A collection of objects is arranged on a light-colored surface. On the left, there is a portion of a chessboard with a blue and brown checkered pattern and several chess pieces. Next to it are several medals and ribbons, including a red one with a circular emblem and a blue one with a similar emblem. A silver star-shaped medal is also visible. In the bottom left corner, there is a round compass with a white face and a black needle. A pair of gold-rimmed glasses with thin temples is positioned in the center, with one temple resting on the chessboard and the other on the surface. The background is a plain, light-colored surface.

# Secure and Reliable Electronic Voting

**Dimitris Gritzalis**

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 two silver star-shaped medals with circular centers. A pair of glasses and a compass are also visible.

# Secure and Reliable Electronic Voting

**Associate Professor Dimitris Gritzalis**

Dept. of Informatics

Athens University of Economics & Business

&

e-VOTE Project

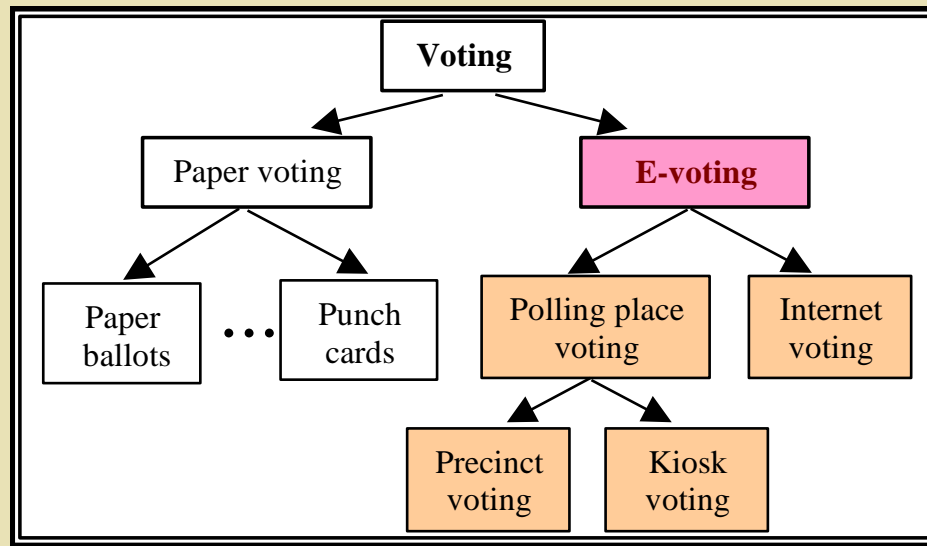
European Commission, IST Programme

**Advanced Networking Technologies  
and Applications 2003**

# What is an electronic voting (system)?

An *electronic voting (e-voting) system* is a voting system in which the election data is recorded, stored, and processed, primarily as digital information.

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



Note: Traditional electronic voting is ...134 years old (T. Edison, *Electrographic Vote Recorder*, U.S. Patent, 1869).



## What are e-voting systems good for?\*

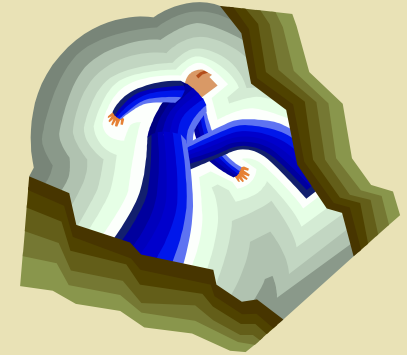
---

- They could lead to increased **voter turnout** (USA 2001: 59%, 18-24 yrs: 39%), thus supporting **democratic process**.
- They could give elections **new potential** (by providing ballots in multiple languages, accommodating lengthy ballots, facilitate early and absentee voting, etc.), thus enhancing **democratic process**.
- They could drastically cut down the **cost of election** process, thus **saving money for public administration**.
- They could open a **new market**, thus supporting the **commerce** and the **employment**.

\* D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA, January 2003.

## Some (*inherent*) gaps

---



### Technological gap:

Disparity between expectations from software/hardware and the performance being delivered (e.g. security flaws).

### Socio-technical gap:

Difference between social policies (e.g. laws, codes) and computer policies (e.g. procedures, functionalities).

### Social gap:

Difference between social policies and human behavior (e.g. equipment misuse).

