Ρέθυμνο 22-10-2012

Προς: **Τα μέλη της Πανεπιστημιακής Κοινότητας του Παν/μίου Κρήτης**

Αγαπητοί συνάδελφοι,

Όπως γνωρίζετε ήδη, οι εκλογές για την ανάδειξη των εσωτερικών νελών του Συμβουλίου του Ιδρύματος, που προβλέπεται από τους ν.4009/11 και 4076/12, δεν έγιναν λόγω παρεμπόδισής τους από μερίδα της Πανεπιστημαικής Κοινότητας.

Σύμφωνα με τις διατάξεις της ανωτέρω νομοθεσίας, το Πρυτανικό Συμβούλιο, ως το αρμόδιο όργανο για την διενέργεια των εκλογών, πρέπει να προχωρήσει στην διαδικασία εκλογής των εσωτερικών μελών του Συμβουλίου, επιλέγοντας, είτε την διαδικασία της επιστολικής ψήφου, είτε της ηλεκτρονικής ψήφου, όπως αυτές ορίζονται στην σχετική Υπουργική Απόφαση (ΥΑ Φ.122.1/764/112039/Β2/21-9-12, ΦΕΚ 2564Β/21-9-12).

Και οι δύο διαδικασίες είναι από ασυνήθεις, έως πρωτόγνωρες, τουλάχιστον για τα ελληνικά δεδομένα Ως εκ τούτου, θα ήθελα να εκθέσω προς τα μέλη του εκλογικού σώματος (που από τον νόμο είναι τα μέλη ΔΕΠ), αλλά και της Πανεπιστημιακής Κοινότητας γενικότερα, μερικές σκέψεις σχετικά με το ενδεχόμενο εφαρμογής της «ηλεκτρονικής ψηφοφορίας», που εισήχθη με τον ν.4076/12, άρθρο 2 παρ.3 και περιγράφεται στα άρθρα 4 έως 6 της προαναφερθείσας ΥΑ, η οποία εκδόθηκε κατ' εξουσιοδότηση της ανωτέρω διάταξης του ν.4076/12. Ας σημειωθεί ότι τα εκτιθέμενα πιο κάτω κοινοποιήθηκαν ηλεκτρονικά και στα μέλη της Συνόδου των Πρυτάνεων κατά την τελευταία έκτακτη συνεδρίασή της στις 20-10-12.

Η διαδικασία της "*ηλεκτρονικής ψήφου*" που περιγράφεται στο κεφ. Β (άρθρα 4 έως 6) της ανωτέρω ΥΑ, κατά την γνώμη μου, παρουσιάζει ελλείψεις και κενά σε σχέση με θέματα:

(Ι) Που αφορούν στην ίδια την **ουσία** της ψηφοφορίας σε μία εκλογική διαδικασία.

(ΙΙ) Τεχνικής φύσεως, για τα οποία, λόγω του εξειδικευμένου τεχνικού/επιστημονικού χαρακτήρα τους, απαιτούνται **εγγυήσεις** προς τα "*Όργανα διενέργειας των εκλογών*" (άρθρο 2 της ανωτέρω ΥΑ) από την νομοθετούσα αρχή ή/και την κυβέρνηση (βλ. Υπουργείο Παιδείας) για την εφαρμοσιμότητα και το αδιάβλητο της όλης διαδικασίας.

Θα πρέπει να σημειωθεί, ότι από όσο γνωρίζω (και αν κάνω λάθος, ας υποδειχθεί τούτο), η μόνη πληροφόρηση που έχουμε είναι οι προαναφερθείσες διατάξεις της νομοθεσίας και μία ιστοσελίδα του Υ.ΠΑΙ.Θ.Π.Α. (https://zeus.minedu.gov.gr) που μάλιστα ενεργοποιήθηκε μόλις στις 17/10/12.

Για το (Ι):

1. Υπάρχει **πλήρης αδυναμία ελέγχου της ταυτοπροσωπίας** του ψηφοφόρου από την εφορευτική επιτροπή ή/και τους υποψηφίους ή τους νόμιμους αντιπροσώπους τους: Κάθε ψηφοφόρος μπορεί να εκχωρήσει το δικαίωμα του ως εκλέκτορας σε άλλο άτομο (ή να πιεστεί να το κάνει), το οποίο δεν νομιμοποιείται να είναι εκλέκτορας. Τούτο δεν είναι δυνατόν σε ψηφοφορία με κοινή κάλπη, έστω και αν ο ψηφοφόρος το θέλει, καθώς πρέπει ο **ίδιος** να παρουσιαστεί στο εκλογικό τμήμα (σημειωτέον, ότι η νομοθεσία δεν επιτρέπει την δυνατότητα έγγραφης εξουσιοδότησης για εκχώρηση του δικαιώματος ψήφου σε άλλο άτομο).

