E-Voting Systems

Ralf Küsters
Universitt Trier, Germany

Systems for electronic voting (e-voting systems), including systems for voting over the Internet and systems for voting in a voting booth, are employed in many countries. However, most of the systems used in practice today do not provide a sufficient level of security. For example, programming errors and malicious behavior easily go undetected. In fact, numerous problems with e-voting systems have been reported in various countries.

Therefore, in recent years modern e-voting systems have been designed that strive to achieve a rich set of fundamental but at the same time intricate and seemingly contradictory security requirements. For example, besides keeping the votes of individual voters private (privacy of votes), they try to allow voters to check that their votes were counted correctly, even if voting machines have programming errors or are outright malicious (verifiability/accountability). Some of these systems also try to prevent vote buying and voter coercion (coercion resistance).

In this course, we will cover central security requirements of e-voting systems, including those mentioned above, and how they can be formally defined and analyzed. While analysis is mostly done based on cryptographic models or even more abstract so-called Dolev-Yao models, we will also discuss approaches to perform (cryptographic) analysis directly on the implementation-/language-level of a system.

References

Available under: `http://infsec.uni-trier.de/publications.html`

[1] R.Küsters, T.Truderung, A.Vogt. *Accountabiliy: Definition and Relationship to Verifiability.* In: Procs. of the 17th ACM Conf. on Computer and Communications Security (CCS'10), pp. 526-535, ACM Press, 2010.

[2] R.Küsters, T.Truderung, A.Vogt. *Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study.* In: IEEE Symposium on Security and Privacy (S&P'11), pp. 538-553, IEEE Computer Society, 2011.

[3] R.Küsters, T.Truderung, A.Vogt. *Clash Attacks on the Verifiability of E-Voting Systems.* In: IEEE Symposium on Security and Privacy (S&P'12), pp. 395-409, IEEE Computer Society, 2012.

[4] R.Küsters, T.Truderung, A.Vogt. *A Game-Based Definition of Coercion-Resistance and its Applications.* Journal of Computer Security (special issue of selected CSF'10 papers), Vol. 20(6/2012), pp. 709-764, 2012.

[5] R.Küsters, T.Truderung, A.Vogt. *Proving Coercion-Resistance of Scantegrity II.* In: Procs. of the 12th International Conf. on Information and Communications Security (ICICS'10), LNCS 6476, pp. 281-295, Springer, 2010.

[6] R.Küsters, T.Truderung. *An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols.* In: 2009 IEEE Symposium on Security and Privacy (S&P'09), pp. 251-266, IEEE Computer Society, 2009.

[7] R.Küsters, T.Truderung, J. Graf. *A Framework for the Cryptographic Verification of Java-like Programs.* In: IEEE Computer Security Foundations Symposium, pp. 198-212, IEEE Computer Society, 2012.