



Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών
Συστημάτων

Διπλωματική Εργασία

Διδάσκων: Κορμέντζας Γεώργιος

Συστήματα ηλεκτρονικής ψηφοφορίας

<3232017029> Ζευγαδίνας Ιωάννης

Σάμος, 30 Ιανουαρίου, 2021



Περίληψη

Σήμερα οι υπηρεσίες ηλεκτρονικής διακυβέρνησης γίνονται ολοένα και πιο δημοφιλείς στο ευρύ κοινό. Η παρούσα εργασία πραγματεύεται το αντικείμενο της ηλεκτρονικής διακυβέρνησης, αποσαφηνίζοντας τις βασικές έννοιες της ηλεκτρονικής κυβέρνησης, διακυβέρνησης και δημοκρατίας καθώς και τις αλληλεπιδράσεις τους. Επίσης, περιγράφονται οι διαθέσιμες υπηρεσίες ηλεκτρονικής διακυβέρνησης για τους πολίτες και τις επιχειρήσεις καθώς και τα πλεονεκτήματά τους.

Η ηλεκτρονική διακυβέρνηση έχει υιοθετηθεί από αρκετά κράτη ανά τον κόσμο και είναι έτσι παρακάτω αναλύονται τα απαιτούμενα για την ηλεκτρονική διακυβέρνηση σύμφωνα με την διεθνή εμπειρία διαβατηρίων. Η μελέτη αυτών των συστημάτων κλείνει με τον σχεδιασμό, ανάλυση και υλοποίηση εφαρμογή ηλεκτρονικής ψηφοφορίας.



Abstract

Today, e-government services are becoming more and more popular with the general public. This paper deals with the subject of e-government, clarifying the basic concepts of e-government, governance and democracy as well as their interactions. It also describes the e-government services available to citizens and businesses as well as their benefits. E-government has been adopted by several countries around the world and so below are the requirements for e-government in accordance with international passports experience. The study of these systems closes with the design, analysis and implementation of an electronic voting application.



Περιεχόμενα

Περίληψη	2
Abstract	3
1 Θεωρητική ανασκόπηση	7
1.1 Ηλεκτρονική ψηφοφορία	7
1.2 Ιστορική αναδρομή - Προηγούμενες προσπάθειες	7
1.3 Πλεονεκτήματα και στόχοι συστημάτων ηλεκτρονικής ψηφοφορίας	11
1.4 Προβλήματα	12
1.5 Υπάρχοντα συστήματα	17
1.6 Sensus: A Security-Conscious Electronic Polling System for the Internet... ..	17
1.7 Το σύστημα E-Vox	18
1.8 Το απόλυτο σύστημα ψηφοφορίας “Direct Recording Election”	19
1.9 InfoPoll Software	20
1.10 Pericles (MIT)	21
1.11 Το ηλεκτρονικό σύστημα ψηφοφορίας της Ιταλικής Ακαδημαϊκής Κοινότητας	21
1.12 TrueBallot, Inc. Democratic Governance Systems	22
1.13 Vivarto Voting Systems	22
1.14 Περιπτώσεις εφαρμογής της ηλεκτρονικής ψηφοφορίας στο εξωτερικό ..	22
1.14.1 Η εμπειρία της Αυστραλίας	22
1.14.2 Το παράδειγμα της Ελβετίας	24
1.14.3 Το παράδειγμα της Εσθονίας	26
1.14.4 Η εμπειρία της Αμερικής	27
2 Τεχνολογίες και Εργαλεία που χρησιμοποιήσαμε	30
2.1 Javascript	30
2.1.1 HTML	31



2.2	PHP.....	32
2.3	CSS.....	34
2.4	SQL	34
2.5	MySQL.....	36
2.6	APACHE.....	37
2.7	JSON	39
2.8	MVC.....	40
2.9	Laravel.....	41
2.10	XAMPP	42
2.11	REST	43
3	Αρχιτεκτονική του συστήματός μας	45
3.1	Τεχνικές απαιτήσεις	45
3.2	Γενικές Απαιτήσεις Συστημάτων Ηλεκτρονικής Ψηφοφορίας.....	46
3.3	Απαιτήσεις Ασφάλειας.....	47
3.4	Ιδιότητες Συστήματος (System Properties).....	50
3.5	Επιμέρους ζητήματα ηλεκτρονικής ψηφοφορίας με χρήση Διαδικτύου	52
3.5.1	Απαιτήσεις σε υλικό	52
3.5.2	Απαιτήσεις σε λογισμικό	53
3.5.3	Απαιτήσεις διασύνδεσης υπολογιστικών συστημάτων	53
4	Νομικό Πλαίσιο της Ηλεκτρονικής Ψηφοφορίας.....	55
4.1	Η Σύσταση (2004) 11 του Συμβουλίου της Ευρώπης.....	55
4.2	Νομικά Πρότυπα	57
4.3	Λειτουργικά Πρότυπα	63
4.4	Τεχνικά Πρότυπα: Το Σύστημα OASIS — EML	64
5	Συμπεράσματα	67
5.1	Προτάσεις για περαιτέρω εργασία	70



6	Βιβλιογραφία	73
7	Παράρτημα.....	78
7.1	Διάγραμμα ER.....	78
7.2	Migrations	79
7.2.1	Για τον πίνακα χρηστών.....	79
7.2.2	Για τον πίνακα ψηφοφοριών.....	80
7.2.3	Πίνακας ψηφοφοριών και χρηστών	81
7.3	Seeders	82
7.3.1	Για τον πίνακα των χρηστών	82
7.3.2	Για τον πίνακα ψηφοφοριών.....	83
7.3.3	Για τον πίνακα ψηφοφοριών - χρηστών.....	85



1 Θεωρητική ανασκόπηση

1.1 Ηλεκτρονική ψηφοφορία

Στη σημερινή εποχή των υπολογιστών και της τεχνολογίας της πληροφορίας εμφανίζεται πλέον ως αναγκαιότητα η λεγόμενη ηλεκτρονική δημοκρατία (e-democracy) με βασικό τμήμα της την ηλεκτρονική ψηφοφορία (e-voting), η οποία αναφέρεται στη χρήση υπολογιστών ή εν γένει υπολογιστικού εξοπλισμού στη διαδικασία της ψηφοφορίας. Ως σύστημα ηλεκτρονικής ψηφοφορίας (electronic voting system) ορίζεται το σύστημα ψηφοφορίας, στο οποίο τα εκλογικά δεδομένα καταγράφονται, αποθηκεύονται και υπόκεινται σε επεξεργασία πρωτίστως ως ψηφιακή πληροφορία. (Neumann, 2014)

Μια τέτοια διαδικασία ωστόσο υπόκειται εγγενώς σε λάθη και όπως έχει αποδειχθεί ιστορικά, σε διαστρέβλωση και απάτη. Απαιτεί συνεπώς εξαιρετική ακεραιότητα (ιδιαίτερα όταν μιλάμε για χρήση υπολογιστικών συστημάτων), όπως επίσης εντιμότητα και εμπειρία των εμπλεκομένων στην οργάνωση και διεξαγωγή των εκλογών ατόμων. Μπορεί επίσης να απαιτεί και ένα minimum δεξιοτήτων από την πλευρά των ψηφοφόρων. Υπό αυτό το πρίσμα λοιπόν, η ψηφοφορία αποτελεί αντιπροσωπευτικό παράδειγμα ενός από άκρο σε άκρο (end- to-end) προβλήματος ασφάλειας: από την καταχώρηση και πιστοποίηση των ψηφοφόρων έως την καθεαυτό ψηφοφορία και καταμέτρηση των αποτελεσμάτων, ενώ περικλείει ένα ευρύ φάσμα τεχνολογικών και κοινωνικών προβλημάτων, που πρέπει να ληφθούν υπόψη. Λόγω της ραγδαίας ανάπτυξης των τεχνολογιών υπολογιστών και των εξελίξεων στην κρυπτογραφία παρουσιάζεται η ηλεκτρονική ψηφοφορία ως εφαρμόσιμη εναλλακτική από τη μία, από την άλλη όμως οι υψηλές απαιτήσεις ασφαλείας εξακολουθούν να την καθιστούν ένα από τα μεγαλύτερα προβλήματα προς επίλυση, κάτι που απαιτεί τη συνεργασία ειδικών σε διάφορους τομείς, όπως λογισμικό, κρυπτογραφία, πολιτική, νομικές, οικονομικές και πολιτικές επιστήμες. (Cetinkaya, 2007)

1.2 Ιστορική αναδρομή - Προηγούμενες προσπάθειες

Από νωρίς άρχισαν να αναζητούνται τρόποι ψηφοφορίας, που δε βασίζονταν στα παραδοσιακά ψηφοδέλτια (paper-ballots), αλλά συνέχιζαν να βασίζονται στο



χαρτί (paper-based). Στις αρχές της δεκαετίας του '60 άρχισε να υιοθετείται η χρήση διάτρητων καρτών (punch cards), η οποία διαδόθηκε αρκετά μέχρι τα τέλη της ίδιας δεκαετίας.

Χρησιμοποιήθηκαν σε δύο μορφές: Votomatic και Datavote, εγκαταλείφθηκαν όμως ύστερα από προβλήματα που παρατηρήθηκαν στις προεδρικές εκλογές της Florida USA το 2000. Παράλληλα χρησιμοποιήθηκε από το 1962 και μέχρι το 2000 περίπου αντί για διάτρητες κάρτες και ένα είδος «οπτικών» ψηφοδελτίων (optical mark-sense ballots) τα οποία στη συνέχεια «σαρώνονταν». Πρέπει, τέλος, να αναφερθεί ότι σε όλο τον 20ό αιώνα, ιδίως μέχρι το 1960, ιδιαίτερα διαδεδομένος ήταν και ο μηχανικός τρόπος ψηφοφορίας (paperless voting), με τη βοήθεια μιας μηχανολογικής εγκατάστασης με μοχλό (mechanical-lever machines). Και αυτός όμως αποδείχτηκε μάλλον ανακριβής, ενώ είχε και το επιπρόσθετο μειονέκτημα ότι δεν διατηρούσε κανενός είδους φυσικό αρχείο ψήφων. Η χρήση τεχνολογιών ηλεκτρονικής ψηφοφορίας επαναοργανώνει την παραδοσιακή εκλογική διαδικασία. Το χάρτινο ψηφοδέλτιο αντικαθίσταται από το ηλεκτρονικό-ψηφιακό. (Evans, 2014)

Τα τοπικά συστήματα ηλεκτρονικής ψηφοφορίας (direct recording electronic (DRE) voting systems) αποτελούν το ηλεκτρονικό ισοδύναμο των mechanical-lever machines και είναι τα μόνα ηλεκτρονικά εκλογικά συστήματα που περιλαμβάνουν εκλογικά κέντρα. Σε όλα τα υπόλοιπα (internet-based), όλες οι διαδικασίες λαμβάνουν χώρα από απόσταση.

Η πρώτη DRE μηχανή ψηφοφορίας (voting machine) χρησιμοποιήθηκε σε πραγματικές εκλογές το 1975 στο Streamwood και Woodstock Illinois. Ήδη όμως από το 1964 είχαν χρησιμοποιηθεί υπολογιστές σε δύο επαρχίες της Georgia στις Η.Π.Α. (Douglas, 2016)

Το 1990 εκδόθηκαν τα πρώτα προαιρετικά VSS (Voting System Standards) από το Federal Election Commission (FEC) Office of Elections Administration (OEA), που πλέον είναι ενσωματωμένη στην Election Assistance Commission (EAC), σύμφωνα με τα οποία στο εξής θα πιστοποιούνταν από τη National Association of State Election Directors (NASD) στα διάφορα από την ίδια εξουσιοδοτημένα ITAs (Independent Testing Authorities) τα εκάστοτε συστήματα ψηφοφορίας, τόσο ως προς το hardware όσο και ως προς το software. Τα συγκεκριμένα standards



αναθεωρήθηκαν και έδωσαν τα 2002 VSS, που ισχύουν μέχρι σήμερα. Τον Δεκέμβρη του 2005 η EAC ομόφωνα υιοθέτησε τα 2005 VSS, που αυξάνουν σημαντικά τις απαιτήσεις ασφάλειας και διευρύνουν την προσβασιμότητα, προσφέροντας περισσότερες δυνατότητες σε άτομα με ποικίλες «ανικανότητες». Θα τεθούν σε ισχύ το Δεκέμβρη του 2007, αντικαθιστώντας τα VSS 2002. (Deutsch and Berger 2014)

Παράλληλα ξεκίνησε το 2001 και από την IEEE το project P1583, που αποτελεί το πρώτο standard για εξοπλισμό ψηφοφορίας που αναπτύχθηκε σε ανοιχτή συναινετική διαδικασία σύμφωνα με τους κανόνες ANSI (American National Standards Institute).

Από τη στιγμή ωστόσο που δημιουργήθηκε η EAC από τη HAVA (Help America Vote Act) θα είναι αυτή υπεύθυνη για την έκδοση standards μέσω του National Institute of Standards and Technology (NIST). (Deutsch and Berger 2014)

Η Βραζιλία το 2000 ήταν η πρώτη χώρα που χρησιμοποίησε σύστημα ψηφοφορίας πλήρως βασισμένο σε υπολογιστές. Η Georgia ήταν επίσης η πρώτη πολιτεία στις Η.Π.Α. που υιοθέτησε εξολοκλήρου μια ενιαία DRE τεχνολογία για ψηφοφορία το 2002. Σε σύγκριση με το 2000, οπότε χρησιμοποιήθηκαν διάφοροι τύποι ψηφοφορίας, το ποσοστό των undervotes (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. (Brit, 2014)

Ένα πείραμα που αξίζει να αναφερθεί σ' αυτά τα πλαίσια είναι το πιλοτικό Internet-based σύστημα ψηφοφορίας SERVE (Secure Electronic Registration and Voting Experiment), που αναπτύχθηκε για το FVAP (Federal Voting Assistance Program) του Υπουργείου Άμυνας των Η.Π.Α. Σχεδιάστηκε με σκοπό να εφαρμοστεί στις εκλογές του 2014, ώστε να επιτρέψει στους εν δυνάμει ψηφοφόρους αρχικά να εγγραφούν στους εκλογικούς καταλόγους της περιοχής τους και στη συνέχεια να ψηφίσουν ηλεκτρονικά μέσω Internet απ' οπουδήποτε στον κόσμο.

Στο πείραμα θα μπορούσαν να συμμετάσχουν εγγεγραμμένοι ψηφοφόροι που βρίσκονταν εκτός συνόρων, οι στρατιωτικοί και οι ψηφοφόροι 50 επαρχιών σε 7 πολιτείες. Η εφαρμογή αυτού του προγράμματος θα χρησίμευε σαν πρότυπο για



γενικευμένη χρήση ηλεκτρονικής ψηφοφορίας στο μέλλον. Οι ερευνητές, βέβαια, προειδοποίησαν για ενδεχόμενα κενά του συστήματος και τελικά δεν εφαρμόστηκε με την αρχική του μορφή στις εκλογές του 2014.

Αλλά και η εφαρμογή του συστήματος ηλεκτρονικής ψηφοφορίας του 2000 δεν έφερε καλύτερα αποτελέσματα. Αξιοσημείωτο είναι το γεγονός ότι στη Florida εμφανίστηκαν ακόμα μεγαλύτερα προβλήματα από τις εκλογές του 2000. Για παράδειγμα σε κάποιες περιπτώσεις το σύστημα κατέρρευσε και είτε χάθηκαν χιλιάδες ψήφων, είτε χρειάστηκε προσφυγή στα κλασικά ψηφοδέλτια (paper ballots) (Jefferson, 2014)

Μια άλλη αντίστοιχη προσπάθεια έγινε και στο 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 μεγαλύτερη προσέλευση. Η παραδοσιακή εκλογική διαδικασία είτε συμπληρώθηκε είτε αντικαταστάθηκαν τμήματά της από ηλεκτρονικές διεργασίες. Οι τεχνολογίες που χρησιμοποιήθηκαν ήταν: Internet voting, telephone voting, Direct Recording e-voting machines (DRE) / Kiosk voting, SMS text message voting, Interactive Digital Television voting. Η προσπάθεια συντονίστηκε από κοινού από την κεντρική διοίκηση (Office of the Deputy Prime Minister) και τις τοπικές αρχές (Local Public Authorities (PAs)). Οι ανεπάρκειες του συστήματος, που θα αποτελέσουν σημαντική βοήθεια για το μέλλον, εντοπίστηκαν κυρίως σε θέματα οργανωτικά, εσωτερικής επικοινωνίας και συνεργασίας των συντελεστών-συνιστωσών της διαδικασίας, μικρής ευελιξίας και δυνατότητας ελέγχου, εξάρτησης από τους εμπορικούς προμηθευτές. Φάνηκε επίσης 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 (UK Electoral Commission, 2002), (Xenakis, 2016)

Ηλεκτρονική ψηφοφορία εφαρμόστηκε επίσης στις δημοτικές εκλογές της Εσθονίας τον Οκτώβρη του 2005, όταν για πρώτη φορά το εκλογικό σώμα μιας ολόκληρης χώρας είχε τη δυνατότητα να ψηφίσει μέσω Internet. Εξαιτίας του γεγονότος ότι για πρώτη φορά εφαρμόστηκε κάτι τέτοιο και οι «ηλεκτρονικοί» ψηφοφόροι ήταν



σχετικά λίγοι, δεν μπορούμε να εξάγουμε απολύτως ασφαλή συμπεράσματα. Ωστόσο η διαδικασία κρίθηκε σε γενικές γραμμές επιτυχής, γι αυτό και χρησιμοποιήθηκε και στις βουλευτικές εκλογές του 2007 στην ίδια χώρα. (Trechsel 2005)

Στη Γαλλία χρησιμοποιήθηκε για πρώτη φορά το σύστημα ηλεκτρονικής ψηφοφορίας το 2003 από Γάλλους πολίτες που ζούσαν στις Η.Π.Α. για τις εκλογές της Ένωσης Γάλλων Πολιτών Εξωτερικού, με συμμετοχή πάνω από 60%. Από την άλλη, η πιλοτική χρήση e-voting τεχνολογίας στις προεδρικές εκλογές του 2007 σε 82 τοποθεσίες προκάλεσε ποικίλα προβλήματα, όπως μεγάλες ουρές, κατάρρευση συστημάτων και δυσκολία εξοικείωσης των ψηφοφόρων. (Wikipedia, 2017)

Κατά καιρούς επιχειρήθηκε εφαρμογή τέτοιων συστημάτων, σε πιο περιορισμένη κλίμακα βέβαια, και σε άλλες χώρες όπως Αυστραλία, Βέλγιο, Βραζιλία, Καναδά, Γερμανία., Ιρλανδία, Ιταλία, Ολλανδία, Ινδία, Νορβηγία, Ρουμανία κι Ελβετία. (Matos Penha-Lopes, 2016)

Αξιίζει σε αυτό το σημείο να αναφέρουμε, ότι οι ειδικοί προβλέπουν 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.

1.3 Πλεονεκτήματα και στόχοι συστημάτων ηλεκτρονικής ψηφοφορίας

Τα εκλογικά συστήματα Internet και DRE έχουν κάποια έμφυτα πλεονεκτήματα σε σχέση με τα παραδοσιακά συστήματα ψηφοφορίας, συμπεριλαμβανομένης της μείωσης του λάθους του ψηφοφόρου. Αν η διεπαφή χρήστη (interface) του συστήματος είναι κατάλληλα σχεδιασμένη, για παράδειγμα, ειδοποιεί για ενδεχόμενη παράλειψη ψήφου ή και για μη έγκυρη ψηφοφορία. Από την άλλη καθίσταται δυνατή η εξυπηρέτηση ψηφοφόρων με ποικίλες αδυναμίες ή ειδικές



ανάγκες, χωρίς να είναι απαραίτητη η ανθρώπινη βοήθεια και κατ' επέκταση μειώνεται η πιθανότητα ανθρώπινης παρέμβασης. Άλλοι παράγοντες που καθιστούν αναγκαία τα συστήματα ηλεκτρονικής ψηφοφορίας και πιθανά οφέλη που πρέπει να ληφθούν υπόψη είναι τα εξής:

- η αυξημένη προσέλευση-συμμετοχή ψηφοφόρων και μείωση της αποχής και η προώθηση με αυτό τον τρόπο της δημοκρατικής διαδικασίας,
- μια νέα δυναμική και νέες δυνατότητες για τις εκλογές (παρέχοντας ψηφοδέλτια σε διάφορες γλώσσες, υποστηρίζοντας μακροσκελή ψηφοδέλτια κλπ),
- το άνοιγμα μιας νέας αγοράς, με συνακόλουθες συνέπειες για το εμπόριο και την απασχόληση,
- η σαφής διευκόλυνση του ψηφοφόρου,
- ο περιορισμός της επέμβασης του ανθρώπινου παράγοντα και συνεπώς της δυνατότητας για νοθεία,
- 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. (Bannet 2014)

1.4 Προβλήματα

Θα πρέπει εδώ να αναφέρουμε ότι υπάρχουν δύο βασικά είδη Internet voting: Polling place (εκλογικό κέντρο) Internet voting και remote (απομακρυσμένο) Internet voting, με το δεύτερο να είναι πολύ πιο ευάλωτο σε εξαπάτηση του ψηφοφόρου, να θέτει σε κίνδυνο το ιδιωτικό απόρρητο και το δικαίωμα της μυστικής ψηφοφορίας, οδηγώντας πιθανώς σε πολιτικό εξαναγκασμό, για παράδειγμα στους χώρους εργασίας ή στο στενό οικογενειακό περιβάλλον. Στο remote electronic voting, οι ψηφοφόροι ψηφίζουν μέσω internet, κυρίως μέσω ενός web browser, από το σπίτι ή από οποιαδήποτε άλλη τοποθεσία, στην οποία υπάρχει πρόσβαση στο internet. (Gritzalis 2002)



Παρόλη τη διάχυτη αισιοδοξία και τις προοπτικές που ανοίγονται, έχει αποδειχθεί τόσο θεωρητικά όσο και στην πράξη, ότι τα συστήματα ηλεκτρονικής ψηφοφορίας που έχουν αναπτυχθεί μέχρι τώρα εμφανίζουν σημαντικά κενά ασφάλειας και κάνουν την εκλογική απάτη πρωτοφανώς απλή.

- Μια εντυπωσιακή στα αποτελέσματά της έρευνα έδειξε ότι σε μεγάλης κλίμακας εκλογές ακόμα και η αλλαγή μιας μόνο ψήφου ανά μηχανήμα είναι ικανή να ανατρέψει το αποτέλεσμα, ενώ μεγαλύτερες αλλαγές επιτυγχάνουν και τα επιθυμητά περιθώρια. Γενικά, μια απειροελάχιστη αλλαγή στο λογισμικό του μηχανήματος αρκεί. Τα πράγματα διευκολύνονται ακόμα περισσότερο, αν πολλές μηχανές τρέχουν το ίδιο λογισμικό. Επιπλέον αξίζει να σημειωθεί ότι τόσο μικρές αλλαγές μπορούν πιθανότατα να μην εντοπιστούν καθόλου, να ερμηνευθούν ως τυχαίος θόρυβος ή να καλυφθούν από λοιπούς θορύβους του συστήματος, ή ακόμα να υποτιμηθεί η σημασία τους μακροσκοπικά και να μην καταμετρηθούν ξανά οι αντίστοιχοι ψήφοι (recount). (Di Franco 2014)

- Ένα επιπλέον σημείο είναι ότι, παρόλο που μετριάζεται η επίδραση του ανθρώπινου παράγοντα, απαιτείται προστασία πλέον όχι μόνο από λάθη και την κακόβουλη δράση ψηφοφόρων και υπευθύνων της εκλογικής διαδικασίας αλλά και από εσκεμμένα ή μη ολισθήματα των αρμόδιων προγραμματιστών, τεχνικών και system administrators. (Jones 2014)

- Επιπρόσθετα αναφέρουμε ότι συστήματα ψηφοφορίας όπως το ηλεκτρονικό, που δεν παράγουν κάποιου είδους φυσικό αρχείο, δημιουργούν θέμα εμπιστοσύνης στο σύστημα, εφόσον χάνεται η δυνατότητα διαφανούς επαλήθευσης. Όλα λοιπόν εξαρτώνται από το αν οι μηχανές λειτουργούν σωστά, οπότε η εμπιστοσύνη ή μη μεταπίπτει στον κατασκευαστή και στα άτομα που τις συντηρούν και τις χειρίζονται. Από την άλλη, η καταγραφή και φύλαξη των ψήφων σε κάποιου είδους φυσικό αρχείο, που είναι απαραίτητες αφενός για την πιστοποίηση και άρα για τον εντοπισμό λάθους ή απάτης, συγκρούονται αφετέρου με τη απαιτούμενη μυστικότητα της ψήφου. Για το τελευταίο βέβαια έχουν γίνει διάφορες προτάσεις, όπως θα δούμε παρακάτω.

