Ηλεκτρονική Ψηφοφορία μέσω Internet: Ουτοπία ή Πραγματικότητα;

Εμμανουήλ Μάγκος[1], Βασίλειος Χρυσικόπουλος[1],
Νίκος Αλεξανδρής[2] και Μάριος Πούλος[1]

[1]Τμήμα Αρχειονομίας και Βιλιοθηκονομίας,
Ιόνιο Πανεπιστήμιο
Παλάιά Ανάκτορα 49100, Κέρκυρα
emagos@unipi.gr ; vchris@ionio.gr ; marios.p@usa.net

[2] Τμήμα Πληροφορικής,
Πανεπιστήμιο Πειραιώς,
80 Καραολή & Δημητρίου, Πειραιάς 18534
alexandr@unipi.gr

Περίληψη. Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και συγκεκριμένα της ψηφοφορίας μέσω Internet, ως εναλλακτικός τρόπος υποβολής της ψήφου αναμένεται να αυξήσει την συμμετοχή των πολιτών στις εκλογές και να αυτοματοποιήσει τις διαδικασίες της υποβολής και της καταμέτρησης των ψήφων, μειώνοντας μακροπρόθεσμα το κόστος διεξαγωγής των εκλογών. Ωστόσο, για να ολοκληρωθεί η μετάβαση σε συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet, πρέπει πρωτίστως να επιλυθούν ζητήματα ασφάλειας και λειτουργικότητας, τα οποία συχνά αγνοούνται από τους σχεδιαστές συστημάτων. Στην εργασία αυτή καθορίζουμε απαιτήσεις ασφάλειας και πρακτικότητας, συζητούμε προϋποθέσεις και περιγράφουμε κρυπτογραφικά μοντέλα ασφάλειας για την υλοποίηση ηλεκτρονικών εκλογών μεγάλης κλίμακας μέσω Internet. Επίσης, αναφέρουμε τις προοπτικές που διαγράφονται για την υιοθέτηση συστημάτων ηλεκτρονικής ψηφοφορίας στα σύγχρονα δημοκρατικά καθεστώτα.

Λέξεις Κλειδιά: Ηλεκτρονική Ψηφοφορία, Ασφάλεια, Λειτουργικότητα, Κρυπτογραφία

1. Εισαγωγή

Στα περισσότερα δημοκρατικά καθεστώτα επικρατεί ανησυχία για τα αυξανόμενα ποσοστά αποχής από τις εθνικές εκλογές, καθώς και για τη διαφαινόμενη τάση αποστασιοποίησης από τα πολιτικά δρώμενα. Για να αντιστραφεί το κλίμα αναζητούνται αλλαγές στον τρόπο συμμετοχής των πολιτών στα κοινά. Ένα από τα μέτρα υπό συζήτηση είναι η υιοθέτηση συστημάτων *ηλεκτρονικής ψηφοφορίας* (e-voting).

Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και μάλιστα της *ψηφοφορίας μέσω Internet* αναμένεται να απλοποιήσει και να περιορίσει τα λάθη κατά τη διαδικασία υποβολής και καταμέτρησης των ψήφων (Mohen,2001), υπόσχεται μεγαλύτερη προσβασιμότητα στα άτομα με ειδικές ανάγκες, καθώς και μικρότερο (μακροπρόθεσμα) οικονομικό κόστος, σε σχέση με το κόστος των παραδοσιακών εκλογών. Ειδικότερα με τα συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet η διαδικασία υποβολής της ψήφου θα είναι φιλική προς τον χρήστη, ενώ ένας μεγάλος αριθμός υπολογιστών που είναι σήμερα διαθέσιμοι σε εύκολα προσβάσιμους χώρους (π.χ. βιβλιοθήκες, σχολεία, πανεπιστήμια, δημόσιες υπηρεσίες) μπορούν να γίνονται διαθέσιμοι στο εκλογικό σώμα την ημέρα των εκλογών.

Έως σήμερα έχουν διεξαχθεί αρκετές εκλογές μέσω Internet, αν και οι περισσότερες από αυτές είχαν ανεπίσημο χαρακτήρα, ενώ αρκετά συστήματα σχεδιάζονται και εφαρμόζονται πιλοτικά με σκοπό τη μελλοντική τους υλοποίηση σε συστήματα μεγάλης κλίμακας. Παραδείγματα αποτελούν (Burmester,2002) οι εκλογές της παράταξης των Δημοκρατικών

στην πολιτεία της Arizona των Η.Π.Α. (νομικά έγκυρες), Μάρτιος 2000; η αποστολή, μέσω Internet, των ψήφων του στρατιωτικού προσωπικού εντός και εκτός των Η.Π.Α (absentee ballots) στις Προεδρικές εκλογές (νομικά έγκυρες), 2000; Οι εκλογές των Ρεπουμπλικάνων στην πολιτεία της Alaska (ανεπίσημα αποτελέσματα), Ιανουάριος 2000; Οι τοπικές και δημοτικές εκλογές στη Μεγ. Βρετανία (ανεπίσημα αποτελέσματα), Μάιος 2002. Σε γενικές γραμμές, κάθε ηλεκτρονική ψηφοφορία αποτελείται από τέσσερα (4) διακριτά στάδια:

- **Εγγραφή.** Πριν από τη διεξαγωγή των εκλογών, οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του δικαιώματος τους να ψηφίσουν (π.χ. όριο ηλικίας). Οι εγγραφόμενοι χρήστες προστίθενται στον εκλογικό κατάλογο.

