Bits or Paper: which should get to carry your vote?

Jan Willemson[1,2]

[1] Cybernetica AS
Ülikooli 2, 51003 Tartu, Estonia
janwil@cyber.ee
[2] Software Technology and Applications Competence Center
Ülikooli 2, 51003 Tartu, Estonia

Abstract. This paper reviews several aspects where 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 criticism about Internet voting has 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 more and more needed in the contemporary, increasingly mobile world. Hence, we need to give Internet voting a chance, even if it means risking with unknown threats.

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 90,646 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 [8].

The history has shown that, contrary to the fear of the 19th century politicians, advances in technology have provided their modern colleagues with a much wider choice of discussion platforms including radio, TV and Internet. However, a certain amount of conservativism seems to be built into a 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 Internet is no exception. Internet voting for example has a 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 on 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 whole communities devoted to criticising electronic voting[3].

Majority of these e-voting-sceptic initiatives seem to rely on the implicit assumption that the conventional paper-based voting systems are somehow 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 on a somewhat reasonable level seems to confirm that paper voting is at least secure enough.

Of course, the *feeling of security* based on historical experience is an important argument when seeking continued acceptance for legacy systems in the 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 hence 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 at balancing this discussion. The author argues that even though paper voting seems to limit the fraud on a reasonable level, this level was not pre-set before paper voting systems were designed, but rather adjusted *post factum* to what such systems were capable of providing. There is no reason why we could not do the same thing with electronic voting.

This paper reviews some of the acclaimed security features of the paper-based voting systems, matching them to the criticism 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.* [18] criticising the Estonian Internet voting system. The following discussion can be regarded as one possible reply to that report.

[3] Examples of such communities include `http://verifiedvoting.org/`, `http://www.handcountedpaperballots.org/`, `http://thevotingnews.com/`, `http://www.votersunite.org/`, etc.

2 Vote secrecy

Vote secrecy is one of the fundamental requirements in contemporary electoral systems with the main aim of limiting manipulation and assuring the freedom of choice for the voter. This requirement has even been considered important enough to mention it in Article 21.3 of the Universal Declaration of Human Rights.[4]

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 [18].

In a typical paper-based voting system, vote secrecy is implemented via 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 [5]. 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.* [18]?

Of course, digital attacks scale better than the physical ones. However, in 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 would be possible, paper elections are 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. UK, Singapore and Nigeria use serial numbers printed directly on ballots, whereas some others like Canada and Pakistan print serial numbers on the counterfoil.[5]

Ballot numbering in UK has been criticised several times by OSCE/ODIHR [1, 2, 4], because election officials have the capability of breaching vote secrecy. However, the system is still perceived as secure in the society "because of the high levels of public trust in the integrity of the electoral process" [1].

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

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

In the author's view, this is an excellent example of the *feeling of security* being based on historical experience rather than rational risk analysis. From the latter point of view, the trusted operational base is much larger, including almost all the election officials, whereas for example the Estonian flavour of Internet voting has only a single point of failure for a large scale vote secrecy violation attack. Sure, a single point of failure 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 UK, the legislation specifying ballot numbering has been in force since 1872 [1], whereas Internet voting in Estonia has only taken place since 2005. So the difference really comes from generations-long experience which Estonian Internet voting system can not yet possibly have.

For even a clearer comparison, let's go through the following mental argument: If we would take all the requirements that we currently have about 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 the citizens.

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

One may argue that the stakes are too high and that the result may be an election being "hijacked" by a wrong party. In this case, please look at history again. We as mankind have come to where we are 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 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 marking the ballot the 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 (you never use pens provided in the voting booth, do you?).

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

vote. To get around possible vote manipulating malware living on the voter's computer, this confirmation must come via an independent channel. For example, Norwegian Internet voting experiment used SMS as the second channel, whereas the Estonian system uses a mobile device to download and verify the vote [11].

Of course, independence of the voter's PC and mobile device is the crucial assumption here. As mentioned by Springall *et al.*, the strength of the verification claim is decreased if this assumption gets violated [18]. They also point out a way of infecting both devices with coordinated malware when the user connects them for, say, regular data transfer.