- Περαιτέρω προβλήματα εμφανίζονται και στο νομικό πεδίο. Οι κανόνες και οι νόμοι των εκλογικών διαδικασιών βασίζονται παραδοσιακά στην υπόθεση των



«υλικών» ψηφοδελτίων, οπότε απαιτείται η αμοιβαία προσαρμογή του κώδικα του νόμου και του προγραμματιστικού κώδικα, ώστε στη συγκεκριμένη περίπτωση η χρήση της τεχνολογίας να διασφαλίζει ουσιαστικά τη δημοκρατία. (Mercuri, 2014)

- Παρ' όλες τις προφυλάξεις, έχουν παρατηρηθεί διάφορες επιπλοκές και παραλείψεις στην πράξη, όπως:

- ο ψηφοφόροι μπορούν να ψηφίσουν περισσότερες από μία φορές, χωρίς αυτό να μπορεί να ανιχνευθεί,
- ο ένα ενδεχόμενο κύμα ψηφοφόρων, είτε τις πρώτες ώρες της ψηφοφορίας (πολλοί είναι αυτοί που θέλουν να είναι οι πρώτοι που ψηφίζουν online) είτε λίγο πριν κλείσουν οι ηλεκτρονικές κάλπες καθιστά εξαιρετικά πιθανή την κατάρρευση του συστήματος και πρέπει να έχουν προβλεφθεί εκ των προτέρων σχετικά μέτρα αντιμετώπισης -οποιοσδήποτε με πρόσβαση στις μηχανές μπορεί να εκτελέσει διαχειριστικές λειτουργίες, όπως να δει προσωρινά αποτελέσματα ή να διακόψει νωρίτερα την ψηφοφορία,
- ο έχουν παρουσιαστεί σοβαρά προβλήματα σε ψηφοφόρους με παλαιότερους browsers και σε ψηφοφόρους που χρησιμοποιούν Macintosh,
- ο η διαδικασία διανομής εκατοντάδων χιλιάδων ψηφιακών πιστοποιητικών για τις ηλεκτρονικές υπογραφές στους εγγεγραμμένους ψηφοφόρους δεν έχει τελειοποιηθεί ακόμα, με αποτέλεσμα να δημιουργούνται επιπρόσθετα κενά ασφάλειας,
- ο η επικοινωνία μεταξύ τερματικών και κεντρικού εξυπηρετητή δεν κρυπτογραφούνται επαρκώς, αφήνοντας «τρύπα» για ενδιάμεση κακόβουλη επέμβαση. (Mohen and Glidden, 2001)

- Δυσκολίες στην αξιολόγηση των εκάστοτε τεχνολογιών δημιουργεί και η closed-source προσέγγιση που επικρατεί μέχρι τώρα. (Bannet 2014)

- Την παρακολούθηση της διαδικασίας και την καταμέτρηση των ψήφων αναλαμβάνει ένας «αντικειμενικός παρατηρητής». Αυτός συνήθως είναι μία εταιρεία, όμως τόσο το ποιος την διοικεί όσο και οι πολιτικές του πεποιθήσεις σπάνια είναι γνωστά, με αποτέλεσμα αυτή η αντικειμενικότητα συχνά να αμφισβητείται.



Σε ό,τι αφορά τις πιθανές επιθέσεις (hacks) θα πρέπει γενικά να έχουμε υπόψιν μας, ότι η παραγωγή λογισμικού απαλλαγμένου από κάθε κενό ασφάλειας είναι σημαντικά δυσκολότερη από το σκοπό του επιτιθέμενου: να βρει και να εκμεταλλευτεί ένα και μοναδικό bug. Οι πιο συνήθεις απειλές για συστήματα ηλεκτρονικής ψηφοφορίας, που έχουν εντοπιστεί μέχρι σήμερα, καταγράφονται συνοπτικά στον παρακάτω πίνακα.



Πίνακας 1: Ο πίνακας περιγράφει, για κάθε πιθανή απειλή των συστημάτων ηλεκτρονικής ψηφοφορίας, τις ικανότητες απαιτούνται από τον εισβολέα, ποιες είναι οι συνέπειες μιας επιτυχημένης τελικά επίθεσης, πόσο πιθανό είναι να παρουσιαστεί η καθεμία και με ποιον τρόπο μπορεί να αντιμετωπιστεί. Πηγή: Jefferson, 2014

Απειλή	Επίπεδο ικανοτήτων που απαιτούνται	Συνέπειες	Πιθανότητες να συμβεί	Μέτρα Αντιμετώπισης
<i>Denial of Service attack</i>	χαμηλό	παραβίαση πολιτικών δικαιωμάτων (πιθανώς επιλεκτικά)	σύνηθες στο Internet	όχι με απλά μέσα: απαιτεί ώρες εργασίας από μηχανικούς δικτύων
<i>Trojan horse attack στο pc με στόχο να παρεμποδιστεί η ψηφοφορία</i>	χαμηλό	παραβίαση πολιτικών δικαιωμάτων	υπάρχουν εκατομμύρια τρόποι για να πραγματοποιηθεί μια τέτοια σύνθετη εργασία	μπορεί να μετριασθεί ο κίνδυνος με προσεχτικό έλεγχο του λογισμικού
<i>on-screen electioneering</i>	χαμηλό	ενόχληση ψηφοφόρου, απογοήτευση, περισπασμός, ανάρμοστη επιρροή	υπερβολικά εύκολο με τη σημερινή web τεχνολογία	ο ψηφοφόρος δεν έχει τη δυνατότητα να το εμποδίσει- απαιτείται νέος νόμος
<i>Spoofing (εξαπάτηση διαφόρων ειδών)</i>	χαμηλό	κλοπή ψήφων, διακύβευση απορρήτου, παραβίαση πολιτικών δικαιωμάτων	σύνηθες και σχετικά εύκολο	δεν αντιμετωπίζεται με κάποιο τρόπο- πολύ πιθανόν να μην ανιχνευθεί
<i>Εξαπάτηση ψηφοφόρου</i>	χαμηλό	παραβίαση πολιτικών δικαιωμάτων	π.χ. : παραποίηση αδειών στα αρχεία cookie	δύσκολο να προβλεφθούν και κυρίως να ανιχνευθούν όλες οι πιθανές απόπειρες εξαπάτησης
<i>Εσωτερικές επιθέσεις στους servers του συστήματος</i>	μέσο	ολοκληρωτική διακύβευση της εκλογικής διαδικασίας	είναι οι πιο συνήθεις επικίνδυνες και οι πιο δύσκολα ανιχνεύσιμες παραβιάσεις	επιθυμητό να επαληθεύει ο ψηφοφόρος την ψήφο του
<i>Αγοραπωλησία ψήφων</i>	μέσο	κατάλυση της δημοκρατίας	απόλυτα ρεαλιστικό, από τη στιγμή που συμμετέχει και ο ίδιος ο ψηφοφόρος	δεν υπάρχουν – η εκάστοτε νομοθεσία είναι πιθανόν να μην αγγίζει τους αγοραστές
<i>Εξαναγκασμός</i>	μέσο	κατάλυση της δημοκρατίας	πιο δύσκολο από την προηγούμενη περίπτωση αλλά κατορθωτό	δεν υπάρχουν – συνήθως δεν ανιχνεύεται
<i>Trojan Horse Attack με στόχο την παραποίηση ψήφων ή την παρακολούθηση τους</i>	υψηλό	κλοπή ψήφων, διακύβευση απορρήτου	ευρέως διαθέσιμο spyware είναι ένα καλό σημείο εκκίνησης	μπορεί να μετριασθεί ο κίνδυνος με προσεχτικό έλεγχο του λογισμικού – δυσκολότερα ελέγχεται σε cyber- cafés ή σε άλλα θεσμικά διαχειριζόμενα δίκτυα – δύσκολα ανιχνεύσιμο



1.5 Υπάρχοντα συστήματα

Η e-ψηφοφορία ή η ηλεκτρονική ψηφοφορία αναφέρεται σε οποιαδήποτε διαδικασία ψηφοφορίας όπου ηλεκτρονικά μέσα χρησιμοποιούνται για τη ρίψη και μέτρηση ψηφοφοριών. Οι μέθοδοι e-ψηφοφορίας περιλαμβάνουν τα συστήματα ψηφοφορίας οπτικός-ανίχνευσης, τα ειδικευμένα συστήματα ψηφοφορίας όπως τα DRE ή τα άμεσα συστήματα ψηφοφορίας και ηλεκτρονικής καταγραφής όπως, τις κάρτες διατρήσεων, το εθνικό IDs, το Διαδίκτυο, τα δίκτυα υπολογιστών, και τα συστήματα τηλεφωνίας. Παρά τα εμπόδια που παρουσιάζουν τα συστήματα δημοσκοπήσεων και ηλεκτρονικής ψηφοφορίας, τα τελευταία χρόνια ένας αριθμός από πανεπιστήμια έχουν αρχίσει να αναπτύσσουν συστήματα ηλεκτρονικής ψηφοφορίας, συχνά για φοιτητικές εκλογές. Όλα όμως αυτά τα συστήματα έχουν σοβαρά μειονεκτήματα. (Virtual Voting)

1.6 Sensus: A Security-Conscious Electronic Polling System for the Internet

Το Sensus (Cranor 1997) είναι ένα πρακτικό και ασφαλές σύστημα για διεξαγωγή δημοσκοπήσεων (ακόμη και εκλογών) μέσω δικτύων. Το Sensus επεκτείνοντας την εργασία των Fujioka, Okamoto και Ohta, χρησιμοποιεί blind signatures προκειμένου από τη μία μεριά να διασφαλίσει ότι μόνο εγγεγραμμένοι ψηφοφόροι μπορούν να ψηφίσουν και κάθε ψηφοφόρος ψηφίζει μόνο μια φορά και από την άλλη να διατηρήσει τη μυστικότητα του ψηφοφόρου. Το Sensus επιτρέπει στο ψηφοφόρο να επαληθεύσει, ατομικά, ότι η ψήφος του μετρήθηκε σωστά και ανώνυμα να ελέγξει την ορθότητα των αποτελεσμάτων της ψηφοφορίας. Το Sensus σχεδιάστηκε αρχικά για να αντικαταστήσει τα συστήματα ψηφοφορίας μέσω ταχυδρομείου. Η ευελιξία του όμως το έκανε να εξυπηρετεί και μια ποικιλία άλλων εκλογικών διαδικασιών συμπεριλαμβανομένων και αυτών που δεν είναι δυνατόν να διεξαχθούν με χρήση των παραδοσιακών εκλογικών συστημάτων. Το Sensus είναι ένα εύκολα προσαρμόσιμο αρθρωτό σύστημα. Το πρωτόκολλο ψηφοφορίας του απαιτεί την ύπαρξη ενός συστήματος επιβεβαιωτή (validator), ενός συστήματος καταμετρητή (tallier) και ενός συστήματος διεξαγωγής της δημοσκόπησης (pollster). Άλλα επιπρόσθετα συστήματα μπορούν να αυξήσουν την λειτουργικότητα του Sensus. Τα υποσυστήματα του Sensus ανταποκρίνονται στα χαρακτηριστικά ενός καλού συστήματος ψηφοφορίας. Το πρωτόκολλο Sensus χρησιμοποιεί blind signatures προκειμένου να παρέχει



ασφάλεια ενώ ταυτόχρονα προστατεύει τη μυστικότητα του χρήστη. Ο χρήστης πρέπει να ετοιμάσει την ψήφο του, να την κρυπτογραφήσει με ένα μυστικό κλειδί και να την αποκρύψει (blind). Στη συνέχεια ο ψηφοφόρος υπογράφει την ψήφο και την αποστέλλει στον επιβεβαιωτή (validator) (Cranor 1997). Ο επιβεβαιωτής επικυρώνει ότι η υπογραφή (signature) ανήκει σε εξουσιοδοτημένο χρήστη ο οποίος δεν έχει ψηφίσει ακόμη. Εάν η ψήφος είναι έγκυρη, ο επιβεβαιωτής υπογράφει την ψήφο και την επιστρέφει στον ψηφοφόρο. Ο ψηφοφόρος αφαιρεί το στρώμα απόκρυψης (blinding layer) και αποκαλύπτει ένα κρυπτογραφημένο μήνυμα υπογεγραμμένο από τον επιβεβαιωτή, το οποίο αποστέλλει στον καταμετρητή (tallier) (Cranor 1997). Ο καταμετρητής ελέγχει την υπογραφή πάνω στο κρυπτογραφημένο ψηφοδέλτιο. Εάν η ψήφος είναι έγκυρη ο καταμετρητής την τοποθετεί σε μια λίστα με έγκυρες ψήφους, η οποία θα δημοσιευτεί μετά το τέλος της ψηφοφορίας. Στη συνέχεια ο καταμετρητής υπογράφει την κρυπτογραφημένη ψήφο και την επιστρέφει σαν απόδειξη στον ψηφοφόρο. Μόλις ο ψηφοφόρος λάβει την απόδειξη αποστέλλει στον καταμετρητή το κλειδί κρυπτογράφησης. Ο καταμετρητής χρησιμοποιεί το κλειδί για να αποκρυπτογραφήσει την ψήφο και να προσθέσει την ψήφο στο τελικό αποτέλεσμα.

1.7 Το σύστημα E-Vox

Χάρη στις τελευταίες εξελίξεις στον τομέα της κρυπτογραφίας μπορούμε να δημιουργήσουμε ένα ασφαλές ηλεκτρονικό σύστημα ψηφοφορίας. Το σύστημα αυτό, που ονομάζεται E-Vox (Bouras 2000) συνδυάζει την ευελιξία ενός συστήματος VBM (Vote By Mail) με την ταχύτητα και την ισχύ των σύγχρονων υπολογιστών. Το σύστημα σχεδιάστηκε να είναι στο σύνολο του φιλικό προς το χρήστη. Με τον όρο φιλικό προς το χρήστη εννοούμε ότι ο εκάστοτε ψηφοφόρος χρειάζεται να εκτελέσει τον ελάχιστο αριθμό βημάτων που απαιτεί η εκλογική διαδικασία και τίποτα άλλο. Τα δύο απαραίτητα βήματα στην όλη διαδικασία είναι η εγγραφή και η ψηφοφορία. Από τη μεριά του ψηφοφόρου και τα δύο βήματα εκτελούνται εύκολα και γρήγορα. Η εγγραφή απαιτεί την προσέλευση του ψηφοφόρου στο κατάλληλο γραφείο εγγραφών, μαζί με τα απαραίτητα δικαιολογητικά. Η διαδικασία της ψηφοφορίας απαιτεί την ύπαρξη ενός υπολογιστή, την εισαγωγή των προσωπικών στοιχείων πρόσβασης και την επιλογή των απαντήσεων. Ο ψηφοφόρος μπορεί να φύγει όντας σίγουρος ότι η διαδικασία ολοκληρώθηκε με ασφάλεια και αξιοπιστία, όπως στα παραδοσιακά συστήματα. (Bouras 2000)



Το E-Vox μπορεί να υποστηρίξει εκλογές στις οποίες συμμετέχουν εκατοντάδες ή μερικές χιλιάδες άνθρωποι. Με έναν ικανοποιητικά γρήγορο server το μέγεθος αυτό μπορεί να αυξηθεί σε μερικές δεκάδες χιλιάδες. Στην πραγματικότητα τα όρια περιορίζονται από την ταχύτητα και το μέγεθος του server και το εύρος των συνδέσεων που μπορούμε να επιτύχουμε. Το σύστημα E-Vox σχεδιάστηκε σαν βελτίωση άλλων παλαιότερων και κάνει πολύ λίγες υποθέσεις σχετικά με το περιβάλλον στο οποίο λειτουργεί. (Bouras 2000) Έτσι δεν χρειάζεται να υποθέσουμε ότι προϋπάρχει οποιοδήποτε σύστημα δημοσίου κλειδιού ή άλλο στοιχειώδες κρυπτογραφικό σύστημα στον τόπο λειτουργίας. Ωστόσο πρέπει να κάνουμε κάποιες υποθέσεις:

- Τα κρυπτογραφικά συστήματα που χρησιμοποιούνται είναι δύσκολο να σπάσουν
- Κάθε ένα από τα εμπλεκόμενα μέρη: ψηφοφόρος, διαχειριστής, σύστημα διατήρησης ανωνυμίας και καταμετρητής δεν έρχονται σε σύγκρουση μεταξύ τους. (Bouras 2000)

1.8 Το απόλυτο σύστημα ψηφοφορίας “Direct Recording Election”

Οι τεχνολογίες πληροφορικής έχουν δημιουργήσει το απόλυτο σύστημα ψηφοφορίας «Direct Recording System» (Κάτσικας 2007). 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 μετριοούνται 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. (Κάτσικας 2007)



Ένα από τα πλεονεκτήματα ενός συστήματος που βασίζεται σε χαρτί είναι ότι η ψηφοφορία αντιπροσωπεύεται φυσικά από ένα κομμάτι χαρτί. Αυτό διαβεβαιώνει ότι οι επιλογές των ψηφοφόρων συνυπολογίζονται. Ακόμη, ένα φυσικό ψηφοδέλτιο δεν διασφαλίζει ότι μια ψηφοφορία θα μετρηθεί σωστά. Πολλοί παράγοντες μπορούν να συμβάλλουν σε μια εσφαλμένη εφαρμογή ψηφοφορίας. Οι τρύπες στις κάρτες δεν μπορούν να ευθυγραμμισθούν πλήρως στην μεμβράνη, με αποτέλεσμα να μετρηθούν λανθασμένα, όπως έγινε το 2000 στις κακόφημες εκλογές στη Φλόριντα. Σχετικά με τις κάρτες οπτικής σάρωσης, μερικά σήματα ή ελλειπείς σημάνσεις μπορούν να παρερμηνευθούν, όταν μετριοούνται. Στους εκτυπωτές οπτικού σήματος, που μπορούν να σαρώσουν κάρτες, εξαντλείται συχνά το μελάνι, με αποτέλεσμα τα ελλιπή εύληπτα σήματα στις κάρτες. Μπορεί επίσης να είναι δυνατό για έναν ψηφοφόρο να ψηφίσει δυο ή περισσότερους υποψηφίους για μια ενιαία θέση, που είναι γνωστό ως overvoting, αυτές οι επιλογές, δεν μετριοούνται από τις συσκευές. Τα φυσικά ψηφοδέλτια μπορούν να χαθούν ή να καταστραφούν πριν από την καταμέτρηση. Ακόμη, είναι πολύ πιο δύσκολο να χαθούν χάρτινα ψηφοδέλτια από ότι είναι να χάσουμε μια ηλεκτρονική καταγραφή των άυλων. (Κάτσικας 2007)

1.9 InfoPoll Software

Τα δεδομένα είναι η ζωογόνο δύναμη για οποιονδήποτε οργανισμό. Παρά ταύτα η συλλογή δεδομένων, σχετικά με τους πελάτες, τους συνεργάτες, τα προϊόντα και τις προσφερόμενες υπηρεσίες, 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 πραγματοποιεί αξιολόγηση ενός Web site, η InfoPoll, επιτρέπει να γίνει εύκολα, γρήγορα και επαγγελματικά. (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 web browser, από



οποιαδήποτε υπολογιστική πλατφόρμα. Η σειρά λογισμικού InfoPoll περιλαμβάνει δύο κύρια συστατικά στοιχεία: τον InfoPoll Σχεδιαστή – Designer (InfoPoll) και τον InfoPoll Εξυπηρετητή – Server (InfoPoll). 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. (InfoPoll)

1.10 Pericles (MIT)

Στο MIT οι φοιτητικές εκλογές διεξάγονται τόσο ηλεκτρονικά όσο και με την παραδοσιακή τους μορφή (χάρτινα ψηφοδέλτια), σε διαφορετικές περιόδους. Το ηλεκτρονικό σύστημα ψηφοφορίας, γνωστό ως Pericles (Electionworld.org), αναπτύχθηκε από τον Paul Kirby. Παρά το ότι είναι ένα σύστημα που βασίζεται στη γλώσσα C «τρέχει» μέσω Mosaic (Electionworld.org).

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. (Electionworld.org)

1.11 Το ηλεκτρονικό σύστημα ψηφοφορίας της Ιταλικής Ακαδημαϊκής Κοινότητας

Η Ιταλική ακαδημαϊκή κοινότητα υλοποίησε ένα σύστημα ψηφοφορίας το οποίο αποτελείται από τα επόμενα συστατικά 1) την αρχή έκδοσης πιστοποιητικών Δημοσίου Κλειδιού, 2) το κεντρικό εκλογικό γραφείο, 3) τη κεντρική κάλπη, 4) το σταθμό ψηφοφορίας, 5) το δίκτυο επικοινωνίας. Πολλά διαφορετικά στάδια πρέπει να ακολουθηθούν, συμπεριλαμβανομένης της έκδοσης έξυπνων καρτών, της έκδοσης λίστας έγκυρων ψηφοφόρων, την παραγωγή προσωπικών κωδικών και κλειδιών αναγνώρισης για κάθε χρήστη, τη διανομή σταθμών ψηφοφορίας και τερματικών, τη στράτευση ανθρώπινου δυναμικού, προκειμένου να γίνει δυνατή η χρήση του συστήματος. Η εκλογική διαδικασία αποτελείται από συνολικά 16 διαφορετικές φάσεις. (Electionworld.org)



1.12 TrueBallot, Inc. Democratic Governance Systems

Άλλο ένα σύστημα που σήμερα είναι διαθέσιμο για ψηφοφορία μέσω Internet είναι αυτό που προσφέρει η TrueBallot, Inc. Democratic Governance Systems (True Ballot). 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. (True Ballot)

1.13 Vivarto Voting Systems

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

1.14 Περιπτώσεις εφαρμογής της ηλεκτρονικής ψηφοφορίας στο εξωτερικό

1.14.1 Η εμπειρία της Αυστραλίας

Ενώ οι επικριτές του στις Ηνωμένες Πολιτείες ανησυχούν όλο και περισσότερο κάθε ημέρα για την ανασφάλεια των μηχανημάτων ηλεκτρονικής ψηφοφορίας, οι Αυστραλοί σχεδίασαν πριν από δύο χρόνια ένα σύστημα που χαλάρωσε τις περισσότερες από αυτές τις ανησυχίες: Επέλεξαν να κάνουν το λογισμικό λειτουργίας του συστήματός τους εντελώς ανοιχτό στο δημόσιο έλεγχο. (Zetter, 2005)



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. Το περισσότερο, είχε καταφέρει τη σύλληψη στην προϊόντος σε έξι μήνες. Θα πέρασε 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 open-source λειτουργικό σύστημα διαθέσιμο στο Διαδίκτυο. (Zetter, 2005)

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 Phillip Green, 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. (Zetter, 2005)

Το 1999, η Αυστραλιανή Εκλογική Επιτροπή προέβη σε δημόσια πρόσκληση για την ηλεκτρονική ψηφοφορία για να δούμε 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 (Zetter, 2005) είπε ότι το 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 Matt Quinn, 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." (Zetter, 2005)

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," είπε Quinn. Λίγα άτομα κατέγραψαν σφάλματα στην έκθεση, συμπεριλαμβανομένου ενός ακαδημαϊκού στο Αυστραλιανό Εθνικό Πανεπιστήμιο που βρήκε το πιο σοβαρό πρόβλημα. «Δεν ήταν ένα λειτουργικό ή ένα θέμα ασφαλείας, αλλά ήταν λάθος, που ήμασταν ευτυχείς που είχε επισημανθεί για εμάς", είπε ο Quinn. (Zetter, 2005)

1.14.2 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. (E-voting, State of Geneva)

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 την τεχνογνωσία 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. (E-voting, State of Geneva)

Σε αντίθεση με τις μηχανές ψηφοφορίας, ωστόσο, και ιδιαίτερα σε αντίθεση με τα μηχανήματα που δεν είναι συνδεδεμένα με ένα δίκτυο, αλλά εργάζονται off-line, 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. (E-voting, State of Geneva)

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 ψήφισαν 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. (E-voting, State of Geneva)

1.14.3 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 που πραγματοποιήθηκαν 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. (Χατζηστυλιανού, 2007)

1.14.4 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 ότι όταν έχουμε να παραλάβουμε ένα πακέτο ψηφοδέλτια και... τα «σημαδεμένα χαρτιά» ή τα «κρυπτογραφημένα μηνύματα προς κομματάρχες» αποκλείονται. (fed.gov)

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. (fed.gov)

Στην Ελβετία - όπου η άμεση δημοκρατία λατρεύεται σχεδόν όσο και στην Αρχαία Αθήνα - έφθασαν 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. Στις 26 Σεπτεμβρίου 2007, 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 Η.Π.Α. 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 Η.Π.Α. 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 της 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». (fed.gov)

Στο καθεστώς αυτό αντέδρασε πρώτη η Rebecca Mercuri, 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. (fed.gov)

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 Doug Jones ανακάλυψε με τρόπο 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. (fed.gov)



2 Τεχνολογίες και Εργαλεία που χρησιμοποιήσαμε

2.1 Javascript

Μια συνηθισμένη εσφαλμένη αντίληψη είναι ότι η JavaScript είναι παρόμοια ή πολύ στενά συσχετισμένη με την Java. Είναι αλήθεια πως και οι δύο μοιάζουν στη σύνταξή τους με την C (που είναι και ο πιο άμεσος πρόγονός τους), όμως οι ομοιότητές τους είναι λίγες. Για παράδειγμα όλες οι λέξεις-κλειδιά της Java χρησιμοποιούνται από τη Javascript, οι στάνταρ βιβλιοθήκες της JavaScript ακολουθούν τις συμβάσεις ονοματολογίας της Java και κάποια αντικείμενα της JavaScript όπως τα Date και Time βασίζονται σε κλάσεις της Java. Εδώ όμως τελειώνουν οι ομοιότητές τους!

