Electronic voting in practice

Andreas Stamoulis, Nikolaos Tsalis

[1] *Dept. of Informatics, Hellenic Open University, Greece*

[2] *Information Security and Critical Infrastructure Protection Laboratory*

Dept. of Informatics, Athens University of Economics & Business, Greece

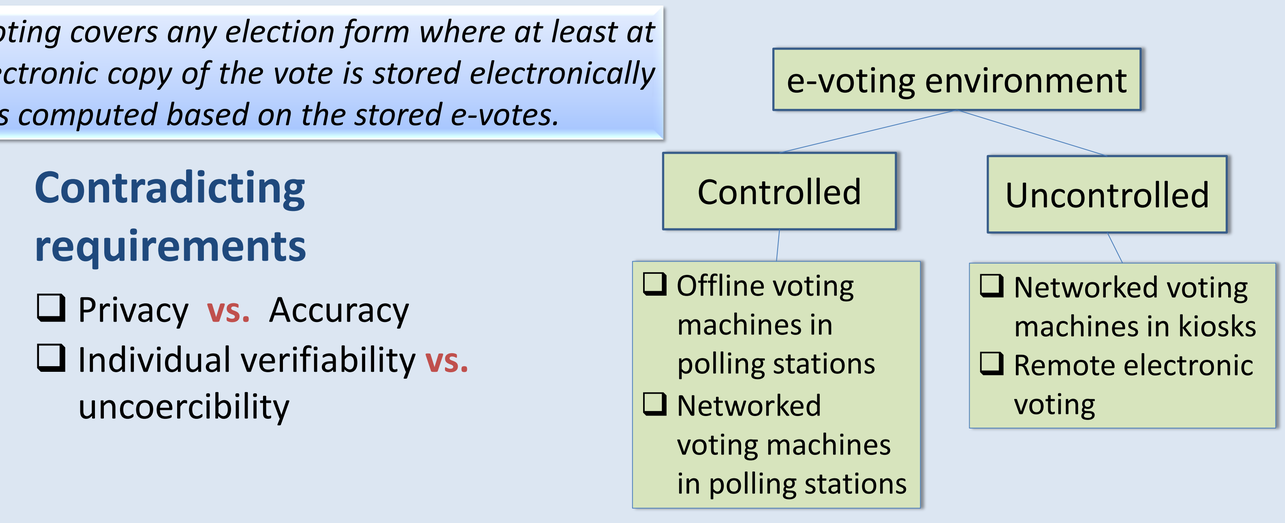
Definition: *Electronic voting covers any election form where at least at one point in time an electronic copy of the vote is stored electronically and the election result is computed based on the stored e-votes.*

Security requirements

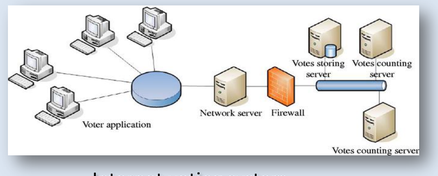
- ❑ Accuracy
- ❑ Democracy
- ❑ Privacy
- ❑ Robustness
- ❑ Verifiability
- ❑ Uncoercibility
- ❑ Fairness

Contradicting requirements

- ❑ Privacy **vs.** Accuracy
- ❑ Individual verifiability **vs.** uncoercibility



e-voting systems and voting machines



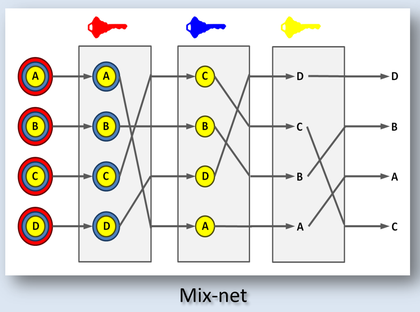
Internet voting system

Optical Scanner

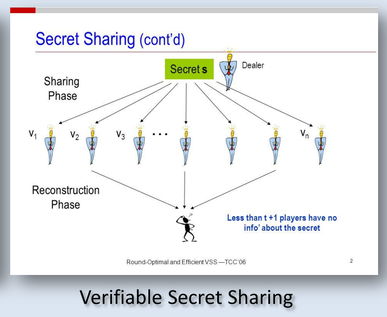
D.R.E. (Direct Recording Electronic) with voter -verified paper audit trail (VVPAT)

Ballot-marking Device

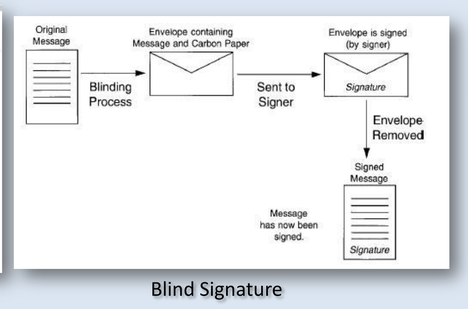
Cryptographic primitives



Mix-net



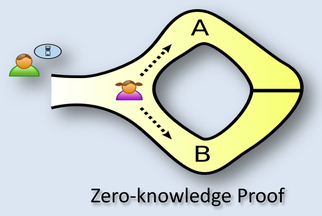
Verifiable Secret Sharing



Blind Signature

$$c_1 \otimes c_2 = E_r\left(m_1 \oplus m_2\right)$$

Homomorphic Encryption



Zero-knowledge Proof

Vulnerabilities, threats, attacks

Types of Attackers	Weaknesses
❑ Outsiders ❑ Voters ❑ Insiders: - Poll workers - Election officials - Vendor employees	❑ Data integrity ❑ Ineffective cryptography ❑ Access control ❑ Software engineering ❑ Viral propagation ❑ Distributed denial of service

Worldwide e-voting practices

Belgium

Population: 11.2 million

E-voting system: DRE

Usage: in large scale since 1994. 44% of total voters vote electronically as of 1999.

