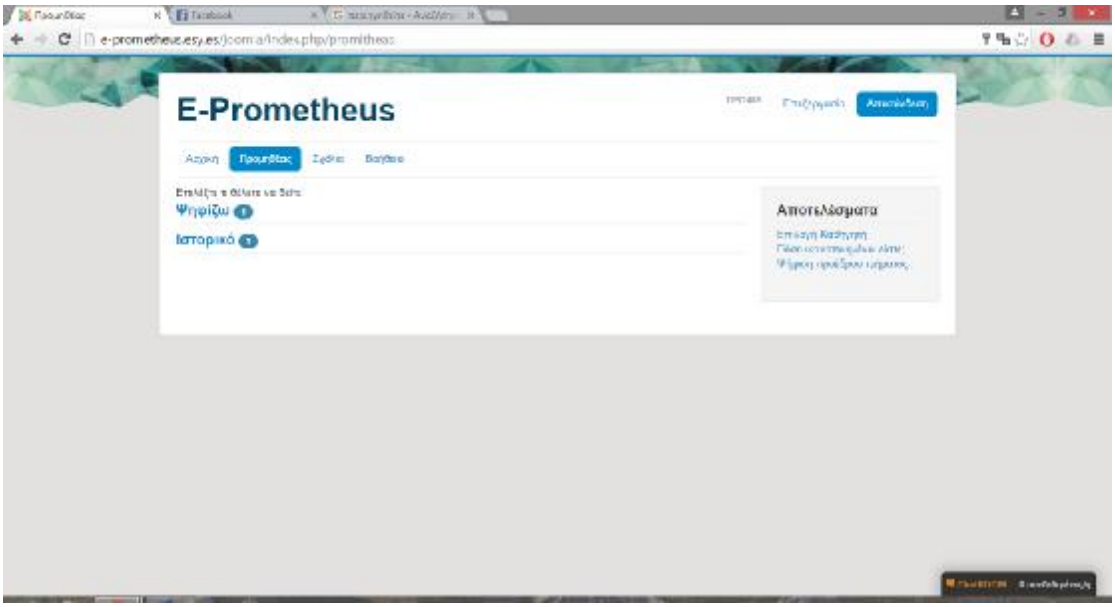
Το **Ευρύ Κοινό** και οι **Καλεσμένοι** δεν έχουν δικαιώματα πάνω στην πλατφόρμα του Προμηθέα.



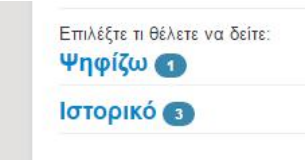
Σελίδα με βάση τα Μέλη της

Από την πλευρά του Χρήστη (π.χ. Μαθητή)

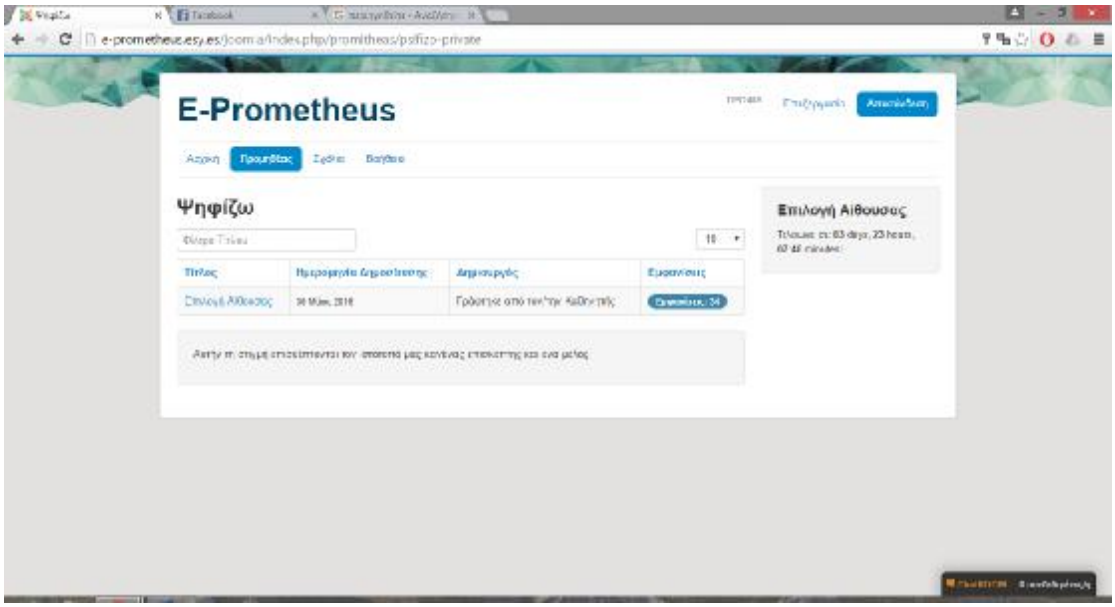
Περιβάλλον εφ' ότου εισαχθεί ο χρήστης με τον λογαριασμό του στην πλατφόρμα.