Η JavaScript (JS) είναι διερμηνευμένη γλώσσα προγραμματισμού για ηλεκτρονικούς υπολογιστές. Αρχικά αποτέλεσε μέρος της υλοποίησης των φυλλομετρητών Ιστού, ώστε τα σενάρια από την πλευρά του πελάτη (client-side scripts) να μπορούν να επικοινωνούν με τον χρήστη, να ανταλλάσσουν δεδομένα ασύγχρονα και να αλλάζουν δυναμικά το περιεχόμενο του εγγράφου που εμφανίζεται. Η JavaScript είναι μια γλώσσα σεναρίων που βασίζεται στα πρωτότυπα (prototype-based), είναι δυναμική, με ασθενείς τύπους και έχει συναρτήσεις ως αντικείμενα πρώτης τάξης. Η σύνταξή της είναι επηρεασμένη από τη C. Η JavaScript αντιγράφει πολλά ονόματα και συμβάσεις ονοματοδοσίας από τη Java, αλλά γενικά οι δύο αυτές γλώσσες δε σχετίζονται και έχουν πολύ διαφορετική σημασιολογία. Οι βασικές αρχές σχεδιασμού της JavaScript προέρχονται από τις γλώσσες προγραμματισμού Self και Scheme. Είναι γλώσσα βασισμένη σε διαφορετικά προγραμματιστικά παραδείγματα (multi-paradigm), υποστηρίζοντας αντικειμενοστρεφής, προστακτικό και συναρτησιακό στυλ προγραμματισμού.

Η JavaScript χρησιμοποιείται και σε εφαρμογές εκτός ιστοσελίδων. Τέτοια παραδείγματα είναι τα έγγραφα PDF, οι εξειδικευμένοι φυλλομετρητές (site-specific browsers) και οι μικρές εφαρμογές της επιφάνειας εργασίας (desktop widgets). Οι νεότερες εικονικές μηχανές και πλαίσια ανάπτυξης για JavaScript (όπως το Node.js) έχουν επίσης κάνει τη JavaScript πιο δημοφιλή για την ανάπτυξη εφαρμογών Ιστού στην πλευρά του διακομιστή (server-side).



Η JavaScript είναι δομημένη γλώσσα, χαρακτηριστικό που κληρονόμησε από τη C. Είναι δυναμική τόσο στη σύνταξή της, π.χ: μια μεταβλητή που περιέχει έναν αριθμό μπορεί αργότερα να αποθηκεύσει κείμενο, όσο και στην εκτέλεσή της που είναι run-time.

Είναι αντικειμενοστρεφής, επίσης είναι συναρτησιακή – κάθε συνάρτηση είναι ένα αντικείμενο, έτσι μπορεί να έχει ιδιότητες και μεθόδους. Υποστηρίζει εμφωλευμένες συναρτήσεις όπως επίσης και ανώνυμες συναρτήσεις.

Η πιο συνηθισμένη χρήση της JavaScript είναι να προσθέσει συμπεριφορά στην HTML στην πλευρά του χρήστη, που είναι γνωστό και ως Δυναμική HTML. Τα script είναι ενσωματωμένα στις HTML σελίδες και αλληλεπιδρούν με το Μοντέλο Αντικειμένου Εγγραφού (DOM – Document Object Model).

Η JavaScript έχει γίνει μία από τις πιο δημοφιλείς γλώσσες προγραμματισμού ηλεκτρονικών υπολογιστών στον Παγκόσμιο Ιστό (Web). Αρχικά, όμως, πολλοί επαγγελματίες προγραμματιστές υποτίμησαν τη γλώσσα διότι το κοινό της ήταν ερασιτέχνες συγγραφείς ιστοσελίδων και όχι επαγγελματίες προγραμματιστές (μαζί με άλλους λόγους). Με τη χρήση της τεχνολογίας Ajax, η JavaScript γλώσσα επέστρεψε στο προσκήνιο και έφερε πιο επαγγελματική προσοχή προγραμματισμού. Το αποτέλεσμα ήταν ένα καινοτόμο αντίκτυπο στην εξάπλωση των πλαισίων και των βιβλιοθηκών, τη βελτίωση προγραμματισμού με JavaScript, καθώς και αυξημένη χρήση της JavaScript έξω από τα προγράμματα περιήγησης στο Web.

2.1.1 HTML

Η HTML (αρχικοποίηση του αγγλικού HyperText Markup Language, ελλ. Γλώσσα Σήμανσης Υπερκειμένου) είναι η κύρια γλώσσα σήμανσης για τις ιστοσελίδες, και τα στοιχεία της είναι τα βασικά δομικά στοιχεία των ιστοσελίδων.

Η HTML γράφεται υπό μορφή στοιχείων HTML τα οποία αποτελούνται από ετικέτες (tags), οι οποίες περικλείονται μέσα σε σύμβολα «μεγαλύτερο από» και «μικρότερο από» (για παράδειγμα <html>), μέσα στο περιεχόμενο της ιστοσελίδας. Οι ετικέτες HTML συνήθως λειτουργούν ανά ζεύγη (για παράδειγμα <h1> και </h1>), με την πρώτη να ονομάζεται ετικέτα έναρξης και τη δεύτερη ετικέτα λήξης (ή σε άλλες περιπτώσεις ετικέτα ανοίγματος και ετικέτα κλεισίματος αντίστοιχα). Ανάμεσα στις



ετικέτες, οι σχεδιαστές ιστοσελίδων μπορούν να τοποθετήσουν κείμενο, πίνακες, εικόνες κλπ.

Ο σκοπός ενός web browser είναι να διαβάζει τα έγγραφα HTML και να τα συνθέσει σε σελίδες που μπορεί κανείς να διαβάσει ή να ακούσει. Ο browser δεν εμφανίζει τις ετικέτες HTML, αλλά τις χρησιμοποιεί για να παρουσιάσει το περιεχόμενο της σελίδας. Τα στοιχεία της HTML χρησιμοποιούνται για να κτίσουν όλους του ιστοτόπους. Η HTML επιτρέπει την ενσωμάτωση εικόνων και άλλων αντικειμένων μέσα στη σελίδα, και μπορεί να χρησιμοποιηθεί για να εμφανίσει διαδραστικές φόρμες. Παρέχει τις μεθόδους δημιουργίας δομημένων εγγράφων (δηλαδή εγγράφων που αποτελούνται από το περιεχόμενο που μεταφέρουν και από τον κώδικα μορφοποίησης του περιεχομένου) καθορίζοντας δομικά σημαντικά στοιχεία για το κείμενο, όπως κεφαλίδες, παραγράφους, λίστες, συνδέσμους, παραθέσεις και άλλα. Μπορούν επίσης να ενσωματώνονται σενάρια εντολών σε γλώσσες όπως η JavaScript, τα οποία επηρεάζουν τη συμπεριφορά των ιστοσελίδων HTML και από στατικές τις κάνουν διαδραστικές.

Οι Web browsers μπορούν επίσης να αναφέρονται σε στυλ μορφοποίησης CSS για να ορίζουν την εμφάνιση και τη διάταξη του κειμένου και του υπόλοιπου υλικού. Ο οργανισμός W3C, ο οποίος δημιουργεί και συντηρεί τα πρότυπα για την HTML και τα CSS, ενθαρρύνει τη χρήση των CSS αντί διαφόρων στοιχείων της HTML για σκοπούς παρουσίασης του περιεχομένου.

2.2 PHP

Η PHP (PHP: Hypertext Preprocessor) είναι μια γλώσσα προγραμματισμού για τη δημιουργία σελίδων web με δυναμικό περιεχόμενο. Μια σελίδα PHP περνά από επεξεργασία από ένα συμβατό διακομιστή του Παγκόσμιου Ιστού (π.χ. Apache), ώστε να παραχθεί σε πραγματικό χρόνο το τελικό περιεχόμενο, που είτε θα σταλεί στο πρόγραμμα περιήγησης των επισκεπτών σε μορφή κώδικα HTML ή θα επεξεργασθεί τις εισόδους δίχως να προβάλλει την έξοδο στο χρήστη, αλλά θα τις μεταβιβάσει σε κάποιο άλλο PHP script.

Η PHP αποτελεί μια από τις πιο διαδεδομένες τεχνολογίες στο Παγκόσμιο Ιστό, καθώς χρησιμοποιείται από πληθώρα εφαρμογών και ιστότοπων. Διάσημες εφαρμογές που



κάνουν εκτενή χρήση της PHP είναι το γνωστό Σύστημα Διαχείρισης Περιεχομένου (Content Management System, WordPress και το Drupal).

Ένα αρχείο με κώδικα PHP θα πρέπει να έχει την κατάλληλη επέκταση (π.χ. *.php, *.php4, *.phtml κ.ά.). Η ενσωμάτωση κώδικα σε ένα αρχείο επέκτασης .html δεν θα λειτουργήσει και θα εμφανίσει στον browser τον κώδικα χωρίς καμία επεξεργασία, εκτός αν έχει γίνει η κατάλληλη ρύθμιση στα MIME types του server. Επίσης ακόμη κι όταν ένα αρχείο έχει την επέκταση .php, θα πρέπει ο server να είναι ρυθμισμένος για να επεξεργάζεται και να μεταγλωττίζει τον κώδικα PHP σε HTML που καταλαβαίνει το πρόγραμμα πελάτη.

Ο συνδυασμός Linux/Apache/MySQL/PHP, που είναι η πιο δημοφιλής πλατφόρμα εκτέλεσης ιστοσελίδων είναι γνωστός και με το ακρωνύμιο LAMP. Παρόμοια, ο συνδυασμός */Apache/MySQL/PHP ονομάζεται *AMP, όπου το πρώτο αρχικό αντιστοιχεί στην πλατφόρμα, στην οποία εγκαθίστανται ο Apache, η MySQL και η PHP (π.χ. Windows, Mac OS X).

Η ιστορία της PHP ξεκινά από το 1994, όταν ένας φοιτητής, ο Rasmus Lerdorf δημιούργησε χρησιμοποιώντας τη γλώσσα προγραμματισμού C ένα απλό script με όνομα php.cgi, για προσωπική χρήση. Το script αυτό είχε σαν σκοπό να διατηρεί μια λίστα στατιστικών για τα άτομα που έβλεπαν το online βιογραφικό του σημείωμα. Αργότερα αυτό το script το διέθεσε και σε φίλους του, οι οποίοι άρχισαν να του ζητούν να προσθέσει περισσότερες δυνατότητες. Η γλώσσα τότε ονομαζόταν PHP/FI από τα αρχικά Personal Home Page/Form Interpreter. Το 1997 η PHP/FI έφθασε στην έκδοση 2.0 αριθμώντας περισσότερους από 50.000 ιστοτόπους που τη χρησιμοποιούσαν, ενώ αργότερα την ίδια χρονιά οι Andi Gutmans και Zeev Suraski ξαναέγραψαν τη γλώσσα από την αρχή, βασιζόμενοι όμως αρκετά στην PHP/FI 2.0. Έτσι η PHP έφθασε στην έκδοση 3.0 η οποία θύμιζε περισσότερο τη σημερινή μορφή της. Στη συνέχεια, οι Zeev και Andi δημιούργησαν την εταιρεία Zend (από τα αρχικά των ονομάτων τους), η οποία συνεχίζει μέχρι και σήμερα την ανάπτυξη και εξέλιξη της γλώσσας PHP. Ακολούθησε το 1998 η έκδοση 4 της PHP, τον Ιούλιο του 2004 διατέθηκε η έκδοση 5, ενώ αυτή τη στιγμή έχουν ήδη διατεθεί και οι πρώτες δοκιμαστικές εκδόσεις της επερχόμενης PHP 6, για οποιονδήποτε προγραμματιστή θέλει να τη χρησιμοποιήσει. Οι περισσότεροι ιστότοποι επί του παρόντος χρησιμοποιούν κυρίως τις εκδόσεις 5, 6 και 7 της PHP.



Ένα αρχείο PHP μπορεί να περιέχει κείμενο, κώδικα HTML, CSS, JavaScript και PHP, με τον κώδικα να εκτελείται στον server και το αποτέλεσμα να επιστρέφει στον browser ως απλές σελίδες HTML.

Σε συνδυασμό και με την MySQL μπορεί να χρησιμοποιηθεί κάλλιστα για την διαχείριση δεδομένων μέσα σε βάσεις. Για παράδειγμα, σε μια ιστοσελίδα που είναι απαραίτητη η εγγραφή των χρηστών, η PHP μπορεί να αποθηκεύει τα ονόματα και τους κωδικούς τους σε μια βάση δεδομένων.

2.3 CSS

Η CSS (Cascading Style Sheets – διαδοχικά φύλλα ύφους ή επάλληλα φύλλα ύφους) είναι μια γλώσσα υπολογιστή που ανήκει στην κατηγορία των γλωσσών φύλλων ύφους που χρησιμοποιείται για τον έλεγχο της εμφάνισης ενός εγγράφου που έχει γραφτεί με μια γλώσσα σήμανσης.

Χρησιμοποιείται δηλαδή για τον έλεγχο της εμφάνισης ενός εγγράφου που γράφτηκε στις γλώσσες HTML και XHTML, δηλαδή για τον έλεγχο της εμφάνισης μιας ιστοσελίδας και γενικότερα ενός ιστοτόπου. Η CSS είναι μια γλώσσα υπολογιστή προορισμένη να αναπτύσσει στυλιστικά μια ιστοσελίδα δηλαδή να διαμορφώνει περισσότερα χαρακτηριστικά, χρώματα, στοίχιση και δίνει περισσότερες δυνατότητες σε σχέση με την html. Για μια όμορφη και καλοσχεδιασμένη ιστοσελίδα η χρήση της CSS κρίνεται ως απαραίτητη.

2.4 SQL

Η SQL (αγγλ. αρκτ. από το Structured Query Language) (προφ. /,εs.kju: 'ελ/) είναι μία γλώσσα υπολογιστών στις βάσεις δεδομένων, που σχεδιάστηκε για τη διαχείριση δεδομένων, σε ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων (Relational Database Management System, RDBMS) και η οποία, αρχικά, βασίστηκε στη σχεσιακή άλγεβρα. Η γλώσσα περιλαμβάνει δυνατότητες ανάκτησης και ενημέρωσης δεδομένων, δημιουργίας και τροποποίησης σχημάτων και σχεσιακών πινάκων, αλλά και ελέγχου πρόσβασης στα δεδομένα. Η SQL ήταν μία από τις πρώτες γλώσσες για το σχεσιακό μοντέλο του Edgar F. Codd, στο σημαντικό άρθρο του το 1970, και έγινε η πιο ευρέως χρησιμοποιούμενη γλώσσα για τις σχεσιακές βάσεις δεδομένων.



Η SQL αναπτύχθηκε στην IBM από τους Andrew Richardson, Donald C. Messerly και Raymond F. Boyce, στις αρχές της δεκαετίας του 1970. Αυτή η έκδοση, αποκαλούμενη αρχικά SEQUEL, είχε ως σκοπό να χειριστεί και να ανακτήσει τα στοιχεία που αποθηκεύτηκαν στο πρώτο RDBMS της IBM, το System R.

Το πρώτο σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων (RDBMS) ήταν το RDMBS που αναπτύχθηκε στο MIT, στις αρχές της δεκαετίας του 1970 και η Ingres, που αναπτύχθηκε το 1974 στο Πανεπιστήμιο Μπέρκλεϋ. Η Ingres εφάρμοσε μία γλώσσα διατύπωσης ερωτήσεων γνωστή ως QUEL, το οποίο αντικαταστάθηκε αργότερα στην αγορά από την SQL.

Προς το τέλος της δεκαετίας του 70 η Relational Software (τώρα Oracle Corporation) είδε τη δυνατότητα αυτών που περιγράφηκαν από Codd, Chamberlin, και Boyce και ανέπτυξε την SQL βασισμένο στο RDBMS, με τις φιλοδοξίες πώλησης του στο Αμερικανικό ναυτικό, την Κεντρική Υπηρεσία Πληροφοριών και άλλες Αμερικανικές Υπηρεσίες.

Το καλοκαίρι του 1979, η Relational Software εισήγαγε την πρώτη διαθέσιμη στο εμπόριο εφαρμογή του SQL και νίκησε την IBM με τη διάθεση του πρώτου εμπορικού RDBMS για μερικές εβδομάδες.

Ένα σύστημα διαχείρισης βάσης δεδομένων (ΣΔΒΔ) (database management system (DBMS)) αποτελείται από ένα σύνολο δεδομένων και προγράμματα πρόσβασης στα δεδομένα αυτά. Το σύνολο των δεδομένων καλείται βάση δεδομένων (database). Στόχος του ΣΔΒΔ είναι η εύκολη και γρήγορη χρήση και ανάκτηση των δεδομένων.

Ο ορισμός της δομής της βάσης δεδομένων βασίζεται σε ένα μοντέλο δεδομένων το οποίο ορίζει τον τρόπο που περιγράφονται τα δεδομένα, οι σχέσεις τους, η σημασία τους και οι περιορισμοί πάνω στα δεδομένα αυτά.

Το σχεσιακό μοντέλο (relational model) δεδομένων παριστάνει δεδομένα και τις σχέσεις τους ως ένα σύνολο πινάκων. Κάθε πίνακας (table) αποτελείται από στήλες (columns) με μοναδικά ονόματα. Μια γραμμή (row) του πίνακα παριστάνει μια σχέση (relationship) ανάμεσα σε ένα σύνολο από τιμές.



2.5 MySQL

Μια βάση δεδομένων είναι ουσιαστικά μία συλλογή δεδομένων κατάλληλα αποθηκευμένων σε έναν υπολογιστή προκειμένου να μπορούν να προσπελαστούν, διαχειριστούν και ενημερωθούν με ευκολία από το άτομο που τις διαχειρίζεται. Οι ενέργειες αυτές επάνω στα δεδομένα γίνονται μέσα από τα Συστήματα Διαχείρισης Βάσεων Δεδομένων (DataBase Management Systems - DBMS), τα οποία έχουν κατάλληλους μηχανισμούς για να προσπελαίνουν οργανωμένες δομές δεδομένων και να τις επεξεργάζονται χωρίς απώλειες και κίνδυνο παραποίησης ή φθοράς των δεδομένων.

Η MySQL είναι ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων που μετρά περισσότερες από 11 εκατομμύρια εγκαταστάσεις. Έλαβε το όνομά της από την κόρη του Μόντυ Βιντένιους, τη Μάι (αγγλ. My). Το πρόγραμμα τρέχει έναν εξυπηρετητή (server) παρέχοντας πρόσβαση πολλών χρηστών σε ένα σύνολο βάσεων δεδομένων.

Η MySQL είναι μία γλώσσα προγραμματισμού για Συστήματα Διαχείρισης Βάσεων Δεδομένων (DBMS). Προκειμένου τα DBMS να μπορούν να έχουν κάποιους κοινούς άξονες αναφοράς έχει αναπτυχθεί η γλώσσα SQL (Structured Query Language) ή οποία επιτρέπει μέσα από ένα σύστημα εντολών, την προσπέλαση των δομημένων δεδομένων που περιέχει ένα DBMS. Κάθε DBMS ουσιαστικά δέχεται και εκτελεί ένα σετ εντολών SQL για να διαχειριστεί τα δεδομένα του. Η MySQL είναι μία διανομή (έκδοση) της γλώσσας SQL και ένα MySQL DBMS είναι ένα σύστημα που δέχεται εντολές της MySQL.

Η MySQL αποτελεί ελεύθερο λογισμικό που μπορεί να χρησιμοποιήσει κανείς ερασιτεχνικά ή επαγγελματικά. Αντίστοιχα με την MySQL υπάρχουν και άλλα συστήματα δωρεάν ή με πληρωμή. Από τα πιο γνωστά DBMS είναι ο SQL Server της Microsoft, ο Oracle SQL server, η DB2 κ.ά.

Καθώς η τεχνολογία των DBMS εξελίχθηκε στο χρόνο προέκυψαν διάφοροι διαχωρισμοί αυτών, ανάλογα με τον τύπο των δεδομένων που αποθηκεύονται σε αυτά. Οι οργανωμένες δομές δεδομένων στις οποίες έχουμε αναφερθεί μέχρι στιγμής, αποθηκεύουν σύνολα δεδομένων (πλειάδες) και τον τρόπο με τον οποίο αυτά συσχετίζονται. Επειδή η λογική πίσω από τη διαχείριση αυτών των δεδομένων είναι η



συσχέτιση (σχέση) των δεδομένων, αυτές οι βάσεις αποκαλούνται Σχισιακές Βάσεις Δεδομένων και τα συστήματά τους σχισιακά (RDBMS - Relational Database Managements Systems). Άλλοι τύποι DBMS είναι τα HDBMS (Hierarchical DBMS) όπου τα δεδομένα αποθηκεύονται σαν δέντρο ή σαν γράφος, οπότε η ίδια η δομή της βάσης υποδηλώνει και τη συσχέτιση των δεδομένων της.

Μια βάση δεδομένων σε MySQL είναι ένας χώρος που έχουμε διαμορφώσει κατάλληλα προκειμένου να αποθηκεύσουμε τα δεδομένα των ιστοσελίδων μας με σχισιακό τρόπο.

Για παράδειγμα αν έχουμε στην ιστοσελίδα μας μία φόρμα παραγγελίας προϊόντων, τότε μπορούμε στη βάση μας να έχουμε τον πίνακα (πλειάδα) των χρηστών όπου θα αποθηκεύουμε τους πελάτες μας και τον πίνακα (πλειάδα) των παραγγελιών όπου θα αποθηκεύουμε τις παραγγελίες τους. Οι δύο αυτοί πίνακες θα σχετίζονται με σχέση 1 προς πολλά (1:N) επειδή ένα πελάτης μπορεί να κάνει πολλές παραγγελίες. Μέσα από αυτό το γενικευμένο παράδειγμα μπορείτε να πάρε μία πρώτη γεύση του τρόπου με τον οποίο μπορεί να γίνει χρήση της MySQL σε θέματα καθημερινής πρακτικής των ιστοσελίδων σας.

