
A collection of objects is arranged on a light-colored surface. On the left, a portion of a chessboard with a blue and brown checkered pattern is visible, featuring several chess pieces. Below the chessboard are several medals and ribbons, including a red ribbon with a circular emblem and a blue ribbon with a similar emblem. A pair of gold-rimmed glasses with thin temples is positioned diagonally across the center. In the bottom left corner, a circular compass with a white face and black markings is visible. The background is a plain, light-colored surface.

Electronic Voting: Securely and Reliably

Dimitris Gritzalis

October 2002

A collection of medals and a compass on a wooden surface. The medals include a red ribbon with a circular emblem, a blue ribbon with a circular emblem, and a silver star-shaped medal with a central emblem. A pair of glasses is also visible. A compass is in the bottom left corner.

8ο Συνέδριο Εφαρμογών Πληροφορικής (Infosystems 2002)
Θεσσαλονίκη, 3-5 Οκτώβρη 2002

Ηλεκτρονικές εκλογές: Με ασφάλεια και αξιοπιστία

Δημήτρης Γκρίτζαλης

Τμήμα Πληροφορικής
Οικονομικό Πανεπιστήμιο Αθηνών
&

e-Vote project

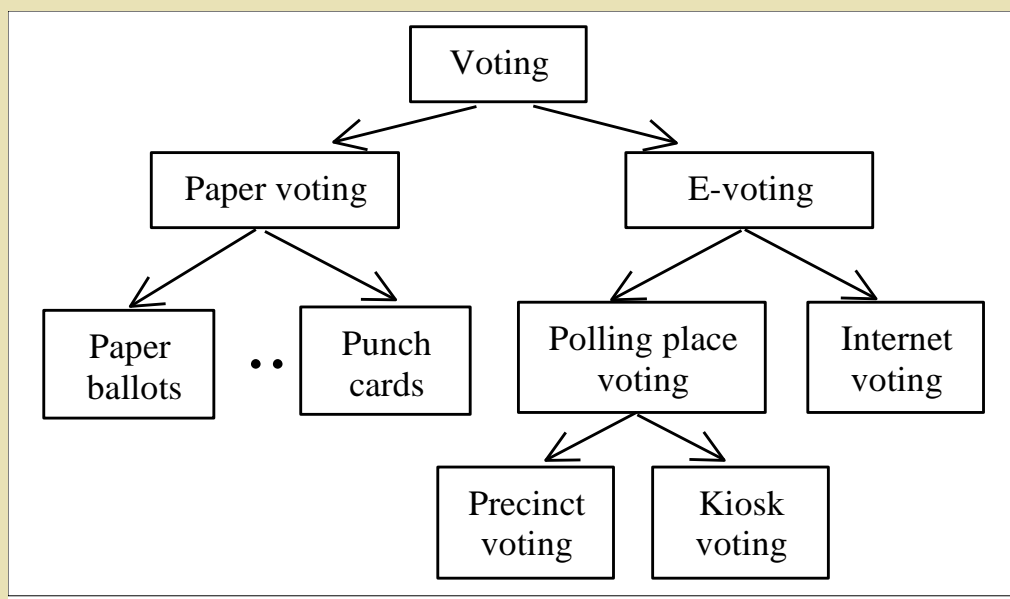
European Commission, IST Programme



Τι είναι οι ηλεκτρονικές εκλογές;

Ηλεκτρονικές εκλογές (e-voting) χαρακτηρίζονται αυτές κατά τις οποίες τα εκλογικά δεδομένα υφίστανται επεξεργασία, κυρίως στην ψηφιακή τους μορφή.

*Network Voting System Standards,
VoteHere Inc., Απρίλης 2002*



Σημ.: Οι ηλεκτρονικές εκλογές είναι ...133 χρόνων! (T. Edison, *Electrographic Vote Recorder*, US Patent, 1869).