- **Επικύρωση.** Κατά τη διάρκεια των εκλογών, και πριν υποβάλλουν τη ψήφο τους, οι ψηφοφόροι ταυτοποιούνται (identification), επιβεβαιώνεται δηλαδή η ταυτότητα τους τη δεδομένη χρονική στιγμή.

- **Υποβολή Ψήφου.** Οι ψηφοφόροι σε αυτό το στάδιο υποβάλλουν την ψήφο τους. Μόνο μια ψήφος επιτρέπεται για κάθε ψηφοφόρο.

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

Κάθε ένα από τα παραπάνω στάδια μπορεί να λάβει χώρα με τη χρήση είτε *φυσικών* είτε *ηλεκτρονικών* διαδικασιών. Διακρίνονται δύο τύποι ηλεκτρονικής ψηφοφορίας: Η *Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία* (Polling Place E-Voting) και η *Ηλεκτρονική Ψηφοφορία μέσω Internet* (Internet Voting).

Ηλεκτρονική Ψηφοφορία σε Εκλογικά Σημεία. Σε ένα εκλογικό σημείο π.χ. *Εκλογικό Κέντρο* ή *Κιόσκι* (California Internet Voting Task Force,2000), τόσο τα συστήματα-πελάτες (voting clients) που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένες οντότητες (π.χ. εκλογικοί αντιπρόσωποι, αστυνομία). Ανάλογα με το είδος του εκλογικού σημείου, το στάδιο της Επικύρωσης μπορεί να γίνει είτε με φυσικές διαδικασίες (έλεγχος απ' ευθείας από τους εκλογικούς αντιπροσώπους) είτε με ηλεκτρονικές (π.χ. κωδικός PIN). Η Υποβολή της ψήφου γίνεται ηλεκτρονικά σε προσωπικούς υπολογιστές ή ειδικές συσκευές με οθόνες αφής (όπως οι Συσκευές Άμεσης Καταμέτρησης – DRE, που χρησιμοποιούνται ευρέως στις Η.Π.Α (Caltec/Mit,2001)). Οι ηλεκτρονικές ψήφοι αποθηκεύονται τοπικά σε αποσπώμενες περιφερειακές μονάδες. Η Καταμέτρηση των ψήφων γίνεται επίσης ηλεκτρονικά: οι ψήφοι καταμετρούνται τοπικά στο εκλογικό κέντρο ή αποστέλλονται στον κεντρικό εξυπηρετητή (server) των εκλογών για τον υπολογισμό των συγκεντρωτικών αποτελεσμάτων. Η μεταφορά στον κεντρικό server μπορεί να γίνει επίσης ηλεκτρονικά, με «ασφαλείς» συνδέσεις (π.χ. μισθωμένες γραμμές οπτικών ινών ή μέσω Internet με τεχνικές IPSEC - Εικονικά Ιδιωτικά Δίκτυα VPNs). Εναλλακτικά, έχει προταθεί η χρήση των δικτύων ATM (Automated Teller Machines) την ημέρα των εκλογών: τα δίκτυα ATM έχουν ορισμένα επιθυμητά χαρακτηριστικά ασφάλειας (μυστικότητα του καναλιού επικοινωνίας, αξιόπιστος εξοπλισμός, ανθεκτικά τερματικά, υψηλό ποσοστό διείσδυσης). Ωστόσο συχνά διατυπώνονται αντιρρήσεις σχετικά με την καταλληλότητα τους για τη διενέργεια ηλεκτρονικών εκλογών (Jefferson,2000).

Ψηφοφορία μέσω Internet. Η ψήφος υποβάλλεται μέσω Internet και τα συστήματα-πελάτες βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (στο σπίτι, στον χώρο εργασίας, σε

βιβλιοθήκες, σχολεία, πανεπιστήμια). Η Εγγραφή μπορεί να γίνει με φυσικές (π.χ. σε εκλογικά γραφεία) ή με ηλεκτρονικές διαδικασίες (π.χ. ψηφιακή υπογραφή, μέθοδοι βιομετρικής). Τα στάδια της Επικύρωσης, της Υποβολής και της Καταμέτρησης γίνονται εξ' ολοκλήρου ηλεκτρονικά.