2.6 APACHE

Ο Apache HTTP γνωστός και απλά σαν Apache είναι ένας εξυπηρετητής του παγκόσμιου ιστού (web). Όποτε ένας χρήστης επισκέπτεται έναν ιστότοπο, το πρόγραμμα πλοήγησης (browser) επικοινωνεί με έναν διακομιστή (server) μέσω του πρωτοκόλλου HTTP, ο οποίος παράγει τις ιστοσελίδες και τις αποστέλλει στο πρόγραμμα πλοήγησης. Ο Apache είναι ένας από τους δημοφιλέστερους εξυπηρετητές ιστού, εν μέρει γιατί λειτουργεί σε διάφορες πλατφόρμες όπως τα Windows, το Linux, το Unix και το Mac OS X. Κυκλοφόρησε υπό την άδεια λογισμικού Apache και είναι λογισμικό ανοιχτού κώδικα. Συντηρείται από μια κοινότητα ανοικτού κώδικα με επιτήρηση από το Ίδρυμα Λογισμικού Apache (Apache Software Foundation). Ο Apache χρησιμοποιείται και σε τοπικά δίκτυα σαν διακομιστής συνεργαζόμενος με συστήματα διαχείρισης Βάσης Δεδομένων π.χ. Oracle, MySQL.

Η πρώτη του έκδοση, γνωστή ως NCSA HTTPd, δημιουργήθηκε από τον Robert McCool και κυκλοφόρησε το 1993. Θεωρείται ότι έπαιξε σημαντικό ρόλο στην αρχική



επέκταση του παγκόσμιου ιστού. Ήταν η πρώτη βιώσιμη εναλλακτική επιλογή που παρουσιάστηκε απέναντι στον εξυπηρετητή http της εταιρείας Netscape και από τότε έχει εξελιχθεί στο σημείο να ανταγωνίζεται άλλους εξυπηρετητές βασισμένους στο Unix σε λειτουργικότητα και απόδοση. Από το 1996 ήταν από τους πιο δημοφιλείς όμως από τον Μάρτιο του 2006 έχει μειωθεί το ποσοστό της εγκατάστασής του κυρίως από τον Microsoft Internet Information Services και την πλατφόρμα .NET. Τον Οκτώβριο του 2007 το μερίδιο του ήταν 47.73% από όλους τους ιστοτόπους. Τον Μάρτιο του 2017, το 49,48% του συνόλου των καταχωρισμένων Ελληνικών τομέων χρησιμοποιούσε το Apache.

Ο Apache ακολουθεί μια προσέγγιση πολλαπλών thread. Παρέχει μια ποικιλία από πολλαπλές μονάδες επεξεργασίας. Αυτά τα προ-ενότητες είναι βασικά τριών τύπων αλγορίθμων χειρισμού αιτημάτων. Ο καθένας προορίζεται για διαφορετικές ανάγκες server. Τα MPM (Multi-Processing Modules) παρέχουν μια ευέλικτη αρχιτεκτονική για την επιλογή διαφορετικής σύνδεσης και διαφορετικών αλγορίθμων χειρισμού. Επίσης, διαφορετικές εκδόσεις του Apache 2 χρησιμοποιούν διαφορετικές ενότητες επεξεργασίας. Από προεπιλογή, ο Apache 2.2 έχει ρυθμιστεί σε Pre-fork mode (mpm_prefork). Ανταποκρίνεται σε έναν καθορισμένο αριθμό διαδικασιών, καθεμιά από τις οποίες μπορεί να εξυπηρετήσει ένα μόνο αίτημα κάθε φορά. Με άλλα λόγια, ο Apache δημιουργεί ένα νέο thread κάθε φορά για να χειρίζεται κάθε αίτημα σύνδεσης.

Ωστόσο, η βασική αρχιτεκτονική του Apache μπορεί να οδηγήσει σε βαριά κατανάλωση πόρων, με αποτέλεσμα να μπορεί να προκαλέσει προβλήματα με το server (π.χ. χαμηλή ταχύτητα).

ο Apache μπορεί να επεξεργαστεί δυναμικό περιεχόμενο μέσα στον ίδιο τον ιστό, χωρίς να χρειάζεται να βασίζεται σε εξωτερικά στοιχεία. Έτσι, μπορεί να χειριστεί τα ίδια τα πιστεύω σας. Λειτουργεί σε όλα τα είδη συστημάτων που μοιάζουν με Unix (π.χ. Linux ή BSD) και έχει πλήρη υποστήριξη για τα Microsoft Windows.

Διαθέτει ένα πλούσιο σύνολο λειτουργιών που μπορούν να ενεργοποιηθούν εγκαθιστώντας μία από τις 60 επίσημες μονάδες. Υπάρχουν επίσης πολλές άλλες ανεπίσημες ενότητες που μπορούν εύκολα να βρεθούν στο διαδίκτυο.



Το σύστημα της μονάδας σας επιτρέπει να φορτώνετε ή να εκφορτώνετε δυναμικά μονάδες για να ικανοποιείτε τις ανάγκες σας. Οι ενότητες του μπορούν να ενεργοποιηθούν ή να απενεργοποιηθούν για να προσθέσουν ή να αφαιρέσουν λειτουργίες και να συνδεθούν στον κύριο διακομιστή. Με λίγα λόγια, ο Apache διαθέτει πολλές ενότητες λειτουργιών για να καλύψει τις ανάγκες σας, αλλά πολλές από αυτές δεν χρησιμοποιούνται συχνά. Προσαρμογές στον web server μπορούν να γίνουν μέσω modules. Το Apache είχε τη δυναμικό module να φορτώνει για το μεγαλύτερο χρονικό διάστημα, έτσι όλα τα Apache modules το υποστηρίζουν.

2.7 JSON

Το JSON (JavaScript Object Notation) είναι ένα ελαφρύ πρότυπο ανταλλαγής δεδομένων. Είναι εύκολο για τους ανθρώπους να το διαβάσουν και γράψουν. Είναι εύκολο για τις μηχανές να το αναλύσουν (parse) και να το παράγουν (generate). Είναι βασισμένο πάνω σε ένα υποσύνολο της γλώσσας προγραμματισμού JavaScript, Standard ECMA-262 Έκδοση 3η - Δεκέμβριος 1999. Το JSON είναι ένα πρότυπο κειμένου το οποίο είναι τελείως ανεξάρτητο από γλώσσες προγραμματισμού αλλά χρησιμοποιεί πρακτικές (conventions) οι οποίες είναι γνωστές στους προγραμματιστές της οικογένειας προγραμματισμού C, συμπεριλαμβανομένων των C, C++, C#, Java, JavaScript, Perl, Python, και πολλών άλλων. Αυτές οι ιδιότητες κάνουν το JSON μια ιδανική γλώσσα προγραμματισμού ανταλλαγής δεδομένων.

Η διαφορά είναι ότι με JSON μπορεί να γίνει ευκολότερα και να γλιτώσουμε πολύπλοκες διαδικασίες για την ανάγνωση δεδομένων. Ουσιαστικά όλες οι μοντέρνες γλώσσες προγραμματισμού τα υποστηρίζουν με τον έναν ή τον άλλον τρόπο. Λογικό είναι πως ένα πρότυπο δεδομένων το οποίο είναι εύκολα μεταβαλλόμενο με γλώσσες προγραμματισμού οι οποίες επίσης είναι βασισμένες σε αυτές τις δομές.

Ένα αντικείμενο (object) είναι ένα άτακτο σύνολο από ζευγάρια ονομάτων/τιμών. Ένα αντικείμενο (object) ξεκινάει με { αριστερό άγκιστρο και τελειώνει με } δεξιό άγκιστρο. Κάθε όνομα ακολουθείται από :άνω-κάτω τελεία και τα ζευγάρια ονόματος/τιμής χωρίζονται από , κόμμα.

Το JSON δεν ήταν το πρώτο που χρησιμοποίησε ζεύγη χαρακτηριστικών-τιμών ως τρόπος μεταφοράς δεδομένων μέσω του Διαδικτύου. Το tech-savvy μεταξύ σας



μπορεί να παρατηρήσει ότι ακούγεται ένα πάρα πολύ σαν XML. Λοιπόν, όπως αποδεικνύεται, το JSON και το XML εκτελούν πολλά από τα ίδια καθήκοντα. Γιατί λοιπόν επιλέγετε το JSON πάνω από την XML;

Στον ιστό του σήμερα, η ασύγχρονη φόρτωση δεδομένων είναι σημαντική. Με άλλα λόγια, οι ιστοσελίδες θέλουν να είναι σε θέση να φορτώσουν νέα δεδομένα χωρίς να χρειάζεται να ανανεώσουν ολόκληρη τη σελίδα για να την αποκτήσουν. Αυτό έχει ως αποτέλεσμα μια πιο ομαλή και πιο ευνοϊκή εμπειρία περιήγησης. Το JSON είναι ιδανικό για την αποστολή και τη λήψη ασύγχρονων δεδομένων, διότι είναι απλό και εύκολο στη χρήση.

Αλλά το XML κάνει το ίδιο πράγμα! Γιατί λοιπόν κάποιοι προτιμούν το JSON; Μια απάντηση σε αυτή την ερώτηση μπορεί να βρεθεί στο όνομα της JSON: JavaScript Notation Object . Αναγνωρίζεται φυσικά από τη JavaScript, η οποία είναι μια από τις πιο δημοφιλείς γλώσσες στον κόσμο. Δεδομένου ότι το JSON είναι ένα υποσύνολο JavaScript, υπάρχει πολύ λίγη επιπλέον μάθηση που πρέπει να κάνετε αφού μάθετε το JavaScript.

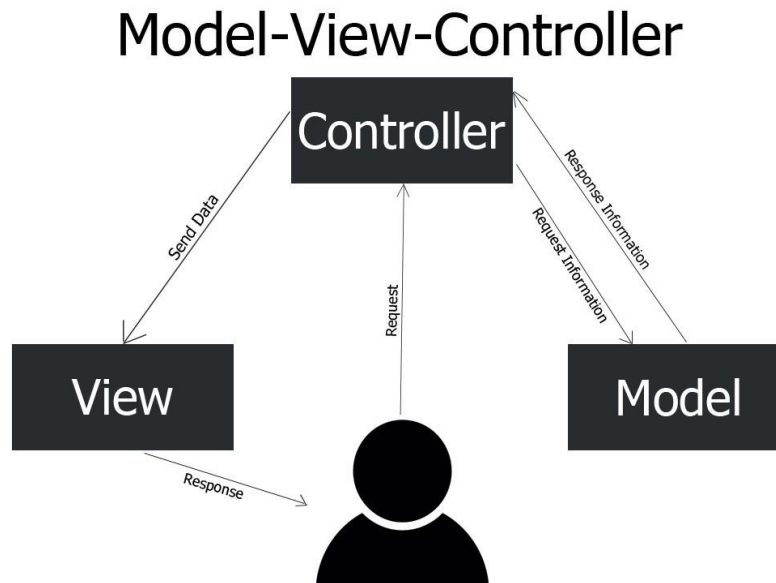
Ένας άλλος λόγος είναι ότι το JSON είναι πιο ευανάγνωστο από το XML. Σίγουρα, είναι εύκολο να συνηθίσετε με την XML όταν την έχετε χρησιμοποιήσει για λίγο, αλλά η ματιά σε ένα αρχείο XML μπορεί να είναι συντριπτική με όλες τις ετικέτες και το λεξιλόγιο της. Το JSON είναι πιο καθαρό, πιο εύκολο για τους αρχάριους να κατανοούν και αρκετά ευέλικτο με τους βασικούς τύπους δεδομένων.

2.8 MVC

Ο Model-view-controller (σε συντομογραφία αναφέρεται ως MVC) είναι ένα μοντέλο αρχιτεκτονικής λογισμικού το οποίο χρησιμοποιείται για τη δημιουργία περιβαλλόντων αλληλεπίδρασης χρήστη. Στο μοντέλο αυτό η εφαρμογή διαιρείται σε τρία διασυνδεδεμένα μέρη ώστε να διαχωριστεί η παρουσίαση της πληροφορίας στον χρήστη από την μορφή που έχει αποθηκευτεί στο σύστημα. Το κύριο μέρος του μοντέλου είναι το αντικείμενο Model το οποίο διαχειρίζεται την ανάκτηση/αποθήκευση των δεδομένων στο σύστημα. Το αντικείμενο View χρησιμοποιείται μόνο για να παρουσιάζεται η πληροφορία στον χρήστη (π.χ. με



γραφικό τρόπο). Το τρίτο μέρος είναι ο Controller ο οποίος δέχεται την είσοδο και στέλνει εντολές στο αντικείμενο Model και στο View.



Το μοντέλο Model-View-Controller (MVC) χρησιμοποιείται συνήθως για να χωρίσει την εφαρμογή μας σε τρία διασυνδεδεμένα μέρη. Αυτό γίνεται για να διαχωριστούν οι εσωτερικές αναπαραστάσεις (οντότητες της βάσης δεδομένων, διαδικασίες κτλ) από τον τρόπο με τον οποίο παρουσιάζονται αυτές οι πληροφορίες στο χρήστη.

2.9 Laravel

Η ανάπτυξη σύνθετων έργων χρειάζεται ακρίβεια και όσο το δυνατόν πιο απλοποιημένη προσέγγιση. Οι περισσότερες web εφαρμογές αναπτύσσονται σε PHP Frameworks. Αυτά τα Frameworks προσφέρουν μεγαλύτερη ασφάλεια, ακεραιότητα και φυσικά ευκολία, άρα μικρότερο κόστος ανάπτυξης.

Το Laravel θεωρείται το καλύτερο PHP Framework αυτή τη στιγμή, από την κοινότητα των προγραμματιστών. Προσθέτει εγκυρότητα και υπεροχή στο σύνολο του έργου ενώ διευκολύνει την ανάπτυξη με τα ενσωματωμένα εργαλεία προγραμματιστών που διαθέτει καθώς και με την ευκολία εγκατάστασης σε σχέση με άλλα frameworks.



2.10 XAMPP

Πρόκειται για τον ευκολότερο τρόπο εγκατάστασης του Apache server για Windows, Mac OS X, Linux και Solaris. Το XAMPP περιλαμβάνει επίσης στο ίδιο πακέτο εγκατάστασης όλα τα υπόλοιπα απαραίτητα λογισμικό και υπηρεσίες που απαιτούνται για να έχετε μέσα σε λιγότερο από μία ώρα έναν Apache Server εγκατεστημένο και έτοιμο να χρησιμοποιηθεί ώστε να μπορείτε να τρέξετε και να δοκιμάσετε τοπικά το web site σας πριν το ανεβάσετε στο διαδίκτυο.

Περιλαμβάνει Apache, MySQL, PHP, phpMyAdmin [βασικό database administration tool], τον FileZilla FTP server, τον Mercury mail server, τα απαραίτητα της προγραμματιστικής γλώσσας Perl, και τον JSP server Tomcat. Το καλύτερο όμως είναι ότι μέσω του μενού χειρισμού του XAMPP όλα τα παραπάνω παύουν να φαίνονται δύσκολα και γίνονται σχετικά εύκολα στην ρύθμιση ακόμα και για τον αρχάριο, αφού το πρόγραμμα τον καθοδηγεί βήμα βήμα!

Ο XAMPP είναι ένα πακέτο προγραμμάτων ελεύθερου λογισμικού, λογισμικού ανοικτού κώδικα και ανεξαρτήτου πλατφόρμας το οποίο περιέχει το εξυπηρετητή ιστοσελίδων http Apache, την βάση δεδομένων MySQL και ένα διερμηνέα για κώδικα γραμμένο σε γλώσσες προγραμματισμού PHP και Perl.

Το XAMPP είναι ελεύθερο λογισμικό το οποίο περιέχει ένα εξυπηρετητή ιστοσελίδων το οποίο μπορεί να εξυπηρετεί και δυναμικές ιστοσελίδες τεχνολογίας PHP/MySQL. Είναι ανεξάρτητο πλατφόρμας και τρέχει σε Microsoft Windows, Linux, Solaris, and Mac OS X και χρησιμοποιείται ως πλατφόρμα για την σχεδίαση και ανάπτυξη ιστοσελίδων με την τεχνολογίες όπως PHP, JSP και Servlets.

Επίσης οι σχεδιαστές του XAMPP προόριζαν το λογισμικό ως εργαλείο ανάπτυξης και δοκιμής ιστοσελίδων τοπικά στον υπολογιστή χωρίς να είναι απαραίτητη η σύνδεση στο διαδίκτυο. Για να είναι δυνατή η χρήση του, πολλές σημαντικές λειτουργίες ασφάλειας έχουν απενεργοποιηθεί [3]. Στην πράξη το XAMPP ορισμένες φορές χρησιμοποιείται και για την φιλοξενία ιστοσελίδων. Υπάρχει ειδικό εργαλείο το οποίο περιέχεται στο XAMPP για την προστασία με κωδικό των σημαντικών μερών. Το XAMPP υποστηρίζει την δημιουργία και διαχείριση βάσεων δεδομένων τύπου MySQL και SQLite.



Όταν το XAMPP εγκατασταθεί στον τοπικό υπολογιστή διαχειρίζεται τον localhost ως ένα απομακρυσμένο κόμβο, ο οποίος συνδέεται με το πρωτόκολλο μεταφοράς αρχείων FTP. Η σύνδεση στον localhost μέσω του FTP μπορεί να γίνει με το όνομα χρήστη «newuser» και το κωδικό «wampp». Για την βάση δεδομένων MySQL υπάρχει ο χρήστης «root» χωρίς κωδικό πρόσβασης.

2.11 REST

Το REST (Representational State Transfer) αποτελεί ένα σύνολο από αρχές σχεδίασης μιας δικτυακής υπηρεσίας που επικεντρώνει στους πόρους (π.χ δεδομένα) ενός συστήματος. Η μεταβολή της κατάστασης (ενέργεια επί) των πόρων του συστήματος περιγράφεται και μεταφέρεται στο σύστημα μέσω του πρωτοκόλλου HTTP από διάφορους clients (ανεξαρτήτως της γλώσσας στην οποία έχουν υλοποιηθεί). Για την ιστορία αξίζει να πούμε ότι το REST πρωτοεμφανίστηκε το 2000 από τον Roy Fielding στην ακαδημαϊκή του διατριβή με τίτλο «Architectural Styles and the Design of Network-based Software Architectures».

Με βάση το REST το URI δεν χρησιμοποιείται πια για την περιγραφή της ενέργειας που θέλουμε να εκτελέσουμε αλλά μόνο τον εντοπισμό του πόρου επί του οποίου θα ασκηθεί η ενέργεια, και τα δεδομένα δεν μεταφέρονται ως παράμετροι στο URI ενός GET αιτήματος αλλά ως XML ή JSON-formatted δεδομένα στο περιεχόμενο μιας POST ή PUT μεθόδου. Με άλλα λόγια σε μια υπηρεσία REST, ένα URI εκφράζει ένα αντικείμενο στο οποίο παρέχει πρόσβαση η υπηρεσία μέσω ενός HTTP αιτήματος. Το είδος του αιτήματος καθορίζει την ενέργεια που θέλουμε να εφαρμόσουμε στο αντικείμενο αυτό και το περιεχόμενο του αιτήματος περιέχει διάφορες εξειδικεύσεις της ενέργειας.

Οπότε ο σχεδιασμός μιας υπηρεσίας REST περιλαμβάνει κυρίως δύο βήματα. Πρώτον, να αποφασίσουμε τι αντικείμενα θα διαθέτουμε δια μέσω της υπηρεσίας και δεύτερον, τι ενέργεια θα εφαρμόζεται στο κάθε αντικείμενο για κάθε μία από τις GET, POST, PUT και DELETE μεθόδους. Αυτά είναι τα όπλα που έχουμε διαθέσιμα. Είναι τα όπλα μας περιορισμένα ή περιοριστικά (για τους σκοπούς μας); Υπό μία έννοια, ναι, γιατί δεν μας επιτρέπει να σχεδιάσουμε/ορίσουμε νέες και πιο εξειδικευμένες μεθόδους/ενέργειες επί των αντικειμένων. Αλλά αυτό είναι μια κοντόφθαλμη άποψη. Ο περιορισμός αυτός είναι καλός γιατί μας αναγκάζει να σχεδιάζουμε υπηρεσίες με ένα



κοινό καθορισμένο τρόπο, κάνοντας χρήση κάποιων απλών και δυνατών κανόνων. Από την άλλη, η εξειδίκευση των ενεργειών δεν είναι αδύνατη. Αρκεί να εφαρμόσουμε τις αρχές του OOP.

Μία υπηρεσία ή χρήστης του REST πρέπει να περιλαμβάνει εντός του HTTP αιτήματος (header και body) όλη την πληροφορία (action, parameters, context,...) που είναι απαραίτητη από τον server για την παραγωγή μιας απόκρισης στο αίτημα αυτό. Τα αιτήματα πρέπει να είναι ολοκληρωμένα και αυτόνομα έτσι ώστε κατά την επεξεργασία τους από τον server να μην απαιτούν την ανάσυρση κάποιας άλλης πληροφορίας η οποία να επηρεάζει την απόκριση στο ερώτημα. Αυτή η «έλλειψη κατάσταση» σε μια υπηρεσία REST απαλλάσσει τον server από την ανάγκη συγχρονισμού των δεδομένων μιας συνόδου με μια εξωτερική εφαρμογή. Ακόμα περισσότερο επιτρέπει στις υπηρεσίες REST να προσαρμόζονται σε περιπτώσεις όπου απαιτούνται υψηλές επιδόσεις χρησιμοποιώντας clusters of servers με διαμοιρασμό φορτίου (load-balancing) και δυνατότητες για failover, proxies και άλλες τοπολογίες οι οποίες θα προωθούν τα αιτήματα από τον ένα server στον άλλο με σκοπό την ελάττωση του συνολικού χρόνου απόκρισης στην κλήση μιας δικτυακής υπηρεσίας.



3 Αρχιτεκτονική του συστήματός μας

3.1 Τεχνικές απαιτήσεις

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

- Το σύστημα θα πρέπει να υποστηρίζει όλες εκείνες τις διαδικασίες που απαιτούνται για την ομαλή οργάνωση και διεξαγωγή των εκλογών. Ανάλογα του είδους των εκλογών οι υπηρεσίες που το σύστημα παρέχει ενδέχεται να περιλαμβάνουν την εγγραφή των ψηφοφόρων, την αυθεντικοποίησή τους, την ίδια τη ψήφο, τον υπολογισμό και την επιβεβαίωση του τελικού αποτελέσματος.
- Το σύστημα θα πρέπει να υποστηρίζει όλες τις συμμετέχουσες οντότητες (ρόλους). Χαρακτηριστικά αναφέρονται οι οργανωτές των εκλογών, οι εκπρόσωποι των κομμάτων οι υποψήφιοι, οι ψηφοφόροι κα.
- Το σύστημα πρέπει να παρέχει ένα φιλικό στο χρήστη περιβάλλον, ώστε να μπορεί να χρησιμοποιείται από οποιοδήποτε απλό φυλλομετρητή του Διαδικτύου (Web Browser).
- Το σύστημα πρέπει να υποστηρίζει ένα σύνολο υπηρεσιών και ενεργειών, ώστε να μπορεί να διευκολύνει το χρήστη κατά την χρησιμοποίησή του.
- Το σύστημα πρέπει να είναι σε θέση να υπολογίζει το τελικό αποτέλεσμα της καταμέτρησης των ψήφων.

Ωστόσο, από τα παραπάνω γίνεται φανερό ότι ένα σύστημα ηλεκτρονικής ψηφοφορίας ορίζει ένα μεγάλο αριθμό ευκαιριών σε επίδοξους επιτιθέμενους, οι



οποίοι ενδέχεται να οδηγήσουν το σύστημα σε κατάρρευση και κατ' επέκταση σε διακοπή (ακύρωση) της εκλογής διαδικασίας. Στο πλαίσιο αυτό γίνεται εμφανές ότι ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να σχεδιάζεται με τέτοιο τρόπο, ώστε να εγγυάται τη διατήρηση της ασφάλειας και της ιδιωτικότητας των συμμετεχόντων οντοτήτων. Το σύστημα, επομένως, πρέπει να βασίζεται σε ένα πρωτόκολλο ψηφοφορίας (voting protocol) το οποίο θα είναι σε θέση να αποτρέπει ευκαιρίες ενδεχόμενης απώλειας της ιδιωτικότητας του χρήστη (ψηφοφόρου). Στη συνέχεια παρουσιάζονται οι απαιτήσεις ασφάλειας που πρέπει να παρέχει κατ' ελάχιστο ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας.

