PerAdaMagazine
towards pervasive adaptation
10.2417/2201008.003228

Verification of electronic voting systems

Mark Ryan

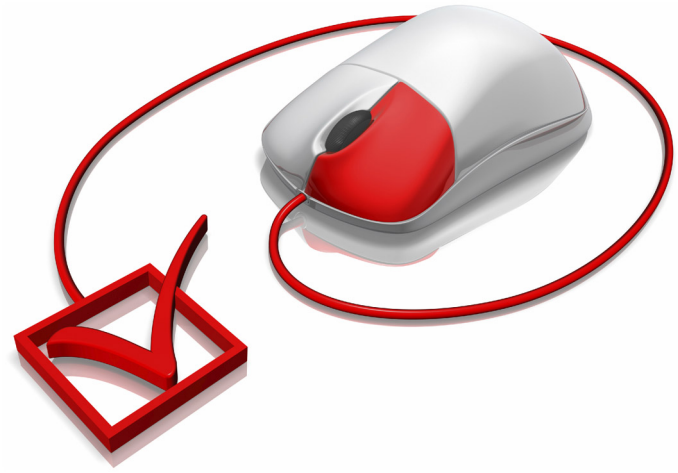
Designing a voting system that satisfies coercion resistance and election verifiability proves challenging to cryptography.

Electronic voting often requires puzzling security properties that appear to be in conflict with each other. On the one hand, we want to implement 'coercion resistance:' it should be impossible for a voter to prove to *anyone* that she voted in a particular way. This is a strong form of ballot secrecy, which implies that no one can discover how a particular person voted, even with his or her cooperation. This strengthening is important, because it protects the voter from bribery or coercion. If she can convince a potential coercer that she voted in a certain way, it becomes worthwhile for the villain to attempt coercion. To avoid that undesirable situation, we want to design a system that makes it impossible for the voter to convince anyone that she voted in a particular way, or even at all.

This is also sometimes called 'receipt freeness,' reflecting the fact that the voter does not get a form of receipt that would enable her to prove how she voted. Receipt freeness is a little weaker than coercion resistance, since the former allows the possibility that the voter proves how she voted through an arbitrary interaction (rather than a single receipt).

Note that the voter is supposed to be unable to prove how she voted *to anyone*, including, for example, the election officials, the candidates and her family members. These different potential coercers represent a range of challenges in our system design. The possibility that the election officials are coercers needs careful thought about the way votes are sent to the officials. The possibility that family members are coercers might require physical separation from other family members (for example, by entering a voting booth) at the time of voting.

On the other hand, another property that appears mandatory for a voting system is 'election verifiability:' voters should be able to check that their vote is correctly recorded. Observers (including voters) should be able to check that only eligible voters were able to record votes and that the sum of the recorded votes is reflected in the declared outcome. This ensures that the correctness of the outcome can be verified independently of the hardware and software (and other procedures) employed by the election authorities. Its importance arises from the fact that it appears much easier to manipulate the outcome with electronic than with paper-based systems. The integrity of the latter can be enforced by procedures such as sealing boxes and the presence of large numbers of observers at each stage of the election process. In the digital world, the equivalents of such procedures and possibilities of observation are harder to achieve. The best way to achieve them is to mandate election verifiability: the system should output enough data that anyone can verify that the computations it has performed are correct.



© *Dreamstime, Slavoijub Pantelic*

The potential conflict between these properties is clear. On the one hand, election verifiability requires that the system outputs evidence for the voter that her vote has been correctly counted. For this evidence to be convincing, it has to contain information that she voted in a certain way. As a minimum, the system has to know that fact. But that contradicts the requirement of coercion resistance, which implies that a coercer (including the system) should not be able to obtain any evidence that a given voter voted in a certain way.

This apparent contradiction can be resolved in a number of ways, many of which require subtle cryptography that allows

Continued on next page

one to construct evidence that would be convincing to some parties but not to others. Thus, the system can construct evidence to prove to a voter that her vote is included in the tally, but this evidence, while convincing to the voter, is not convincing to a coercer. For example, the evidence might be fakeable by the voter: if the voter sees such evidence, she knows that she did not create it, so she can know that it is valid. However, the coercer does not know whether or not the voter faked the evidence and so cannot accept it.

While these two properties can be reconciled by careful definition and clever cryptography, a third property appears just as important and very hard to achieve in the context of the other two, namely usability. A voting system should be easy to use. It should be easily understood by voters and require simple interaction. In particular, there are more specific requirements for voters with disabilities.

Governments that are experimenting with or implementing electronic voting systems (including the USA, the UK, the Netherlands, Brazil and Estonia) have been criticized for providing insufficient security. Unfortunately, their preferred security standard is one that is well suited for an e-commerce website, and it falls far short of the strong requirements of incoercibility and independent verifiability. The fact that government solutions fail even to meet 'standard' security requirements shows an immense gulf between what they have and what is needed.

Building voting systems that implement these subtle properties while maintaining usability has proved challenging. Substantial developments have been achieved in both theory and practice in the last 20 years. Several groups around the world are working on developing such systems, including a large project led by the Universities of Birmingham and Surrey (UK) in collaboration with the University of Luxembourg. The project's aim is to design a voting system that satisfies these and several other properties. This includes formal definitions of the properties (including coercion resistance and verifiability) and mathematical analysis of the extent to which they are satisfied,[1,2] as well as gauging usability through user focus groups and trials.

Author Information

Mark Ryan
University of Birmingham
Birmingham, UK

References

1. S. Delaune, S. Kremer, and M. D. Ryan, *Verifying privacy-type properties of electronic voting protocols*, **J. Comput. Secur. 17** (4), pp. 435–487, 2009.
2. S. Kremer, M. D. Ryan, and B. Smyth, *Election verifiability in electronic voting protocols.*, **Proc. 15th Eur. Symp. Res. Comput. Secur. (ESORICS'10): Lect. Notes Comput. Sci. 6345**, pp. 389–404, 2010.