# Opportunities for e-voting

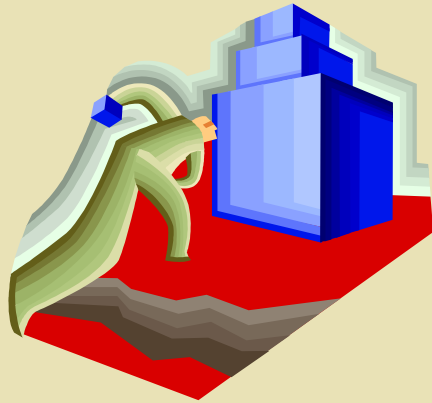
---



- ✓ Most countries believe that Internet voting will occur within 10 years.
- ✓ Internet voting options satisfy voter's desire for convenience.
- ✓ Internet voting can meet the voting needs of the physically disabled.
- ✓ Several countries are ready to try Internet voting for a small application immediately.
- ✓ Several countries are contemplating voting system replacement and are frustrated with the limited number of options available.
- ✓ Many countries are interested in touch screen systems.
- ✓ Many countries pursue the delivery of e-government services to their citizens.

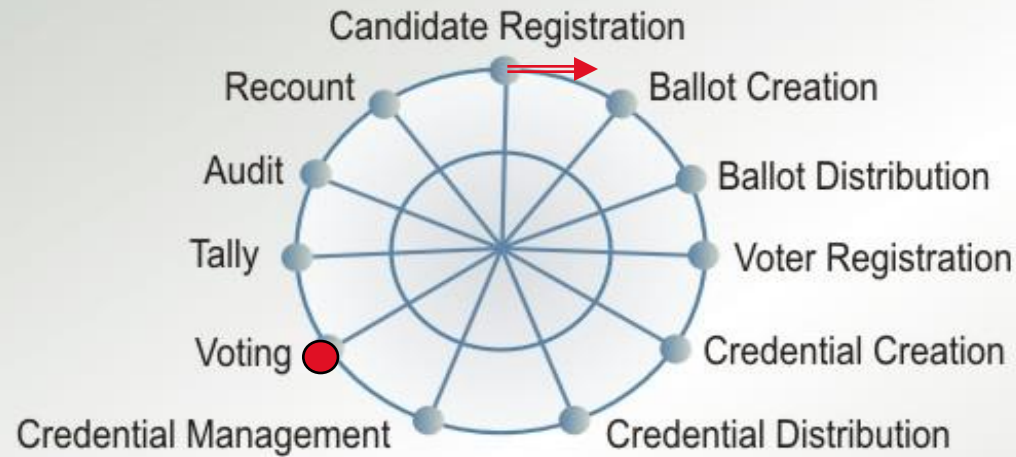
# Barriers to e-voting

---



- ✓ Lack of common voting system standards across nations.
- ✓ Time and difficulty of changing national election laws.
- ✓ Time and cost of certifying a voting system.
- ✓ Security and reliability of electronic voting.
- ✓ Equal access to Internet voting for all socioeconomic groups.
- ✓ Difficulty of training election judges on a new system.
- ✓ Political risk associated with trying a new voting system.
- ✓ Need for security and election experts.
- ✓ Lack of trust on new technology and reluctance in the adoption of new processes.

# Time-sequence of a typical voting process\*



- Time Synchronization: sequence and overlap
- Interdependencies: election phases are not independent
- Supervision: most tasks are not performed in isolation
- Cross-verification: prevents errors and fraud
- Redundancy: leads to fault-tolerance

An election is an *open-loop* process!

APC0354b

\* E. Gerck, "Private, secure, and auditable Internet voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2003.



# Generic voting principles

---

- Only eligible persons vote.
- No person can vote more than once.
- The vote is secret.
- Each (correctly cast) vote gets counted.
- The voters trust that their vote is counted.