Ποιό πρόβλημα μπορεί να αντιμετωπιστεί με τις ηλεκτρονικές εκλογές;*

- Μειούμενη συμμετοχή στην εκλογική διαδικασία

πχ. Εκλογές ΗΠΑ 2001:

Γενική συμμετοχή 59%

Συμμετοχή νέων (18-24 χρ.) 39%



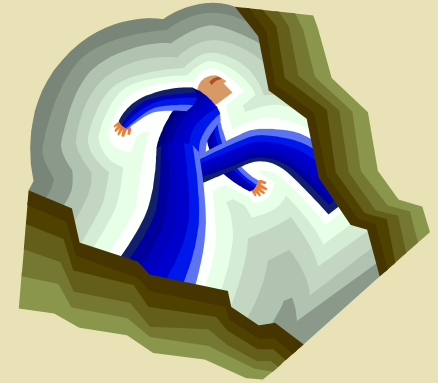
- Δυσκολία συμμετοχής σειράς πληθυσμιακών ομάδων, ειδικά σε πολυ-πολιτισμικό περιβάλλον.
πχ. ΑΜΕΑ, μετανάστες, υπέργηροι, ξενόγλωσσοι κλπ.



Ποιές νέες δυνατότητες μπορεί να προσφέρει;

- Υποστήριξη διαδικασιών (οικονομικά πρόσφορης και συχνής διεξαγωγής) άμεσης έκφρασης γνώμης, αξιολόγησης και αποτίμησης.
πχ. τοπικά δημοψηφίσματα,
σφυγμομετρήσεις κοινής γνώμης κλπ.
- Ανάπτυξη νέας αγοράς και ενδυνάμωση της απασχόλησης.
πχ. απαιτείται ειδικός εξοπλισμός και λογισμικό, ειδικοί επιστήμονες και τεχνικοί, αξιόπιστα δίκτυα κλπ.

Ενδογενή χάσματα...



Τεχνολογικό χάσμα:

Υπάρχει διαφορά μεταξύ προσδοκιών από τις ΤΠΕ και αποτελεσμάτων από την πρακτική εφαρμογή τους.

Κοινωνικό-τεχνολογικό χάσμα:

Υπάρχει διαφορά μεταξύ κοινωνικών πρακτικών (έθιμα, ήθη κλπ.) και ψηφιακών διεργασιών (διαδικασίες, μοντέλα κλπ.).

Ψηφιακό χάσμα:

Οι δυνατότητες κατανόησης και αξιοποίησης των ΤΠΕ, μεταξύ διαφορετικών κοινωνικών ομάδων, διαφέρουν.





- ✓ Πολλές κυβερνήσεις έχουν πεισθεί ότι ηλεκτρονικές εκλογές θα διεξάγονται συστηματικά στην επόμενη δεκαετία.
- ✓ Η ψηφοφορία μέσω Internet, κινητών τηλεφώνων, ψηφιακής TV κλπ. διευκολύνει πολλούς εκλογείς
- ✓ Πολλές χώρες είναι έτοιμες να διεξαγάγουν αμέσως πειραματικές ηλεκτρονικές εκλογές μικρής κλίμακας.
- ✓ Πολλές χώρες είναι έτοιμες να εκσυγχρονίσουν τον εκλογικό εξοπλισμό τους, αλλά υπάρχουν ελάχιστες τεχνολογικές εναλλακτικές λύσεις.
- ✓ Ορισμένες χώρες ενδιαφέρονται για ηλεκτρονικά εκλογικά συστήματα με οθόνες αφής.

...και μη αμελητέα εμπόδια



- ✓ Δεν υπάρχουν ενιαία διεθνή εκλογικά πρότυπα.
- ✓ Οι εκλογικοί νόμοι δεν αλλάζουν εύκολα.
- ✓ Η πιστοποίηση ενός εκλογικού συστήματος είναι δαπανηρή και χρονοβόρα.
- ✓ Απαιτείται υψηλή ασφάλεια και ειδικοί επιστήμονες.
- ✓ Δεν έχουν όλες οι κοινωνικές ομάδες ίσες δυνατότητες πρόσβασης στις ΤΠΕ.
- ✓ Οι δικαστικοί, δικηγόροι, δημόσιοι υπάλληλοι και άλλοι εμπλεκόμενοι δεν έχουν επαρκή εκπαίδευση.
- ✓ Υπάρχει πολιτική επικινδυνότητα στην εφαρμογή ηλεκτρονικών εκλογικών διαδικασιών.