3.2 Γενικές Απαιτήσεις Συστημάτων Ηλεκτρονικής Ψηφοφορίας

Παρόλο το μεγάλο αριθμό πλεονεκτημάτων που παρέχει ένα σύστημα ηλεκτρονικής ψηφοφορίας, τόσο όσο αφορά την οργάνωση των εκλογών όσο και την ίδια τη ψηφοφορία, η απόφαση για το σχεδιασμό και την υλοποίηση ενός τέτοιου συστήματος δεν είναι καθόλου απλή. Ο κυριότερος λόγος είναι ότι πρέπει ένα μεγάλο σύνολο απαιτήσεων να ικανοποιηθούν. Μια επιπλέον δυσκολία είναι ότι οι απαιτήσεις ασφάλειας ορίζονται με βάση διάφορες αφηρημένες έννοιες (π.χ. αρχές) προκειμένου να αποτελέσουν ένα σύνολο λειτουργικών και μη-λειτουργικών απαιτήσεων. Οι λειτουργικές απαιτήσεις ενός συστήματος ηλεκτρονικής ψηφοφορίας καθορίζουν κατά ελάχιστο ένα σύνολο υπηρεσιών (λειτουργιών) που το σύστημα πρέπει να υποστηρίζει διασφαλίζοντας ταυτόχρονα την ομαλή ροή αυτών, καθώς και τις ενδεχόμενες αλληλεπιδράσεις τους.

Για παράδειγμα, ο αριθμός και ο τύπος των εκάστοτε εκλογικών διαδικασιών που υποστηρίζονται από ένα σύστημα ηλεκτρονικής ψηφοφορίας καθορίζονται από το σύνολο των λειτουργικών του απαιτήσεων. Επιπλέον, οι λειτουργικές απαιτήσεις σχετίζονται με πολλές από τις ιδιότητες χρήσης του συστήματος καθορίζοντας τις λειτουργίες και τα χαρακτηριστικά που αυτό πρέπει να παρέχει κατά τη χρήση του. Από την άλλη μεριά, οι μη-λειτουργικές απαιτήσεις σχετίζονται με τη βασική υποδομή του συστήματος, δεν είναι άμεσα εμφανείς στους χρήστες και καθορίζουν πολλά από τα χαρακτηριστικά της αρχιτεκτονικής του συστήματος.



Οι απαιτήσεις ασφάλειας ορίζουν διάφορες ιδιότητες που αφορούν το σύστημα στο σύνολό του, όπως η ευελιξία του, η αποδοτικότητά του κ.ά., και προέρχονται από το σύνολο των μη-λειτουργικών απαιτήσεων.

Βασική αρχή, αποτελεί ότι οι λειτουργικές απαιτήσεις των συστημάτων ηλεκτρονικής ψηφοφορίας ενδέχεται να διαφέρουν από σύστημα σε σύστημα και αυτό διότι καθορίζονται από το σκοπό που το σύστημα καλείται να επιτελέσει. Αντιθέτως, η μεγάλη πλειοψηφία των απαιτήσεων ασφάλειας είναι κοινή σε όλα τα συστήματα ηλεκτρονικής ψηφοφορίας, αφού καθορίζουν τη συμμόρφωση του συστήματος με τις αρχές που διέπουν την εκάστοτε εκλογική διαδικασία, καθώς και με τα ζητήματα ασφάλειας και ιδιωτικότητας, τα οποία καθορίζονται από το εκάστοτε νομοθετικό και ρυθμιστικό πλαίσιο. Οι απαιτήσεις ασφάλειας στο σύνολό τους ικανοποιούνται από το πρωτόκολλο ψηφοφορίας που χρησιμοποιείται στο εκάστοτε σύστημα ηλεκτρονικής ψηφοφορίας. Επίσης, το πρωτόκολλο αυτό ορίζει την πλειονότητα των ιδιοτήτων του συστήματος στο σύνολό του (system wide attributes).

3.3 Απαιτήσεις Ασφάλειας

Στη συγκεκριμένη ενότητα παρουσιάζονται οι απαιτήσεις ασφάλειας που το πρωτόκολλο ηλεκτρονικής ψηφοφορίας πρέπει να παρέχει.

- Ορθότητα-Ακρίβεια (Accuracy)

Η ορθότητα απαιτεί ότι το τελικό ανακοινωθέν αποτέλεσμα της εκλογικής διαδικασίας είναι το ίδιο με το πραγματικό αποτέλεσμα των εκλογών, όπως αυτό προκύπτει από την καταμέτρηση των ψήφων. Αυτό κατ' επέκταση, σημαίνει ότι κανένας δεν είναι σε θέση να αλλάξει την ψήφο κάποιου άλλου ψηφοφόρου (inalterability), όλες οι έγκυρες ψήφοι συμπεριλαμβάνονται στο τελικό αποτέλεσμα (completeness) και καμία μη έγκυρη ψήφος δεν συμπεριλαμβάνεται στο τελικό αποτέλεσμα (soundness). (Ikonomopoulos 2002)

- Δημοκρατία (Democracy)

Ένα σύστημα χαρακτηρίζεται δημοκρατικό αν και μόνο αν νόμιμοι χρήστες επιτρέπεται να ψηφίσουν και κάθε νόμιμος χρήστης μπορεί να ψηφίσει μόνο μία



φορά. Ένα επιπλέον χαρακτηριστικό είναι ότι κανένας δεν είναι σε θέση να ψηφίσει εκ μέρους κάποιου άλλου. (Ikonomopoulos 2002)

- Ιδιωτικότητα (Privacy)

Η συγκεκριμένη απαίτηση σχετίζεται με το γεγονός ότι κανένας δεν είναι σε θέση να συνδέσει την ταυτότητα ενός ψηφοφόρου με την εκάστοτε ψήφο του.

Η υπολογιστική ιδιωτικότητα (computational privacy) αποτελεί μια ασθενή μορφή ιδιωτικότητας διασφαλίζοντας ότι η σχέση μεταξύ ψηφοδελτίου παραμένει μυστική για ένα μεγάλο χρονικό διάστημα, χρησιμοποιώντας ακόμα και τα πιο σύγχρονα και ισχυρά υπολογιστικά συστήματα. Η ιδιωτικότητα που βασίζεται στη θεωρία των πληροφοριών (informationtheoretic privacy) αποτελεί μια πιο ισχυρή μορφή διατήρησης της ιδιωτικότητας, η οποία διασφαλίζει ότι κανένα ψηφοδέλτιο δεν μπορεί να συσχετισθεί με κάποιο ψηφοφόρο όσο χρονικό διάστημα η θεωρία των πληροφοριών παραμένει ισχυρή. (Ikonomopoulos 2002)

- Ανθεκτικότητα (Robustness)

Η απαίτηση αυτή εγγυάται ότι δεν μπορεί να λάβει χώρα μια προσωρινή συνεργασία είτε ψηφοφόρων είτε αρχών (νόμιμη η κακόβουλη), η οποία θα μπορούσε να διακόψει την εκλογική διαδικασία. Η κατάσταση αυτή περιλαμβάνει τη δυνατότητα αποχής των ψηφοφόρων χωρίς την εμφάνιση προβλημάτων, καθώς, επίσης, και την αποτροπή παράνομων ενεργειών οι οποίες ενδέχεται να ακυρώσουν το αποτέλεσμα των εκλογών. Η απαίτηση της ανθεκτικότητας (ρωμαλεότητα, robustness) αφορά επίσης και το ότι η ασφάλεια του συστήματος πρέπει να ικανοποιείται και σε σχέση με εξωτερικές απειλές και επιθέσεις π.χ. επιθέσεις άρνησης υπηρεσιών (DoS attacks). (Ikonomopoulos 2002)

- Επαληθευσιμότητα (Verifiability)

Η επαληθευσιμότητα σχετίζεται με το ότι υπάρχουν μηχανισμοί για τον έλεγχο της εκλογικής διαδικασίας προκειμένου να διασφαλιστεί ότι αυτή διεξήχθη κανονικά. Η επαληθευσιμότητα μπορεί να επιτευχθεί σε τρεις (3) διαφορετικές μορφές:



- 1) οικουμενική επαληθευσσιμότητα, η οποία σχετίζεται με το ότι ο οποιοσδήποτε (ψηφοφόροι, αρχές, εξωτερικοί ελεγκτές κ.ά.) είναι σε θέση να επιβεβαιώσουν το αποτέλεσμα μετά την καταμέτρηση των ψήφων,
- 2) μεμονωμένη επαληθευσσιμότητα με ανοικτή αντίρρηση στην καταμέτρηση, η οποία επιτρέπει σε κάθε ψηφοφόρο να επιβεβαιώσει ότι η ψήφος του όντως καταμετρήθηκε σωστά, χωρίς, όμως, να αποκαλυφθεί το περιεχόμενο αυτής και
- 3) μεμονωμένη επαληθευσσιμότητα, η οποία επιτρέπει την ατομική επιβεβαίωση της ψήφου για κάθε ψηφοφόρο, αλλά από την άλλη απαιτεί την αποκάλυψη του ψηφοδελτίου του ψηφοφόρου σε περίπτωση καταγγελίας. (Ikonomopoulos 2002)

- Μη εξαναγκασμός (Uncoercibility)

Ένα σχήμα χωρίς απόδειξη (receipt-free scheme) είναι σε θέση να πείσει τους ψηφοφόρους ότι η ψήφος τους καταμετρήθηκε, χωρίς όμως να μπορεί να παρέχει απόδειξη για αυτό. Ένα σχήμα μη εξαναγκασμού (uncoercible scheme) δεν επιτρέπει στους ψηφοφόρους να πείσουν οποιονδήποτε για το τι έχουν ψηφίσει. Πιο συγκεκριμένα, στην περίπτωση αυτή ο ψηφοφόρος δεν κατέχει ούτε μπορεί να δημιουργήσει μια απόδειξη που να δείχνει το περιεχόμενο της ψήφου. Ενώ η έννοια του μη-εξαναγκασμού είναι πιο ισχυρή από το σχήμα χωρίς απόδειξη, η δεύτερη έννοια συνηθίζεται να χρησιμοποιείται στη βιβλιογραφία σαν το επικρατέστερο μέσο προκειμένου να διασφαλιστεί η ασφάλεια του συστήματος ηλεκτρονικής ψηφοφορίας. (Ikonomopoulos 2002)

- Αμεροληψία (Fairness)

Η ιδιότητα αυτή διασφαλίζει ότι κανένας δεν είναι σε θέση να μάθει το αποτέλεσμα της εκλογικής διαδικασίας πριν την τελική καταμέτρηση των ψήφων. Συνεπώς, διασφαλίζει ότι δεν θα επηρεαστούν οι τελευταίοι χρονικά ψηφοφόροι μέσω της ανακοίνωσης μιας εκτίμησης του αποτελέσματος και ότι δεν παρέχεται ένα πλεονέκτημα σε ένα συγκεκριμένο σύνολο οντοτήτων. (Ikonomopoulos 2002)

- Επαληθεύσιμη συμμετοχή (Verifiable participation)

Η συγκεκριμένη απαίτηση διασφαλίζει ότι υπάρχει δυνατότητα να βρεθεί αν ένας συγκεκριμένος ψηφοφόρος πήρε μέρος στην εκλογική διαδικασία ή όχι. Η



συγκεκριμένη απαίτηση είναι αναγκαία στις περιπτώσεις όπου η συμμετοχή στη ψηφοφορία είναι υποχρεωτική (πχ. Ελλάδα, Αυστραλία, Βέλγιο κα) ή σε περιπτώσεις οργανισμών ή σωματείων που ακόμα και το μέγεθος της αποχής έχει κάποιο συγκεκριμένο νόημα. (Ikonomopoulos 2002)

3.4 Ιδιότητες Συστήματος (System Properties)

Επιπρόσθετα με τις απαιτήσεις ασφάλειας ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να ικανοποιεί ένα σύνολο μη λειτουργικών απαιτήσεων.

Για παράδειγμα, το σύστημα πρέπει να είναι αξιόπιστο, φιλικό στο χρήστη, πρέπει να παρέχει την αρχή της «ίσης εκλογής», πρέπει να βασίζεται σε ανοικτές υπολογιστικές αρχιτεκτονικές και λογισμικό κ.ά. Στην ενότητα αυτή περιγράφονται οι ιδιότητες του συστήματος που σχετίζονται με το πρωτόκολλο ψηφοφορίας και αφορούν την ευκολία συμμετοχής των ψηφοφόρων, την δυνατότητα ψηφοφορίας από οποιαδήποτε τοποθεσία, την ευελιξία και την αποδοτικότητα.

- Ευκολία συμμετοχής των ψηφοφόρων (Voter convenience)

Η ευκολία συμμετοχής των ψηφοφόρων σχετίζεται με τη δυνατότητα της άμεσης ψηφοφορίας, όπως στις συμβατικές εκλογές, που οι ψηφοφόροι μπορούν να ψηφίσουν σε σύντομο χρονικό διάστημα, χωρίς να είναι αναγκαία η επιστροφή τους και η συνεργασία με τους αρμόδιους φορείς προκειμένου να ολοκληρωθεί η εκλογική διαδικασία. Είναι εμφανές ότι η συγκεκριμένη απαίτηση σχετίζεται μόνο με τη διαδικασία της ψηφοφορίας και για καμία άλλη διαδικασία των εκλογών, όπως η εγγραφή των ψηφοφόρων ή η καταμέτρηση των ψήφων. Επιπρόσθετα, η συγκεκριμένη ιδιότητα διασφαλίζει ότι μόνο συγκεκριμένο υλικό (hardware) είναι αναγκαίο για τη συμμετοχή κάποιου ψηφοφόρου στην εκλογική διαδικασία. Συνήθως το υλικό αυτό είναι ένας απλός προσωπικός υπολογιστής, χωρίς όμως να αποκλείονται άλλες συσκευές όπως ένα κινητό τηλέφωνο, μια ψηφιακή τηλεόραση κ.ά.

- Δυνατότητα ψηφοφορίας από οποιαδήποτε τοποθεσία (Voter mobility)

Προκειμένου να ελαχιστοποιηθούν οι περιορισμοί που ορίζουν οι συμβατικές εκλογικές διαδικασίες δεν πρέπει να υπάρχουν περιορισμοί όσο αφορά την τοποθεσία



όπου ένα ψηφοφόρος μπορεί να ψηφίσει. Ενώ φαίνεται ότι η συγκεκριμένη απαίτηση σχετίζεται με την ύπαρξη μιας κατάλληλα οριζόμενης και ασφαλούς κεντρικής βάσης δεδομένων στην πραγματικότητα ορίζονται σημαντικές δυσκολίες σε αρκετά εκλογικά σχήματα, τα οποία στηρίζονται σε διάφορες φυσικές παραδοχές για τη διασφάλιση αντιφατικών ιδιοτήτων ασφάλειας, όπως η επαληθευσιμότητα και η ιδιωτικότητα.

- Ευελιξία (flexibility)

Ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να επιτρέπει μια μεγάλη ποικιλία στη μορφή των ψηφοδελτίων, στις υποστηριζόμενες γλώσσες, καθώς και να μπορεί εύκολα να προσαρμοσθεί σε διάφορους τύπους εκλογικών διαδικασιών. Η δυνατότητα υποστήριξης ανοικτών ερωτήσεων (open-ended questions) μπορεί επίσης να υποστηριχθεί μέσω της συγκεκριμένης ιδιότητας, αλλά δεν είναι συμβατική με το σχήμα χωρίς απόδειξη (receipt-freeness).

- Αποδοτικότητα (Efficiency)

Με βάση τις τελευταίες εξελίξεις στο χώρο της τεχνολογίας, που σχετίζονται κυρίως με την απόδοση των υλικών και τη χωρητικότητα των επικοινωνιακών διαύλων, γίνεται σαφές ότι η απόδοση ενός συστήματος ηλεκτρονικής ψηφοφορίας αποτελεί μια ιδιότητα η οποία δεν μπορεί να αγνοηθεί. Στην πραγματικότητα σχεδόν κάθε μορφή εκλογικής διαδικασίας προϋποθέτει την ύπαρξη ισχυρών κρυπτογραφικών μηχανισμών, ενώ το φορτίο της δικτυακής επικοινωνίας αυξάνει ανάλογα των αριθμό των συμμετεχόντων οντοτήτων. Έτσι, η πολυπλοκότητα ενός σχήματος εκλογικής διαδικασίας αποτελεί μια σημαντική παράμετρο του συστήματος. Ο χρόνος που απαιτείται από ένα ψηφοφόρο προκειμένου να ολοκληρώσει τη διαδικασία ψηφοφορίας ορίζει ένα ανώτερο όριο στον αριθμό των ψηφοφόρων που επιτρέπεται να πάρουν μέρος στις εκλογές (scalability), στο χρόνο κατά τον οποίο επιτρέπεται η ηλεκτρονική ψηφοφορία καθώς και στους διαθέσιμους πόρους που χρησιμοποιούνται. (Ikonomopoulos 2002)



3.5 Επιμέρους ζητήματα ηλεκτρονικής ψηφοφορίας με χρήση Διαδικτύου

Τα θέματα που αναλύθηκαν προηγουμένως, αποτελούν θεμελιώδεις απαιτήσεις για τη διενέργεια γενικών, ελεύθερων, ισότιμων, ευθέων και δημοκρατικών εκλογών. Στη συνέχεια θα αναλύσουμε κάποιες απαιτήσεις ασφαλείας, που σχετίζονται, κυρίως, με θέματα ασφαλείας υπολογιστικών συστημάτων, έχουν, όμως, άμεση σχέση με μία εκλογική διαδικασία που βασίζεται σε υπολογιστές και τεχνολογίες δικτύου και κατ' επέκταση αφορούν εξ' ολοκλήρου τη διαδικασία μιας ηλεκτρονικής ψηφοφορίας.

3.5.1 Απαιτήσεις σε υλικό

Αρχικά πολύ σημαντικό ζήτημα είναι η επιλογή και συντήρηση κατάλληλου υλικού εξοπλισμού (hardware). Στην υπάρχουσα εκλογική διαδικασία το κυριότερο, αν όχι το μοναδικό υλικό, που χρησιμοποιείται είναι οι κάλπες και τα παραβάν. Όπως είναι προφανές δεν έχει νόημα να αναφέρουμε αυτό το θέμα ως απαίτηση ασφαλείας της συμβατικής εκλογικής διαδικασίας. Στην ηλεκτρονική ψηφοφορία, όμως, το θέμα του υλικού εξοπλισμού είναι πολύ σημαντικό. Ο τρόπος λειτουργίας του, καθώς και η ποιότητα των τμημάτων που το αποτελούν, πρέπει να είναι όσο το δυνατόν καλύτερης ποιότητας. Οι κίνδυνοι που μπορεί να προκύψουν από ελλιπές ή ελαττωματικό υλικό δεν προκύπτουν μόνο από ηθελημένη και κακόβουλη τροποποίηση του, αλλά και από ακούσια βλάβη. Όσον αφορά την κακόβουλη τροποποίηση του υλικού εξοπλισμού πρέπει να υπάρχουν εντατικοί έλεγχοι και κατά την κατασκευή του, αλλά και κατά το χρονικό διάστημα που θα ακολουθήσει μέχρι να χρησιμοποιηθούν. Πιθανή προσπάθεια τροποποίησης των μηχανημάτων, που χρησιμοποιούνται σε μια εκλογική διαδικασία, θα πρέπει να οδηγεί είτε σε αποτυχία της προσπάθειας είτε σε καταστροφή του μηχανήματος, έτσι ώστε ένα μηχάνημα που λειτουργεί να είναι σίγουρο πως δεν έχει υποστεί τροποποίηση. Όσον αφορά τυχόν βλάβη κατά τη διάρκεια της εκλογικής διαδικασίας, πρέπει να υπάρχει ειδικευμένο και εξουσιοδοτημένο προσωπικό σε κάθε εκλογικό κέντρο, ώστε να μπορεί άμεσα να επιδιορθώνει το πρόβλημα και να αποκαθιστά την ορθή λειτουργία του υλικού. Μέχρι τώρα έχουν γίνει διάφορες προτάσεις για ειδικά μηχανήματα που μπορούν να χρησιμοποιηθούν για μια εκλογική διαδικασία με επικρατέστερα μέχρι στιγμής τα DREs. Να αναφέρουμε πως μέσα στις ανάγκες για κατάλληλο υλικό μπορεί να



αναφερθεί τυχόν χρήση έξυπνων καρτών (smart cards) για αυθεντικοποίηση των χρηστών.

3.5.2 Απαιτήσεις σε λογισμικό

Εξίσου σημαντικό ζήτημα είναι και η ανάπτυξη και ο έλεγχος του λογισμικού που χρησιμοποιείται. Τα σημαντικότερα θέματα που φαίνεται να σχετίζονται με το λογισμικό έχουν να κάνουν με τους κρυπτογραφικούς αλγόριθμους και με τη διαφάνεια του κώδικα. Η κρυπτογραφία είναι, ίσως, το σημαντικότερο εργαλείο για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των ψήφων, αλλά και των μηχανισμών αυθεντικοποίησης των ψηφοφόρων. Η διαφάνεια του κώδικα είναι, επίσης, πολύ σημαντικό θέμα. Αρχικά, ο κώδικας πρέπει να είναι όσο το δυνατόν πιο απλός και ευκολονόητος, χωρίς βέβαια αυτό να σημαίνει υποβάθμιση της ασφάλειας. Όσο πιο απλός είναι ο κώδικας, τόσο πιο ευκολονόητος θα είναι και τόσο πιο εύκολος θα είναι ο έλεγχός του. Το να είναι ευκολονόητος ο κώδικας είναι βασικό στοιχείο για τη διαφάνεια του. Αυτό δεν σημαίνει βέβαια πως πρέπει οποιοσδήποτε, χωρίς κατάλληλο υπόβαθρο γνώσεων, να μπορεί να τον καταλάβει, αλλά δεν πρέπει ο κώδικας να είναι κατανοητός μόνο στην προγραμματιστική ομάδα που το δημιούργησε, όσο έμπιστη και κοινής αποδοχής και να είναι. Επίσης, ένας απλός και καλά δομημένος κώδικας μπορεί να οδηγήσει στην εύκολη και έγκαιρη ανίχνευση κάποιας προσθήκης μη-εξουσιοδοτημένων τμημάτων (δούρειοι ίπποι, ιοί, κ.λπ.).

3.5.3 Απαιτήσεις διασύνδεσης υπολογιστικών συστημάτων

Ένα ακόμα πολύ σημαντικό ζήτημα, που μπορεί να θέσει σε κίνδυνο μία ηλεκτρονική ψηφοφορία είναι το θέμα της διασύνδεσης των διαφόρων υπολογιστικών συστημάτων που μετέχουν στην διαδικασία. Όσο μεγαλύτερη είναι η χρήση δικτυακής τεχνολογίας, τόσο περισσότεροι είναι και οι κίνδυνοι που δημιουργούνται. Το κατά πόσο η διαδικασία της ηλεκτρονικής ψηφοφορίας θα προϋποθέτει χρήση δικτύου είναι κάτι που θα εξαρτηθεί από την ακριβή δομή της. Γεγονός είναι, πάντως, πως όσο μεγαλύτερη χρήση δικτυακών επικοινωνιών γίνεται, η διαδικασία γίνεται πιο λειτουργική, αλλά παράλληλα αυξάνονται και οι πιθανότητες για παραβίαση της ασφάλειάς της. Διάφορες προτάσεις που έχουν γίνει ανά διαστήματα προσεγγίζουν το ζήτημα με διαφορετικούς τρόπους. Το ότι σε κάθε εκλογικό κέντρο θα υπάρχουν ειδικά μηχανήματα που θα ψηφίζουν οι πολίτες δεν σημαίνει αυτόματα πως αυτά θα πρέπει να επικοινωνούν μεταξύ τους μέσω δικτύου. Η συγκέντρωση των



αποτελεσμάτων θα μπορούσε να γίνει με την χρήση CDs, η ακόμα και με τη χρήση διαφόρων μορφών κινητής μνήμης. Με αυτόν τον τρόπο η διαδικασία γίνεται πολύ πιο χρονοβόρα και το θέμα της ασφάλειας μετατίθεται στη φερεγγυότητα των ανθρώπων και των διαδικασιών μεταφοράς.



