Journal of Information Security and Applications 38 (2018) 124–131

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Bits or paper: Which should get to carry your vote?☆

Jan Willemson

[a] Cybernetica AS, Ülikooli, Tartu, 2, 51003, Estonia
[b] Software Technology and Applications Competence Center, Ülikooli, Tartu, 2, 51003 Estonia

ARTICLE INFO

Article history:
Available online 27 November 2017

Keywords:
Electronic voting
Paper voting
Risk evaluation

ABSTRACT

This paper reviews several dimensions in terms of which electronic/Internet and paper voting can be compared (vote secrecy, verifiability, ballot box integrity, transparency and trust base). We conclude that, for many vulnerabilities of Internet voting systems, there exist related weakness in paper systems as well. The main reason why paper-based elections are perceived as more secure is historical experience. We argue that recent criticisms of Internet voting have unfairly concentrated on the associated risks and neglected the benefits. Remote electronic voting lowers the cost of election participation and provides the most secure means for absentee voting. The latter is something that is urgently required in the contemporary, increasingly mobile world. Hence, we need to give Internet voting a chance, even if it means risking unknown threats and learning by trial and error.

1. Introduction

The idea of using electronic means to assist in elections is as old as human use of electricity itself. On June 1, 1869 Thomas A. Edison received U.S. Patent 90646 for an "electrographic vote-recorder" to be used in Congress elections. The system was never used, and the reason is very instructive – politicians felt that machine-assisted elections would speed up the voting process so much that they would lose their familiar way of verbal discussions about the political matters [1].

The history has shown that, contrary to the fears of the 19th century politicians, advances in technology have provided their modern colleagues with a much wider choice of discussion platforms including radio, TV, Internet and social networking. However, a certain amount of conservatism seems to be built into human nature, and hence many innovations have been met with opposition, ranging from caution to active objections.

The idea of casting a vote via electronic means or even via the Internet is no exception. Internet voting, for example, has the potential to change the whole election process so drastically that it must be threatening for at least someone. Improved absentee voting could mobilise many expatriates, a younger generation otherwise indifferent towards paper-based alternatives could start participating in democratic processes more actively, etc. All of these factors have a chance to bias the unstable political balance that many of the modern democracies seem to have trouble with.

Hence, there are a lot of reasons to retain the *status quo* of the election mechanism. However, the accessibility improvements provided by electronic voting are significant enough that they must at least be considered. The problem from the e-voting opponent's point of view, is that the argument of introducing a new bias into the electorate is not a valid counter-argument, at least in front of the public.

Luckily, there are other arguments, with security of the new technologies being at top of the list. Since almost any means of communication can, in principle, be used for vote transmission, any problem with any of these almost automatically translates into an argument against electronic voting. There is an extensive body of research revealing potential weaknesses in many of the proposed systems and even entire communities devoted to criticising electronic voting[1].

The majority of these e-voting-sceptic initiatives seem to rely on the implicit assumption that the conventional paper-based voting systems are inherently more secure, so that mankind can always fall back to them once all the electronic alternatives are banned. Of course, the history of paper-based election fraud is as old as such systems themselves. Still, the mere fact that life goes on and societies have learnt to limit this fraud to a somewhat acceptable level seems to confirm that paper voting is at least secure enough.

☆ This is an extended version of a paper presented at the E-Vote-ID 2017 conference.

E-mail addresses: jan.willemson@cyber.ee, janwil@cyber.ee

[1] Examples of such communities include http://verifiedvoting.org/, http://www.handcountedpaperballots.org/, http://www.votersunite.org/, etc.

https://doi.org/10.1016/j.jisa.2017.11.007
2214-2126/

Of course, the *feeling of security* based on historical experience is an important argument when seeking continued acceptance for legacy systems in society. However, we argue that, apart from a longer history, there is little in the paper-based technology itself that ensures its superiority over electronic solutions. Sure, the two have different characteristics and thus possess different strengths and weaknesses, but only comparing strengths of one system to the weaknesses of another is presenting a biased view.

The current paper aims to balance this discussion. The author argues that even though paper voting seems to limit the fraud to a reasonable level, this level was not pre-set before paper voting systems were designed, but rather adjusted *post factum* to the level that systems are capable of providing. There is no reason why we could not do the same with electronic voting.

This paper reviews some of the security features of paper-based voting systems, matching them to the criticisms against electronic ones. We also point out some (often unfairly neglected) benefits that Internet voting provides over paper elections.

The current paper was partly motivated by the recent report of Springall et al. [2] criticising the Estonian Internet voting system. The following discussion can be considered as one possible reply to that report.