Βασικές αρχές μιας δημοκρατικής εκλογικής διαδικασίας

- Μόνον οι εγγεγραμμένοι εκλογείς ψηφίζουν.
- Κάθε εκλογέας ψηφίζει το πολύ μια φορά.
- Η ψήφος είναι μυστική.
- Όλες οι έγκυρες ψήφοι προσμετρώνται.
- Οι εκλογείς εμπιστεύονται τη διαδικασία καταμέτρησης των ψήφων.

Internet Policy Institute,
Report of the National Workshop on Internet Voting,
USA, March 2001




Αρχές Σχεδίασης Ασφαλών Ηλεκτρονικών Εκλογικών Συστημάτων*

- Authentication:** Ψηφίζουν μόνον οι εγγεγραμμένοι εκλογείς.
- Uniqueness:** Κανένας δεν ψηφίζει πάνω από μια φορά.
- Accuracy:** Οι ψήφοι καταμετρώνται σωστά.
- Integrity:** Οι ψήφοι δεν μπορεί να αλλοιωθούν χωρίς αυτό να γίνει αντιληπτό.
- Verifiability:** Είναι δυνατή η επιβεβαίωση της ορθότητας της καταμέτρησης των ψήφων.
- Auditability:** Διατηρούνται ελέγξιμα και αξιόπιστα αρχεία των εκλογών.
- Reliability:** Η εκλογική διαδικασία είναι δυνατή ακόμη και σε δυσχερείς συνθήκες.

* Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, USA, March 2001.

Αρχές Σχεδίασης Ασφαλών Ηλεκτρονικών Εκλογικών Συστημάτων*

- 
- Secrecy:** Κανένας δεν μπορεί να εντοπίσει τι ψήφισε ένας ψηφοφόρος.
- Uncoercibility:** Οι ψηφοφόροι δεν μπορούν να αποδείξουν τι ψήφισαν.
- Flexibility:** Τα ψηφοδέλτια πρέπει να μπορούν να σχεδιαστούν με ευελιξία.
- Convenience:** Πρέπει να χρειάζονται ελάχιστες γνώσεις για να ψηφίσει ένας εκλογέας.
- Certifiability:** Τα ηλεκτρονικό εκλογικό σύστημα πρέπει να μπορεί να αξιολογηθεί.
- Transparency:** Οι εκλογείς πρέπει να μπορούν να κατανοήσουν πως λειτουργεί το σύστημα.
- Cost-effectiveness:** Το ηλεκτρονικό εκλογικό σύστημα πρέπει να είναι οικονομικά συμφέρον.

* Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, USA, March 2001.

Τεχνολογίες ασφαλών ηλεκτρονικών εκλογικών Πληροφοριακών Συστημάτων

Κρυπτογραφία

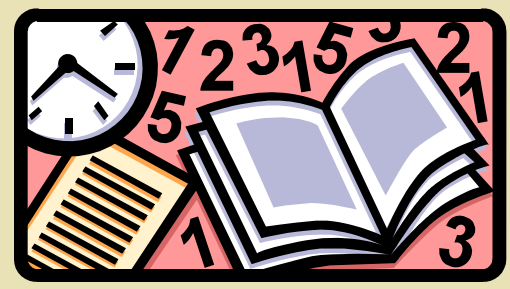
Ομομορφική Κρυπτογράφηση, Ψηφιακές Υπογραφές, Εμπιστες Τρίτες Οντότητες, Ψηφιακά Πιστοποιητικά