What Springall *et al.* do not say is that this attack is something the voter can avoid by informed activity. Just like you should take care when marking the ballot in a readable way, you can choose a verification device that is definitely independent from your PC. The main reason why voters do not do it already is insufficient understanding of the associated risks. Again, we may expect this situation to improve in time when people gather more experience with vulnerabilities of digital communication devices.

The first real difficulty with both paper and electronic ballots manifests itself in the storage stage as the ballot box integrity problem. In case of Estonian Internet voting, integrity of the vote storage server is maintained using organisational measures. One may argue that cryptographic techniques would give a higher level of assurance, and since organisational and cryptographic measures do not exclude each other, this would apparently be true.

But let's look at the ballot box integrity assurance problem in case of paper voting. If a voter wants to make sure that her vote is counted, she must check that her vote was not maliciously removed before counting. The ballot box may be sealed and stamped and the voter may even believe that the seal is checked before counting, but if it was sealed once, there is a technical way to do it again if someone would like to break it in the meantime.

Hence, the only way to be sure that the ballot is still intact is to stay next to the ballot box during the time period between vote casting and counting. The author had a discussion with professor Melanie Volkamer from Darmstadt University, Germany, and she claimed to do exactly that. To make the time frame manageable, she would go to the polling station 5 minutes before closing and then follow the box to the counting area.

In this way, anyone can in principle observe the polling station workers counting the ballots and later perform the recount him/herself. Can the observer now be 100% sure that his/her vote was included in the final tally? No, unfortunately not.

Human attention is limited and no single person can not observe all the poll workers all the time. So it is still possible for a malicious official to silently put some of the ballots aside and not count them.

Of course, the number of ballots in the box would then be smaller than the number of issued empty ballot sheets, but what do you do? It is legal for a

voter to obtain an empty ballot and not to cast a vote, so there is a plausible explanation to this discrepancy.

Hence, if the observer really wants to be sure that his/her vote ended up in the counted-pile, he/she should mark her ballot. However, this introduces another problem – ballot marking can be used as a proof in the act of vote selling. It is possible for a vote buyer to act as a legal observer during the counting and demand to see a ballot with a prearranged sign on it. In Netherlands, for example, a ballot sheet with a mark making it uniquely identifiable may be considered invalid for that reason.

Thus, being sure that your vote safely reaches the counting stage only goes as far as another requirement – vote anonymity for coercion resistance – allows it to. Even if marked ballots are not declared void in some jurisdictions, the mere need for such a measure to check ballot box integrity is a deviation from clean voting practices paper-based elections supposedly provide.

The next problem of universal verifiability, in turn, translates to the question how transparently the vote counting procedure of paper voting can be managed.

4 Transparency and accuracy of counting

One of the fundamental properties of paper-based voting is the possibility of independent recount. Ideally, written marks on paper ballots should be the *lingua franca* that every human auditor perceives the same way, so that it will be easy for a group of people to agree on the counting result (even if some of them have a political motivation to bias the result).

However, reality is not that simple. A recent study by Goggin *et al.* [9] has shown that, depending on the paper vote counting method used, the human error rate is roughly between 1-2%. This is more than enough to raise reasonable doubt in close cases, of which the history of democratic elections is very rich. (Just recall the 2000 US presidential elections where the outcome was depending on the convention to be used when counting ambiguous ballots.)

Even if the count is not close, an independent observer may still claim distrust in the accuracy of the result and demand recounting. This opens up opportunities of attacks against the paper vote counting procedure. Namely, the auditor demanding the recount and possibly even performing it may be an attacker himself. Having access to the first result, he knows exactly by how much the second count has to differ to provide a different end result [21]. It is also possible for a dishonest auditor to create havoc just by claiming that his count does not match the previous count(s), and keep doing so for numerous times.

Of course, in practical systems there must be safeguards protecting against such misuses. For example, the guidelines given to the returning officers in UK [3] state:

> 6.35 You must consider any recount request but by law may refuse if, in your opinion, the request is unreasonable. [...]

This introduces an interesting dilemma between the transparency advertised by the paper-voting advocates, and practical resilience against system misuse. Ultimately, a simple official will decide whether someone is allowed to exercise his/her legal right to become convinced in correct vote counting, or whether such a request is considered erroneous.