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



# Identifying e-voting requirements

---

An e-voting system may be specified:

- *as a set of the guidelines to be adopted for ensuring conformance to the legislation*  
(“State Authority” point of view)

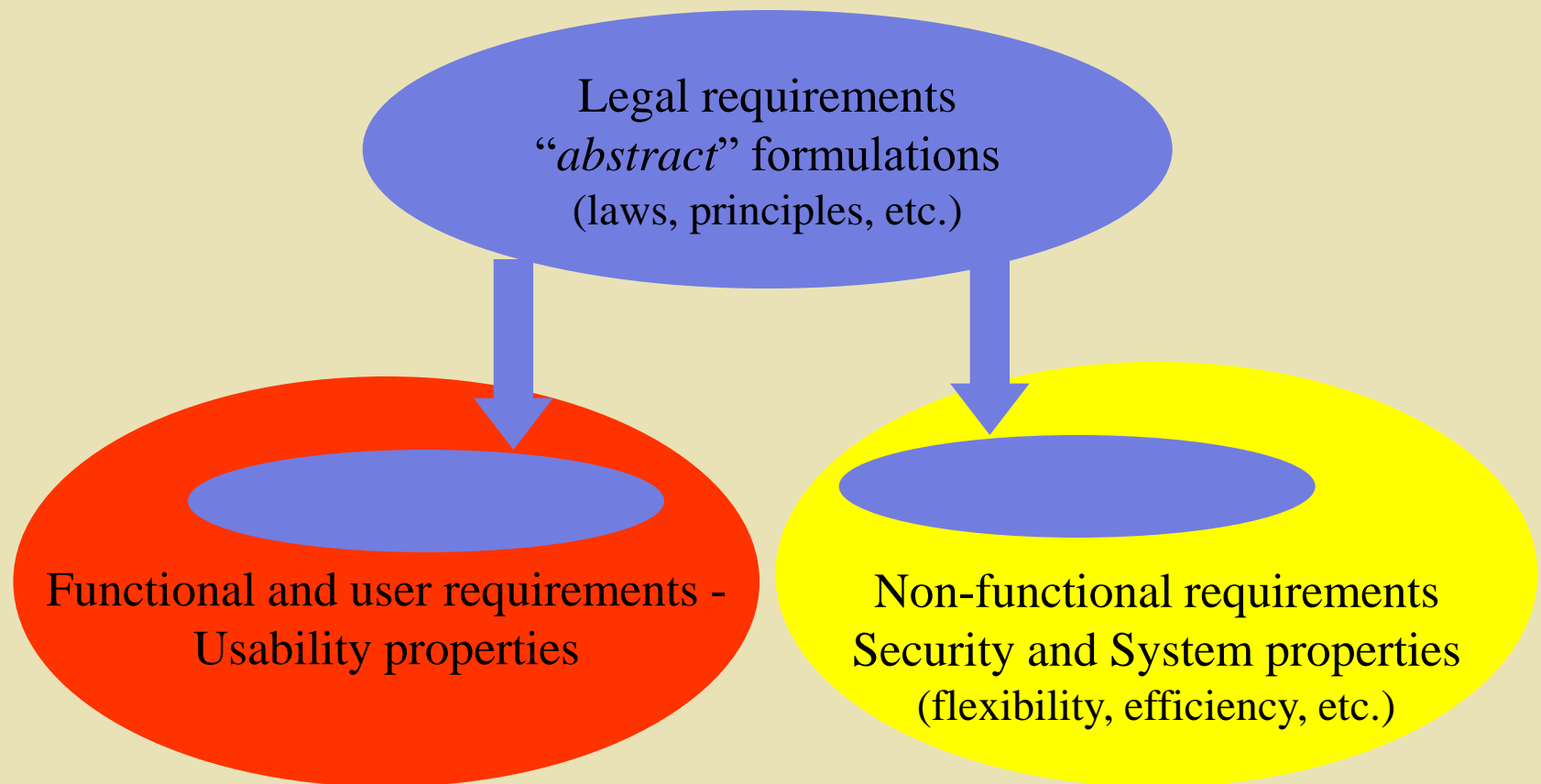
or

- *in terms of the problems associated with the provision of the adequate level of security*  
(*anonymity, authentication, tractability, etc.*)  
(“System Engineer” point of view)

# Identifying e-voting requirements

---

...none of these approaches is complete





# Identifying e-voting requirements

---

A new approach, proposed by the **e-VOTE** project:

- Requirements elicitation based on a *Generic Voting Model*, taking into account the:
  - ✓ European Union *legislation*
  - ✓ User *needs* and *expectations*
  - ✓ *Organisational* details of the conventional voting processes
  - ✓ *Opportunities* offered and *constraints* imposed by state-of-the-art technologies
- Aim of the developers is to express:
  - ✓ The *legal* requirements
  - ✓ The *security* (non-functional) requirements
  - ✓ The *functional* requirementsas a *User Requirements Specification* document that sets specific *Design Criteria*.



