Journal of Information Security and Applications 000 (2017) 1–7

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Third-party verifiable voting systems: Addressing motivation and incentives in e-voting

Robbie Simpson*, Tim Storer

University of Glasgow, Glasgow G12 8QQ, United Kingdom

ARTICLE INFO

Article history:
Available online xxx

ABSTRACT

Voter-verifiable voting systems place significant demands of both effort and knowledge onto ordinary voters who have only limited incentives to participate. We suggest the use of third-party verifiable voting systems, harnessing the very strong incentives for candidates and observers to verify that votes are correctly counted. A generic modification enabling this via the use of pre-filled ballots and secure depositing is outlined and we demonstrate this modification by applying it to two major voter-verifiable voting systems. Additionally, potential vulnerabilities of this approach are discussed.

1. Introduction

Receipt-free, voter-verifiable voting systems are the current gold standard in electronic voting system research, with numerous authors having proposed a plethora of schemes, including Scantegrity [1,2]; ThreeBallot [3]; Scratch and vote [4,5]; Chaum's visual cryptography scheme [6]; Prêt à Voter [7,8]; Randell and Ryan's [9] scheme modelled on fruit machines [9]; Reynold's [10] scheme and voter verified secured paper audit trails [11].

A Receipt-free voter-verifiable (RFVV) scheme enables a voter to obtain assurances that the election has been operated fairly and that their vote has been counted, without the unfortunate side-effect of revealing the voter's choice to anyone else (and violating voting privacy, a requirement in many democratic jurisdictions). This property mitigates the perceived difficulty of verifying the machinery of an election directly (as is done in paper-based elections) due to the complexity and opacity of computer-based technology. As a consequence, elections can leverage the greater efficiency and accuracy of computer based elections, without compromising on the integrity or transparency of the result. An important characteristic of receipt-free voting is that voters themselves must not be able to prove how they voted; this prevents voters from being coerced or bribed.

In a typical RFVV scheme, a voter interacts with the voting system in a secure, isolated environment, such as a polling booth, to vote and also construct a *witness* for their vote. The witness is a document that provides the voter with some assurance that their vote has been counted correctly (that the voting system has committed to the value of their vote and cannot change it without detection). Most commonly this witness is constructed using cryptographic methods that allow some information about the vote to be recorded, without revealing the particular candidate or option voted for. As a result, the voter cannot use their witness to prove how they voted.

The voter must submit their vote to the voting system, just as in a paper based election. However, unlike the vote, the voter may remove the witness from the polling station and use it later to audit information published about the election by the voting system. If the witness shows that the voter's choice has not been correctly counted the voter may be able to have the result overturned or corrected. Crucially, the witness only provides sufficient information for the voter to confirm that their vote has been correctly counted: it does not provide sufficient information for a third party to reconstruct *how* the voter voted.

A necessary consequence of the use of a RFVV scheme for an election is that responsibility for assuring an election result is placed on the voters in the election. This is significant: the design of voting schemes is often treated as a purely technical or even theoretical problem, in which the various actors are treated as neutral agents or software processes. However, voting schemes are implemented as socio-technical voting systems, involving a range of organisations and actors all with their own expectations, incentives and capabilities. These factors can impose significant constraints on the design of a voting scheme.

By contrast, the design of all RFVV schemes makes several implicit assumptions about the majority of voters who participate in real elections:

* Corresponding author.
E-mail addresses: robbie.simpson@glasgow.ac.uk (R. Simpson), timothy.storer@glasgow.ac.uk (T. Storer).

https://doi.org/10.1016/j.jisa.2017.11.005
2214-2126/

- That voters understand the general purpose of the verification method and the information provided (and not provided) by the witness.
- That voters can perform the witness construction process correctly and determine if their witness is an accurate encoding of their vote.
- That voters are able to correctly operate the vote verification mechanism and can distinguish between a correctly and incorrectly counted vote.
- That voters are motivated to perform the verification of their vote using the witness.
- That voters are able and willing to invoke dispute resolution procedures if they believe their witness is incorrectly recorded.

The available research suggests that all of these assumptions may be unsafe. A study undertaken using the Prêt à Voter scheme identified several problems and showed that had difficulties understanding several of the key Prêt à Voter concepts and mechanisms [12]. Voters were unsure why they had to separate the two columns of the ballot paper and destroy the left hand column containing the ordering of candidates. One group in the study failed to destroy it at all, leading to a degraded mode of operation that threatened vote secrecy.

