Potential and Limitations of a Secure Electronic Voting Capability

Dimitris Gritzalis

September 2003

7th Computer Security Incidents Response Teams Workshop
Syros, Greece, September 2003

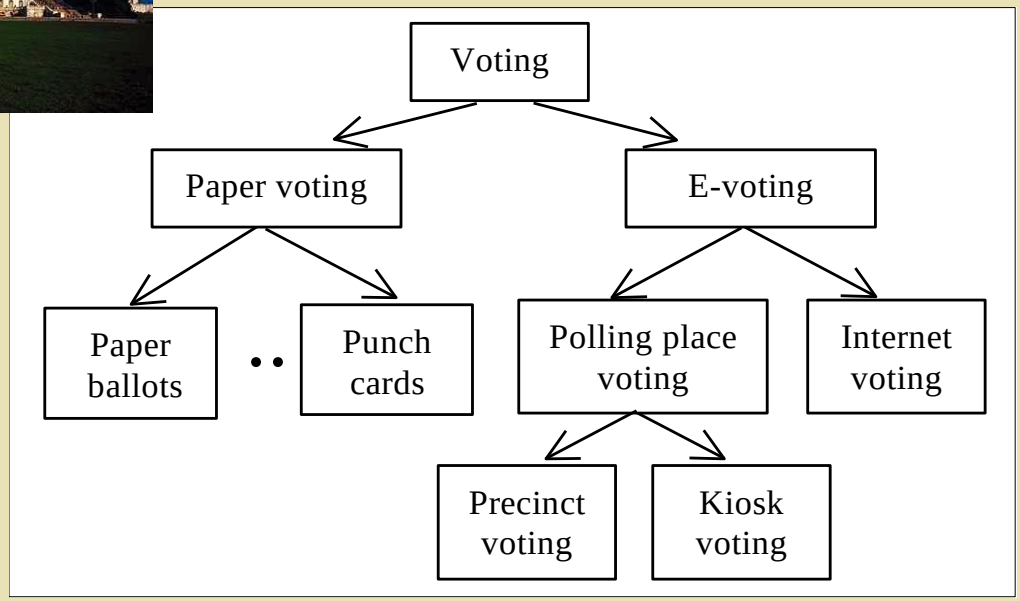
Potential and Limitations of the Secure Electronic Voting Capability

Dimitris Gritzalis
Dept. of Informatics
Athens University of Economics & Business
&
Data Protection Commission of Greece

What is 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 …132 years old! (T. Edison, *Electrographic Vote Recorder*, US Patent, 1869).

Do we need electronic voting systems*?

- 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 open a new market, thus supporting the commerce and the employment.

* D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.

Inherent gaps

Technological gap:

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

Socio-technical gap:

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

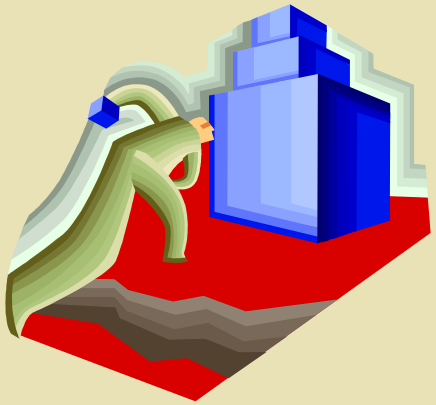
Social gap:

Difference between social policies and human behavior (equipment misuse, etc.).