2. Vote secrecy

Vote secrecy is one of the fundamental requirements of contemporary electoral systems with the main aim of limiting manipulation and assuring the freedom of choice for the voter. This requirement has been considered important enough to mention it in Article 21.3 of the Universal Declaration of Human Rights.[2]

Estonian Internet voting has been criticised for its potential to break vote secrecy if sufficiently many server-side actors collaborate either maliciously or due to an attack [2].

In a typical paper-based voting system, vote secrecy is implemented via an anonymous ballot paper. What is typically not advertised while setting up such a system is that on a physical level, fully unidentifiable paper is very difficult to achieve. Real sheets of paper can be fingerprinted based on slight variations in colour or 3D surface texture of paper, requiring only a commodity desktop scanner and custom software [3,4]. This requires malicious access to the ballot sheets both before and after the vote casting, but isn't malicious activity also what is assumed by Springall et al. [2]?

Of course, digital attacks scale better than physical ones. However, in the case of harming vote secrecy, the attacker is not necessarily after the scaling effect anyway. Recall that the requirement of secret ballots is established to guarantee voting freedom and non-coercion. On the other hand, coercion is an inherently personal thing. This means that, in order to fully utilise a large-scale vote secrecy violation, the attacker would need to additionally take a number of non-scaling real-life steps. This makes paper fingerprinting attacks comparable to digital vote disclosure in terms of effort/effect ratio.

Even if perfectly unidentifiable paper were possible, paper elections would still be still susceptible to various types of fraud. Ballot box stuffing is the most well-known example here, but voter impersonation may also lead to problems if an impersonator manages to cast a vote (unfortunately, voter authentication is not always as strong as we would like it to be). In this case, a legitimate voter may later discover that a vote has already been submitted on her behalf. If the ballots are completely anonymous, there is no way of recovering from this attack.

With such problems in mind, several countries have made trade-offs between vote secrecy and fraud-resistance. The UK, Singapore and Nigeria use serial numbers printed directly on ballots, whereas others, such as Canada and Pakistan, print serial numbers on the counterfoil.[3]

Ballot numbering in the UK has been criticised several times by OSCE/ODIHR [5–7], because it gives officials the ability to breach vote secrecy. However, the system is still perceived as secure in the society at large "because of the high levels of public trust in the integrity of the electoral process" [5].

In the author's view, this is an excellent example of the *feeling of security* being based on historical experience rather than on rational risk analysis. From the latter point of view, the trusted operational base is much larger, including almost all the election officials, whereas the Estonian flavour of Internet voting has only a single point of failure for a large scale vote secrecy violation attack. A single point of failure admittedly makes the stakes higher, but on the other hand, it is also much easier to secure, if done properly.

Unfortunately, convincing the public that everything is done properly is hard. In case of the UK, the legislation specifying ballot numbering has been in force since 1872 [5], whereas Internet voting in Estonia has only taken place since 2005. The difference really comes from generations-long experience which Estonian Internet voting system does not yet have.

For an even clearer comparison, let's go through the following mental argument: If we would take all the requirements that apply to paper voting, and apply them to early elections, could we call those elections secure? The answer would probably be no, since, for example, pre-19th century elections did not typically feature vote privacy nor equal suffrage for all citizens.

Does this mean that all early elections should be declared void and all their results disqualified retrospectively? Of course not. It is impossible to build a practical system by first imagining all possible restrictions. A real working system has to evolve with trial and error.

One may argue that the stakes are too high and that the result may be an election being "hijacked" by the wrong party. In this case, look at history again. We, as mankind, have come to our current situation through a long series of experiments, including failed ones. This is the nature of development.

3. Individual verifiability and ballot box integrity

When designing and evaluating Internet voting systems, two properties often required are individual and universal verifiability. Individual verifiability essentially means that any voter can verify that her own vote ended up in the ballot box the way she intended it to. Universal verifiability, on the other hand, refers to the situation where anyone is able to check that the ballots in the box(es) have been counted correctly.

In fact, these are reasonable requirements for any kind of a voting system, and paper-based systems should comply with them as well. But, how far does this compliance go?

Indeed, everything can be made fine with individual verifiability of paper voting up to the point where the voter drops her ballot into the box. It is possible for a voter to take care in marking the ballot in such a way that it would get counted correctly with high probability. You can even use your own pen that you trust not to have come with self-erasing ink. Yet, using pens (or even pencils like in the UK) provided in the voting booth is a very common practice. If we are genuinely concerned with individual verifiability of paper voting, we should at least educate the voters that such a behaviour is risky.

Contemporary Internet voting systems also possess the means to get a confirmation from the vote storage server about the safe

[2] http://www.un.org/en/universal-declaration-human-rights/.

[3] http://aceproject.org/electoral-advice/archive/questions/replies/912993749.