Η ψηφοφορία μέσω Internet απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου. Ενώ η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο, μπορούν εν δυνάμει να αντιμετωπιστούν με τεχνικές που ήδη χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών (π.χ. ψηφιακές υπογραφές - ψηφιακά πιστοποιητικά), οι επιπλέον απαιτήσεις όπως *μυστικότητα* και *ανωνυμία* της ψήφου, *οικουμενική επαληθευσιμότητα*, καθώς και *προστασία από καταναγκασμό*, συνθέτουν ένα πολύπλοκο μοντέλο απαιτήσεων ασφάλειας το οποίο έως σήμερα δεν έχει αντιμετωπιστεί με μεθόδους που να είναι ασφαλείς και παράλληλα πρακτικές. Οι επικριτές των συστημάτων ηλεκτρονικής ψηφοφορίας μέσω Internet θεωρούν ότι οι υπάρχουσες τεχνολογίες δεν είναι ακόμα ώριμες να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν. Επίσης θεωρούν ότι η υιοθέτηση τους θα οδηγούσε στον κοινωνικό αποκλεισμό των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών (Dictson,2000, Philips,2001).

2. Απαιτήσεις Ασφάλειας και Πρακτικότητας

Ένα σύστημα ηλεκτρονικής ψηφοφορίας που πρόκειται να χρησιμοποιηθεί σε εκλογές μεγάλης κλίμακας πρέπει να είναι (Internet Policy Institute,2001, Schneier,1996):

α) Ασφαλές, δηλαδή:

- *Δημοκρατικό* (Democratic). Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους, και κανείς ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.

- *Ακριβές* (Accurate). Καμία ψήφος δεν είναι δυνατόν να αλλοιωθεί, να καταμετρηθεί περισσότερες από μια φορές, να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς / εξωτερικούς εχθρούς.

- *Μυστικό* (Secret). Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε, ενώ όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων.

- *Προστατευμένο από Καταναγκασμό* (Uncoercible). Κανένας χρήστης δεν έχει τη δυνατότητα να αποδείξει τη ψήφο του σε κάποιον τρίτο.

- *Οικουμενικά Επαληθεύσιμο* (Universally Verifiable). Κάθε εξωτερικός παρατηρητής μπορεί να πειστεί ότι το σύστημα είναι ακριβές και ότι το αποτέλεσμα του υπολογισμού των ψήφων της κάλπης αντανακλά τη βούληση των ψηφοφόρων που τις υπέβαλλαν.

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

Πρέπει να τονίσουμε πως σε αρκετά δημοκρατικά καθεστώτα (π.χ. Αυστραλία, Ελλάδα, Βέλγιο), όπου η συμμετοχή των πολιτών στις εκλογές είναι υποχρεωτική από το νόμο, μια επιπλέον απαίτηση ασφάλειας είναι η εύρεση των ψηφοφόρων που δεν άσκησαν το εκλογικό τους δικαίωμα.

β) Πρακτικό

Το σύστημα πρέπει να είναι εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π), λειτουργικό (Στις εκλογές του 2000 στην Florida των Η.Π.Α ένας μεγάλος αριθμός άκυρων ψήφων υποβλήθηκε λόγω ελλιπούς σχεδίασης των ψηφοδελτίων), και να απευθύνεται σε όλες τις κατηγορίες πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet κ.λ.π.. Επίσης, το σύστημα πρέπει να υποστηρίζει μια ποικιλία από format ψήφων, συμπεριλαμβανομένων και των λεγόμενων «λευκών» ή άκυρων ψήφων. Το σύστημα θα πρέπει να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλεκτορικού σώματος ή των υποψηφίων (scalability), ενώ οι υπηρεσίες ασφάλειας που προσφέρει θα πρέπει να είναι διαφανείς (transparent) στον χρήστη.

3. Επιθέσεις σε Συστήματα Ηλεκτρονικής Ψηφοφορίας

Ουδείς παραγνωρίζει ότι τα κίνητρα για μια επίθεση στην ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας, ιδιαίτερα σε εθνικές εκλογές, είναι πολλά (πολιτικές επιδιώξεις, χρηματική αμοιβή, διεκδίκηση εξουσίας, εμπλοκή μυστικών υπηρεσιών, τρομοκρατικές οργανώσεις). Το είδος και η μορφή των επιθέσεων ποικίλουν (California Internet Voting Task Force,2000, Coleman,2002, Internet Policy Institute,2001, Philips,2001).

α) Ηλεκτρονική Ψηφοφορία (Γενικά). Είναι γνωστό ότι τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πιο εύκολα από ότι οι φυσικές ψήφοι. Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από *εσωτερικούς εχθρούς* (insider attacks) καθώς και σε επιθέσεις *Άρνησης Εξυπηρέτησης* (Denial Of Service – DOS). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας επίσης διαθέτουν ανεπαρκή *στοιχεία ελέγχου* (audit trail) (Philips,2001) και δεν παρέχουν οικουμενική επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση.

β) Ψηφοφορία μέσω Internet. Από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Internet είναι περισσότερο ευάλωτες σε *επιθέσεις καταναγκασμού* (coercion) (Burmester,2003) όπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου. Επιπρόσθετα, σε ένα σύστημα εξ' αποστάσεως ψηφοφορίας οι ψηφοφόροι ενδεχομένως θα πρέπει να δημιουργήσουν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), π.χ. προτού υποβάλλουν τη ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Internet παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web. Παράλληλα, τα συστήματα ψηφοφορίας μέσω Internet είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

- *Στα συστήματα-πελάτες*: Ιοί τύπου «*σκουλήκια*» (worms) ή «*δούρειοι ίπποι*» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί. Επίσης, ο εισβολέας μπορεί εξ' αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web.