2. Στην συνήθη ψηφοφορία με κοινή κάλπη, οι υποψήφιοι ή και οι εξουσιοδοτημένοι εκπρόσωποι των υποψηφίων **μπορούν να παρακολουθούν** την ψηφοφορία καθ' όλη την διάρκειά της, ώστε να εγγυηθούν το αδιάβλητο της διαδικασίας, ή και να υποβάλουν ενστάσεις μετά. Η ηλεκτρονική ψηφοφορία δεν δίνει καμία τέτοια δυνατότητα. Κατά συνέπεια, τα αναφερόμενα στην ανωτέρω ιστοσελίδα ότι «*αρκεί να*

υπάρχει ένα και μόνο τίμιο μέλος στην [εφορευτική] *επιτροπή*» για να εξασφαλιστεί το **απόρρητο** της ψήφου, δεν εξασφαλίζουν πράγματι το απόρρητο, καθώς δεν μπορεί να υπάρξει κανένας έλεγχος της εφορευτικής επιτροπής επ' αυτού, από κανέναν άλλο (βλ. και παρ.Ι.2(α) πιο κάτω).

3. Οι διαδικασίες ανάδειξης των διοικητικών οργάνων των ΑΕΙ είναι αρμοδιότητα **αποκλειστικά** των ίδιων των ΑΕΙ. Διαφορετικά, νομίζω ότι η έννοια της "πλήρους αυτοδιοίκησης" που προβλέπεται από το Σύνταγμα, πλήττεται άμεσα. Εν προκειμένω, μέσω της ηλεκτρονικής ψηφοφορίας, η αρμοδιότητα εκλογής των εσωτερικών μελών του συμβουλίου εκχωρείται κατά μέγα μέρος στο Υπουργείο Παιδείας, και μάλιστα εντελώς απρόσωπα! Καταθέτω ενδεικτικά από την προαναφερθείσα ΥΑ, άρθρο 5 παρ.2: «*... Το σύστημα "ΖΕΥΣ" εξάγει τα τελικά αποτελέσματα και προσδιορίζει τον/τους εκλεγέντα/ες*».

Για το σύστημα «ΖΕΥΣ» (όπως και για κάθε άλλο) υπάρχει κάποιος διαχειριστής (ή διαχειριστές), που έχει την εποπτεία και την ευθύνη όλου του συστήματος, και ο οποίος σε κάποιο (άγνωστο) βαθμό μετέχει της διαδικασίας (ενδεχομένως να έχει έλεγχο σε ουσιώδη βήματά της), χωρίς να αποτελεί μέλος κανενός ΑΕΙ, χωρίς φυσικά να έχει εξουσιοδοτηθεί από το *Όργανο διενέργειας των εκλογών* (που εν προκειμένω είναι το Πρυτανικό Συμβούλιο) και χωρίς να είναι καν γνωστός ως φυσικό πρόσωπο.

Ως εκ τούτου, τίθεται το **ουσιώδες** ερώτημα, αν νομιμοποιείται το *Όργανο διενέργειας των εκλογών*, ή τα υπ' αυτού εξουσιοδοτημένα πρόσωπα για την υποβοήθηση της διαδικασίας (ΥΑ, άρθρο 2 παρ.2) να χρησιμοποιήσει για την εκλογική διαδικασία, τεχνικό ή άλλο μέσο, το οποίο εποπτεύεται και ελέγχεται από τρίτους και μάλιστα από το ίδιο το εποπτεύον υπουργείο.

Για το (ΙΙ):

1. Κάθε ΑΕΙ, καλείται δια του *Οργάνου διενέργειας των εκλογών* να υλοποιήσει την διαδικασία εκλογής των εσωτερικών μελών του συμβουλίου μέσω ηλεκτρονικής ψηφοφορίας. Κατά συνέπεια, και δεδομένου ότι είναι μια καινοφανής (για τα ελληνικά δεδομένα τουλάχιστον) εκλογική διαδικασία που απαιτεί/προϋποθέτει ειδικές τεχνικές και επιστημονικές γνώσεις, θα πρέπει **επισήμως και ενυπόγραφα** να δίνονται **εγγυήσεις** για την εφαρμοσιμότητά της και τον αδιάβλητο χαρακτήρα της.