Once they had obtained their receipt many participants were disappointed by the unintuitive nature of it; some expected a document saying who they actually voted for, rather than the weaker guarantees required to maintain receipt-freeness. At the verification stage participants again expressed apathy - some participants opined that current elections run fine without the use of receipts and others felt that the comparison of receipts to bulletin-board values did not provide them with useful information. Storer et al. [13] identified similar limitations in a study of a scheme with significantly simpler verification mechanisms (that was not receipt-free). Additionally, studies of the usability of voter-verifiable voting systems (such as Winckler et al.'s [14] study of Prêt à Voter) suggest that voters considered such methods less usable than paper- or machine-based alternatives.

Voters' uptake of the post-election verification processes tends to be low, such as the 4% recorded during a real-world deployment of Scantegrity [15]. It is currently difficult to quantify what level of uptake is necessarily to obtain reasonable confidence in the accuracy of the result. Risk-limiting audits can provide high confidence with very small samples [16], but this relies on obtaining a random sample of ballots, while the self-selecting sample of verifying voters is likely to be demographically biased.

Separately, the verification elements of the system in the Prêt à Voter study also led the participants to doubt the security of the system. In broad terms they felt that a secure system would not need verification and so conversely the presence of verification must imply a risk of insecurity and consequently be untrustworthy. This perception was also detected during trials for public body elections in the Netherlands [17].

Consequently, this paper argues that existing RFVV schemes do not take adequate account of the socio-technical context in which voting takes place. Specifically, RFVV schemes assume capabilities and motivations on the behalf of voters that are not realistic in a real election context.

RFVV schemes generally ignore the other actors in a voting system and the role that they might play in assuring the correctness of a result. In established democracies, the voting system has evolved in theory and practice to support the role the candidates and other participants play, and practical verifiable voting systems should harness these resources as well.

Political candidates and parties play an important role in the running and auditing of elections. In the United Kingdom, the candidate's appointed counting agents act as scrutineers of election results, alongside election administrators and independent observers [18]. The parties' records from supporters and canvassing can also be used to 'sanity check' the results of the election. This arrangement reflects the very strong incentives for candidates to ensure the correct counting of votes, as this could make the difference between winning and loosing the election. While each individual candidate has no incentive to ensure that votes for other candidates are correctly counted (indeed, they have incentives to encourage the opposite) the candidates as an aggregation have strong incentives to ensure that all votes are correctly counted.

In many countries an important role is also played by Non-Governmental Organisations (NGOs) which aim to promote effective democracy and the fair running of elections. These can include international bodies and observers (e.g. the OCSE), domestic campaign groups (e.g. the Electoral Reform Society in the UK) and civic organisations (e.g. the League of Women Voters). These organisations are non-partisan, and often run campaigns to improve turnout and combat electoral fraud. In less mature democracies the reports of these organisations contribute significantly to the international recognition (or not) of the fairness of the result. It is therefore important that any implementation of RFVV systems provides similar opportunities for external observation and audit as currently used paper-based elections, which has been identified as a difficulty by the Council of Europe [19].

Consequently, this paper proposes that the limitations of voter verification can be mitigated by harnessing the motivation and resources of third-parties to ensure fair elections. The paper is structured as follows. Section 2 examines related work on third-parties in electronic voting and other secure systems. Section 3 outlines a generic adaptation to RFVV schemes that allows the act of election verification to be transferred from voters to third parties without violating voting privacy. Section 4 applies the adaptation to several existing RFVV schemes and analyses the modification for the introduction of vulnerabilities. Section 5 examines different configurations of the generic approach and discusses the viability of several attacks on the generic principle. Section 6 concludes with an overview of the paper and outlines the advantages of this approach.

2. Related work

Relatively little previous work has considered the role of third-parties in verifiable elections, but some important aspects have been discussed.

In their paper on Scratch & Vote Adida and Rivest [5] suggest a goal of cryptographic voting is to 'trust third parties as little as possible'. However, they also suggest the use of 'helper organisations' including political parties and campaign groups who would provide the equipment necessary for voters to perform their pre-voting validation, presumably via by their presence in the polling station. Similarly, Rivest and Smith [3] sketch out a modified version of their OneBallot system where voters receive the receipts of *previous* voters and suggest the involvement of external organisations to verify the receipts' digital signatures.

The most substantial work on third-party verification is by Neumann et al. [20], who propose the use of third-party websites and mobile apps to verify votes cast using the Helios [21] remote electronic voting system. In this adaptation, respected third-parties provide services by which voters can verify both whether their vote has been correctly constructed and whether it has been correctly stored. This is performed by communicating the voter's witness to a third-party, which then performs the necessary cryptographic checks. User studies using prototype websites suggest a high but not complete rate of success (~80%) in using these verification services. However, this differs from the scheme presented in this paper in a number of important ways:

Please cite this article as: R. Simpson, T. Storer, Third-party verifiable voting systems: Addressing motivation and incentives in e-voting, Journal of Information Security and Applications (2017), https://doi.org/10.1016/j.jisa.2017.11.005