Στο μενού **Προμηθέας** εμφανίζονται οι εξής επιλογές Ψηφίζω και Ιστορικό όπως και στην εικόνα.

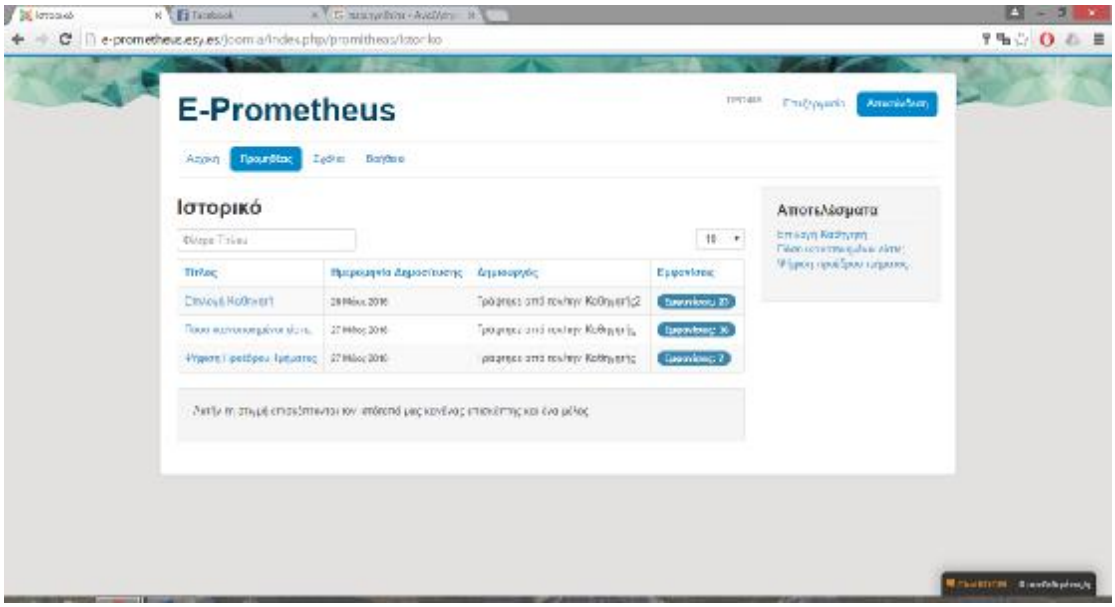


Ανοίγοντας το **Ψηφίζω** ο χρήστης εισέρχεται στις ψηφοφίες που βρίσκονται υπό εξέλιξη.



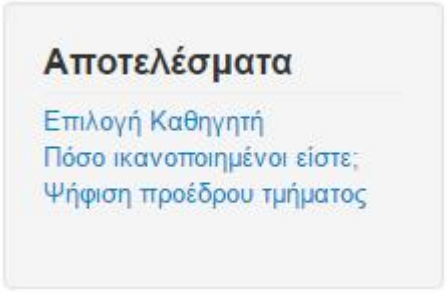
Στα δεξιά της σελίδας Ψηφίζω εμφανίζεται πόσος χρόνος χρειάζεται για την λήξη της αναγράφουσας ψηφοφορίας.

Ανοίγοντας το **Ιστορικό** ο χρήστης εισέρχεται στις ψηφοφορίες που έχουν λήξει.



ΠΡΟΣΟΧΗ!!!
Στο Ιστορικό δεν εμφανίζονται αναγκαστικά οι ψηφοφορίες που έχει συμμετάσχει ο χρήστης. Αλλά εμφανίζονται όλες οι ψηφοφορίες που ανήκουν στο παρελθόν και δεν είναι ενεργές στο παρόν.

Στα δεξιά της σελίδας Ιστορικό εμφανίζονται τα αποτελέσματα των ψηφοφοριών. Επιλέγοντας ανοίγει νέα καρτέλα που μεταβαίνει στα αποτελέσματα. Προϋπόθεση να έχει προκαθορισθεί από το GoogleFormsη εμφάνιση των αποτελεσμάτων. Αν δεν έχει ορισθεί στέλνεται αίτημα προβολής στο κάτοχο της φόρμας.



Από την πλευρά του Δημιουργού Ψηφοφοριών (π.χ. Δασκάλου)

Αφ' ότου γίνει εισαγωγή των στοιχείων του στο σύστημα εμφανίζεται το ίδιο περιβάλλον με αυτήν των χρηστών.

Όμως η διαφορά είναι ότι του δίνεται η ικανότητα να επεξεργαστεί λίγο πολύ το σύστημα όπως:

Την επεξεργασία του τρέχοντος άρθρου(ψηφοφορίας) που έχει συντάξει ο ίδιος. Πατώντας όπως φαίνεται το σχετικό εικονίδιο στην σελίδα.