Αντ' αυτού

(α) Το μόνο τέτοιο σημείο που υπάρχει αυτή τη στιγμή, είναι η διατύπωση στην παρ.1 του άρθρου 4 της ανωτέρω ΥΑ: «*... Η εκλογική διαδικασία πραγματοποιείται μέσω ειδικού πληροφοριακού συστήματος (σύστημα "ΖΕΥΣ") του Υ.ΠΑΙ.Θ.Π.Α., η πρόσβαση στο οποίο πραγματοποιείται από την ηλεκτρονική διεύθυνση zeus.minedu.gov.gr Το σύστημα "ΖΕΥΣ" υποστηρίζεται από το ...ΕΔΕΤ και βασίζεται σε **διεθνώς αναγνωρισμένα** τεχνολογικά πρότυπα για την διεξαγωγή ηλεκτρονικών ψηφοφοριών, **που διασφαλίζουν** το αδιάβλητο και απόρρητο της εκλογικής διαδικασίας*» (η έμφαση δική μου).

Στο σημείο αυτό θα έπρεπε, είτε στην ΥΑ, είτε - έστω - σε **ενυπόγραφη εγκύκλιο** από την **πολιτική ηγεσία** του Υ.ΠΑΙ.Θ.Π.Α. να αναφέρονται ρητά τα «*διεθνώς αναγνωρισμένα πρότυπα*».

(β) Το Πρυτανικό Συμβούλιο το μόνο που γνωρίζει είναι τα αναφερόμενα στην ανωτέρω ιστοσελίδα του Υ.ΠΑΙ.Θ.Π.Α., η οποία είναι **ανυπόγραφη** (φέρει απλώς τον λογότυπο του υπουργείου), χωρίς αναφορά υπεύθυνης υπηρεσίας και ονόματα υπευθύνων.

2. Από την ανωτέρω ιστοσελίδα σταχυολογώ ερωτηματικά και ζητήματα - κατά την γνώμη μου ουσιώδη - που αν δεν απαντηθούν, η όλη διαδικασία πάσχει σοβαρά (σε παράρτημα του παρόντος εμφανίζονται πιο εξειδικευμένα σχόλια και αντιρρήσεις, καθώς και εξειδικευμένη σχετική βιβλιογραφία).

(α) Από τα "Γενικά": " *Η επικοινωνία των αρχών και των ψηφοφόρων με το πληροφοριακό σύστημα «Ζευς» γίνεται μέσω ενός απλού προγράμματος περιήγησης του Παγκόσμιου Ιστού (web browser), ενώ **προστατεύεται όπως ακριβώς και οι οικονομικές συναλλαγές** μέσω Διαδικτύου*". **Ποιος** ως πρόσωπο, **εγγυάται** αυτό το επίπεδο ασφάλειας και **γιατί** αυτό είναι **επαρκές** και μάλιστα για μια διαδικασία **εντελώς άλλου χαρακτήρα**, όπως είναι η εκλογική διαδικασία;

- Παρά ταύτα, "*Το απόρρητο της ψήφου είναι **ευθύνη της εφορευτικής επιτροπής**, και είναι **πρακτικά** εξασφαλισμένο καθώς αρκεί να υπάρχει ένα και μόνο τίμιο μέλος στην επιτροπή*." Η εφορευτική επιτροπή έχει μεν την ευθύνη, χωρίς να της έχει παράσχει κάποιος τις εγγυήσεις, ενώ ταυτόχρονα δεν μπορεί να ελεγχθεί από κανένα στο σημείο αυτό (βλ. παρ.Ι.2 πιο πάνω).

- Παραμένει ασαφές το τί ακριβώς σημαίνει "*Το απόρρητο είναι...πρακτικά εξασφαλισμένο*". Στο κεφάλαιο Απαντήσεις για τους ψηφοφόρους, αναφέρεται ότι "*... το απόρρητο είναι **πρακτικά** εξασφαλισμένο, αφού αρκεί να μείνει ασφαλής ένας και μόνο Κωδικός από όλους*". Και αν αυτό δεν συμβεί; Στην συνήθη ψηφοφορία μπορεί να παρίστανται ακόμα και όλοι οι υποψήφιοι ή και οι αντιπρόσωποί τους. Εν προκειμένω δεν υπάρχει καμία τέτοια δυνατότητα (βλ. παρ.Ι.2 πιο πάνω).