- *Στο επίπεδο της επικοινωνίας*: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις *πλαστοπροσωπίας* (spoofing) DNS ονομάτων ή IP διευθύνσεων, και οι *επιθέσεις ενδιάμεσης οντότητας* (man in the middle) (Schneier,1996). Η επικοινωνία μεταξύ πελάτη και εξυπηρετητή μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π.

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

4. Προϋποθέσεις για τη Διεξαγωγή Εκλογών μέσω Internet

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

Πρωτόκολλα / Λογισμικό. Για να είναι ασφαλής η ηλεκτρονική ψηφοφορία, το σύστημα θα πρέπει να υλοποιεί ένα κρυπτογραφικό πρωτόκολλο (τα υποψήφια μοντέλα περιγράφονται στην Ενότητα 5) που ικανοποιεί τις απαιτήσεις ασφάλειας (Ενότητα 2). Για λόγους αξιοπιστίας επίσης, θεωρούμε πως το σύστημα θα πρέπει να υλοποιηθεί με *ανοικτό λογισμικό* (open source). Το σύστημα πρέπει επίσης να συνοδεύεται από τους κατάλληλους μηχανισμούς παρακολούθησης (monitoring) και επαλήθευσης (audit) της λειτουργίας του. Ανεξάρτητοι ηλεκτρονικοί ή φυσικοί μηχανισμοί επαλήθευσης ενδεχομένως να αυξήσουν την εμπιστοσύνη των πολιτών στο αποτέλεσμα των εκλογών. Για παράδειγμα, η Mercuri (1992) πρότεινε την εκτύπωση των επιλογών του ψηφοφόρου σε χαρτί, το οποίο ο ψηφοφόρος θα ρίχνει σε μια φυσική κάλπη για τις ανάγκες μιας δεύτερης καταμέτρησης.

Υποδομή Δημόσιου Κλειδιού. Οι εκλογές μέσω Internet θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής έως και το στάδιο της Καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής *Υποδομή Δημόσιου Κλειδιού* (Public Key Infrastructure – PKI), όπου η ταυτοποίηση των ψηφοφόρων στο στάδιο της Εγγραφής και της Επικύρωσης θα γίνεται με τη χρήση ψηφιακών υπογραφών / ψηφιακών πιστοποιητικών, ενώ η ακεραιότητα και η εμπιστευτικότητα των επικοινωνιών θα υποστηρίζονται από κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού. Παράλληλα, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο Εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως *SSL/TLS* (Secure Socket Layer/Transport Layer Security) και *SSH* (Secure Shell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.

Ασφάλεια Πληροφοριακού Συστήματος. Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία *firewalls* στα συστήματα-πελάτες, καθώς και *Συστήματα Ελέγχου Εισβολής* (Intrusion Detection Systems) και *firewalls* στα συστήματα-εξυπηρετητές. Παράλληλα επιβάλλεται η χρήση διαδικασιών *πλεονασμού* (redundancy), ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται. Ένα συμπληρωματικό μέτρο για τη βελτίωση της διαθεσιμότητας του συστήματος θα ήταν και η παράταση της περιόδου υποβολής ηλεκτρονικών ψήφων, πλέον της μίας ημέρας (αρκεί βεβαίως οι ηλεκτρονικές ψήφοι να καταμετρούνται ταυτόχρονα με τις φυσικές, προκειμένου να διατηρηθεί η νομιμότητα των εκλογών).

Νομικά Θέματα. Πέρα από την ολοκλήρωση της θεσμοθέτησης για τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, όπου ήδη έχουν γίνει σημαντικά βήματα (Σιούλης,2003), απαραίτητη προϋπόθεση αποτελεί και η ύπαρξη νομολογίας που θα κατοχυρώνει την μυστικότητα της ηλεκτρονικής ψήφου και θα προβλέπει επιθέσεις όπως καταναγκασμός του ψηφοφόρου, ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π.

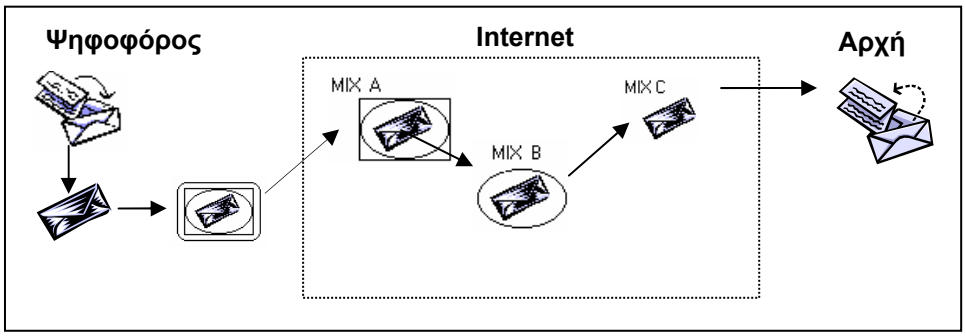
Σε κάθε περίπτωση, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής *πολιτικής ασφάλειας* που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις. Το προσωπικό που εμπλέκεται στην ανάπτυξη, λειτουργία και διαχείριση συστημάτων ηλεκτρονικής ψηφοφορίας πρέπει να επιλέγεται προσεκτικά. Καταλήγοντας, θα λέγαμε ότι οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας.