Norway

Population: 5.1 million

E-voting system: Internet voting pilots

Usage: 2011 and 2013 in selected municipalities.

Estonia

Population: 1.3 million

E-voting system: Internet voting

Usage: 2005-13. 22% of total voters voted electronically in the 2013 elections.

Japan

Population: 127.1 million

E-voting system: DRE pilots

Usage: 23 times in 10 selected municipalities between 2002-13.

U.S.A.

Population: 318.1 million

E-voting system: DRE, optical scanners, ballot marking devices.

Usage: Nationwide.

Massive introduction of e-voting equipment since the "HAVA" enactment in 2002.

India

Population: 1.25 billion

E-voting system: DRE

Usage: Nationwide since 2004.

Philippines

Population: 99.6 million

E-voting system: Optical scanners

Usage: Nationwide as of 2010.

Venezuela

Population: 29.3 million

E-voting system: DRE

Usage: Nationwide as of 1998.

Australia

Population: 23.5 million

E-voting system: DRE and Internet voting pilots

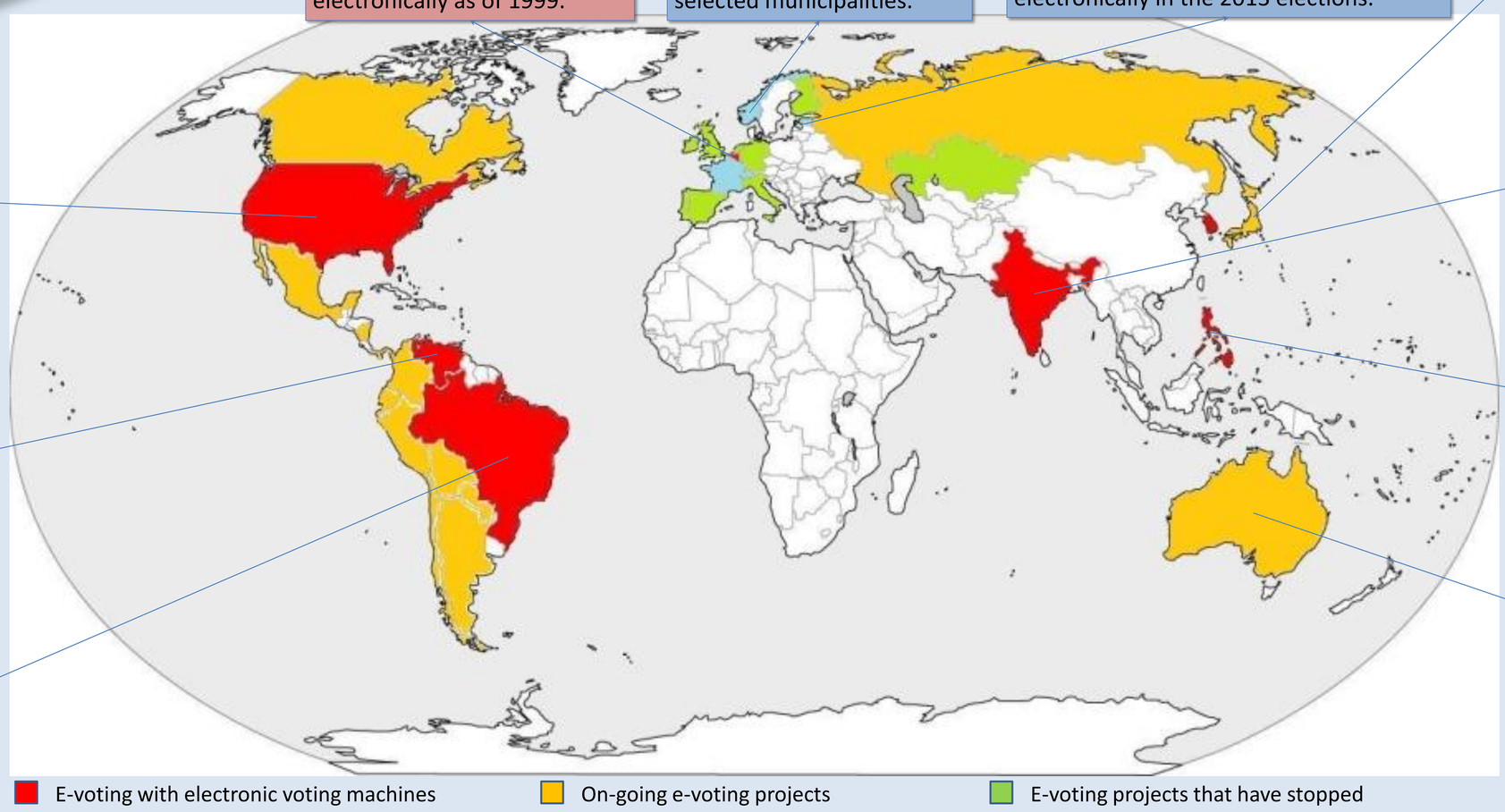
Usage: Selected municipalities between 2001-11.