(β) Από τα "Γενικά": "*Η ακεραιότητα της ψηφοφορίας είναι **μαθηματικά επαληθεύσιμη** από **τον καθένα** μέσω της χρήσης κρυπτογραφίας, και χωρίς καμία προσβολή του απόρρητου*": Ποιος είναι ο "*καθένας*" που έχει την τεχνογνωσία να επαληθεύσει την ακεραιότητα της ψηφοφορίας, μέσω κρυπτογραφίας;

(γ) Από την "Εφορευτική Επιτροπή": "*Τα μέλη της επιτροπής λαμβάνουν ειδικά κρυπτογραφικά κλειδιά, τους **Κωδικούς Ψηφοφορίας**. Οι κωδικοί αυτοί είναι όλοι απαραίτητοι για τη διεξαγωγή της ψηφοφορίας καθώς και για την αποκρυπτογράφηση των αποτελεσμάτων. **Εάν χαθεί έστω και ένας, η ψηφοφορία δεν θα μπορέσει να ολοκληρωθεί**, καθώς θα είναι αδύνατη η αποκρυπτογράφηση των ψηφοδελτίων. Κάθε **μέλος** της εφορευτικής επιτροπής είναι **υπεύθυνο** για τη διαφύλαξη του δικού του Κωδικού, ενώ το σύστημα **«Ζευς»** έχει και αυτό ένα **Κωδικό** για κάθε ψηφοφορία, **σαν** να ήταν **μέλος** της επιτροπής.*"

- Είναι προφανές ότι **οποιοδήποτε μέλος** της Εφορευτικής Επιτροπής μπορεί, για καθαρά προσωπικούς (και ενδεχομένως ιδιοτελείς) λόγους, να **ακυρώσει εντελώς** την ψηφοφορία! Τούτο είναι ανέφικτο στην συνήθη ψηφοφορία με φυσική παρουσία ενώπιον κάλπης.

- Το σύστημα "ΖΕΥΣ" συμμετέχει ως μέλος της Εφορευτικής Επιτροπής. Δεν εγγυάται κανένας ότι ο διαχειριστής του συστήματος δεν γνωρίζει και δεν θα χρησιμοποιήσει τον κωδικό αυτόν.

(δ) Από την "Μίξη των ψηφοδελτίων": " *Όπως και με την επιτροπή, **αρκεί και μόνο ένας τίμιος** συμμέτοχος στη μίξη για να εξασφαλιστεί το απόρρητο*". Τί είδους **εχέγγυα** μπορεί να δοθούν υπεύθυνα και ενυπόγραφα γι' αυτό;

(ε) Από τις Απαντήσεις για τους ψηφοφόρους: "*Κάθε ψηφοφόρος μπορεί να ψηφίσει όσες φορές θέλει μέχρι να λήξει η διαδικασία της ψηφοφορίας... Κάθε νέα ψήφος στην απόδειξη της καταχώρησής της αναφέρει σαφώς την ακύρωση της προηγούμενης ψήφου*". Αρκεί η απόδειξη αυτή, ή υπάρχει η πιθανότητα λάθους (καταχώρηση διπλής ψήφου, ενώ υπάρχει αποδεικτικό ακύρωσης της τελευταίας), Τί είδους **εχέγγυα** μπορεί να δοθούν υπεύθυνα και **ενυπόγραφα** γι' αυτό;

(στ) Από τις Απαντήσεις για τους ψηφοφόρους: Στο ερώτημα "*Μπορεί κάποιος να ψηφίσει αντί για μένα;*" δεν δίνεται απάντηση, πέραν του ότι "*... οφείλετε να ειδοποιήσετε αμέσως την εφορευτική επιτροπή για να διερευνήσει το θέμα και για να σας εξασφαλίσει το δικαίωμα ψήφου*".