Opportunities for electronic voting

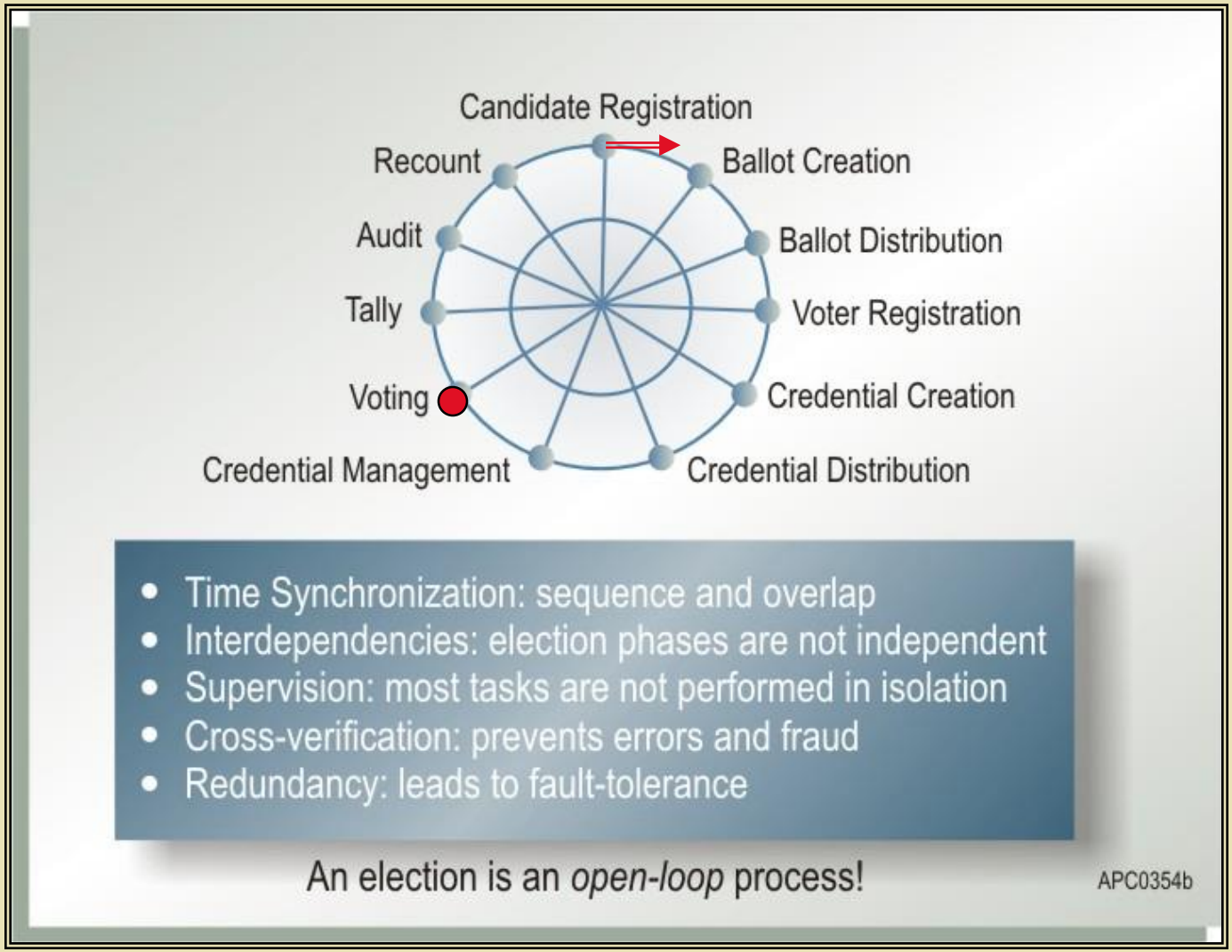
- ✓ Most countries believe that Internet voting will occur within the next decade.
- ✓ Internet voting options satisfy voter's desire for convenience.
- ✓ Internet voting can meet the voting needs of the physically disabled.
- ✓ Several countries are ready to try Internet voting for a small application 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.

Barriers to electronic 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.

Time-sequence of a typical voting process*



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

Generic voting principles

- Only eligible persons vote.
- No person gets to 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

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: 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.

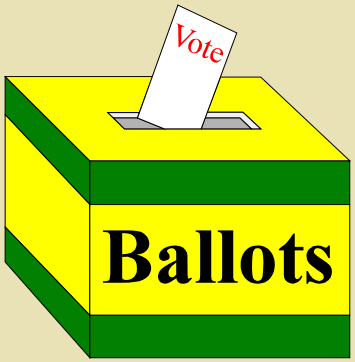
Voting systems design criteria*

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.
Certifiability:	Systems should be testable against essential 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										
	Inalterability	Completeness	Soundness	Eligibility	Unreusability	Privacy	Robustness	Verifiability	Uncoercibility	Fairness	Verifiable participation	"Walk-away"	Voter mobility	Flexibility
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														
Schoen-makers	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

Security voting systems technologies

Cryptography

Homomorphic encryption, digital signatures, blind signatures, Trusted Third Parties, digital certificates, etc.)