5. Κρυπτογραφικά Μοντέλα Ασφάλειας

Τα βασικά κρυπτογραφικά μοντέλα ηλεκτρονικής ψηφοφορίας που έχουν προταθεί έως σήμερα είναι: το μοντέλο *MIX-net* (Chaum,1981), το μοντέλο των *«τυφλών» υπογραφών* (Fujioka et al.,1993), και το *ομομορφικό μοντέλο* (Cramer et al.,1997). Σχεδόν όλα τα πρωτόκολλα που έχουν προταθεί ως σήμερα βασίζονται στα παραπάνω τρία μοντέλα.

Το Μοντέλο MIX-net. Ο Chaum (1981) εισήγαγε την έννοια των δικτύων MIX-net (MIX networks) τα οποία αποτελούν έναν κρυπτογραφικό μηχανισμό για την κατασκευή ανώνυμων καναλιών (anonymous channels) σε εφαρμογές υψηλής ασφάλειας. Ένα δίκτυο MIX-net αποτελείται από έναν αριθμό εξυπηρετητών, συνδεδεμένων μεταξύ τους, που καλούνται κόμβοι MIX. Κάθε κόμβος MIX λαμβάνει ως είσοδο (input) ένα σύνολο μηνυμάτων (π.χ. τις κρυπτογραφημένες ψήφους), κάνει ορισμένους τυχαίους μετασχηματισμούς και επιστρέφει στην έξοδο (output) ένα διαφορετικό σύνολο (των ίδιων, μετασχηματισμένων) μηνυμάτων, κατά τρόπο ώστε τα μηνύματα της εξόδου να μη μπορούν να συνδεθούν με τα μηνύματα της εισόδου. Κατ' αυτόν τον τρόπο, καμία συνεργία οποιουδήποτε αριθμού κόμβων MIX (εκτός από την περίπτωση όπου συνεργούν όλοι οι κόμβοι) δε μπορεί να αποφανθεί περί του *ποια* ψήφος αντιστοιχεί σε *ποιόν* ψηφοφόρο

Στην (Chaum,1981) κάθε ψήφος κρυπτογραφείται διαδοχικά με τα δημόσια κλειδιά όλων των κόμβων MIX, με σειρά αντίστροφη της σειράς των κόμβων – Σχήμα 1. Η ψήφος κρυπτογραφείται πρώτα με το δημόσιο κλειδί του MIX_C που θα παραλάβει τελευταίο τη λίστα με τις κρυπτογραφημένες ψήφους, στη συνέχεια με το κλειδί του προτελευταίου MIX_B και τέλος με το δημόσιο κλειδί του πρώτου τη τάξει MIX_A. Κάθε κόμβος MIX αποκρυπτογραφεί τη λίστα των ψήφων που του αποστέλλονται, τη μετασχηματίζει (π.χ. προσθέτοντας τυχαιότητα σε κάθε ψήφο και αναδιατάσσοντας τη λίστα με τις ψήφους που προκύπτει), και στη συνέχεια την προωθεί στον επόμενο κόμβο. Αυτό το μοντέλο καλείται MIX-net *αποκρυπτογράφησης* (Chaum,1981). Σε ένα παραπλήσιο μοντέλο, σε κάθε κόμβο MIX λαμβάνει χώρα μόνον ο μετασχηματισμός των ψήφων, και στη συνέχεια όλοι οι κόμβοι συνεργάζονται για την αποκρυπτογράφηση της τελικής λίστας των ψήφων (Hirt,2000).



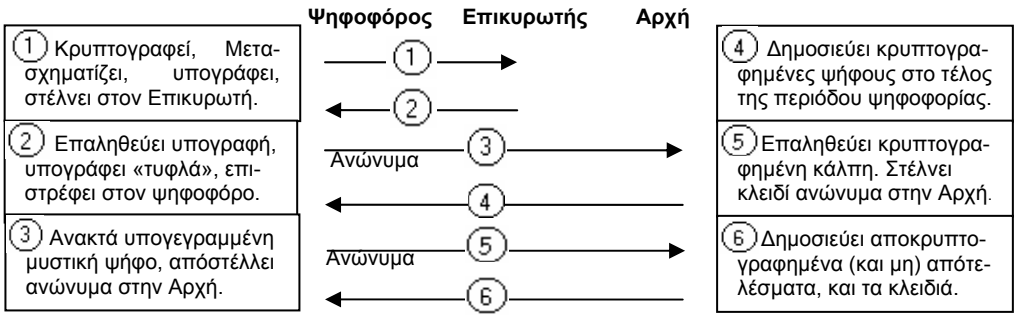
Σχήμα 1 Ένα παράδειγμα ενός δικτύου MIX-net με τρεις κόμβους MIX

Ένας άλλος τύπος είναι το MIX-net *επανακρυπτογράφησης* (Jakobsson,1999), όπου όλες οι ψήφοι κρυπτογραφούνται με το δημόσιο κλειδί του πρώτου κόμβου MIX, και στη συνέχεια σε κάθε κόμβο MIX λαμβάνει χώρα ο μετασχηματισμός και η κρυπτογράφηση με το δημόσιο κλειδί του επόμενου κόμβου, κατά τρόπο επαληθεύσιμο (μεταξύ των κόμβων ή/και για τους εξωτερικούς παρατηρητές).