επιλέγοντας το 

Την δημιουργία νέου άρθρου(ψηφοφορίας) κουμπί Νέο όπως φαίνεται στην εικόνα.

Την δημιουργία νέων module-*ενθεμάτων*. Το κουμπί αυτό που απεικονίζεται  συμβολίζει την επεξεργασία του τρέχοντος module. Όμως έχει αποτραπεί η ικανότητα επεξεργασίας των moduleγια λόγους ασφαλείας από τον διαχειριστή της σελίδας. Με λίγα λόγια εφ' όσον επιλεχθεί το απεικονιζόμενο κουμπί ο δημιουργός θα οδηγηθεί στον πίνακα ελέγχου των module, όπου εκεί μπορεί να δημιουργήσει ένα.

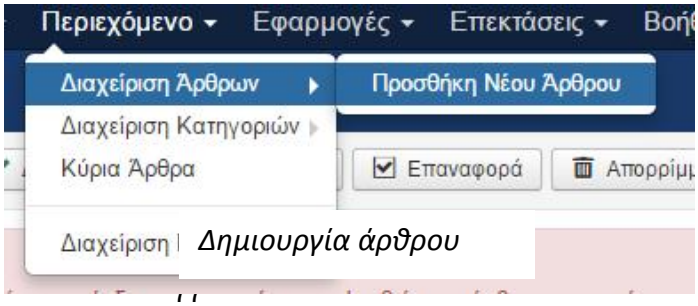
Εισαγωγή φορμών(ψηφοφοριών)

ΒΗΜΑ1:Πρωτού γίνουν όλα πρέπει να ανατρέξουμε στον εκάστοτε κειμενογράφο,TinyMCEστην προκειμένη περίπτωση και να σβήσουμε τον περιορισμό iFrame, αυτό γίνεται για να μας επιτρέψει όταν εισάγουμε iFrame να εμφανίζεται κανονικά και όχι να το εμφανίζει σαν σύνδεσμο ή και καθόλου αντίστοιχα.

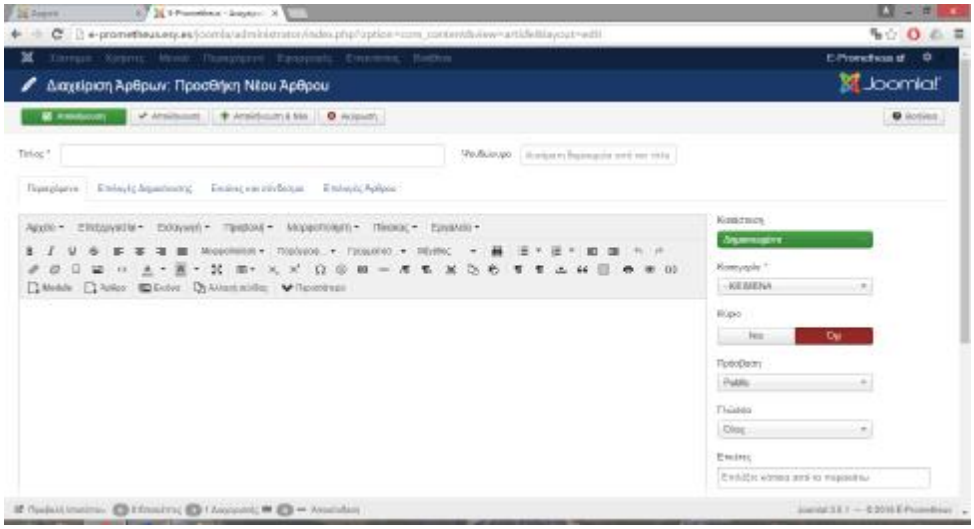
Γίνεται με την δημιουργία ενός νέου άρθρου στην σελίδα. Για να γίνει αυτό πρέπει πρώτα να γίνει η σύνδεση του δημιουργού στον πίνακα ελέγχου του συστήματος e-Prometheus.