# Voting systems design criteria\*

---

- Authentication:** Only authorized voters should be able to vote.
- Uniqueness:** No voter should be able to vote more than once.
- Accuracy:** Voting systems should record the votes correctly.
- Integrity:** Votes should not be able to be modified without detection.
- Verifiability:** It should be possible to verify that votes are correctly counted for in the final tally.
- Auditability:** There should be reliable and demonstrably authentic election records.
- Reliability:** Systems should work robustly, even in the face of numerous failures.

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



# Voting systems design criteria\*

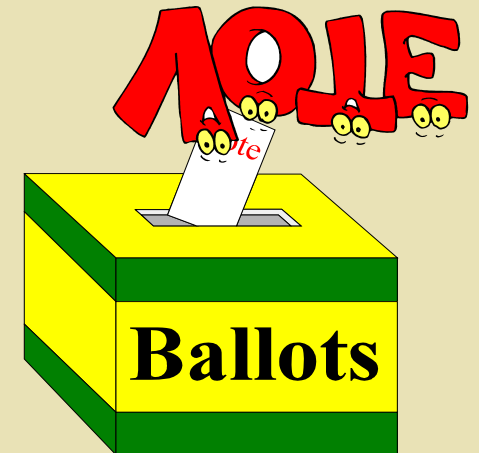
---

- Secrecy:** No one should be able to determine how any individual voted.
- Non-coercibility:** Voters should not be able to prove how they voted.
- Flexibility:** Equipment should allow for a variety of ballot question formats.
- Convenience:** Voters should be able to cast votes with minimal equipment and skills.
- Certiability:** Systems should be testable against certain criteria.
- Transparency:** Voters should be able to possess a general understanding of the whole process.
- Cost-effectiveness:** Systems should be affordable and efficient.

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

# Voting systems security requirements

Voting Protocols and Schemes	Security Requirements											System Wide Properties		
	Accuracy			Democracy								"Walk-away"	Voter mobility	Flexibility
	Inalterability	Completeness	Soundness	Eligibility	Unreusability	Privacy	Robustness	Verifiability	Uncoercibility	Fairness	Verifiable participation			
TRUSTED AUTHORITIES														
Karro	Yes	Yes	Yes	Yes	Yes	Cmp	No	Indi	No		Yes	Yes	Yes	Yes
ANONYMOUS VOTING														
Fujoka	Yes	Yes	No	Yes	Yes	Cmp	No	Opn	No	Yes	No	No	Yes	Yes
Baraani	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	No	Yes	Yes	Yes
HOMOMORPHIC ENCRYPTION														
Schoenmakers	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	Yes	Yes	Yes	No
Hirt	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Indi	Yes	Yes	Yes	Yes	No	No
Damgaard	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	Yes	Yes	Yes	No
Baudron	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	Yes	Yes	Yes	No