Brazil

Population: 202.6 million

E-voting system: DRE

Usage: Nationwide as of 2000.



E-voting with electronic voting machines
On-going e-voting projects
E-voting projects that have stopped
Internet voting on-going projects
No e-voting

E-voting usage on developed and developing countries

No	Country	Literacy rate (%)	Internet penetration (%)	Use of e-voting
1	Germany	99	83.0	Has stopped e-voting
2	United Kingdom	99	83.6	Has stopped e-voting
3	Ireland	99	76.8	Has stopped e-voting
4	Spain	98	67.2	Has stopped e-voting
5	France	99	79.6	Internet voting for French citizens living abroad
6	Netherlands	99	92.9	Has stopped e-voting

No	Country	Literacy rate (%)	Internet penetration (%)	Use of e-voting
1	Brazil	90	45.6	National level
2	Venezuela	96	41.0	National level
3	India	62	11.4	National level
4	Philippines	93	32.4	National level

Verifiability status and cryptography evaluation

No	Country	Verifiability status	Evaluation of Cryptosystem (*)
1	United States	30% not verifiable ✗ 70% verifiable ✓	🔒🔒
2	Brazil	not verifiable ✗	🔒🔒
3	Estonia	not verifiable ✗	🔒🔒🔒
4	India	not verifiable ✗	⚠
5	Japan	not verifiable ✗	🔒🔒
6	Venezuela	verifiable ✓	🔒🔒🔒🔒
7	Norway	verifiable ✓	🔒🔒🔒
8	Belgium	verifiable ✓	🔒🔒🔒
9	Philippines	verifiable ✓	🔒🔒
10	Australia	verifiable ✓	🔒🔒

(*) Optimum evaluation for cryptography: 5 "locks"

Conclusions and recommendations

- ❑ The **security** of the existing e-voting systems is (at best) **questionable**.
- ❑ **Developed countries of Western Europe** are **skeptical** towards e-voting.
- ❑ **Developing countries of Latin America and Asia** tend to **introduce** e-voting.
- ❑ Remote e-voting on a **large scale** could be **dangerous**.
- ❑ Robust **cryptosystems** are difficult to develop and use.
- ❑ **Venezuela** appears to be the **most** promising **case**, while **India** as the **least** one.
- ❑ **DRE** should print a voter-verified paper audit trail (**VVPAT**).
- ❑ The **availability** of the **source code** of voting machines appears to be **very important**.

References

1. Balzarotti D., Banks G., Cova M., Felmetsger V., Kemmerer R., Robertson W., Valeur F., Vigna G., "An Experience in Testing the Security of Real-world Electronic Voting Systems", *IEEE Transactions on Software Engineering*, Vol. 36, Issue 4, pp. 453-473, 2010.
2. Barrat J., Goldsmith B., Turner J., *International Experience with E-Voting,* International Foundation for Electoral Systems, USA 2012.
3. Goldsmith B., Ruthrauff H., *Implementing and overseeing electronic voting and counting technologies*, National Democratic Institute for International Affairs, USA 2013.
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., "Embedding privacy in IT applications development", *Information Management and Computer Security,*, Vol. 12, no. 1, pp. 8-26, 2004.
6. Magkos E., Kotzanikolaou P., Douligeris C., "Towards Secure Online Elections – Models, Primitives and Open Issues", *International Journal of Electronic Government*, Vol. 4, No 3, p 249-298, 2007.
7. 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, USA 2002.
8. Mitrou L., Gritzalis D., Katsikas S., Quirchmayr G., "Electronic voting: Constitutional and legal requirements, and their technical implications", in *Secure Electronic Voting*, pp. 43-60, Kluwer, USA 2003.
9. Mercuri R., *Electronic Vote Tabulation Checks and Balances*, Ph.D. thesis, Univ. of Pennsylvania, USA 2000.
10. McDaniel P., Blaze M., Vigna G., *EVEREST: Evaluation and validation of election-related equipment, standards and testing*, Ohio Secretary of State's EVEREST Project Report, 2007.
11. Mylonas A., Dritsas S., Tsoumas V., Gritzalis D., "Smartphone Security Evaluation - The Malware Attack Case", in *Proc. of the 9th International Conference on Security and Cryptography*, pp. 25-36, SciTePress, Spain 2011.
12. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66, 2013.
13. Smith P., Mulder M., Goodman S., *Counting Votes 2012: A State by State Look at Voting Technology Preparedness*, The Verified Voting Foundation, USA 2012.
14. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA 2009