Οι πλέον χρήσιμες ιδιότητες των δικτύων MIX-net, ειδικά για εκλογές μεγάλης κλίμακας, είναι η *οικουμενική επαληθευσιμότητα* της ορθότητας των μετασχηματισμών και της αποκρυπτογράφησης που προσφέρουν, καθώς και η *ανθεκτικότητα* τους έναντι συνεργιών μεταξύ (έως) ενός ορισμένου αριθμού MIX. Για αυτούς τους λόγους τα δίκτυα MIX-net έχουν χρησιμοποιηθεί κατά καιρούς για την επίτευξη ανωνυμίας σε εφαρμογές ηλεκτρονικού εμπορίου. Έως σήμερα πάντως, κανένα σύστημα ηλεκτρονικής ψηφοφορίας δεν έχει υλοποιηθεί με χρήση τεχνικών MIX-net.

Το Μοντέλο των «Τυφλών» Υπογραφών. Η έννοια της «τυφλής» υπογραφής (blind signature) παρουσιάστηκε αρχικά ως μια κρυπτογραφική μέθοδος για την υπογραφή ενός μηνύματος χωρίς τη γνώση του μηνύματος καθ' αυτού. Θα μπορούσαν, χρησιμοποιώντας ένα παράδειγμα της καθημερινής ζωής, να αντιστοιχιστούν με την υπογραφή (εξωτερικά) ενός σφραγισμένου φακέλου που περιέχει ένα χαρτί τοποθετημένο κάτω από καρμπόν. Όταν ο φάκελος αργότερα ανοιχτεί από τον νόμιμο παραλήπτη, το χαρτί θα έχει αποτυπωμένη την υπογραφή (Schneier,1996).

Αυτή η μέθοδος, αν και εφαρμόστηκε αρχικά σε εφαρμογές *ηλεκτρονικού χρήματος* (e-cash), χρησιμοποιήθηκε επίσης για την επίλυση του προβλήματος της Επικύρωσης των ψήφων με παράλληλη προστασία της μυστικότητας τους (Fujioka et al.,1993) - Σχήμα 2.



Σχήμα 2 Ένα παράδειγμα ηλεκτρονικής ψηφοφορίας με «τυφλές» υπογραφές

Έως σήμερα έχουν προταθεί αρκετά σχήματα που βασίζονται στον μηχανισμό των «τυφλών» υπογραφών (π.χ. (Okamoto,1997)). Επίσης, αρκετά συστήματα έχουν υλοποιηθεί πιλοτικά σε εκλογές μικρής κλίμακας (Το σύστημα SENSUS – διενέργεια ηλεκτρονικών εκλογών μέσω Internet, το σύστημα EVOX - εκλογές προπτυχιακών φοιτητών στο MIT) (Burmester,2002).

Ένα πλεονέκτημα των συστημάτων που ακολουθούν το μοντέλο των «τυφλών» υπογραφών είναι ότι απαιτούν χαμηλό επικοινωνιακό φόρτο και υπολογιστικό κόστος, ακόμα και όταν ο αριθμός των ψηφοφόρων / υποψηφίων είναι μεγάλος (scalability). Επιπλέον, η μυστικότητα των ψήφων επαφίεται στους ψηφοφόρους, κάτι που ευνοεί την εύκολη και ασφαλή διαχείριση του συστήματος από την (συνήθως μια) Αρχή.

Ένα σημαντικό μειονέκτημα των συστημάτων «τυφλής» υπογραφής είναι ότι απαιτούν από τον ψηφοφόρο να είναι ενεργός (online) σε όλα τα στάδια της ψηφοφορίας. Επίσης τα συστήματα αυτά προσφέρουν μόνο *ατομική επαληθευσιμότητα* (οι ψηφοφόροι μπορούν να εντοπίζουν και να διορθώνουν τα λάθη που αφορούν μόνον τη δική τους ψήφο). Πρόσφατα έχουν επίσης προταθεί πρωτόκολλα όπου η δύναμη του Επικυρωτή είναι κατανεμημένη (distributed), με τη χρήση κρυπτογραφικών τεχνικών τύπου *threshold* (Durette,1999).