ΒΗΜΑ2:Εφόσον εισαχθεί πηγαίνουμε στο μενού όπως φαίνεται στην εικόνα

Περιβάλλον εισόδου στον κεντρικό πίνακα της



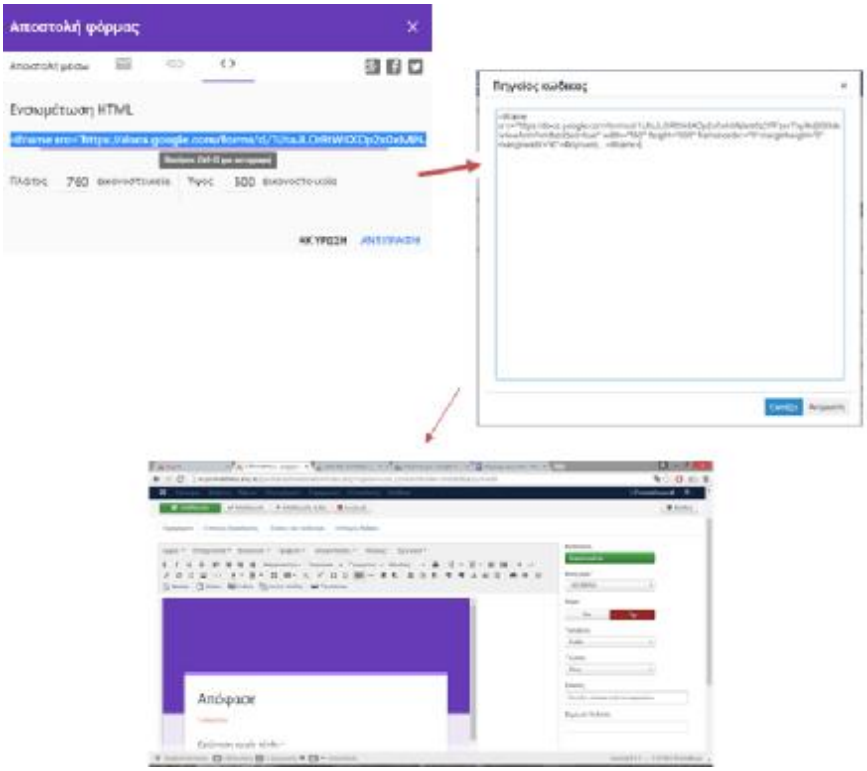
Δημιουργία άρθρου



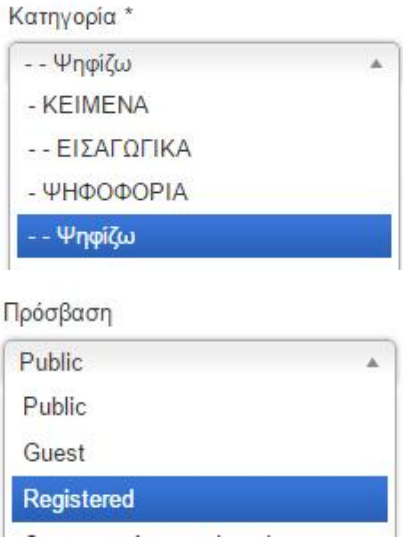
Περιβάλλον δημιουργίας άρθρου

ΒΗΜΑ3:Επιλέγουμε το  εικονίδιο από τον κειμενογράφο όπου κάνουμε επικόλληση την εντολή που έχουμε αντιγράψει από την φόρμα.

Στην συνέχεια εμφανίζεται η φόρμα στον κειμενογράφο.



Πρωτού γίνει η δημοσίευση πρέπει πρώτα να οριστεί ο τίτλος της ψηφοφορίας.



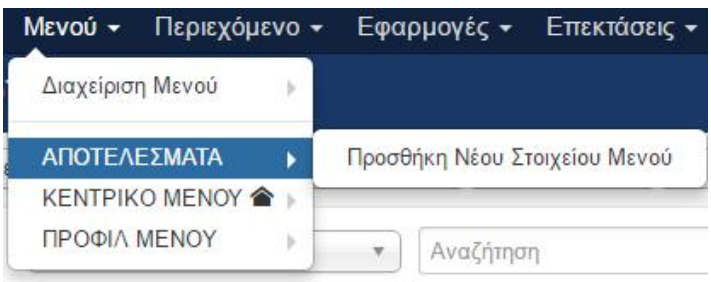
ΒΗΜΑ4:

Δεύτερον να οριστεί η κατηγορία του άρθρου. Δηλαδή ως τρέχων(Ψηφίζω) ή ως λήξαν(Ιστορικό).

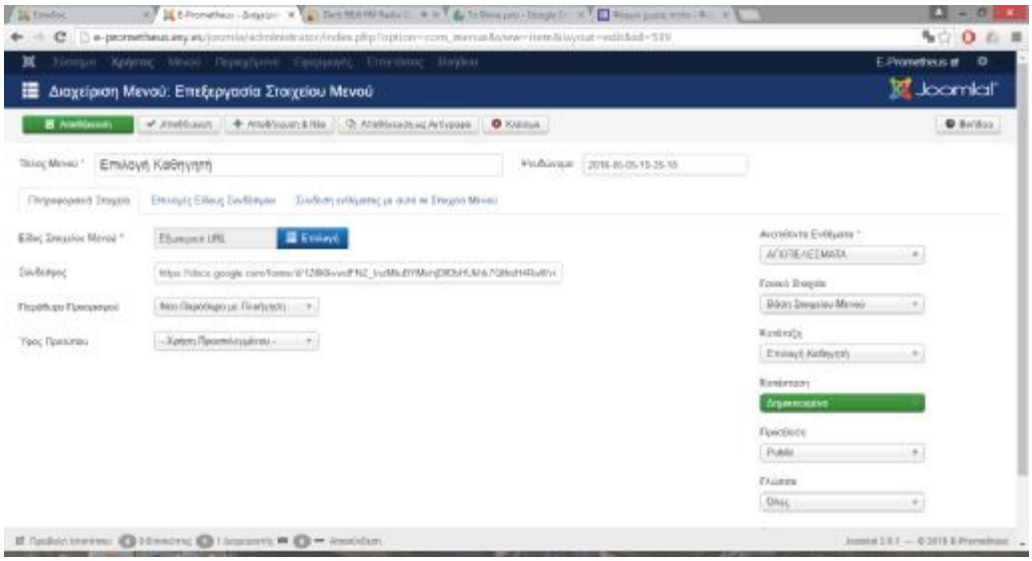
ΒΗΜΑ5:

Τρίτον να οριστεί η ορατότητα του άρθρου σε Registedγια να μην μπορεί να είναι προσβάσιμο μέσω της αναζήτης και όχι μόνο από τους μη χρήστες.Είναι έτοιμο για δημοσίευση.

Προσθήκη Αποτελεσμάτων Ψηφοφορίας



Πάμε στο μενού ΑΠΟΤΕΛΕΣΜΑΤΑ όπου εμφανίζονται τα αποτελέσματα των ψηφοφοριών από εκεί πατάμε το κουμπί Νέο. Έπειτα στο είδος Στοιχείου μενού επιλέγουμε το Εξωτερικό URL όπως είναι ήδη επιλεγμένο και στην εικόνα.



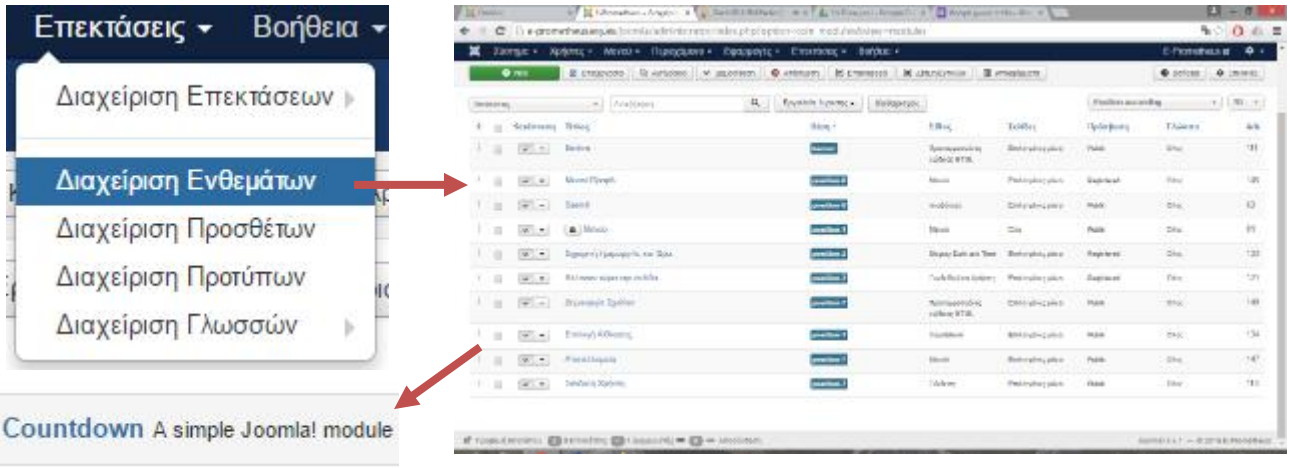
Πρόσθετα

Δημιουργία module Χρόνου

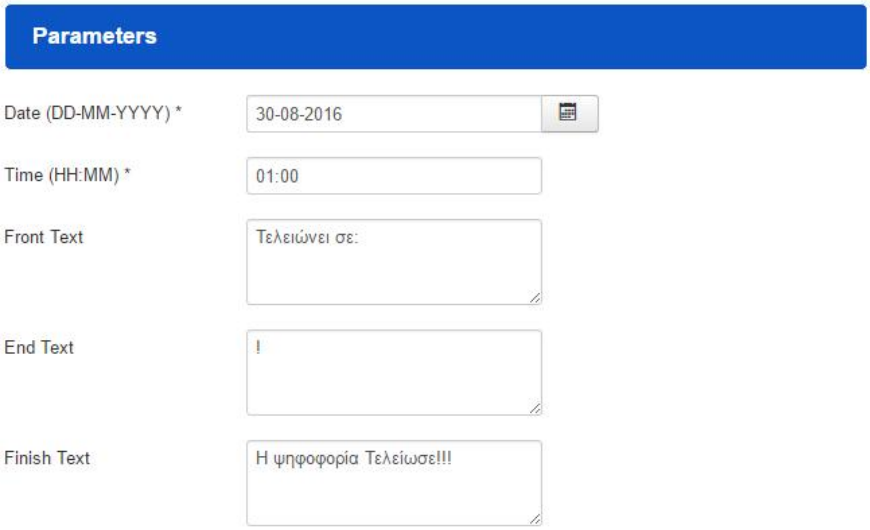
Για την δημιουργία module Χρόνου, εμφάνισης δηλαδή, του εναπομείναντα χρόνου, πάμε όπως φαίνεται στην εικόνα. Από εκεί πατάμε το κουμπί και επιλέγουμε το moduleCountdown.

