A secure electronic voting primer

Andreas Stamoulis, Nikolaos Tsalis

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

[2] *Information Security and Critical Infrastructure Protection Research Laboratory, Dept. of Informatics, Athens University of Economics & Business, Greece*

S/n	Constitutional requirements	E-voting systems Design Principles
1	General	1.1 Institutionally equivalent to traditional 1.2 Eligibility (registration and identification)
2	Free	2.1 Uncoercibility 2.2 No propaganda in the e-voting site 2.3 Non-valid voting capability
3	Equal	3.1 Equality of candidates 3.2 Equality of voters 3.3 One voter – one vote
4	Secret	4.1 Secrecy 4.2 Balance security vs. transparency
5	Direct	5.1 Not monitored ballot recording and counting
6	Democratic	6.1 Trust and transparency 6.2 Verifiability and accountability 6.3 Reliability and security 6.4 Simplicity

Figure 1: Constitutional requirements and design principles for e-voting systems

Security Requirements

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

Figure 2: Security requirements for e-voting systems

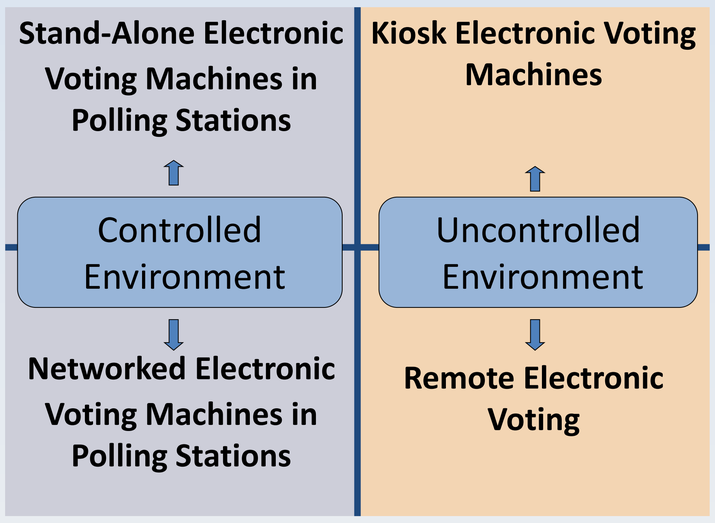
Contradicting Requirements

- **Privacy** (Unlinkability) vs **Verifiability** (Linkability)
- **Individual Verifiability** vs **Uncoercibility**