Το Ομομορφικό Μοντέλο Κρυπτογράφησης. Το μοντέλο αυτό (Cramer et al.,1997) χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγορίθμων κρυπτογράφησης για να εδραιώσει οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων. Κατά την ομομορφική κρυπτογράφηση υπάρχει μια πράξη $\oplus$ ορισμένη στο σύνολο των μηνυμάτων και μια πράξη $\otimes$ ορισμένη στο σύνολο των κρυπτογραφημάτων (συνήθως οι πράξεις αυτές είναι το άθροισμα και ο πολλαπλασιασμός, modulo έναν μεγάλο αριθμό), τέτοιες ώστε το «γινόμενο» των κρυπτογραφήσεων οποιωνδήποτε δύο ψήφων $v_1, v_2 : E(v_1) \otimes E(v_2)$, να ισούται με την κρυπτογράφηση $E(v_1 \oplus v_2)$ του «αθροίσματος» των ψήφων. Κατ' αυτόν τον τρόπο, η ταυτότητα του ψηφοφόρου δεν χρειάζεται να προστατευτεί με τεχνικές ανωνυμίας (π.χ. δίκτυα MIX-net, «τυφλές» υπογραφές), αφού καμία ψήφος δεν αποκρυπτογραφείται μεμονωμένα, αλλά όλες οι ψήφοι συνδυάζονται και το τελικό κρυπτογράφημα αποκρυπτογραφείται από τις Αρχές του συστήματος.

Το σύστημα VoteHere (Adler et al.,2000), το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί μια υλοποίηση του ομομορφικού μοντέλου κρυπτογράφησης. Ένα μειονέκτημα των συστημάτων που βασίζονται στο ομομορφικό μοντέλο είναι η περιορισμένη *ευκαμψία* τους (flexibility), καθώς οι ψήφοι συνήθως

περιορίζονται σε δίτιμες ψήφους του τύπου «Ναι»/«Όχι» (π.χ. {+1, -1}). Για μεγάλο αριθμό υποψηφίων, οι υλοποιήσεις του μοντέλου συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Ωστόσο πρόσφατα έχουν προταθεί εναλλακτικά κρυπτογραφικά σχήματα, των οποίων η υπολογιστική πολυπλοκότητα είναι είτε *γραμμική* (linear) είτε *λογαριθμική* (logarithmic) ως προς τον αριθμό των υποψήφιων (Damgard et al., 2003).

6. Το Μέλλον

Η διείσδυση του Internet στις σύγχρονες κοινωνίες καθιστά επωφελή την υιοθέτηση ηλεκτρονικών μεθόδων για την εξ' αποστάσεως συμμετοχή του πολίτη στις δημοκρατικές αποφάσεις (ψηφοφορίες, referenda, δημοσκοπήσεις κ.λ.π). Τα συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet, μαζί με άλλες διαδικασίες που εφαρμόζονται σήμερα σε δημοκρατικά καθεστώτα (π.χ. ψηφοφορία μέσω ταχυδρομείου στην Ελβετία (Trechsel et al.,2003)) αναμένεται να απλοποιήσουν την υποβολή της ψήφου και να αυξήσουν τη συμμετοχή των πολιτών στις εκλογές. Σε κάθε περίπτωση, η υποβολή ψήφου μέσω Internet θα πρέπει να αποτελέσει μια *εναλλακτική* και όχι τη μοναδική δυνατότητα συμμετοχής του πολίτη στις εκλογές. Σε αντίθετη περίπτωση, θα προέκυπταν ζητήματα κοινωνικού αποκλεισμού και συνταγματικότητας των εκλογών (Mitrou et al.,2002). Σε γενικές γραμμές οι κυριότεροι παράγοντες που αποτρέπουν σήμερα την υιοθέτηση συστημάτων εξ' αποστάσεως ψηφοφορίας μέσω Internet είναι: α) Μη ασφαλή συστήματα υπολογιστών, β) Έλλειψη Υποδομών Δημοσίου Κλειδιού, γ) Έλλειψη Προτύπων (Standards). Παράλληλα, η μετάβαση σε εκλογές μέσω Internet πιθανόν αρχικά να συνεπάγεται υψηλό κόστος αγοράς και συντήρησης υπολογιστικών μηχανών, λογισμικού βάσεων δεδομένων και συστημάτων δρομολόγησης, ωστόσο μακροπρόθεσμα το κόστος αναμένεται να είναι μειωμένο σε σχέση με τις παραδοσιακές εκλογές.

Η μετάβαση σε συστήματα εξ' αποστάσεως ψηφοφορίας μέσω Internet αναμένεται να γίνει σταδιακά, αρχής γενομένης με ψηφοφορίες σε Εκλογικά Σημεία, όπου το φυσικό περιβάλλον και οι επικοινωνίες μπορούν να ελεγχθούν επαρκώς. Θεωρούμε πως, παρά το γεγονός ότι η πρώτη αυτή φάση δεν θα προσφέρει ουσιαστικά πλεονεκτήματα έναντι των παραδοσιακών τρόπων ψηφοφορίας, ωστόσο θα προσφέρει ένα σημαντικό πεδίο για συζήτηση και απόκτηση εμπειριών για τη μετάβαση σε περισσότερο «φιλελεύθερα» συστήματα (χρήση συσκευών τύπου ATM σε Κιόσκια, PC σε σχολεία, βιβλιοθήκες, δημόσιες υπηρεσίες) με απώτερο σκοπό τη δυνατότητα υποβολής ψήφου από το σπίτι ή το χώρο εργασίας μέσω Internet. Ως προς την ασφάλεια ενός τέτοιου συστήματος, δεν είναι ρεαλιστικό να πιστεύουμε ότι ένα σύστημα ψηφοφορίας μέσω Internet θα μπορέσει ποτέ να αντιμετωπίσει όλα τα ζητήματα ασφάλειας που θέσαμε, όντας παράλληλα πρακτικό και λειτουργικό: αυτό που θα έπρεπε (και μπορούμε) να περιμένουμε είναι ένα σύστημα τουλάχιστον τόσο ασφαλές όσο και τα παραδοσιακά εκλογικά συστήματα.