Εμφανίζεται το 

περιβάλλον του Countdown όπου μπορούμε να κάνουμε πολλές ρυθμίσεις. Παρακάτω φαίνονται το μήνυμα που θα εμφανίζεται πριν και μετά την λήξη της ψηφοφορίας, καθώς και την ακριβή ημέρα και



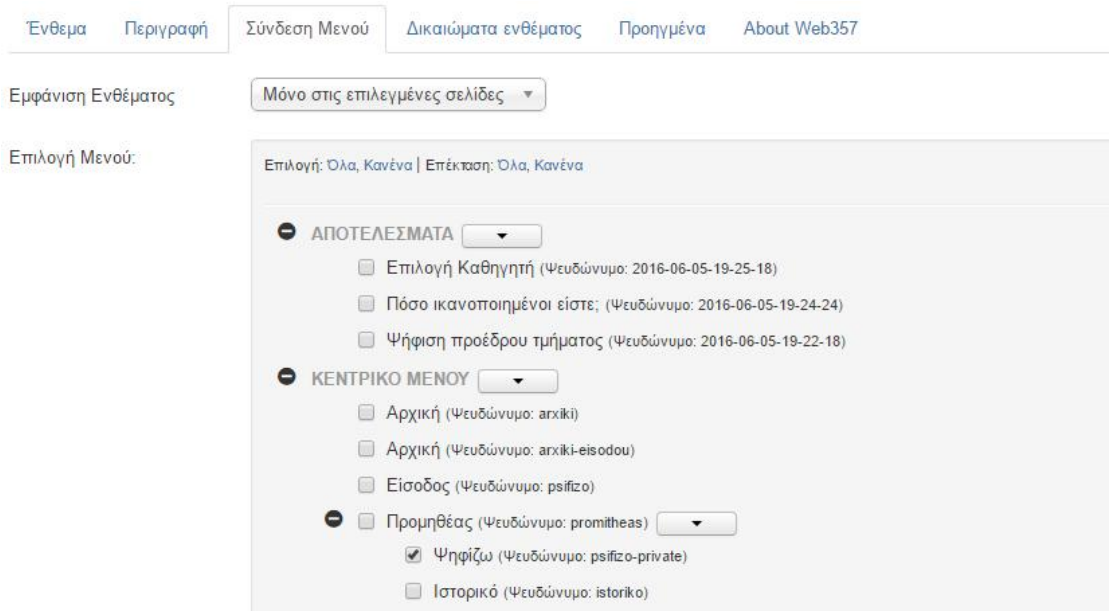
ώρα που θα πάψει να ισχύει.



Ακόμα δύο παράμετροι είναι εκτός από τον τίτλο που πρέπει να οριστεί η θέση που θα εμφανίζεται καθώς και στο ποιες σελίδες.

Συγκεκριμένα έχει επιλεχθεί η θέση position-7, δηλαδή πάνω δεξιά.

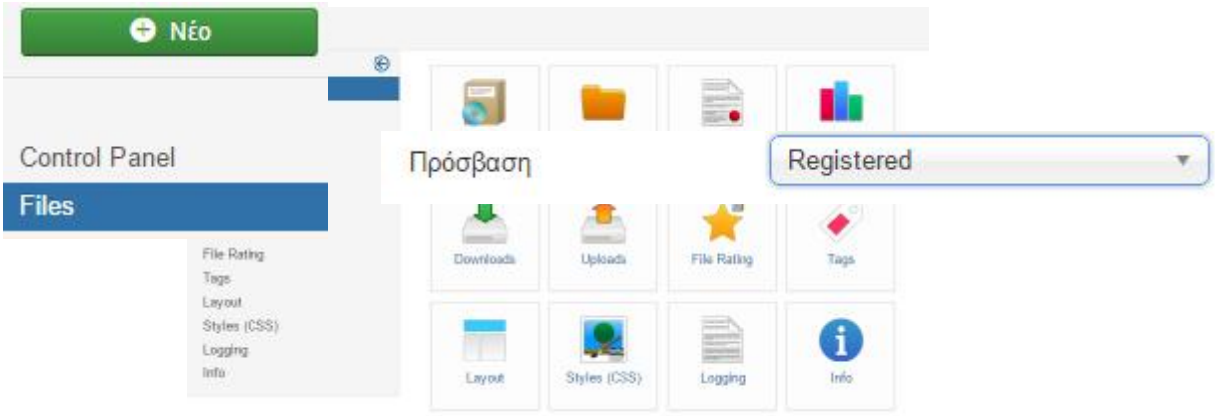
Επιλέγουμε να εμφανίζεται στις επιλεγμένες σελίδες, δηλαδή, την σελίδα Ψηφίζω.