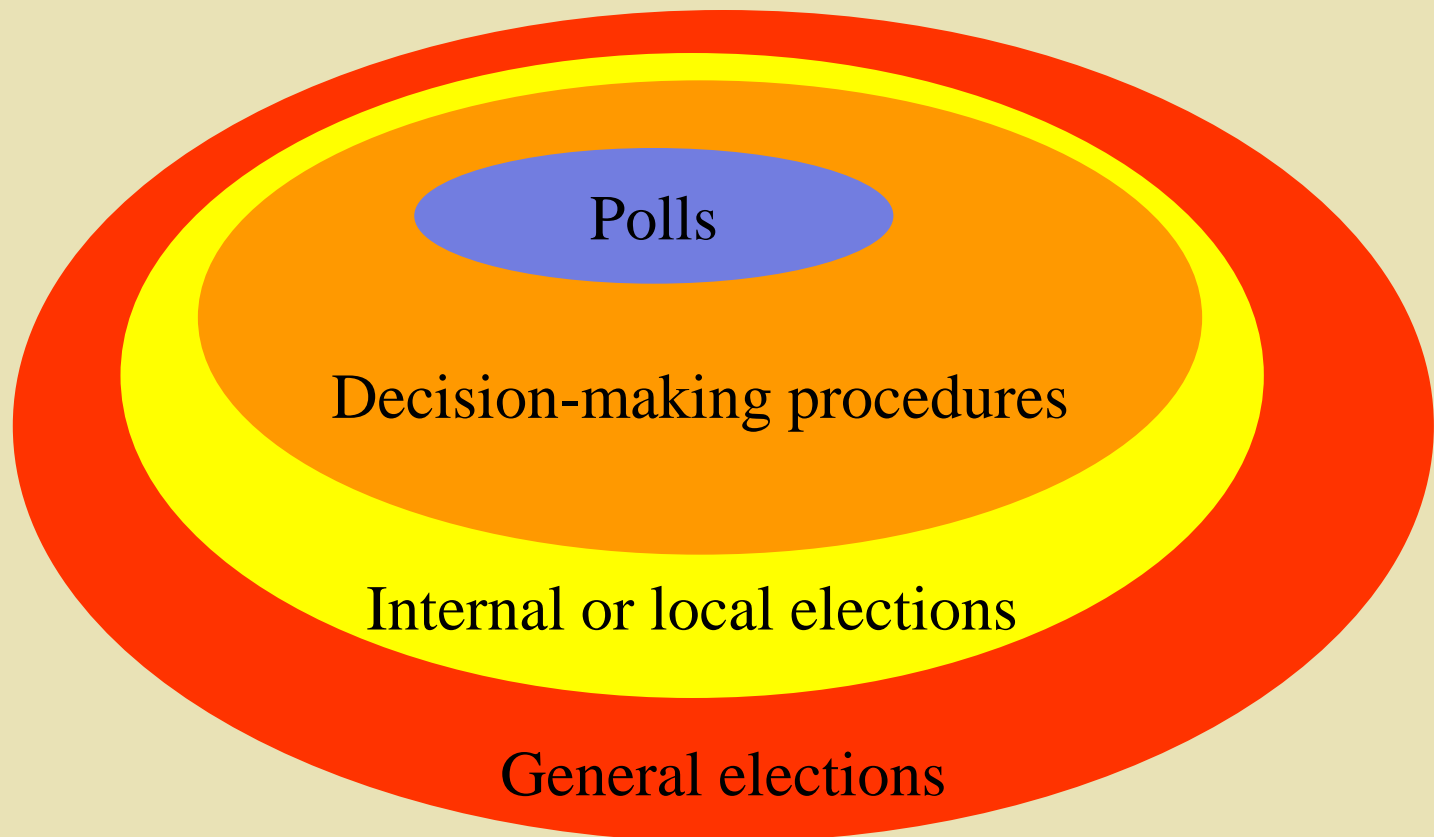


Privacy: Inf=Information-theoretical, Cmp=Computational  
 Verifiability: Indi=Individual, Opn=Individual with open objection, Uni=Universal

# Requirements for different types of election process

---

The General Election requirements are practically a superset of those regarding the other election processes



# (Secure) e-voting: (instead of) Conclusions

---

- ✓ Rapidly emerging issue...
  - ✓ Of a socio-technical nature...
  - ✓ Contradicting views...
  - ✓ Several questions remain open...
  - ✓ Context-dependent answers...
  - ✓ Security experts and skillful judges needed...
  - ✓ Further experimentation is needed...
- ... in the meantime, as complementary only!





# e-voting technology: Things to remember\*

---

- Voting is not like any other electronic transaction.
- Types of Internet voting: Polling-place Internet voting, and Remote-Internet voting.
- Remote Internet voting: a) is susceptible to voter fraud, b) may erode the right to cast a secret ballot and lead to political coercion in the workplace, and c) poses a threat to personal privacy.
- There is a (huge) politics and technology information gap.
- There is a generational technology gap.
- Changing technology is not enough; voter education is needed.
- Transparency in the voting process fosters voter confidence.
- Software used should be open to public inspection.

\* 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.