Βιβλιογραφία

Adler, J., Dai, W., Green, R., Neff, A., (2000). Computational Details of the VoteHere Homomorphic Election System. At: http://www.votehere.net/ada_compliant

Burmester, M., Magkos, E., (2002). Towards Secure and Practical e-Elections in the New Era. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers, pp. 63-76.

Burmester, M., Magkos, E., Chrissikopoulos, V., (2003). Uncoercible e-bidding Games. In: Electronic Commerce Research Journal, Special Issue on Security Aspects in E-Commerce, Kluwer Academic Publishers. To be published.

California Internet Voting Task Force, (2000). A Report on the Feasibility of Internet Voting, Jan 2000, at: http://www.ss.ca.gov/executive/ivote/

CALTEC/MIT,(2001). Voting Technology Project. www.vote.caltech.edu/reports/index.html

Chaum, D., (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: Communications of the ACM, Vol. 24(2), pp. 84-88.

Coleman, S., (2002). Elections in the 21st Century: From Paper Ballot to E-Voting. Report by the Independent Commission on Alternative Voting Methods, London, Electoral Reform Society.

Cramer, R., Gennaro, R., Schoenmakers, B., (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 103-118.

Damgard, I., Groth, J., Salomonsen, G., (2003). The Theory and Implementation of an Electronic Voting System. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers, pp. 77-98.

Dictson, D., Ray, D., (2000). The Modern Democratic Revolution: An Objective Survey of Internet-based Elections. White Paper, January 2000, at: www.securepoll.com

Durette, B. W., (1999). Multiple Administrators for Electronic Voting. Bachelor's Thesis, Massachusetts Institute of Technology.

Fujioka, A., Okamoto, T., Ohta, K., (1993). A Practical Secret Voting Scheme for Large Scale Elections. In: Proceedings of AUSCRYPT '92, Lecture Notes in Computer Science, Vol. 718, Springer-Verlag, pp. 244-251.

Hirt, M., Sako, K., (2000). Efficient Receipt-Free Voting Based on Homomorphic Encryption. In: Advances in Cryptology - EUROCRYPT '2000, Lecture Notes in Computer Science, Vol. 1807, Springer-Verlag, pp. 539-556.

Internet Policy Institute, 2001. Report of the National Workshop on Internet Voting, March 2001, at: http://www.internetpolicy.org

Jakobsson, M., (1999). Flash Mixing. In: Proceedings of the 18th ACM Symposium on Principles of Distributed Computing - PODC '99, ACM Press, pp. 83-89.

Jefferson, D. (2000). ATM Network Voting: A non-Starter. In: The Risks Digest, Vol. 21(15), 2000, at: http://catless.ncl.ac.uk/Risks/21.15.html#subj2

Mercuri, R., (1992). Physical Verifiabiblity of Computer Systems. In: Proceedings of the 5th International Virus and Security Conference, http://www.notablesoftware.com/evote.html

Mitrou, L., Gritzalis, D., Katsikas, S., (2002). Revisiting Legal and Regulatory Requirements for E-voting. In: Proceedings of the 17th IFIP International Information Security Conference, Kluwer Academic Publishers, pp. 469-480.

Mohen, J., Glidden, J., (2001). The Case for Internet Voting. In: Communications of the ACM, Vol. 44(1), pp. 72-82.

Okamoto, T., (1997). Receipt-Free Electronic Voting Schemes for Large Scale Elections. In: Proceedings of the 5th Security Protocols Workshop '97, Lecture Notes in Computer Science, Vol. 1163, pp. 125-132.

Philips, D., Spakovsky, H., (2001). Gauging the Risks of Internet Elections. In: Communication of the ACM, Vol. 44(1), pp. 72-85.

Schneier, B., (1996). Applied Cryptography, Second Edition - Protocols, Algorithm and Source Code in C. John Wiley and Sons.

Σιούλης, Χ., (2003). Η Ευρωπαϊκή Νομοθεσία για τις Ηλεκτρονικές Υπογραφές (Ανάλυση & Σχολιασμός). www.Sioulis.gr

Trechsel, A., Mendez, F., Kies R., (2003). Remote Voting via the Internet? The Canton of Geneva Pilot Project. In: Advances in Information Security - Secure Electronic Voting, Kluwer Academic Publishers, pp. 181-194