Σαν σύνδεσμο τοποθετούμε το URLπου αντιστοιχεί στα αποτελέσματα της ψηφοφορίας. Η τοποθέτηση του μενού έχει προκαθοριστεί από τον πίνακα ελέγχου module.

PhocaDownload

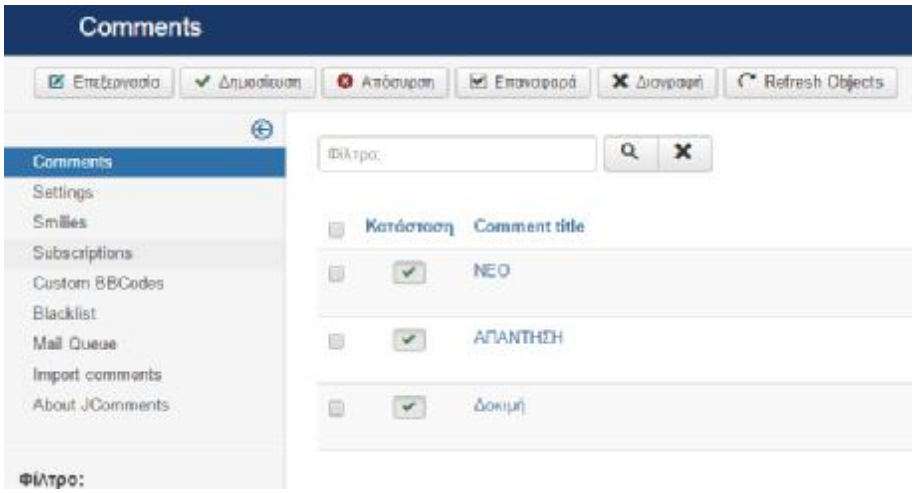
Πρόκειται για ένα πρόσθετο που μας επιτρέπει να ανεβάσουμε αρχεία στην σελίδα, ώστε να είναι προσβάσιμααπό τα μέλη της. Δίνοντάς τους έτσι την δυνατότητα να τα κατεβάσουν στον προσωπικό τους υπολογιστή.



Για την εισαγωγή αρχείων πηγαίνουμε Files>Νέο ορίζουμε το όνομα και τους χρήστες που μπορούν να το δουν και στην συνέχεια όπως φαίνεται παρακάτω στην εικόνα ανεβάζουμε το αρχείο που θέλουμε.

JComments

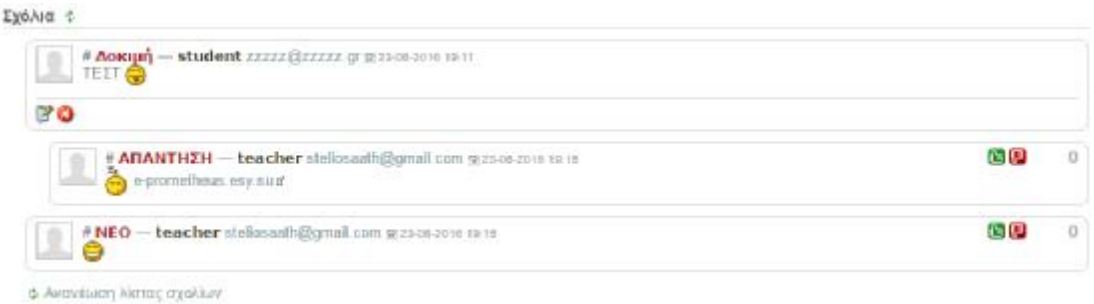
Με αυτό το πρόσθετο δίνει την δυνατότητα στους χρήστες να σχολιάζουν ένα άρθρο. Στην προκειμένη περίπτωση τις Ανακοινώσεις.



3 Σχόλια Εμφανίζεται αυτό το εικονίδιο όπου διακρίνεται πόσα σχόλια έχουν γίνει στο συγκεκριμένο άρθρο.

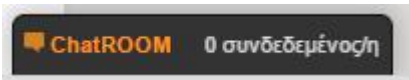
Μορφή υποβολής σχολίου από τον χρήστη.

Παρακάτω παρουσιάζεται μια δοκιμαστική συζήτηση.

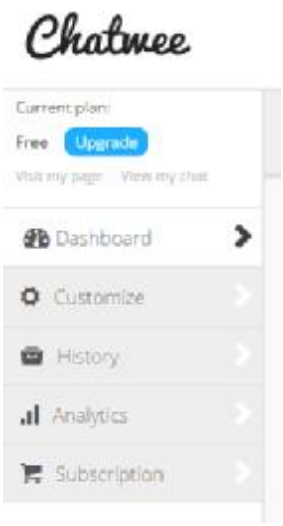


Chatwee

Αποτελεί το πρόσθετο που επιτρέπει την online συνομιλία μεταξύ των μελών.

