Exploration of End-to-End Verifiable Voting Systems

Mikhail Skobov and Keyan Pishdadian

December 2020

Summary

We present a brief overview of the motivation for and goals of secure electronic voting systems and the most common current techniques used to tackle this problem. The focus of our work is the discussion of one particular solution to the electronic voting problem which leverages split-value-representations [**?**].

Introduction

Despite the rapid digitalization of life, most voting systems remain quaintly stuck using dated methods of paper recording and machine-assisted human tabulation. Though attempts have been made in the United States to transition to voting machines and electronic tablets (Direct-Recording Electronics [DRE]), these tools still ultimately rely on the same paper record and manual tallying procedures as a source of truth [**?**]. These systems do not allow members of the public to personally verify their vote was indeed counted and not manipulated, nor do they allow for a verification of the election outcome itself. As we have seen just this year, these deficiencies pose a serious risk towards maintaining public trust in elections and we will be so bold as to say this puts democracy itself at risk.

The goal of End-to-End Verifiable Voting (E2EVV) systems are to provide an alternative which achieves the following generally agreed upon requirements [**?**]:

1. individual voters can verify their vote but cannot prove what they voted for (to prevent coercion)
2. individual privacy is maintained
3. the election is accurate and votes cannot be altered
4. the outcome is verifiable by anyone

Though not often mentioned in the literature, an aspirational requirement is, or at least should be, that the election mechanism is also relatively understandable to the public. This element is crucial in being able to create public trust in any election proof or verification method.

We do not survey the field of E2EVV, but summarize that the existing systems are broadly categorized into three groups based on the core cryptographic component being used to faciliate them: mix-nets, homomorphic encryption, and blind signatures [**?**]. There have been production systems for E2EVV though they have not been broadly deployed and trusted to run real elections. The most well known systems found in our research were ElectionGuard [**?**][**?**], which uses homomorphic encryption, and Helios [**?**], which uses mix-nets. The former of these, ElectionGuard, has actually been used experimentally in at least one real small scale election (alongside traditional paper voting for verification) [**?**].

Voting using Split Value Representations

Implementation

Figure 1: Overview of architecture of the voting system.

Conclusion

References

[1] Michal Rabin and Ronald Rivest. 2014. Efficient End to End Verifiable Electronic Voting Employing Split Value Representations.

[2] https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

[3] Ronald Rivest. 2004. Lecture 17: Introduction to Electronic Voting, lecture notes, 6.837: Advanced Topics in Cryptography, Massachusetts Insitute of Technology, delivered April 8 2004.

[4] https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-democratic-elections-through-secure-verifiable-voting/

[5] https://github.com/microsoft/electionguard

[6] Ben Adida. 2008. Helios: web-based open-audit voting. In Proceedings of the 17th conference on Security symposium (SS'08). USENIX Association, USA, 335–348.

[7] https://www.newyorker.com/news/the-future-of-democracy/can-our-ballots-be-both-secret-and-secure