(ζ) **Κυρίως όμως στην ίδια την ιστοσελίδα του συστήματος "*Helios*"** http://heliosvoting.org/frequently-asked-questions/ **στο οποίο βασίζεται το σύστημα "*ΖΕΥΣ*"** (όπως αναφέρεται στην ιστοσελίδα του *ΖΕΥΣ*, χωρίς όμως περαιτέρω διευκρινίσεις τι ακριβώς σημαίνει αυτό) υπάρχει **αυτούσια** η ακόλουθη ερωτο-απάντηση (η έμφαση δική μου):

Ερώτηση: *Should we start using Helios for public-office elections? Maybe US President 2012?*

Απάντηση: ***No, you should not.*** *Online elections are appropriate when one **does not expect a large attempt at defrauding or coercing** voters. For some elections, notably US Federal and State elections, the stakes are too high, and **we recommend against capturing votes over the Internet**. This has nothing to do with Helios itself: we just **don't trust that people's home computers are secure enough** to withstand significant attacks.*

*If you'd like to use **a truly verifiable voting system** for your **public-office election**, **we recommend an in-person election**. Helios could be adapted to the in-person, precinct voting setting, but **we have not done this work yet**, and we intend to focus on online elections first.*

Θα μπορούσαν να διατυπωθούν και άλλα ζητήματα που θέτουν σε αμφισβήτηση την διαδικασία της ηλεκτρονικής ψήφου. Στο παράρτημα που ακολουθεί παρατίθενται μερικά πιο εξειδικευμένα ζητήματα.

Κων/νος Τζανάκης

****

ΠΑΡΑΡΤΗΜΑ

Μερικά πρόσθετα σχόλια σχετικά με την διαδικασία της ηλεκτρονικής ψηφοφορίας

(i) Όλες οι κρυπτογραφήσεις χρησιμοποιούν ψηφιακά πιστοποιητικά της μορφής δημόσιου-ιδιωτικού κλειδιού. Ισχύει όμως ότι οι διαχειριστές της διαδικασίας έχουν πάντα στα χέρια τους όλα τα ιδιωτικά κλειδιά. Αυτά αρκούν για την αποκρυπτογράφηση των πάντων. Όλες οι ενέργειες που κάνει ένας υπολογιστής είναι εφαρμογή αντιστρέψιμων (1-1) απεικονίσεων. Ό,τι μπορεί να αντιστρέψει μόνος του ο υπολογιστής μπορεί να αντιστραφεί από τον καθένα που θα έχει όλα τα κλειδιά. Οι διαχειριστές έχουν το πρώτο λόγο και τον έλεγχο πάντα.

(ii) Στην ιστοσελίδα του συστήματος «ΖΕΥΣ», στο τέλος της παραγράφου με τίτλο «*Η Μίξη των Ψηφοδελτίων*», αναφέρεται ότι για την διασφάλιση του απορρήτου της ψηφοφορίας, αρκεί ένα "τίμιο" πρόσωπο στην εφορευτική, όπως και στην δια ζώσης ψηφοφορία. Αυτό δεν ευσταθεί, διότι η εφορευτική επιτροπή δεν ελέγχεται από κανένα, αφού οι υποψήφιοι, ή οι εκπρόσωποί τους δεν μπορεί να έχουν εικόνα της ψηφοφορίας, όπως στην συνήθη δια ζώσης ψηφοφορία.

(iii) Η ασφαλής σύνδεση γίνεται με το zeus.minedu.gov.gr μέσω κρυπτογράφησης δημόσιου-ιδιωτικού κλειδιού. Ο server γνωρίζει και τα δύο. Δηλαδή τα γνωρίζει ο διαχειριστής (ή οι διαχειριστές), ο οποίος τα αντέγραψε στον server του, από όποιον του τα παρέσχε. Το σύστημα του Υπουργείου, δηλαδή κάποιος υπολογιστής, θα καταγράψει ποιος ψηφοφόρος συνδέθηκε, από ποια ηλεκτρονική διεύθυνση συνδέθηκε, τί ώρα και τί ψήφισε και όλα αυτά θα κρυπτογραφηθούν με το κλειδί του server. Δηλαδή, θα αλλάξει η εμφάνιση των δεδομένων με κάποιο (έστω περίπλοκο) τρόπο, αλλά ό,τι και όσες διαδικασίες κι αν κάνει το σύστημα, θα πρέπει τελικά να μπορέσει να αποκρυπτογραφήσει τη ψήφο για να βγάλει αποτέλεσμα. Άρα η διαδικασία κρυπτογράφησης **εν τέλει θα αντιστραφεί**. Και τα κλειδιά για την αντιστροφή τα έχουν στα χέρια τους οι διαχειριστές του συστήματος, άρα το Υπουργείο. Ούτως ή άλλως, η κρυπτογραφία στο διαδίκτυο χρησιμοποιείται μόνο για να προστατεύσει την μεταδιδόμενη πληροφορία από ξένους ενδιάμεσους (hackers).