4 Νομικό Πλαίσιο της Ηλεκτρονικής Ψηφοφορίας

Η Αναζήτηση ενός Ευρωπαϊκού Νομικού Πλαισίου για τη Ηλεκτρονική Ψηφοφορία

4.1 Η Σύσταση (2004) 11 του Συμβουλίου της Ευρώπης

Η ανάγκη για καθιέρωση ομοιόμορφων προτύπων λειτουργίας για τη διεξαγωγή ηλεκτρονικής ψηφοφορίας στα ευρωπαϊκά κράτη, έγινε αντιληπτή από το Συμβούλιο της Ευρώπης, το οποίο συγκρότησε μια πολυεπιστημονική ad hoc Επιτροπή, με τη συμμετοχή ειδικών σε θέματα νομικών, λειτουργικών και τεχνικών προτύπων, ώστε να καθοριστούν συστάσεις για την ηλεκτρονική ψηφοφορία. Στόχος υπήρξε η ανάπτυξη προτύπων που θα μπορούσαν να προταθούν στα κράτη μέλη που ενδιαφέρονται για εφαρμογή προγραμμάτων ηλεκτρονικής ψηφοφορίας. Τα πρότυπα αυτά παρουσιάζονται στη Σύσταση (2004) 11 που υιοθετήθηκε από την Επιτροπή Υπουργών των κρατών μελών του Συμβουλίου της Ευρώπης στις 30 Σεπτεμβρίου 2004 (Rec. 2004). Η Σύσταση παρουσιάζει εξαιρετικό ενδιαφέρον, εφόσον στην απουσία αντίστοιχου κειμένου της Ευρωπαϊκής Ένωσης, συνιστά το μοναδικό διεθνές νομικό κείμενο που αφορά στις αρχές διεξαγωγής της ηλεκτρονικής ψηφοφορίας. Στόχο της σύστασης αποτελεί η υιοθέτηση περαιτέρω δράσης μέσα σε σύντομο χρονικό διάστημα, που κατ' αρχήν καθορίστηκε σε δύο έτη από την υιοθέτηση της Σύστασης.

Η Σύσταση (2004) 11 στηρίζεται στην αρχή ότι τόσο η αντιπροσωπευτική, όσο και η άμεση δημοκρατία συνιστούν μέρος της κοινής κληρονομιάς των ευρωπαϊκών κρατών μελών και συνιστούν τη βάση της συμμετοχής των πολιτών στην πολιτική ζωή σε εθνικό, περιφερειακό και τοπικό επίπεδο, όσο και στο επίπεδο της Ευρωπαϊκής Ένωσης. Αναγνωρίζεται επομένως από το Συμβούλιο της Ευρώπης ότι η άμεση δημοκρατία συνιστά μέρος του ευρωπαϊκού συστήματος συμμετοχικής δημοκρατίας και ότι περαιτέρω το δικαίωμα ψήφου είναι πρωταρχικό θεμέλιο του δημοκρατικού θεσμού. Για το λόγο αυτό οποιοδήποτε σύστημα ηλεκτρονικής ψηφοφορίας θα πρέπει να συμβαδίζει προς τις δημοκρατικές αρχές που εφαρμόζονται τόσο σε εκλογές, όσο και σε δημοψηφίσματα. Το Συμβούλιο της Ευρώπης περαιτέρω σημειώνει ότι οι νέες τεχνολογίες χρησιμοποιούνται ολοένα και περισσότερο στην καθημερινή πραγματικότητα και για το λόγο αυτό τα κράτη μέλη οφείλουν να λάβουν υπόψη τις εξελίξεις αυτές κατά την άσκηση των δημοκρατικών τους πρακτικών. (Rec.



2004) Στη Σύσταση σημειώνεται ότι αρκετά κράτη μέλη χρησιμοποιούν ήδη μεθόδους ηλεκτρονικής ψηφοφορίας για την ικανοποίηση αριθμού στόχων τους και συγκεκριμένα:

- Για τη διευκόλυνση της διαδικασίας ψηφοφορίας.
- Για την παροχή δυνατότητας ψηφοφορίας σε ετεροδημότες ή πρόσωπα που διαμένουν ή βρίσκονται στην αλλοδαπή.
- Για την παροχή πρόσβασης στη ψηφοφορία σε πρόσωπα με αναπηρίες ή άλλα πρόσωπα που αντιμετωπίζουν δυσκολίες στο να παρευρίσκονται στα εκλογικά σημεία.
- Για την αύξηση της συμμετοχής στις εκλογικές διαδικασίες και στα δημοψηφίσματα, με δεδομένο ότι παρατηρείται μια διαρκώς αυξανόμενη και ανησυχητική τάση αποχής των ψηφοφόρων από τις διαδικασίες αυτές.
- Για την μείωση του συνολικού κόστους της ψηφοφορίας ή της εκλογικής διαδικασίας.
- Για την ταχύτερη ετοιμασία και ανακοίνωση των αποτελεσμάτων των εκλογών ή της ψηφοφορίας, μέσα από την υιοθέτηση και χρήση της νέας τεχνολογίας. (Rec. 2004)

Για το λόγο αυτό το Συμβούλιο της Ευρώπης δηλώνει θετικά διακείμενο προς την προώθηση των συστημάτων ηλεκτρονικής ψηφοφορίας, εφόσον διασφαλίζεται ότι αυτά είναι ασφαλή, αξιόπιστα, αποτελεσματικά, τεχνικά προστατευμένα, ανοικτά σε ανεξάρτητη αξιολόγηση και εύκολα προσβάσιμα στους ψηφοφόρους. Η ηλεκτρονική ψηφοφορία θα πρέπει απαραίτητα να είναι αξιόπιστη και ασφαλής, τουλάχιστον όσο και μια δημοκρατική ψηφοφορία που δεν διεξάγεται με ηλεκτρονικά μέσα και θα πρέπει επομένως να εφαρμόζονται όλες οι αρχές που διέπουν τις δημοκρατικές εκλογές και τα δημοψηφίσματα. Προς το σκοπό αυτό η πολυεπιστημονική προσέγγιση του ζητήματος της ηλεκτρονικής ψηφοφορίας είναι απαραίτητη, εφόσον κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν θα είναι ποτέ αποτελεσματικό ή θα τυγχάνει κοινωνικής αποδοχής, παρά μόνο αν τόσο οι νομικές, όσο και οι λειτουργικές και τεχνικές παράμετροι αντιμετωπιστούν συνδυασμένα. Οποιαδήποτε



ανάλυση των τεχνικών παραμέτρων, χωρίς να πραγματοποιείται ταυτόχρονα και ανάλυση των νομικών παραμέτρων, ώστε το σύστημα ηλεκτρονικής ψηφοφορίας να ενταχθεί μέσα στο πλαίσιο της συζήτησης για το νόημα της δημοκρατίας ως πολιτικού συστήματος διακυβέρνησης, θα παρέμενε εκ των πραγμάτων ελλιπής. Η ηλεκτρονική ψηφοφορία αφορά άμεσα τη δημοκρατία και την υπόσταση της πολιτείας και ως τέτοια απαιτεί πολύπλευρη και επιστημονική ανάλυση των διαφόρων πτυχών της, νομικών, λειτουργικών και τεχνικών. Για το λόγο αυτό τα νομικά πρότυπα σχετίζονται με το νομικό πλαίσιο μέσα στο οποίο επιτρέπεται η διεξαγωγή ηλεκτρονικής ψηφοφορίας, τα λειτουργικά πρότυπα σχετίζονται με τον τρόπο με τον οποίο λειτουργούν και διατηρούνται τα υλισμικά και λογισμικά συστήματα, ενώ τα τεχνικά πρότυπα σχετίζονται με την κατασκευή και λειτουργία των υλισμικών και λογισμικών συστημάτων ηλεκτρονικής ψηφοφορίας. (Rec. 2004)

Η υιοθέτηση κοινών προτύπων, ενός δηλαδή ευρωπαϊκού πλαισίου για τη διεξαγωγή της ηλεκτρονικής ψηφοφορίας στα κράτη μέλη του Συμβουλίου της Ευρώπης, θεωρήθηκε ως απαραίτητη ώστε να κατοχυρωθεί η τήρηση των δημοκρατικών αρχών κατά τρόπο που να υπάρξει αύξηση της εμπιστοσύνης των πολιτών στα επί μέρους κρατικά συστήματα ηλεκτρονικής ψηφοφορίας. Η διακρατική συνεργασία μπορεί εξάλλου να καταστήσει τα συστήματα περισσότερη ασφαλή και αποτελεσματικά, μέσω της ανταλλαγής εμπειριών και να οδηγήσει στη μείωση του κόστους λειτουργίας των συστημάτων αυτών. Κατά την κατάρτιση των προτύπων λήφθηκαν υπόψη τα θεμελιώδη διεθνή κείμενα που αφορούν σε εκλογικές διαδικασίες, όπως η Οικουμενική Διακήρυξη Ανθρωπίνων Δικαιωμάτων του ΟΗΕ, το Διεθνές Σύμφωνο για Αστικά και Πολιτικά Δικαιώματα, η Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών και ιδιαίτερα το Πρωτόκολλο 1, ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ε.Ε. και ο Κώδικας Ορθής Πρακτικής σε Εκλογικά Ζητήματα, που υιοθετήθηκε από το Συμβούλιο Δημοκρατικών Εκλογών του Συμβουλίου της Ευρώπης. (Venice Commission 2003)

4.2 Νομικά Πρότυπα

Ως ηλεκτρονική ψηφοφορία ορίζεται σύμφωνα με τη Σύσταση οποιαδήποτε εκλογική διαδικασία ή δημοψήφισμα που περιλαμβάνει την χρήση ηλεκτρονικών μέσων σε ό,τι αφορά την ψηφοφορία. Ως απομακρυσμένη ηλεκτρονική ψηφοφορία



όμως νοείται η ηλεκτρονική ψηφοφορία στην οποία η ψηφοφορία διεξάγεται μέσω οργάνου που δεν ελέγχεται από τους εκλογικούς λειτουργούς. Θα πρέπει στο σημείο αυτό να αναφερθεί ότι η Ευρωπαϊκή Επιτροπή για τη Δημοκρατία μέσα από το Δίκαιο (European Commission for Democracy through Law — Venice Commission), συνέταξε έκθεση που αφορά τη συμβατότητα της απομακρυσμένης ψηφοφορίας και κατά συνέπεια και της απομακρυσμένης ηλεκτρονικής ψηφοφορίας, με τις αρχές του Συμβουλίου της Ευρώπης και κατέληξε στο συμπέρασμα ότι η απομακρυσμένη ψηφοφορία δεν αντίκειται προς τα πρότυπα του Συμβουλίου της Ευρώπης, εφόσον λαμβάνονται ορισμένα αναγκαία μέτρα προστασίας. (Venice Commission 2004) Τα νομικά πρότυπα που θα πρέπει να διέπουν μια ηλεκτρονική ψηφοφορία είναι τα ακόλουθα:

α) Καθολική Ψηφοφορία: Η διαδικασία ψηφοφορίας θα πρέπει να είναι εύκολα κατανοητή και χρηστική, χωρίς να τίθενται επιπρόσθετες προϋποθέσεις για τη συμμετοχή του ψηφοφόρου στη διαδικασία. Αν και κανένα σύστημα ψηφοφορίας δεν μπορεί εκ των πραγμάτων να γίνεται κατανοητό και να είναι χρηστικό σε κάθε δυνητικό ψηφοφόρο, θα πρέπει πάντως να καταβάλλεται προσπάθεια ώστε το σύστημα να είναι εύκολα κατανοητό και χρηστικό στη συντριπτική πλειοψηφία του πληθυσμού, χωρίς να παρεμποδίζεται οποιοσδήποτε από το να συμμετέχει στη διαδικασία ψηφοφορίας λόγω πολύπλοκων διαδικασιών εγγραφής ή ταυτοποίησης ή επαλήθευσης της ταυτότητας. Τα συστήματα ηλεκτρονικής ψηφοφορίας θα πρέπει να είναι σχεδιασμένα με τέτοιο τρόπο, ώστε να αυξάνονται οι πρακτικές δυνατότητες συμμετοχής στη διαδικασία των προσώπων με αναπηρίες στο μέγιστο δυνατό βαθμό. Ενώσω η δυνατότητα απομακρυσμένης ψηφοφορίας δεν παρέχεται καθολικά στους ψηφοφόρους, η ηλεκτρονική ψηφοφορία θα πρέπει να παραμένει μόνο ως επιπρόσθετη και προαιρετική μέθοδος ψηφοφορίας. Στόχος της χρήσης της ηλεκτρονικής ψηφοφορίας είναι η ενίσχυση της συμμετοχής, η μείωση της αποχής και η ενδυνάμωση της αρχής της καθολικότητας της ψηφοφορίας. Για το λόγο αυτό η ηλεκτρονική ψηφοφορία δεν θα πρέπει να συνιστά την αποκλειστική μέθοδο ψηφοφορίας, όσο υπάρχουν πρόσωπα που για οποιοδήποτε λόγο δεν έχουν πρόσβαση σε υπολογιστές λόγω οικονομικών ή κοινωνικών συνθηκών ή ικανότητα να χρησιμοποιούν υπολογιστές λόγω ηλεκτρονικού αναλφαριθμητισμού. (Νομικά Πρότυπα 1–4)



β) Τση Ψηφοφορία: Ο ψηφοφόρος σε οποιαδήποτε εκλογική διαδικασία ή δημοψήφισμα θα εμποδίζεται από το να ψηφίσει περισσότερο από μια φορά. Ο ψηφοφόρος θα δικαιούται να ψηφίσει, μόνο εφόσον εξακριβωθεί ότι η ψήφος του δεν έχει ακόμα εισαχθεί στην κάλπη. Επομένως το σύστημα θα πρέπει να παρεμποδίζει τις πολλαπλές ψήφους από τον ίδιο ψηφοφόρο, κάτι που θα παραβίαζε εκ των πραγμάτων την ισότητα της ψήφου και θα προσέδιδε περισσότερα δικαιώματα σε ένα ψηφοφόρο σε σύγκριση προς τους υπόλοιπους. Κάτι τέτοιο θα μπορούσε να συμβεί μεταξύ άλλων, και αν ένα τρίτο πρόσωπο χρησιμοποιούσε τα στοιχεία του ψηφοφόρου ώστε να ψηφίσει στο όνομα του τελευταίου και είχε ψηφίσει και ο ίδιος ο ψηφοφόρος. Για το λόγο αυτό η τοπική νομοθεσία θα πρέπει να προβλέπει για μεθόδους αυθεντικοποίησης των στοιχείων του ψηφοφόρου. Επιπρόσθετα, το σύστημα ηλεκτρονικής ψηφοφορίας θα πρέπει να εμποδίζει τον ψηφοφόρο από το να ψηφίζει μέσω περισσότερων από μια μεθόδους ψηφοφορίας. Κάθε ψήφος που θα κατατίθεται στην κάλπη μέσω ηλεκτρονικών μεθόδων ψηφοφορίας, θα προσμετράται μόνο μια φορά. Σε περίπτωση που χρησιμοποιούνται κατά την ίδια εκλογική αναμέτρηση, τόσο ηλεκτρονικές, όσο και μη ηλεκτρονικές μέθοδοι ψηφοφορίας, θα πρέπει να υφίσταται μια ασφαλής και αξιόπιστη μέθοδος για να προσμετρώνται όλες οι ψήφοι και να υπολογίζεται το ορθό αποτέλεσμα. (Νομικά Πρότυπα 5–8)

γ) Ελεύθερη Ψηφοφορία: Η οργάνωση της ηλεκτρονικής ψηφοφορίας θα διασφαλίζει την ελεύθερη διαμόρφωση και έκφραση της γνώμης του ψηφοφόρου και όποτε απαιτείται, την αυτοπρόσωπη άσκηση του δικαιώματος ψήφου. Η μέθοδος με την οποία οι ψηφοφόροι θα καθοδηγούνται μέσα από την διαδικασία της ηλεκτρονικής ψηφοφορίας θα είναι τέτοιας φύσης, ώστε να εμποδίζεται η απερίσκεπτη ψηφοφορία, δηλαδή χωρίς να παρέχεται χρόνος στον ψηφοφόρο να συλλογιστεί την ψήφο του. Για το λόγο αυτό, οι ψηφοφόροι θα έχουν τη δυνατότητα να μεταβάλουν την ψήφο τους σε οποιοδήποτε σημείο της διαδικασίας ηλεκτρονικής ψηφοφορίας, προτού ψηφίσουν, χωρίς να καταγράφονται οι προηγούμενες επιλογές τους ή να καθίστανται αυτές διαθέσιμες σε τρίτα πρόσωπα. Επομένως το σύστημα θα πρέπει να επισημαίνει με σαφήνεια το χρονικό σημείο κατά το οποίο η ψήφος έχει επιτυχώς κατατεθεί στην κάλπη και το σημείο ολοκλήρωσης της διαδικασίας ψηφοφορίας. Οι πιο πάνω ρυθμίσεις αναφέρονται σε πρακτικές όπως της Δανίας και της Σουηδίας στις οποίες γίνεται δεκτή η λεγόμενη προκαταρκτική ψηφοφορία που μεταγενέστερα μπορεί να



μεταβληθεί. Σε αντίθεση όμως με το Εσθονικό σύστημα για το οποίο έγινε λόγος πιο πάνω, τα πρότυπα της Σύστασης του Συμβουλίου της Ευρώπης καθορίζουν ότι το σύστημα ηλεκτρονικής ψηφοφορίας θα εμποδίζει τη μεταβολή της ψήφου, μετά την επιτυχή κατάθεσή της στην κάλπη. Το σύστημα ηλεκτρονικής ψηφοφορίας δεν πρέπει επίσης να επιτρέπει την άσκηση οποιασδήποτε αθέμιτης επιρροής στον ψηφοφόρο κατά τη διάρκεια της ψηφοφορίας και να παρέχει στον ψηφοφόρο τη δυνατότητα να συμμετάσχει στη διαδικασία, ακόμα και χωρίς να εκφράζει οποιαδήποτε προτίμηση για κάποια από τις επιλογές ψηφοφορίας, όπως μέσα από την κατάθεση λευκής ψήφου. Ήχοι που μπορούν να συνδεθούν με ένα υποψήφιο ή επιλογή, παρεμβολές στην οθόνη που προωθούν μια συγκεκριμένη επιλογή και παρόμοιες μέθοδοι, θα πρέπει να αποφεύγονται στο μέτρο του δυνατού, διότι θεωρούνται ως άσκηση αθέμιτης επιρροής. (Νομικά Πρότυπα 9–15)

δ) Μυστική Ψηφοφορία: Η ηλεκτρονική ψηφοφορία θα οργανώνεται με τέτοιο τρόπο ώστε να εξαιρεί σε οποιοδήποτε στάδιο της διαδικασίας ψηφοφορίας και ιδιαίτερα κατά το σημείο αυθεντικοποίησης των στοιχείων του ψηφοφόρου, οτιδήποτε το οποίο θα μπορούσε πιθανώς να θέσει σε κίνδυνο τη μυστικότητα της ψήφου. Η μυστικότητα θα πρέπει να εφαρμόζεται τόσο κατά το στάδιο πριν από την ψηφοφορία, όπως κατά τη μεταβίβαση των ηλεκτρονικών ψήφων ή των κωδικών ασφαλείας στους ψηφοφόρους, όσο και κατά το στάδιο της ψηφοφορίας, αλλά και κατά το στάδιο της καταμέτρησης και επανακαταμέτρησης των ψήφων. Το σύστημα ηλεκτρονικής ψηφοφορίας θα κατοχυρώνει ότι οι ψήφοι που βρίσκονται στην ηλεκτρονική κάλπη και οι ψήφοι που καταμετρούνται, είναι και θα παραμείνουν ανώνυμοι και ότι δεν θα είναι δυνατό να ανακατασκευασθεί σύνδεση μεταξύ του ψηφοφόρου και της ψήφου. Σε ορισμένες περιπτώσεις είναι γεγονός ότι η νομοθεσία απαιτεί την ύπαρξη ενός μόνιμου συνδέσμου μεταξύ της ψήφου και του ψηφοφόρου που θα διατηρείται κατά την εκλογική περίοδο και για καθορισμένη μεταγενέστερη χρονική περίοδο. Παρόμοια στοιχεία θα μπορούν να αποκαλύπτονται μόνο μετά από απόφαση αρμόδιου δικαστηρίου και ακόμα και αν αποκαλυφθούν, δεν θα πρέπει να υποχρεώνεται ένας ψηφοφόρος να αποκαλύπτει πως ψήφισε παρά τη θέλησή του. Το σύστημα ηλεκτρονικής ψηφοφορίας θα σχεδιασθεί με τέτοιο τρόπο ώστε ο αναμενόμενος αριθμός ψήφων σε κάθε ηλεκτρονική ψηφοφορία να μην επιτρέπει τη σύνδεση μεταξύ του αποτελέσματος και ατομικών ψηφοφόρων. Θα λαμβάνονται



επίσης μέτρα, ώστε να διασφαλίζεται πως οι πληροφορίες που χρειάζονται κατά τη διάρκεια της ηλεκτρονικής διαδικασίας δεν θα χρησιμοποιούνται κατά παράβαση της μυστικότητας της ψήφου. Παρόμοια μέτρα μπορεί να περιλαμβάνουν την τυχαία τοποθέτηση των ψήφων στην ηλεκτρονική κάλπη, κατά τρόπο ώστε να μην μπορεί να ανασκευαστεί η σειρά με την οποία οι ψήφοι τοποθετήθηκαν στην κάλπη. (Νομικά Πρότυπα 16–19)

Στη Σύσταση προβλέπονται εξάλλου διαδικαστικά νομικά πρότυπα τα οποία θα πρέπει να ακολουθούνται κατά την εκλογική διαδικασία. Αυτά είναι:

ι) Διαφάνεια: Τα κράτη μέλη θα λαμβάνουν μέτρα ώστε να διασφαλίζεται πως οι ψηφοφόροι κατανοούν και έχουν εμπιστοσύνη στο σύστημα ηλεκτρονικής ψηφοφορίας που χρησιμοποιούν. Για το λόγο αυτό οι πληροφορίες αναφορικά με τη λειτουργία του συστήματος ηλεκτρονικής ψηφοφορίας θα πρέπει να καθίστανται δημόσια διαθέσιμες, ενώ οι ψηφοφόροι θα έχουν τη δυνατότητα να δοκιμάσουν οποιαδήποτε νέα μέθοδο ηλεκτρονικής ψηφοφορίας πριν και ξεχωριστά από την τελική διεξαγωγή της ψηφοφορίας. Η εμπιστοσύνη των ψηφοφόρων στο σύστημα ψηφοφορίας είναι απαραίτητο συστατικό, όχι μόνο για την αύξηση της συμμετοχής των ψηφοφόρων, αλλά επίσης και για την υγιή ανάπτυξη της δημοκρατίας. Χωρίς κατανόηση δεν μπορεί να υπάρξει και εμπιστοσύνη. Με δεδομένο ότι η εισαγωγή συστημάτων ηλεκτρονικής ψηφοφορίας καθιστά εκ των πραγμάτων την εκλογική διαδικασία μέσω των συστημάτων αυτών, πρωτόγνωρη για τους ψηφοφόρους, θα πρέπει να ληφθούν μέτρα ώστε να αναπτυχθεί η κατανόηση και εμπιστοσύνη των ψηφοφόρων, προτού καταστεί δυνατή η εισαγωγή οποιουδήποτε συστήματος το οποίο να φιλοδοξεί να αντικαταστήσει μόνιμα και συνολικά τα παραδοσιακά συστήματα ψηφοφορίας. Ιδιαίτερη προσοχή θα πρέπει να δοθεί σε πρόσωπα μεγαλύτερης ηλικίας ή πρόσωπα που δεν είναι εξοικειωμένα με την χρήση υπολογιστών, τα οποία χρειάζονται περισσότερης επεξήγησης. Οποιοιδήποτε παρατηρητές, στο βαθμό που επιτρέπεται από το νόμο, θα δικαιούνται να παρίστανται και να σχολιάζουν τη διαδικασία ηλεκτρονικής ψηφοφορίας και την εξακρίβωση των αποτελεσμάτων. Τέτοιοι παρατηρητές προβλέπονται μεταξύ άλλων από τα Έγγραφα της Συνάντησης της Κοπεγχάγης σχετικά με την Ανθρώπινη Διάσταση του ΟΑΣΕ και μπορεί να