Antiviral software

Firewalls

Biometrics

Smart cards

A simple electronic voting model*: Generic description

1. the voter constructs an "anonymous electronic ballot";
2. the voter shows adequate proof of identity to the election authority;
3. the authority "stamps" the ballot after verifying that no other ballot has been stamped for this voter;
4. the voter anonymously inserts the ballot into an electronic mail box.

Note: After the voting deadline passes, votes are counted and a database containing all ballots are made public. Anybody can verify that his/her vote is contained in the database.

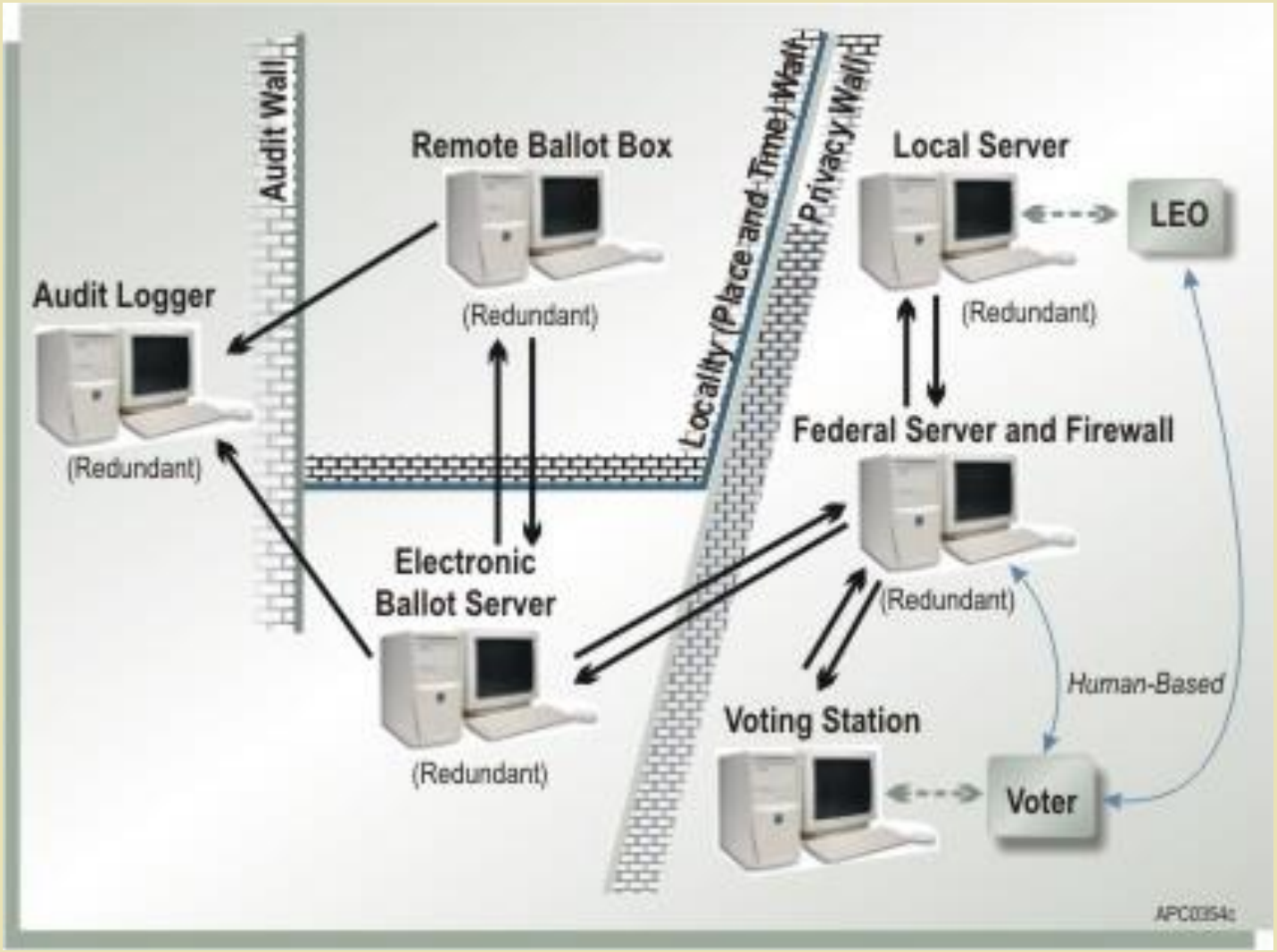
* R. Peralta, "Issues, non-issues, and cryptographic tools for Internet-based voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.