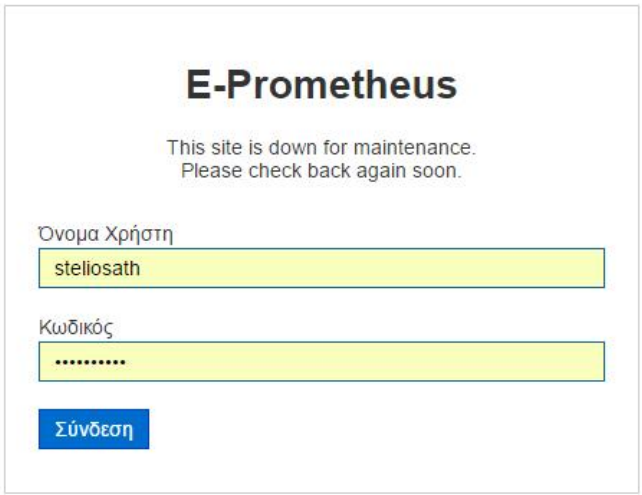


Η διαχείρισή του γίνεται μέσω του συνδέσμου: https://www.chatwee.com/client/script



Στην εικόνα εμφανίζονται οι επιλογές που μας προσφέρει το Chatwee.

Τέλος να αναφέρουμε πως ο Διαχειριστής της σελίδας έχει πλήρη πρόσβαση σε όλες τις λειτουργίες ακόμα και αν το σύστημα έχει οριστεί εκτός διαδικτύου.



Βιβλιογραφία

Σύστημα ψηφοφορίας DRE:
https://en.wikipedia.org/wiki/DRE_voting_machine

Είδη ηλεκτρονικής ψηφοφορίας, Μορφές:
http://www.dimiourgiaxana.gr/el/e-voting/ηλεκτρονικές-ψηφοφορίες-στην-ελλάδα/1684-τι-είναι-η-ηλεκτρονική-ψηφοφορία

Πληροφορίες συστήματος Ζευς:
http://www.dimiourgiaxana.gr/el/e-voting/βασικές-πληροφορίες/το-σύστημα-ζευσ

Απόσπασμα 1εφαρμογήςηλεκτρονικήςψηφοφορίαςστηνβουλή:
http://www.newsit.gr/default.php?pname=Article&art_id=314265&catid=9

Απόσπασμα2 εφαρμογήςηλεκτρονικήςψηφοφορίαςστηνβουλή:
http://www.newsbomb.gr/politikh/news/story/470257/premiera-gia-tin-ilektroniki-psifoforia-sti-voyli

Απόσπασμα Ο Έλληνας που καθιέρωσε την ηλεκτρονική ψηφοφορία στις εκλογές:
http://www.newsbeast.gr/weekend/arthro/1938257/o-ellinas-pou-kathierose-tin-ilektroniki-psifoforia-stis-ekloges

Θεμελιώδεις Απαιτήσεις Ασφάλειας, Διαδικασία Ηλεκτρονικής Ψηφοφορίας, Υπάρχοντα Συστήματα:
https://el.wikipedia.org/wiki/Προστασία_της_ιδιωτικότητας_στην_ηλεκτρονική_ψηφοφορία

Εφαρμογή Ηλεκτρονικής ψηφοφορίας διεθνώς:
http://electionresources.org/europe.html

Θεμελιώδης Αρχές Ασφάλειας:
www.icsd.aegean.gr/website_files/metaptyxiako/215363813.ppt

Τεχνολογικές απειλές:
http://digiservice.gr/Technology_Threats.htm

Απειλές συστήματος ηλεκτρονικής ψηφοφορίας:

www.nist.gov/itl/**vote**/upload/**threat**worksummary.pdf

www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf

Κρυπτογραφία, ορισμοί, είδη, ορισμοί:
https://el.wikipedia.org/wiki/Κρυπτογραφία

Κρυπτογράφηση Συμμετρικού Κλειδιού:
https://el.wikipedia.org/wiki/Κρυπτογράφηση_Συμμετρικού_Κλειδιού

Κρυπτογράφηση Δημόσιου Κλειδιού, Ψηφιακές Υπογραφές:
https://el.wikipedia.org/wiki/Κρυπτογράφηση_Δημόσιου_Κλειδιού

Κρυπτογράφηση συστήματος ηλεκτρονικής ψηφοφορίας:
http://openlife.cc/blogs/2013/january/cryptographic-e-voting-algorithms-general
www0.cs.ucl.ac.uk/staff/J.Groth/**Voting**Scheme.pdf

Google Drive:
https://el.wikipedia.org/wiki/Google_Drive