προέρχονται είτε από άλλα κράτη μέλη, είτε και από ιδιωτικούς οργανισμούς. Οι παρατηρητές θα πρέπει να βρίσκονται σε θέση να επιβεβαιώσουν ότι ο σχεδιασμός και η λειτουργία του συστήματος σέβεται τις θεμελιώδεις αρχές για τη διεξαγωγή δημοκρατικών εκλογών και δημοψηφισμάτων και κατά συνέπεια θα πρέπει να έχουν τη δυνατότητα πρόσβασης σε έγγραφα και ελεγκτικές πληροφορίες που αφορούν στα συστήματα ηλεκτρονικής ψηφοφορίας που χρησιμοποιούνται, σε λογισμικό, σε μέτρα ασφαλείας, αλλά και στην ίδια τη διαδικασία όπως ακολουθείται στην πράξη. (Νομικά Πρότυπα 20–23)

ii) Επαληθευσιμότητα: Τα συστατικά στοιχεία του συστήματος ηλεκτρονικής ψηφοφορίας θα αποκαλύπτονται στις αρμόδιες εκλογικές αρχές για σκοπούς επαλήθευσης και πιστοποίησης, ενώ ένα ανεξάρτητο όργανο που θα διορίζεται από τις εκλογικές αρχές θα επαληθεύει ότι το σύστημα ηλεκτρονικής ψηφοφορίας λειτουργεί ορθά και ότι όλα τα αναγκαία μέτρα ασφάλειας έχουν ληφθεί. Είναι αναγκαίο να πιστοποιηθούν μέσα από ενδελεχή εξέταση, μεταξύ άλλων, ο σχεδιασμός του συστήματος, ο πηγαίος κωδικός, τα συστατικά στοιχεία του συστήματος ασφαλείας και να διεξαχθούν αν χρειάζεται δοκιμές ώστε να εξακριβωθεί η αξιοπιστία του συστήματος. Το σύστημα εξάλλου θα πρέπει να παρέχει τη δυνατότητα επανακαταμέτρησης των ψήφων. Η επανακαταμέτρηση μπορεί να συνίσταται σε μια απλή δεύτερη καταμέτρηση εντός του συστήματος, αλλά μπορεί επίσης να συνίσταται σε μεταφορά της ηλεκτρονικής κάλπης σε ένα παρόμοιο, αλλά ξεχωριστό σύστημα ηλεκτρονικής ψηφοφορίας στο οποίο θα διενεργηθεί η δεύτερη καταμέτρηση. Μια τρίτη επιλογή συνιστά η επανακαταμέτρηση από ένα διαφορετικό σύστημα που να λειτουργεί παράλληλα προς το σύστημα ηλεκτρονικής ψηφοφορίας (Νομικά Πρότυπα 24–27).

iii) Αξιοπιστία και Ασφάλεια: Οι αρχές των κρατών μελών θα διασφαλίζουν την αξιοπιστία και ασφάλεια του συστήματος ηλεκτρονικής ψηφοφορίας, λαμβάνοντας όλα τα αναγκαία μέτρα ώστε να αποφεύγεται η πιθανότητα απάτης ή μη εξουσιοδοτημένης παρέμβασης που να επηρεάζει το σύστημα κατά τη διάρκεια της διαδικασίας ψηφοφορίας. Οι αρχές των κρατών μελών οφείλουν να ικανοποιηθούν εξάλλου ότι το σύστημα ηλεκτρονικής



ψηφοφορίας είναι γνήσιο και λειτουργεί με ορθό τρόπο. Η πιο πάνω πιστοποίηση δεν μπορεί να διεξάγεται μόνο από τον ιδιώτη προμηθευτή, στην απουσία των κρατών μελών, ακόμα και αν ο ιδιώτης προμηθευτής είναι διατεθειμένος να παράσχει έγγραφες διαβεβαιώσεις, διότι η πιστοποίηση της Δημοκρατίας δεν μπορεί να αφεθεί στα χέρια ιδιωτών. Σημειώνεται ότι μόνο πρόσωπα που έχουν διοριστεί από τις εκλογικές αρχές θα έχουν πρόσβαση στη βάση δεδομένων εκλογής, ενώ ομάδες αποτελούμενες από δύο τουλάχιστον πρόσωπα θα αναλαμβάνουν τους κρίσιμους τεχνικούς ελέγχους. Το σύστημα θα πρέπει επίσης να περιλαμβάνει μέτρα για τη διατήρηση της διαθεσιμότητας των υπηρεσιών του κατά τη διάρκεια βλαβών, επιθέσεων ή και κατάρρευσης του συστήματος. Είναι βέβαια γεγονός ότι η πιθανότητα κατάρρευσης δεν μπορεί ποτέ να αποκλειστεί πλήρως και κατά συνέπεια όλοι οι έλεγχοι θα πρέπει να διεξάγονται με κριτήριο την εύλογη άσκηση της μέγιστης δυνατής επιμέλειας. Θα πρέπει επίσης να διατηρεί τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των ψήφων και να τους τηρεί σφραγισμένους ή κρυπτογραφημένους μέχρι και την καταμέτρηση. Κρυπτογραφημένες θα παραμένουν και οι πληροφορίες που αφορούν στους ψηφοφόρους. (Νομικά Πρότυπα 28–35)

4.3 Λειτουργικά Πρότυπα

Τα Λειτουργικά Πρότυπα της Σύστασης του Συμβουλίου της Ευρώπης μπορούν να χωριστούν σε τρία στάδια: το στάδιο πριν από την ψηφοφορία, το στάδιο της ψηφοφορίας και το στάδιο μετά την ψηφοφορία.

Α) Στάδιο πριν από την Ψηφοφορία: Η τοπική νομοθεσία πρέπει να προβλέπει σαφή χρονοδιαγράμματα αναφορικά με όλα τα στάδια της διαδικασίας και η χρονική περίοδος διεξαγωγής της ψηφοφορίας και ιδιαίτερα της απομακρυσμένης ψηφοφορίας θα πρέπει να είναι γνωστή εκ των προτέρων από το κοινό με σαφή και κατανοητή γλώσσα. Θα πρέπει να υπάρχει ένα μητρώο ψηφοφόρων που θα ανανεώνεται συχνά, ώστε ο ψηφοφόρος να μπορεί να επιτηρεί και επιβεβαιώνει τις πληροφορίες που περιέχονται σε αυτό και τον αφορούν. Θα πρέπει επίσης να εξεταστεί η δυνατότητα δημιουργίας μηχανισμού που να επιτρέπει την υποβολή αίτησης για εγγραφή στους εκλογικούς καταλόγους μέσω του διαδικτύου, όπως και η



δυνατότητα υποβολής υποψηφιότητας μέσω του διαδικτύου. (Λειτουργικά Πρότυπα 36–43)

Β) Στάδιο Ψηφοφορίας: Η απομακρυσμένη ψηφοφορία μέσω ηλεκτρονικών συστημάτων μπορεί να εκκινεί ή να τερματίζεται σε χρονικό σημείο νωρίτερο από αυτό της αντίστοιχης ψηφοφορίας σε εκλογικά κέντρα, αλλά δεν θα τερματίζεται σε καμιά περίπτωση σε χρονικό σημείο μεταγενέστερο της λήξης της αντίστοιχης ψηφοφορίας σε εκλογικά κέντρα. Η ηλεκτρονική ψήφος δεν θα περιλαμβάνει οποιαδήποτε άλλη πληροφορία, εκτός από εκείνες που αυστηρά απαιτούνται ώστε να μπορεί ο ψηφοφόρος να ασκήσει το δικαίωμά του, ώστε να αποφεύγονται περιπτώσεις αθέμιτου επηρεασμού της επιλογής των ψηφοφόρων. Πριν την έναρξη της ψηφοφορίας θα πρέπει να επιστηθεί η προσοχή των ψηφοφόρων στη σοβαρότητα της διαδικασίας και στο γεγονός ότι η εκλογή ή το δημοψήφισμα είναι πραγματικά και όχι δοκιμές. (Λειτουργικά Πρότυπα 44–52)

Γ) Στάδιο μετά την Ψηφοφορία: Το σύστημα ηλεκτρονικής ψηφοφορίας δεν θα επιτρέπει την αποκάλυψη του αριθμού των ψήφων, μέχρι τη λήξη της περιόδου ψηφοφορίας και δεν θα επιτρέπει την αποκάλυψη της ψήφου ενός συγκεκριμένου ψηφοφόρου. Κατά την καταμέτρηση των ψήφων, το αρμόδιο εκλεκτορικό όργανο ή και παρατηρητές θα προβαίνουν στην καταμέτρηση των ψήφων και θα τηρείται μητρώο της διαδικασίας ηλεκτρονικής καταμέτρησης (Λειτουργικά Πρότυπα 53–58).

4.4 Τεχνικά Πρότυπα: Το Σύστημα OASIS — EML

Το πρότυπο Election Markup Language (EML) είναι αποτέλεσμα της εργασίας του διεθνούς μη κερδοσκοπικού οργανισμού OASIS (Organization for the Advancement of Structured Information Standards), ο οποίος οδηγεί την ανάπτυξη, σύγκληση και εφαρμογή προτύπων για εφαρμογές ηλεκτρονικού εμπορίου (oasis-open.org). Ο οργανισμός αποτελεί μια ανεξάρτητη και ανοικτή συνεργασία άλλων οργανισμών, ατόμων, κυβερνήσεων και βιομηχανικών ομάδων με περισσότερα από 500 μέλη. Τα πρότυπα αναπτύσσονται στο OASIS μέσα από ανοικτές και δημοκρατικές διαδικασίες, διατηρώντας ουδετερότητα ως προς τους προμηθευτές των συστημάτων. Κανένας οργανισμός δεν υπαγορεύει τα πρότυπα, και στόχος είναι το τελικό αποτέλεσμα να ικανοποιεί όλους τους εμπλεκόμενους, ενώ οι συζητήσεις είναι ανοικτές για δημόσιο διάλογο (Borras 2005).



Το πρότυπο EML (4η έκδοση) που περιέλαβε το Συμβούλιο της Ευρώπης στη Σύστασή του για το θέμα της ηλεκτρονικής ψηφοφορίας, αναπτύχθηκε από την Τεχνική Επιτροπή του OASIS για τις Υπηρεσίες Εκλογών και Ψηφοφόρων. Η ανάγκη για το πρότυπο αυτό προέκυψε από το γεγονός πως κατά τη διαδικασία των ηλεκτρονικών εκλογών, διενεργείται ανταλλαγή πληροφοριών μέσω διαφόρων καναλιών επικοινωνίας και επεξεργασία σε διάφορα συστήματα. Ειδικότερα με τις διαφορετικές εταιρίες που προσφέρουν λύσεις για τις εκλογές, καθίσταται αναγκαία η θέσπιση κοινών κανόνων και προτύπων, ώστε όλα τα συστήματα να επικοινωνούν και να ανταλλάζουν πληροφορίες χωρίς πρόβλημα, με ασφάλεια καθ' όλη τη διαδρομή και με διαφανείς μεθόδους.

Σε αυτή την τεχνική επιτροπή ανατέθηκε τον Μάιο του 2001 η ανάπτυξη προτύπου για τη δομημένη ανταλλαγή δεδομένων ανάμεσα σε υλισμικό, λογισμικό και παρόχους υπηρεσιών, που εμπλέκονται στη παροχή υπηρεσιών σε εκλογές και ψηφοφόρου, για δημόσιους ή ιδιωτικούς οργανισμούς. (Cover, 2004) Ανάμεσα στις προκλήσεις του έργου είναι να παραχθούν πρότυπα τα οποία θα μπορούν να εφαρμοστούν διεθνώς, να είναι αποτελεσματικά για διάφορα είδη ψηφοφορίας (διαδίκτυο, μέσω ταχυδρομείου ή με απλό ψηφοδέλτιο), να είναι εύκολο να μεταφραστούν, να μπορούν να προσαρμοστούν για τον ιδιωτικό ή δημόσιο τομέα και τέλος, να έχουν τη δυνατότητα να διασφαλίζουν τα σχετικά δεδομένα από απώλειες και βλάβες. Το τελικό πρότυπο περιλαμβάνει τις εξής προδιαγραφές: (Ross 2006)

- ανακήρυξη υποψηφιοτήτων, έγκριση και λίστες υποψηφίων
- ανακήρυξη επιλογών δημοψηφίσματος, έγκριση και λίστα επιλογών
- πληροφορίες εγγραφής ψηφοφόρων και λίστα εγκεκριμένων ψηφοφόρων
- επικοινωνία μεταξύ ψηφοφόρων και εκλογικών υπευθύνων για τα εκλογικά κέντρα, ανακοινώσεις κλπ
- πληροφορίες για τις εκλογές, τα αξιώματα και τους αντίστοιχους υποψήφιους
- αυθεντικοποίηση ψηφοφόρων



- κατάθεση ψήφου και επιβεβαίωσή της
- καταμέτρηση και τελικά αποτελέσματα
- πληροφορίες για έλεγχο εύκαμπτο, ούτως ώστε να μπορεί να χρησιμοποιηθεί σε εκλογές ή δημοψηφίσματα που χρησιμοποιούν κυρίως χάρτινα ψηφοδέλτια, ή ηλεκτρονική ψηφοφορία

Το πρότυπο αυτό χρειάζεται να προσαρμόζεται ξεχωριστά για κάθε κράτος μέλος ανάλογα προς τις τοπικές συνθήκες. Ήδη το Ηνωμένο Βασίλειο και το Βέλγιο έχουν εντάξει το πρότυπο αυτό στο σχεδιασμό των συστημάτων ηλεκτρονικής ψηφοφορίας. Σημειώνεται ότι στα Τεχνικά Πρότυπα, στις παραγράφους 66–68, προτείνεται όπως χρησιμοποιούνται «ανοικτά πρότυπα», ώστε να διασφαλιστεί ότι τα διάφορα τεχνικά μέρη ή υπηρεσίες σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, τα οποία μπορεί να προήλθαν από διάφορους προμηθευτές, λειτουργούν αρμονικά μεταξύ τους. Η σύσταση αναφέρει ένα τέτοιο πρότυπο, το Election Markup Language (EML), το οποίο είναι ανοικτό, και προτείνει στις χώρες μέλη να το χρησιμοποιούν όποτε είναι δυνατό όταν διεξάγονται εκλογές και δημοψηφίσματα με ηλεκτρονικά μέσα. Το πρότυπο μπορεί να προσαρμοστεί ανάλογα με τις ανάγκες κάθε περιοχής που το εφαρμόζει, επεκτείνοντας ή περιορίζοντας τις πληροφορίες που χρειάζεται, παραμένοντας συμβατό με τη γενική έκδοση του EML.



5 Συμπεράσματα

Η παρούσα εργασία επιχείρησε να επιλύσει αρκετά από τα προβλήματα που προκύπτουν κατά τη χρήση συστημάτων ηλεκτρονικής ψηφοφορίας. Αρχικά θα πρέπει να αναφερθεί ότι πρόκειται για ένα κατακευματισμένο, υβριδικό σύστημα ηλεκτρονικής ψηφοφορίας.

Επιπλέον δεν υπάρχει η απαίτηση κατοχής του εξειδικευμένου λογισμικού από ιδιώτες, γεγονός που δημιουργεί καλύτερες προϋποθέσεις για μεγαλύτερη συμμετοχή. Αφετέρου γίνεται χρήση των τεχνολογιών διαδικτύου και επιπρόσθετων μηχανισμών ασφάλειας. Σε ό,τι αφορά την παρέμβαση του ανθρώπινου παράγοντα, είναι αντιληπτό ότι δεν μπορεί να προβλεφθεί ή ελεγχθεί πλήρως, είτε πρόκειται για δολιοφθορά είτε για ακούσιο λάθος ή παράλειψη. Για το λόγο αυτό γίνεται η παραδοχή ότι δεν υπάρχει κανενός είδους πρόσβαση στο υλικό και το λογισμικό του συστήματος, όλα λειτουργούν όπως ακριβώς έχουν σχεδιαστεί και οι εκάστοτε διαχειριστές είναι αντικειμενικοί και αμερόληπτοι. Στην πράξη, αυτό επιτυγχάνεται με τον περιορισμό της πρόσβασης σε κρίσιμες παραμέτρους του συστήματος (κρυπτογραφημένες βάσεις δεδομένων, trusted computing).

Προκειμένου να αποφευχθεί η αντιστοίχιση των ψήφων με τους ψηφοφόρους και κατ' επέκταση η παραβίαση της μυστικότητας, η ψήφος και ο αναγνωριστικός αριθμός κάθε ψηφοφόρου μεταφέρονται μέσα από διαφορετικά κανάλια και σε ασυσχέτιστες μεταξύ τους χρονικές στιγμές. Ακόμα και ο πίνακας που αποθηκεύει προσωρινά και μόνο τοπικά τους σειριακούς αριθμούς των πιστοποιητικών των ψηφοφόρων διαγράφεται ανά τακτά χρονικά διαστήματα.

Επίσης αντιμετωπίστηκε επαρκώς η περίπτωση νοθείας, μέσω της δημιουργίας και συνεχούς ενημέρωσης των βάσεων δεδομένων, τόσο σε περιφερειακό όσο και σε κεντρικό επίπεδο. Μέσω αυτού του μηχανισμού, είναι δυνατόν να αποτραπεί επιπλέον και η κατάρρευση του συστήματος λόγω φόρτου, εφόσον η συχνότητα ενημέρωσης των βάσεων μπορεί να ρυθμιστεί, ώστε να είναι επαρκώς μεγάλη, οπότε κάθε φορά θα μεταφέρεται όχι απαγορευτικός όγκος δεδομένων.

Ως μηχανισμός διανομής πιστοποιητικών και πιστοποίησης επιλέχθηκαν οι έξυπνες κάρτες, οι οποίες θεωρούνται ανθεκτικές στην παραβίαση. Η κρυπτογράφηση της



ψήφου εξασφαλίζει τη μυστικότητα της κατά τη μεταφορά, ενώ η ψηφιακή υπογραφή της πιστοποιεί την αυθεντικότητα τόσο της ίδιας όσο και του πράκτορα.

Σε ό,τι αφορά τη μεταφορά της ψήφου με τη βοήθεια κινητών πρακτόρων, εναλλακτικές υλοποιήσεις θα ήταν είτε να «φορτώνονται» περισσότερες από μία ψήφοι στον πράκτορα είτε να υπάρχουν περισσότεροι από έναν πράκτορες σε κάθε αντιπροσωπεία. Ένα πλήρως αποκεντροποιημένο σύστημα ψηφοφορίας και γενικότερα μία αποκεντροποιημένη εφαρμογή παρουσιάζει διάφορες προκλήσεις υλοποίησης τόσο τεχνικές όσο και θεωρητικές.

Όντας σύστημα κρίσιμης σημασίας όλα τα σενάρια πρέπει να είναι σωστά υλοποιημένα ενώ οι αποφάσεις σχεδίασης, οι επιλεγμένοι αλγόριθμοι και η αρχιτεκτονική πρέπει να έχουν λάβει υπ' όψιν τους όλες τις πιθανές μη αναμενόμενες καταστάσεις, επιθέσεις και ακραίες περιπτώσεις και να τις αντιμετωπίζουν κατάλληλα. Συγκεκριμένα για ένα σύστημα ηλεκτρονικής ψηφοφορίας:

1. Απαιτείται πολύ μεγάλη προσοχή στην επιλογή των κρυπτοσυστημάτων που θα χρησιμοποιηθούν. Ιδανικά πρέπει να εκμεταλλευόμαστε αλγορίθμους με αρκετά μεγάλο παρελθόν οι οποίοι βασίζονται σε ορθό μαθηματικό υπόβαθρο και γνωστά θεωρήματα. Επιπλέον έμφαση πρέπει να δοθεί και στην υλοποίηση του κρυπτοσυστήματος, κάτι που συχνά αποτελεί αδύνατο σημείο και επίκεντρο επιθέσεων από κακόβουλες πλευρές.
2. Απαιτείται επιπλέον πολύ μεγάλη προσοχή και στην επιλογή των εργαλείων, πρωτοκόλλων επικοινωνίας και γενικότερα των στοιχείων που αποτελούν την υποδομή της εφαρμογής. Για άλλη μια φορά, εργαλεία με αποδεδειγμένες ικανότητες και κυρίως σταθερή απόδοση χωρίς προβλήματα είναι προτιμότερα. Από τις υλοποιήσεις πρωτοκόλλων επικοινωνίας μέχρι τη γλώσσα προγραμματισμού, κάθε κομμάτι του συστήματος πρέπει να περάσει από εξονυχιστικό έλεγχο.
3. Ολόκληρος ο σχεδιασμός του συστήματος πρέπει να είναι όσο πιο λιτός γίνεται. Κάθε στοιχείο που συμμετέχει στην υλοποίηση προσθέτει μεγάλη πολυπλοκότητα και δυσκολεύει τόσο τον έλεγχο ορθότητας όσο και την επιδιόρθωση ή επέκτασή της.



Η δημιουργία ενός ορθού και εμπιστεύσιμου συστήματος ηλεκτρονικής ψηφοφορίας σίγουρα θα αποτελέσει τεχνολογικό επίτευγμα παρ' όλα αυτά δεν φαντάζει αδύνατο. Σε αυτό βοηθά και η έλευση της τεχνολογίας blockchain η οποία προσφέρει λύσεις σε διάφορα προβλήματα των πατροπαράδοτων συστημάτων.

1. Επιτρέπει τη λειτουργία ενός συστήματος χωρίς κεντρική διαχείριση και συνεπώς χωρίς κεντρικά σημεία προβλημάτων. Τόσο η έλλειψη εμπιστοσύνης στους διαχειριστές, όσο το γεγονός ότι τα συστήματα αυτά αποτελούν στόχο εξωτερικών επιθέσεων, ένα αποκεντροποιημένο σύστημα καθίσταται προτιμότερο για ηλεκτρονικές ψηφοφορίες.
2. Προτιμάται η χρήση blockchain συστήματος συγκεκριμένα υλοποιημένο για το σκοπό της ψηφοφορίας. Η χρήση τρίτων συστημάτων όπως π.χ. του Ethereum blockchain που έγινε στο case study προσθέτουν πολυπλοκότητα ενώ τα πιθανά προβλήματα που έχουν κληρονομούνται και στο σύστημα ψηφοφορίας.

Τα ομομορφικά κρυπτοσυστήματα και οι αποδείξεις μηδενικής γνώσης καθίστανται σχεδόν απαραίτητα σε ένα αποκεντροποιημένο σύστημα ψηφοφορίας. Χωρίς την ύπαρξη κεντρικής διαχείρισης με ταυτόχρονη απαίτηση τη μυστικότητα της ψήφου, η ομομορφική κρυπτογραφία φαίνεται να είναι η βέλτιστη επιλογή, σε συνδυασμό πάντα με κάποιο συμβατό σύστημα απόδειξης μηδενικής γνώσης ώστε να υπάρχει διασφάλιση της εγκυρότητας της ψήφου.

Τέλος, η δημιουργία ενός συστήματος ψηφοφορίας είναι ένα δύσκολο και απαιτητικό εγχείρημα το οποίο πρέπει να γίνει με τη συνεργασία πολλών ειδημόνων από διάφορους τομείς. Επιπλέον όλα τα στοιχεία που αποτελούν το σύστημα, από την υλοποίηση του blockchain πρωτοκόλλου μέχρι και το μεταγλωττιστή της επιλεγμένης γλώσσας προγραμματισμού πρέπει να είναι ανοιχτού κώδικα και διαθέσιμα για έλεγχο από όλους. Η λύση που παρουσιάστηκε στη συγκεκριμένη εργασία καλύπτει κάποιες από τις παραπάνω προϋποθέσεις, σε καμία περίπτωση όμως δεν πλησιάζει το σημείο όπου θα μπορούσε να χρησιμοποιηθεί με ασφάλεια και σιγουριά.