Αντι-ιομορφικό Λογισμικό

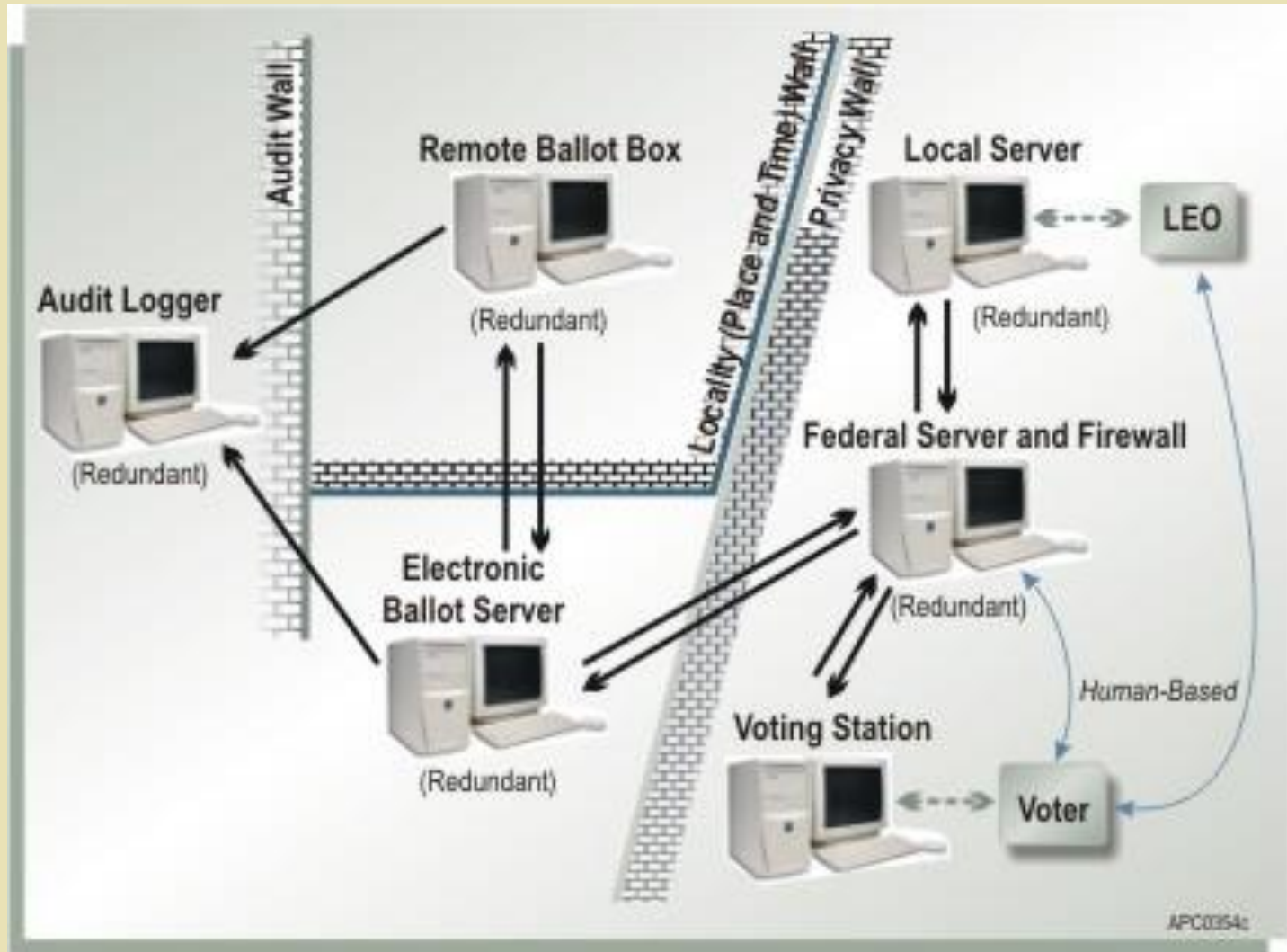
Firewalls

Βιομετρία

Εξυπνες κάρτες



Αρχιτεκτονική ενός ασφαλούς ηλεκτρονικού εκλογικού Πληροφοριακού Συστήματος*



* E. Gerck, "Private, secure, and auditable Internet voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.