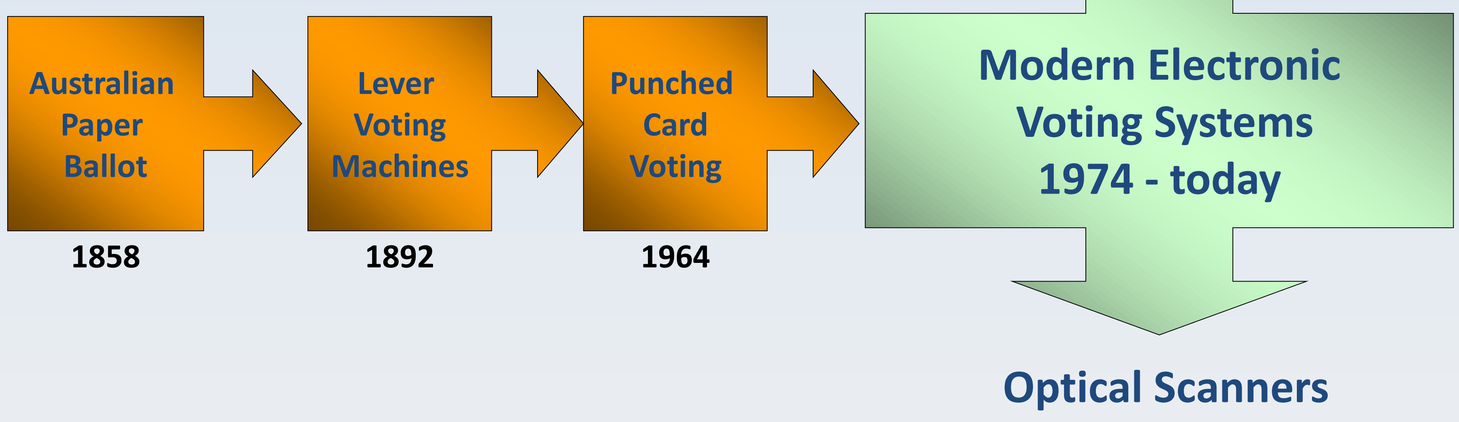
The 4 stages of elections

- Registration
- Validation
- Vote casting
- Vote tallying

Classification of Electronic Voting Systems



History of Voting Technologies



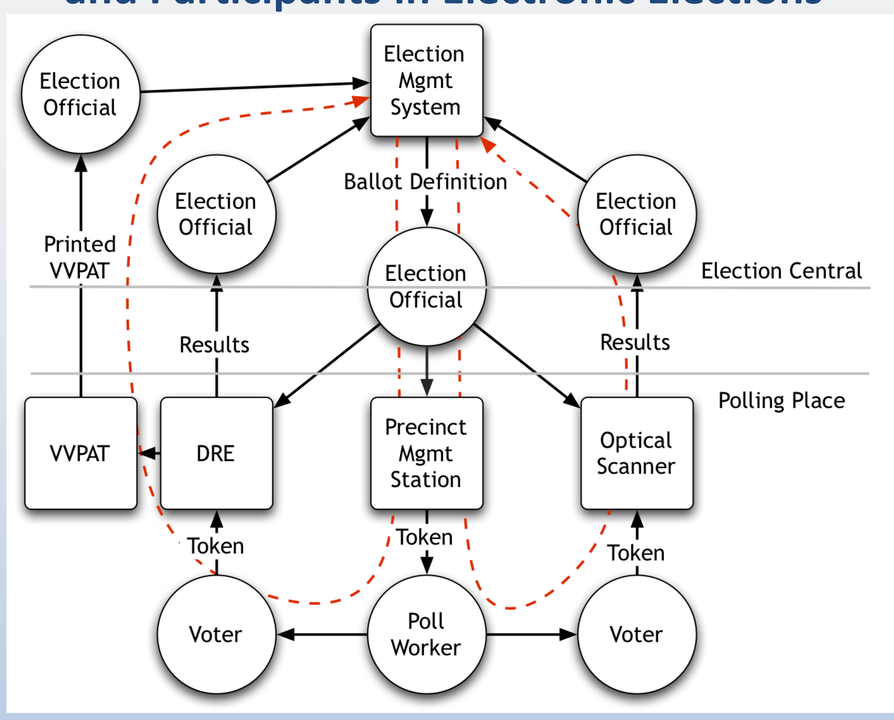
Cryptographic Models for e-voting

- Mix-nets
- Homomorphic Encryption
- Verifiable Secret Sharing
- Blind Signatures
- Zero Knowledge Proofs

Components of E-voting Systems

- **Election Management System** (central voting software)
- **DREs with Voter Verifiable Paper Audit Trails** (VVPAT)
- **Paper ballot optical scanners** (in the polling place)
- **High-speed paper ballot optical scanners** (at Election Central)
- **Removable media**
  - Smart cards
  - Memory packs
  - Result cartridges

Flow of Information Among the Components and Participants in Electronic Elections



Types of Attackers

- **Outsiders**
- **Voters**
- **Insiders**
  - Poll workers
  - Election Officials
  - Vendor employees

Security weaknesses found in real e-voting systems

- Ineffective mechanisms for assuring data integrity
- Misuse of cryptography
- Ineffective access control
- Dangerous development practices in software engineering

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, No 4, pp. 453-473, 2010.
2. Blaze, M., Cordero, A., Engle, S., Karlof, C., Sastry, N., Sherr, M., Stegers, T., Yee, K., *Source Code Review of the Sequoia Voting System*, Technical Report, California Secretary of State, 2007.
3. Burmester, M., Magkos, E., "Towards secure and practical e-elections in the new era", in *Secure Electronic Voting*, Gritzalis D. (Ed.), pp. 63-76, Springer, 2003.
4. Gritzalis, D., *Secure Electronic Voting*, Springer, 2003.
5. Gritzalis, D., "Principles and requirements for a secure e-voting system", *Computers & Security*, Vol. 21, No 6, pp. 539-556, 2002.
6. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An insider threat prediction model", *Proc. of the 7th International Conference on Trust, Pri-vacy, and Security in Digital Business*, pp. 26-37, Springer, 2010.
7. Kohno, T., Stubblefield, A., Rubin, AD., "Analysis of an Electronic Voting System", *Proc. of the 25th IEEE Symposium on Security and Privacy*, pp. 27-42, IEEE, 2004.
8. Lambrinoudakis, C., Gritzalis, D., Tsoumas, V., Karyda, M., Ikonomopoulos, S., "Secure electronic voting: The current landscape", in *Secure Electronic Voting*, Gritzalis D. (Ed.), pp. 101-122, Springer, 2003.
9. Magkos, E., Kotzanikolaou, P., Douligeris, C., "Towards secure online elections: Models, primitives and open issues", *International Journal of Electronic Government*, Vol. 4, No 3, pp. 249-298, 2007.
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, USA, 2007.
11. 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, 2002.
12. 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.
13. Ribarski, P., Antovski, L., "Mixnets: Implementation and performance evaluation of decryption and re-encryption types", *Proc. of the 34th International Conference on Information Technology Interfaces*, pp 43-498, IEEE, 2012.