5.1 Προτάσεις για περαιτέρω εργασία

Οι παρακάτω τομείς απαιτούν βελτίωση και περαιτέρω έρευνα:

1. Επίλυση των προβλημάτων ψηφοφορίας πολλαπλών επιλογών. Όπως ειπώθηκε και στα προηγούμενα κεφάλαια, κάθε διαθέσιμη επιλογή ψηφοφορίας πρέπει να κωδικοποιείται με μια αριθμητική τιμή, τέτοια ώστε το άθροισμα όλων των πιθανών συνδυασμών αυτών να παράγει πάντα ένα αποτέλεσμα από το οποίο να μπορεί να εξαχθεί ένα συμπέρασμα για τον αριθμό των ψήφων που έλαβε κάθε διαθέσιμη επιλογή.
2. Βελτίωση παραγωγής μοναδικού αναγνωριστικού χρήστη (UID). Αυτή τη στιγμή, για λόγους ευκολίας, για την παραγωγή του UID χρησιμοποιείται ένας κωδικός πρόσβασης σε συνδυασμό με ένα μοναδικό χαρακτηριστικό όπως το φοιτητικό email ή το ΑΦΜ πολίτη. Παρ' όλα αυτά, κρίνεται σκόπιμη η αντικατάσταση ενός κωδικού πρόσβασης με κάτι πιο εύκολα διαχειρίσιμο, ειδικά για τη διευκόλυνση τεχνολογικά ακατάρτιστων ομάδων και ομάδων με δυσκολία συγκράτησης πληροφορίας. Η ασφάλεια ενός κωδικού πρόσβασης εξαρτάται από την πολυπλοκότητά του, είτε σε αριθμό είτε στο συνδυασμό μεγάλης γκάμας χαρακτήρων, κάτι το οποίο αυξάνει την πιθανότητα να ξεχαστεί. Αυτό έχει ως αποτέλεσμα σε πολλές περιπτώσεις οι χρήστες να καταγράφουν τον κωδικό σε φυσική μορφή το οποίο ουσιαστικά ρίχνει τη δυσκολία πρόσβασης από τρίτους στο να βρουν το σημείωμα και να αντιγράψουν τον κωδικό πρόσβασης. Για να αντιμετωπιστεί το παραπάνω πρόβλημα χρειάζεται κάποιου άλλου είδους μη αντιγράψιμο και εύκολα προσβάσιμο χαρακτηριστικό χρήστη, για παράδειγμα ένα είδος βιομετρικού αναγνωριστικού όπως το δακτυλικό αποτύπωμα, η αναγνώριση ίριδας ή προσώπου. Παρ' ότι τέτοιες μέθοδοι χρησιμοποιούνται είδη σε προϊόντα τεχνολογίας όπως για το ξεκλείδωμα smartphone, στη δική μας περίπτωση η ίδια μεθοδολογία δεν μπορεί να εφαρμοστεί. Ο λόγος είναι διότι το αποτέλεσμα βιοαναγνώρισης είναι μη ντετερμινιστικό και βασίζεται σε πιθανοτικές μεθόδους, κάτι το οποίο είναι εμπόδιο όταν η τιμή αυτή πρέπει να χρησιμοποιηθεί ως seed για την παραγωγή μιας μοναδικής τιμής UID (η οποία στην περίπτωσή μας είναι το public key ενός ασύμμετρου ζεύγους).



Απαιτείται λοιπόν περαιτέρω έρευνα στις μεθόδους βιομετρικής αναγνώρισης ή και στην χρήση των αποτελεσμάτων αυτής.

3. Διερεύνηση μεθόδων επιβεβαίωσης εγκυρότητας της εφαρμογής ψηφοφορίας αλλά και της συσκευής εκτέλεσης αυτής. Παρ' ότι η εφαρμογή είναι ανοιχτού κώδικα και η υλοποίηση μπορεί να ελεγχθεί από τον οποιονδήποτε, μεταξύ του κώδικα και της εφαρμογής η οποία τρέχει σε μια συσκευή υπάρχουν πολλά σημεία τα οποία μπορούν να εμφανίσουν θέματα ασφάλειας. Παραδείγματα είναι η διάθεση ενός πειραγμένου binary ή η παράνομη εγκατάσταση κακόβουλου λογισμικού στις συσκευές των χρηστών, το οποίο μπορεί είτε να υποκλέψει τα στοιχεία του χρήστη είτε να επηρεάσει τη λειτουργία της εφαρμογής ψηφοφορίας.
4. Υλοποίηση συστήματος ελέγχου της διαδικασίας και των αποτελεσμάτων αυτής. Παρ' ότι δεν υπάρχει ένας συγκεκριμένος κάτοχος του συστήματος και η πληροφορία είναι ελεύθερα διαθέσιμη σε όλους τους χρήστες, η μορφή αυτής δεν είναι εύκολα διαχειρίσιμη και προσπελάσιμη. Απαιτείται λοιπόν κάποιο σύστημα ελέγχου (auditing) ώστε να μπορεί να επιβεβαιωθεί από τους διαχειριστές μιας ψηφοφορίας ότι η διαδικασία εκτελέστηκε σωστά. Επιπλέον σε περιπτώσεις όπου εμφανίζονται προβλήματα είναι απαραίτητο να μπορεί να εντοπιστεί η πηγή αυτών, ειδικά στην περίπτωση όπου ευθύνεται κάποιος κακόβουλος χρήστης, ώστε να αντιμετωπιστούν κατάλληλα.
5. Έρευνα για την επίλυση προβλήματος ασφάλειας κατά το βήμα της παραγωγής υπερκλειδιού αποκρυπτογράφησης. Όπως παρουσιάστηκε και στο 5ο κεφάλαιο, ένα από τα τελευταία στάδια της διαδικασίας είναι η παραγωγή του υπερκλειδιού αποκρυπτογράφησης του ομομορφικού αθροίσματος των ψήφων. Για να επιτευχθεί αυτό χρησιμοποιείται η τεχνική ασφαλούς υπολογισμού πολλαπλών μερών (secure multi-party computation) η οποία όμως αυτή τη στιγμή πάσχει από ένα βασικό πρόβλημα το οποίο μπορεί να εμποδίσει την ολοκλήρωση της ψηφοφορίας. Εάν κάποιος χρήστης, όταν κληθεί να μοιραστεί τα Shamir secret shares του κρυφού κλειδιού που χρησιμοποίησε για την κρυπτογράφηση της ψήφου του, επιλέξει να μοιραστεί τα shares μιας άλλης τιμής, τότε το παραγόμενο υπερκλειδί δεν θα μπορεί να



αποκρυπτογραφήσει το ομομορφικό άθροισμα των ψήφων και επιπλέον θα είναι αδύνατον να εντοπιστεί ποιος από τους ψηφοφόρους έχει μολύνει τη διαδικασία. Ιδέες για την επίλυση του προβλήματος είναι η διερεύνηση ενός non-interactive proof of value για το πολυώνυμο που χρησιμοποιήθηκε για τα Shamir shares, είτε η ανάπτυξη κάποιας μεθόδου εντοπισμού κακόβουλων χρηστών που μολύνουν τη διαδικασία παραγωγής υπερκλειδιού.



6 Βιβλιογραφία

- Alexander H. Trechsel, Fabian Breuer, “E-voting in the 2005 Local Elections in Estonia and the broader impact for future e-voting projects”
- Alexandros Xenakis and Prof. Ann Macintosh, “E-electoral Administration: Organizational Lessons Learned from the Deployment of E-voting in the UK”
- Anthony Di Franco, Andrew Petro, Emmett Shear, AND Vladimir Vladimirov, “Small Vote Manipulations Can Swing Elections”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10 43
- Aviel D. Rubin, “Security Considerations for Remote Electronic Voting”, COMMUNICATIONS OF THE ACM December 2002/Vol. 45, No. 12
- Borrás, J., ‘Standards for E — Voting: The Results of the Work of the Election & Voter Services Technical Committee’ 2006, www.oasis-open.org
- Bouras C., Kastaniotis S., Triantafyllou V. (2000). Citizen Information Services Using Internet Technologies. ECIS 2000, European Conference on Information Systems, Vienna, Austria, July 3-5, pp. 1123-1130
- Brit J. Williams AND Merle S. King, “Implementing Voting Systems: the Georgia Method”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10 39
- Carolyn Coggins, “Independent Testing of Voting Systems”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10 34
- Code of good practice in electoral matters (Venice Commission — Opinion 190/2002), endorsed by Parliamentary Assembly Resolution 1320 (2003).
- Cover, R., (ed), Election Markup Language (EML) Recommended to Member States by Council of Europe, Cover Pages Newsletter, 10 November 2004, <http://xml.coverpages.org/ni2004-11-10-a.html>



- Cranor L.F., Cytron R.K. (1997). Sensus: A Security – Conscious Electronic Polling System for the Internet. Proceeding of the Hawaii I International Conference on System Science, January 7-10, Wailea, Hawaii, USA.
- David Jefferson, Aviel D. Rubin, Barbara Simons AND David Wagner, “Analyzing Internet Voting Security”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10 59
- Dimitris Gritzalis, “Secure Electronic Voting”, 7 Pth Computer Security Incidents Response Teams Workshop, Syros, Greece, September 2002
- Douglas W. Jones, “Auditing”, October 2014/Vol. 47, No. 10 COMMUNICATIONS OF THE ACM 46
- Electionworld.org / Elections around the world:<http://www.electionworld.org>
- E-voting, Welcome to the State of Geneva website
- Georgios V. Lioudakis, Nikolaos L. Dellas, Eleftherios A. Koutsoloukas, Dimitra I. Kaklamani, Iakovos S. Venieris, “A Delay Performance Evaluation of Cryptographic Algorithms”, Technical Report, National Technical University of Athens, Athens, Jan. 2007.
- Greg Goth, “News: Cradle of Liberty Lags on E-Voting”, IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2006 Published by the IEEE Computer Society, Vol. 7, No. 4; April 2006
- Herb Deutsch and Stephen Berger, “Voting Systems: Standards and Certifications”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10
- <http://www.oasis-open.org/>
- Ikonomopoulos S., Lambrinoudakis C., Gritzalis D., Kokolakis S. and Vassiliou K., “Functional Requirements for a Secure Electronic Voting System”, Proc. of the 16th IFIP International Information Security Conference (IFIP/SEC-2002) M. el



- InfoPoll, <http://www.infopoll.com/>
- Kim Zetter “Aussies Do It Right: E-Voting”, 11-3-2005,
- Przemysław Kubiak, Mirosław Kutylowski, Filip Zagórski, “Kleptographic Attacks on a Cascade of Mix Servers”
- Rebecca T. Mercuri AND L. Jean Camp, “The Code of Elections”, COMMUNICATIONS OF THE ACM October 2014/Vol. 47, No. 10 53
- Rec. (2004) 11: Legal, Operational and Technical Standards for E — Voting, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory Memorandum, Council of Europe: Strasbourg, 2005. Βλ. ακόμα Remmert, M., Developing a Common Framework for E — Voting in Europe: The Council of Europe’s Draft Recommendation on the Legal, Operational and Technical Aspects of E — Voting, International Workshop on Electronic Voting in Europe, 2004
- Ross, J., Spencer, P., Borrás, J., Ahmed, F., Aoun, C., Elton, B., O’Donnell, J., Hill, R., Van Acker, B., Von Spakovsky, H., EML v. 4.0 Process and Data Requirements, OASIS Standard, OASIS Open, 1 February 2006.
- Seymour Bosworth, M.E. Kabay, “Computer Security Handbook”, John Wiley and sons, Inc., fourth edition, USA, 2002, pp. 23.1-23.13.
- Study n. 260, 2003 Strasbourg, adopted by the Venice Commission on 12–13 March 2004.
- The Help America Vote Act of 2002. http://www.fed.gov/hava/law_ext.txt
- Theodoros Balopoulos, Stefanos Gritzalis, Sokratis K. Katsikas, “Specifying Electronic Voting Protocols in Typed MSR”
- True Ballot, Democratic Governance Systems, <http://www.ozemail.com.au/~jjjacq/evote/>



- UK Electoral Commission, August 2002, “Modernising Elections --- A strategic evaluation of the 2002 electoral pilot schemes”, “Securing the vote --- Report and recommendations”
- Virtual Voting: <http://www.acm.org/technews/articles/2003-5/0625w.html#item12>
- ViVarto <http://www.vivarto.com/o2/eng/index2.html>
- Ιάκωβος Στ. Βενιέρης, Ευγενία Νικολούζου, “Τεχνολογίες διαδικτύου”, Εκδόσεις Τζιόλα, Αθήνα 2003, pp. 89-97.
- Κάτσικα Σωκράτης “Συστήματα ηλεκτρονικής ψηφοφορίας: Το μέλλον της Δημοκρατίας”, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων - διευθυντή, Εργαστήριο Ασφάλειας Πληροφοριακών & Επικοινωνιακών Συστημάτων - πρύτανης Πανεπιστημίου Αιγαίου, 28-9-2007
- Λειτουργικά Πρότυπα 36–43 και παράγραφοι 75–85 του Επεξηγηματικού Μνημονίου.
- Λειτουργικά Πρότυπα 44–52 και παράγραφοι 86–102 του Επεξηγηματικού Μνημονίου.
- Λειτουργικά Πρότυπα 53–58 και παράγραφοι 103–104 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 1–4 και παράγραφοι 27–31 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 16–19 και παράγραφοι 45–53 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 20–23 και παράγραφοι 55–61 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 24–27 και παράγραφοι 62–65 του Επεξηγηματικού Μνημονίου.



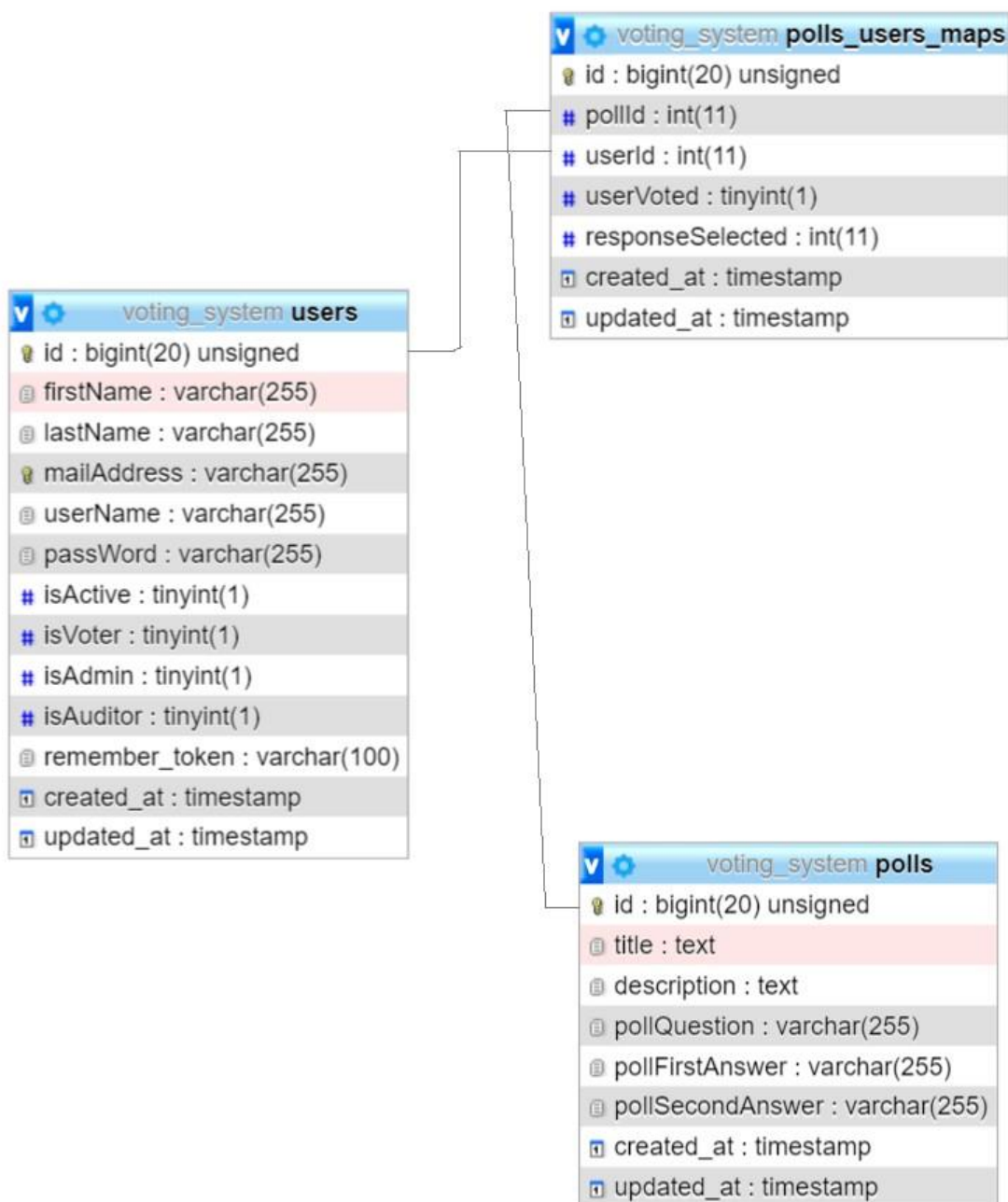
- Νομικά Πρότυπα 28–35 και παράγραφοι 66–74 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 5–8 και παράγραφοι 32–34 του Επεξηγηματικού Μνημονίου.
- Νομικά Πρότυπα 9–15 και παράγραφοι 35–44 του Επεξηγηματικού Μνημονίου.
- Χατζηστυλιανος Μιχάλη “Καταψήφισαν το e-voting”, 25-9-2007, http://www.simerini.com/nqcontent.cfm?a_id=312727



7 Παράρτημα

7.1 Διάγραμμα ER

Παρακάτω φαίνεται το διάγραμμα της βάσης δεδομένων.





Ο πίνακας polls περιέχει τις εγγραφές που αφορούν τις ψηφοφορίες.

Ο πίνακας polls_users_map περιέχει τις εγγραφές που συνδέουν τους χρήστες με τις ψηφοφορίες που είναι να κάνουν.

Ο πίνακας users περιέχει τους χρήστες είτε αυτοί είναι διαχειριστές είτε απλά ψηφοφόροι.

Παρακάτω φαίνεται ο κώδικας με τον οποίο δημιουργούμε την βάση με την μέθοδο των migrations.

7.2 Migrations

7.2.1 Για τον πίνακα χρηστών.

```
class CreateUsersTable extends Migration
{
    public function up()
    {
        Schema::create('users', function (Blueprint $table)
        {
            $table->id();

            $table->string('firstName');

            $table->string('lastName');

            $table->string('mailAddress')->unique();

            $table->string('userName');

            $table->string('passWord')->default('');

            $table->boolean('isActive')->default(false);

            $table->boolean('isVoter')->default(false);

            $table->boolean('isAdmin')->default(false);
```



```
$table->boolean('isAuditor')->default(false);  
$table->rememberToken();  
  
$table->timestamp('created_at')->useCurrent();  
$table->timestamp('updated_at')->useCurrent();  
});  
}  
  
public function down()  
{  
    Schema::dropIfExists('users');  
}  
}
```

7.2.2 Για τον πίνακα ψηφοφοριών.

```
class CreatePollsTable extends Migration  
{  
    public function up()  
    {  
        Schema::create('polls', function (Blueprint $table)  
        {  
            $table->id();  
  
            $table->text('title');  
            $table->text('description');  
  
            $table->string('pollQuestion');  
            $table->string('pollFirstAnswer');  
            $table->string('pollSecondAnswer');
```



```
$table->timestamp('created_at')->useCurrent();

$table->timestamp('updated_at')->useCurrent();
});
}

public function down()
{
    Schema::dropIfExists('polls');
}
}
```


7.2.3 Πίνακας ψηφοφοριών και χρηστών

```
class CreatePollsUsersMap extends Migration
{
    public function up()
    {
        Schema::create('polls_users_maps', function (Blueprint $table)
        {
            $table->id();

            $table->integer('pollId');

            $table->integer('userId');
            $table->boolean('userVoted')->default(false);
            $table->integer('responseSelected')->default(0);
            $table->timestamp('created_at')->useCurrent();
        });
    }
}
```



```
$table->timestamp('updated_at')->useCurrent();  
});  
  
}  
  
public function down()  
{  
    Schema::dropIfExists('polls_users_maps');  
}  
}
```

7.3 Seeders

Παρακάτω φαίνεται ο κώδικας με τον οποίο θα γεμίσουμε δεδομένα τη βάση μέσω Seeders.

7.3.1 Για τον πίνακα των χρηστών

```
class UsersSeeder extends Seeder  
{  
    public function run()  
    {  
        DB::table('users')->  
            insert([  
                'firstName' => 'test1',  
                'lastName' => 'test1',  
                'mailAddress' => 'test1@test1.t1',  
                'userName' => 'user1'  
            ]) ;  
    }  
}
```



```
DB::table('users')-  
  >insert( [  
    'firstName' => 'test2',  
    'lastName' => 'test2',  
    'mailAddress' => 'test2@test2.t2',  
    'userName' => 'user2'  
  ]  
);  
DB::table('users')-  
  >insert( [  
    'firstName' => 'test3',  
    'lastName' => 'test3',  
    'mailAddress' => 'test3@test3.t3',  
    'userName' => 'user3'  
  ]  
);  
}  
}
```

7.3.2 Για τον πίνακα ψηφοφοριών

```
class PollsSeeder extends Seeder
```

```
{  
  public function run()  
  {  
    DB::table('polls')-  
      >insert( [  
        'question' => 'What is the best way to learn PHP?',  
        'answer' => 'By reading the documentation and practicing',  
        'user' => 'user1',  
        'score' => 100  
      ]  
    );  
  }  
}
```



```
'title' => 'Poll Title 1',

'description' => 'Poll Description 1',

'pollQuestion' => 'Question 1',
'pollFirstAnswer' => 'First 1',

'pollSecondAnswer' => 'Second 1'
]
);
DB::table('polls')-
>insert( [

'title' => 'Poll Title 2',
'description' => 'Poll Description 2',
'pollQuestion' => 'Question 2',
'pollFirstAnswer' => 'First 2',

'pollSecondAnswer' => 'Second 2'

]
);
DB::table('polls')-
>insert( [

'title' => 'Poll Title 3',
'description' => 'Poll Description 3',
'pollQuestion' => 'Question 3',

'pollFirstAnswer' => 'First 3',
'pollSecondAnswer' => 'Second 3'

]
);
}
```



}

7.3.3 Για τον πίνακα ψηφοφοριών - χρηστών

```
class PollsUsersMapSeeder extends Seeder
```

```
{
```

```
    public function run()
```

```
    {
```

```
        DB::table('polls_users_maps')->insert(
```

```
        [
```

```
            'pollId' => 1,
```

```
            'userId' => 1,
```

```
            'userVoted' => false,
```

```
            'responseSelected' => 0
```

```
        ]
```

```
    );
```

```
        DB::table('polls_users_maps')->insert(
```

```
        [
```

```
            'pollId' => 2,
```

```
            'userId' => 1,
```

```
            'userVoted' => false,
```

```
            'responseSelected' => 0
```

```
        ]
```

```
    );
```

```
        DB::table('polls_users_maps')->insert(
```

```
        [
```

```
            'pollId' => 3,
```

```
            'userId' => 1,
```

```
            'userVoted' => false,
```



```
'responseSelected' => 0
]
);
DB::table('polls_users_maps')->insert(
[
    'pollId' => 1,
    'userId' => 2,
    'userVoted' => false,
    'responseSelected' => 0
]
);
DB::table('polls_users_maps')->insert(
[
    'pollId' => 2,
    'userId' => 2,
    'userVoted' => false,
    'responseSelected' => 0
]
);
DB::table('polls_users_maps')->insert(
[
    'pollId' => 3,
    'userId' => 2,
    'userVoted' => false,
    'responseSelected' => 0
]
);
DB::table('polls_users_maps')->insert(
[
    'pollId' => 1,
```



```
'userId' => 3,  
'userVoted' => false,  
'responseSelected' => 0  
]  
);  
DB::table('polls_users_maps')->insert(  
[  
    'pollId' => 2,  
    'userId' => 3,  
    'userVoted' => false,  
    'responseSelected' => 0  
]  
);  
DB::table('polls_users_maps')->insert(  
[  
    'pollId' => 3,  
    'userId' => 3,  
    'userVoted' => false,  
    'responseSelected' => 0  
]  
);  
}  
}
```