Ηλεκτρονικές εκλογές: Τι είναι καλό να θυμάται κανείς*

- ◆ Η ηλεκτρονική ψηφοφορία διαφέρει από κάθε άλλη ηλεκτρονική διαδικασία.
- ◆ Υπάρχει διαφορά στην ψηφοφορία μέσω του Internet από το εκλογικό κέντρο ή από άλλο χώρο.
- ◆ Στις εκλογές απόαπόσταση, μέσω Internet, ενυπάρχουν κίνδυνοι απάτης.
- ◆ Η από απόσταση ψηφοφορία, μέσω του Internet, θέτει σε κίνδυνο τη μυστικότητα της ψήφου.
- ◆ Η ψηφοφορία μέσω Internet εγκυμονεί κινδύνους για την ιδιωτικότητα.
- ◆ Υπάρχει χάσμα μεταξύ πολιτικών πρακτικών και τεχνολογικών εφαρμογών.
- ◆ Υπάρχει τεχνολογικό χάσμα μεταξύ της γενιάς που έρχεται και των σημερινών γενιών.
- ◆ Η αλλαγή της τεχνολογίας δεν αρκεί, χρειάζεται εκπαίδευση.
- ◆ Η διαφάνεια στην εκλογική διαδικασία αυξάνει την εμπιστοσύνη των εκλογέων.
- ◆ Το εκλογικό λογισμικό πρέπει να είναι ανοικτό σε δημόσια κρίση.

* K. Alexander, "Ten things I want people to know about voting technology", *Democracy Online Project's National Task Force*, National Press Club, Washington D.C., USA, January 18, 2001.

Γενικά, οι απόψεις δίστανται...

*“The shining lure of this “hype-tech” voting schemes is only a **technological fool’s gold** that will create new problems far more intractable than those they claim to solve”*

Dr. Peter Neumann (Stanford), 2002

*“An Internet voting system would be the **first secure networked application** ever created in the history of computers”*

Dr. Bruce Schneier (Counterpane), 2002

*“At least a decade of **further research and development** on the security of home computers is required before Internet voting from home should be contemplated”*

Prof. Ron Rivest (MIT), 2001

Προς το παρόν...

**Μεταξύ υπεραισιοδοξίας-τεχνολαγνείας
και μηδενισμού-αναβλητικότητας,
ας προκρίνουμε
ρεαλισμό και νηφαλιότητα**



References

1. CALTECH-MIT Voting Technology project, *Voting: What is, what could be*, USA, 2001.
2. *E-Voting Security Study*, X/8833/4600/6/21, United Kingdom, 2002.
3. Gritzalis, D., *Secure Electronic Voting*, Springer, USA, 2003.
4. Gritzalis, D., “Principles and requirements for a secure e-voting system”, *Computers & Security*, vol. 21, no. 6, pp. 539-556, 2002.
5. Ikonomopoulos, S., Lambrinouidakis, C., Gritzalis, D., “Functional requirements of a secure electronic voting system”, in *Proc. of the 17th IFIP International Information Security Conference*, pp. 507-520, Kluwer, 2002.
6. Internet Policy Institute, *Report of the National Workshop on Internet Voting*, USA, 2001.
7. Lambrinouidakis, C., Gritzalis, D., Katsikas, S., “Building a reliable e-voting system: Functional requirements and legal constraints”, in *Proc. of the 13th International Workshop on Database and Expert Systems Applications*, pp. 435-446, 2002.
8. Mitrou, L., Gritzalis, D., Katsikas, S., “Revisiting legal and regulatory requirements for secure e-voting”, *Proc. of the 17th IFIP International Information Security Conference*, pp. 469-480, Kluwer Academic Publishers, 2002.
9. US Dept. of Defense, *Voting Over the Internet Pilot Project Assessment Report*, USA, 2001.
10. Pavlopoulos, S., Gritzalis, D., et al., “Vital signs monitoring from home with open systems”, in *Proc. of the 16th International Congress for Medical Informatics*, pp. 1141-1145, IOS Press, 2000.
11. Spinellis, D., Gritzalis, D., “PANOPTIS: Intrusion detection using process accounting records”, *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, 2002.
12. Spirakis, P., Katsikas, S., Gritzalis, D., Allegre, F., Darzentas, J., Gigante, C., Karagiannis, D., Kess, P., Putkonen, H., Spyrou, T., “SECURENET: A network-oriented intelligent intrusion prevention and detection system”, *Network Security*, Vol. 1, No. 1, 1994.