Η διαβλητότητα του συστήματος ηλεκτρονικής ψηφοφορίας Ήλιος*

(*Το πρόγραμμα που χρησιμοποιεί το Υπουργείο Παιδείας για τις εκλογές των Συμβουλίων Ιδρύματος στα ΑΕΙ/ΤΕΙ)

Ο φιλόσοφος/διανοητής Ludwig Wittgenstein στο «Παρατηρήσεις στα θεμέλια των Μαθηματικών» γράφει ότι «ο λόγος που το 1+1=2 είναι σωστό, δεν είναι άλλος από το ότι μέχρι στιγμής δεν βρέθηκε κάποιος να πει: 'ωχ, εδώ κάτι μας έχει ξεφύγει!'». Προφανώς ο Wittgenstein δεν έχει βάλει στο στόχαστρο το 1+1=2. Αυτό που μας λέει εδώ είναι ότι η ορθότητα στην επιστήμη δεν βασίζεται στην αυθεντία κάποιων, αλλά στον συνεχή και καθημερινό δημόσιο έλεγχο.

Ξεκινώντας με αυτή την παρατήρηση θέλω να θέσω το εξής ερώτημα: Το πρόγραμμα Ήλιος ισχυρίζεται ότι κάνει κάποια πράγματα. Ποιος είναι σε θέση από αυτούς που καλούνται να το χρησιμοποιήσουν να ελέγξουν τον κώδικα του προγράμματος ότι πράγματι κάνει αυτά που λέει; Από που προκύπτει ότι εγώ, που δεν έχω την δυνατότητα να ελέγξω τις χιλιάδες γραμμές κώδικα του προγράμματος, πρέπει να εμπιστευτώ τους δημιουργούς του; Προσέξτε: την διαδικασία εκλογής με φυσική παρουσία μπορεί να την ελέγξει κάθε ένας από τους εκλογείς. Είτε είναι επιστήμονας είτε απλός εργάτης ή αγρότης. Τη διαδικασία του Ήλιος ποιος μπορεί να την ελέγξει; Πρακτικά ελάχιστοι. Οι υπόλοιποι καλούνται να τους εμπιστευτούν. Αυτό δεν απέχει καθόλου (μάλιστα είναι πανομοιότυπο) με το να πει κάποιος «δώσε μου την ψήφο σου, εγώ θα τη βάλω στην κάλπη που έχω στο σπίτι μου, θα βγάλω τίμια τα αποτελέσματα, και εσύ απλά θα πρέπει να με εμπιστευτείς». Ένα απλό μειδίαμα αρκεί για να καταρρεύσει η ασφάλεια του συστήματος.

Προσωπικά θεωρώ ότι το παραπάνω αρκεί για να απορριφθεί η όποια ασφάλεια του συστήματος. Υπάρχουν όμως και άλλα αν κανείς θέλει να ακούσει περισσότερα. Ας παρουσιάσω μερικά από αυτά.

Στις συχνές ερωτήσεις (FAQ) στην σελίδα του Ήλιος (http://heliosvoting.org/frequently-asked-questions/) οι δημιουργοί του συστήματος γράφουν την ερώτηση (τελευταία ερώτηση) «Να αρχίσουμε να χρησιμοποιούμε το Ήλιος στις εκλογές για την διοίκηση; Ίσως για την εκλογή Προέδρου 2012;» Και μόνοι τους απαντούν ορθά κοφτά «Όχι, δεν πρέπει.» Στη συνέχεια προσπαθούν να δικαιολογήσουν αυτή τους την άρνηση λέγοντας στην ουσία ότι το ρίσκο είναι ευθέως ανάλογο της σπουδαιότητας των εκλογών. Δηλαδή, υπάρχει ρίσκο! Μόνοι τους παραδέχονται ότι το σύστημα δεν είναι ασφαλές (απλά συνδέουν την παραβίαση της ασφάλειας με το πόσο πολύ θέλεις να το παραβιάσεις), για να καταλήξουν «για τις εκλογές διοίκησης προτείνουμε εκλογές με φυσική παρουσία».

Ας πάμε όμως και σε απλά θέματα τεχνικής φύσεως μιλώντας όσο πιο απλά γίνεται (αν και με βάση τα παραπάνω τα θεωρώ περιττά). Το σύστημα του Υπουργείου, ο υπολογιστής, θα καταγράψει ποιος συνδέθηκε για να ψηφίσει από πού. Θα καταγράψει την ηλεκτρονική διεύθυνση από την οποία συνδέθηκε ο χρήστης, ενδεχομένως θα κρυπτογραφήσει αυτά τα στοιχεία, και θα δεχθεί κρυπτογραφημένη κάθε ψήφο. Τι σημαίνει «θα κρυπτογραφήσει» και πώς θα διαχειριστεί μια «κρυπτογραφημένη ψήφο»; Σημαίνει ότι θα αλλάξει την εμφάνιση των δεδομένων με κάποιο (έστω περίπλοκο) τρόπο αλλά ό,τι και όσες διαδικασίες κάνει θα πρέπει να μπορεί τελικά να διαβάσει την ψήφο για να βγάλει αποτελέσματα. Δηλαδή, η διαδικασία κρυπτογράφησης εν τέλει θα αντιστραφεί. Και τα κλειδιά για την αντιστροφή αυτή τα έχει στα χέρια του το Υπουργείο (μέσω των διαχειριστών του συστήματος), αλλιώς δεν μπορεί να αποκρυπτογραφήσει. Όλα τα υπόλοιπα που παρου-

σιάζονται στη σελίδα του συστήματος zeus.minedu.gov.gr είναι για να πείσουν τον αδαή. Η κρυπτογραφία στο Internet δεν χρησιμοποιείται (δεν μπορεί να χρησιμοποιηθεί) για να μην έχουν πρόσβαση στα στοιχεία ο αποστολέας και ο παραλήπτης. Η κρυπτογραφία χρησιμοποιείται για να μην υπάρξουν ενδιάμεσοι (χάκερς) που θα διαβάσουν τα στοιχεία. Σκεφτείτε: αν ο παραλήπτης (της ψήφου, του αριθμού πιστωτικής κάρτας, κλπ) δεν έχει πρόσβαση στα στοιχεία σας, η συνδιαλλαγή σας με αυτόν δεν μπορεί να πραγματοποιηθεί. Ο μόνος τρόπος να μην έχει πρόσβαση στα στοιχεία σας πχ σε μια αγορά στο διαδίκτυο, είναι μέσου τρίτου έμπιστου (τράπεζας). Να τη πάλι η εμπιστοσύνη...

Για να μην μακρηγορώ, αναρωτηθείτε για το εξής: Αν το σύστημα επέτρεπε την προσθήκη σχολίων σε κάποιο πεδίο, και κάποιος έγραφε «Έχω ένα υπέροχο σχέδιο για να δολοφονήσω μέχρι αύριο το πρωί τον πρωθυπουργό της χώρας» σε πόση ώρα νομίζετε ότι θα τον έχουν συλλάβει οι διωκτικές αρχές;

Αντώνης Τσολομύτης

Αναπληρωτής Καθηγητής
Πανεπιστήμιο Αιγαίου
Τμήμα Μαθηματικών