A simple electronic voting model: The ballot design

ELECTION IDENTIFICATION	VOTER'S NONCE
VOTE	SIGNATURE OF ELECTION AUTHORITY

- The Election Identification is a "long number", which identifies the specific election.
- The Voter's Nonce is a "long number", which is kept secret and is different for each voter.
- The Vote Field is a "short number", which denotes the confidential voter's selection(s).
- The Signature of Election Authority is a cryptographic signature of the other three fields.

DVS: An e-voting system architecture*



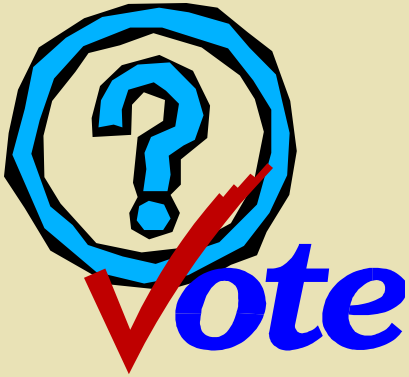
* E. Gerck, "Private, secure, and auditable Internet voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.

DVS: Functionalities implementation table

Modules	*Layer*	*Sub-Modules*	*Functions*
CPF (Central Processor & Firewall)	Central (Federal)	Probe DVC Verifier Reverse Proxy Receipt Interface Log	Probe and Protect Client Verify and Decrypt DVCs Provide Pass-Through Service Provide Notice of Receipt Interface with Client and other Modules Postmark and Register Events
LS (Local Server)	Local (County)	DVC Issuer Receipt Interface Log	Issue and Encrypt DVCs; Register Voters Provide Notice of Receipt Interface with Client and other Modules Postmark and Register Events
EBS (Electronic Ballot Server)	Group (State)	DVC Verifier Ballot Server Receipt Interface Log	Verify and Decrypt DVCs Provide Ballot Views Protect Server and Client Provide Notice of Receipt Interface with Client and other Modules Postmark and Register Events
RBB (Remote Ballot Box)	Group Local	DVC Verifier Ballot Box Receipt Tally Audit Report Interface Log	Verify and Decrypt DVCs Receive Return Ballots Distribute Return Ballots Provide Notice of Receipt; Verify Voter Receipt Calculate Tally Audit Inputs & Outputs Report Results Interface with other Modules Postmark and Register Events
AL (Audit Logger)	Central, Group, Local	DVC Verifier Interface Log	Verify and Decrypt DVCs Interface with other Modules Postmark and Register Events

(Secure) Electronic voting: (instead of) Conclusions

- Rapidly emerging issue...
- Of a socio-technical nature...
- There are contradicting views...
- Several questions remain open...
- Context-dependent answers…
- Security experts and skillful judges needed...
- Need for further experimentation…
- In the meantime, complementary only...



Electronic voting technology: Things to remember*

- Voting is not like any other electronic transaction.
- There are two kinds of Internet voting: Polling place Internet voting, and remote Internet voting.
- Remote Internet voting is highly susceptible to voter fraud
- Remote Internet voting may erode our right to cast a secret ballot and lead to political coercion in the workplace.
- Remote Internet voting 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.

There is a debate 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. Neumann (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*"

R. Rivest (MIT), 2001

Looking for a moto

Regarding electronic and Internet voting,

between optimism and pessimism

let's choose realism!

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. Gritzalis, D., Katsikas, S., "High level security policy guidelines", *Studies in Health Technology and Informatics*, pp. 164-188, December 1996.
6. Gritzalis, D., Kantzavelou, I., Katsikas, S., Patel, A., "A classification of health information systems security flaws", *Proc. of the 11th International Information Security Conference*, pp. 453-464, Chapman & Hall, 1995.
7. Internet Policy Institute, *Report of the National Workshop on Internet Voting*, USA, 2001.
8. Lambrinoudakis, C., Gritzalis, D., Katsikas, S., "Building a reliable e-voting system: Functional requirements and legal constraints", *Proc. of the 13th International Workshop on Database and Expert Systems Applications*, pp. 435-446, 2002.
9. 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.
10. 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.
11. US Dept. of Defense, *Voting Over the Internet Pilot Project Assessment Report*, USA, 2001.