# e-voting: Real-life cases

---



## USA, Midterm elections (2002)

*Touch-screen Technology* (~510 counties, 10%)

*Optical Scanning* (~1200 counties, 27%)

*Punch Cards Machines* (32%)

*Computerized Voting capability* (e.g. Georgia)



**USA (Oct. 2002):**  
\$3.9 billion  
for “updating  
the nation’s election  
procedures”

## United Kingdom, Local elections (2002)

*Internet Voting capability* (Swindon 11%, Bristol 2.7%, Croydon 3.4%)

*Phone Voting capability* (Swindon 5%)

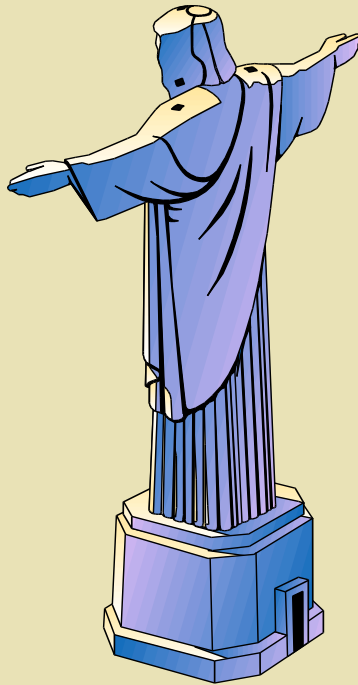
*Turnout increased* (Swindon 3.5%)



# e-voting: Real-life cases

---

## **Brazil, General elections (2002)**



*Full-scale national elections*

*115.000.000 registered voters*

*406.000 touch-screen machines*

*700 US\$ per machine*

*~300.000.000 US\$ for hardware and software alone*

*Voters were able to vote at any polling station, not just where they live*

“...the touch-screen systems are worse than punch cards... This is like trusting a calculator that somebody made in their garage... It’s not just about the integrity, it’s about the perception of the integrity and people’s willingness to participate” (D. Chaum, 2002).

# e-voting: Real-life cases

---

## Greece, Local Authority's Poll (2003)

*Local Authority: City of Amaroussion*

*Pilot application funded by IST/e-VOTE  
([www.instore.gr/evote](http://www.instore.gr/evote))*



*Poll referred to local issues (Olympic Games 2004 and the City of Amaroussion)*

*1092 citizens participated (voted)*

*Voting capability lasted 5 days (31.3-4.4.2003)*

*Government encouragement received*

*Consortium: Q&R (GR), Univ. of the Aegean, Cryptomathic (DK), Univ. of Essen (D), City of Amaroussion*



## The debate is still going on...

---

*“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”.*

P. Newmann (SRI) (2002)

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

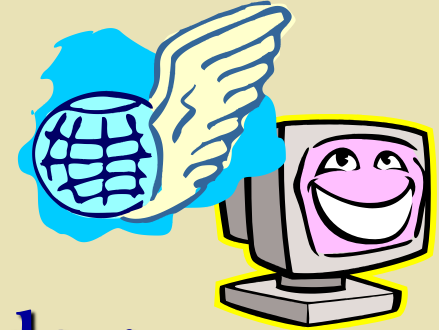
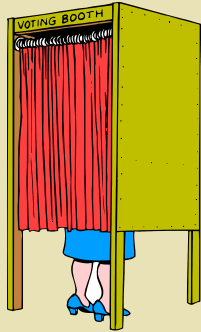
B. Schneier (Counterpane) (2002)

*“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”.*

Ron Rivest (MIT) (2001)

To cut the long story short...

---



**Electronic voting today:**

**Between the pessimism of bureaucracy  
and the optimism of technology,  
let's focus on the realism of democracy!**





## 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. Internet Policy Institute, *Report of the National Workshop on Internet Voting*, USA, 2001.
6. Lambrinouidakis, C., Gritzalis, D., Katsikas, S., “Building a reliable e-voting system: Functional requirements and legal constraints”, *Proc. of the 13<sup>th</sup> International Workshop on Database and Expert Systems Applications*, pp. 435-446, 2002.
7. Mitrou, L., Gritzalis, D., Katsikas, S., Quirchmayr, G., “Electronic voting: Constitutional and legal requirements, and their technical implications”, in *Secure Electronic Voting*, Gritzalis, D. (Ed.), pp. 43-60, Springer, 2003.
8. Mitrou, L., Gritzalis, D., Katsikas, S., “Revisiting legal and regulatory requirements for secure e-voting”, *Proc. of the 17<sup>th</sup> 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.