(iv) Σε κάποιο σημείο της ιστοσελίδας του συστήματος «ΖΕΥΣ» αναφέρεται η τυχαία διαδικασία μίξης. Αυτό μπορεί να μην είναι αντιστρέψιμο. Όμως αυτό απαιτεί ενδελεχή έλεγχο του πηγαίου κώδικα του προγράμματος. Αυτό είναι **εγγενής αδυναμία**: Η **μη διαβλητότητα** της διαδικασίας με **φυσική** παρουσία μπορεί **να ελεγχθεί** από **κάθε αδαή ψηφοφόρο**, όμως το **να ελεγχθεί** ότι όντως ο **πηγαίος κώδικας** κάνει αυτό που ισχυρίζονται ότι κάνει εκείνοι που προωθούν το σύστημα αυτό, απαιτεί **τεχνογνωσία που λίγοι διαθέτουν**. Δηλαδή, **δεν υπάρχει λόγος να εμπιστευτεί κανείς a priori τη διαδικασία αφού δεν μπορεί να την ελέγξει**, και αντ' αυτού καλείται να εμπιστευτεί τους προγραμματιστές. Και εδώ είναι το πρόβλημα: Ποιος μπορεί να εγγυηθεί, ή να ισχυριστεί ενυπόγραφα, ότι η ύπαρξη σφάλματος (bug) στο software που κυκλοφορεί είναι σπάνιο φαινόμενο;

Σχετική εξειδικευμένη βιβλιογραφία παρατίθεται πιο κάτω:

Για κείμενα κάπως πιο γενικά για τα εγγενή προβλήματα της ηλεκτρονικής ψήφου, ιδιαίτερα μέσω διαδικτύου:

1. Internet Voting in USA . B. Simons - D.W. Jones. Communications of the ACM. Oct. 2012. Vol 55, No 10, pp 68-77 (http://dl.acm.org/citation.cfm?id=2347736.2347754)
2. Electronic Voting - A challenge to democracy? . Jason Kitcat, E-voting Co-ordinator, Open Rights Group. January 2007. *Παρουσίαση των αδυναμιών και των προβλημάτων που αντιμετωπίζουν τα συστήματα ηλεκτρονικής ψηφοφορίας.* (http://www.openrightsgroup.org/uploads/org-evoting-briefing-pack-final.pdf)

Για το σύστημα Helios στο οποίο βασίζεται το σύστημα ΖΕΥΣ του Υπουργείου Παιδείας (το υπ' αριθμ.7 αφορά γενικότερα συστήματα e-voting συμπεριλαμβανομένου του Helios):

3. Exploiting the Client Vulnerabilities in Internet E-voting Systems : Hacking Helios 2.0 as an Example. Saghar Estehghari - Yvo Desmedt. AIST, Japan. August 9, 2010 http://static.usenix.org/event/evtwote10/tech/full_papers/Estehghari.pdf
4. The Bug That Made Me President a Browser- and Web-Security Case Study on Helios Voting . Mario Heiderich , Tilman Frosch , Marcus Niemietz , Jörg Schwenk. http://www.nds.rub.de/research/publications/SecurityCaseStudyHeliosVoting/

E-Voting and Identity : Lecture Notes in Computer Science Volume 7187, 2012, pp 89-103. http://link.springer.com/book/10.1007/978-3-642-32747-6/page/1

5. Replay attacks that violate ballot secrecy in Helios . Ben Smyth, Toshiba Corporation, Kawasaki, Japan. May 10, 2012 (http://eprint.iacr.org/2012/185.pdf)
6. Results on a real life case study: Helios 2.0 . Véronique Cortier and Steve Kremer. January 16, 2012. (http://www.lsv.ens-cachan.fr/Projects/anr-avote/RAPPORTS/deliv4-3.pdf)
7. Clash Attacks on the Verifiability of E-Voting Systems . Ralf Kusters, Tomasz Truderung and Andreas Vogt. University of Trier, Germany. March 2012. (http://eprint.iacr.org/2012/116.pdf)