One way or another, we can argue that such a guideline is written for a reason. Quite probably once upon a time there was someone who tried to abuse the system by over-exaggerated references to his/her right of vote recount. That person may have been forgotten long ago, but the regulation is still there, expressing the current social agreement about the reasonable limitations to the transparency enforcement. Again, there is no reason why a similar agreement could not be achieved in case of electronic voting. It's just that this medium for vote transmission is yet too young for such a settlement.

Even though the error rates of hand counting and the implied disputes can be decreased by adopting more error resistant practices [9], the errors and disputes will never come down to zero. The root cause of this problem is the fact that a paper vote (unlike its electronic counterpart) has no strictly defined semantics. There will always be people with poor handwriting or intentionally willing to spoil their ballot (and one may even argue that it is their legal right to do so). This in turn means that until we stick with paper voting, there will always be an option for a dispute.

Of course, electronic voting is not free from related problems either, but they have a different nature. Namely, humans are very poor at perceiving bits directly, so they need a mediating device, which may then become a target of attack on its own. For example, a proof-of-concept malware was presented during 2011 Estonian Parliamentary elections changing the visual image displayed to the user on the computer screen, allowing for undetected vote manipulation [10].

Ultimately, the problems with both paper and electronic votes come down to agreeing on a single interpretation by all the parties. As already seen above, with paper votes this is in principle not achievable, since an analogue medium can not have a strict formal meaning. With electronic votes this is at least theoretically possible. However, the problem of agreeing that everyone has the same view on the bits still remains.

This is generally known as a secure bulletin board problem, and despite its simple statement, it turns out to be highly non-trivial to implement. What seems to be the difficult point is achieving consensus about the state of a digital system in a distributed manner.

One interesting option for solving this problem is provided by a public hash block chain in the style of BitCoin [15]. There are properties of vanilla BitCoin protocol that make it less appealing from the viewpoint of voting, like involved financial incentives. But at least as a proof-of-concept it shows that community-wide agreement on a digital asset is possible in practice.

Of course, using a block chain does not prevent all integrity attacks on its own. For example, BitCoin's block chain "history" can be rewritten if more than 50% of the participating peers decide to collaborate. However, even the depre-

cated/rewritten branches have still been made public, and hence such attacks can easily be detected.

There have already been first attempts of using block chain technology as a part of a voting system. One of the most prominent players is NASDAQ that has offered shareholders a remote voting opportunity, using BitCoin as a public log integrity provider.[6] Another interesting initiative was taken by a minor Danish political party (the Liberal Alliance) that reported using block chain based voting technology during their meeting.[7]

Of course, the problem of shareholder voting is an easier one compared to, say, parliamentary elections, since in the former case the vote secrecy requirement is not that strict. BitCoin provides a privacy layer in the form of pseudonymous public keys, but unfortunately it is not directly usable for real elections, since one user may establish many pseudonyms, hence breaking the one-man-one-vote requirement. Another block chain voting initiative, BitCongress[8], acknowledges this problem and admits that some collaboration with a central voter registration service is still necessary. Other new implementations of block chain based voting systems are being constantly developed, too.[9] [10]

There has also been a resent proposal by Culnane and Schneider for a bulletin board implementation targeted specifically for use in e-voting systems not using block chain technology [6]. For correct operations, it relies on a threshold of (a relatively few) computing peers to behave honestly. However, integrity violations can always be detected by means of verifiable receipts, and this is the most important property we expect any voting system to have.

All in all, it seems that the secure bulletin board problem is solvable in practice, allowing at least in principle higher accuracy of counting than the paper voting can ever provide.

5 Trust base

Elections are an inherently social thing, involving millions of people, registration lists, ballots, logistics, counting, etc. This means that no single person can do it all, we have to rely on someone.

Relying implicitly assumes trust and this in turn makes attacking elections really simple. You tell me what/whom you trust, I tell you I manipulate that entity and my attack is complete.

This is the essence of the most severe claims that Springall *et al.* make about Estonian Internet voting [18]. So you say that you use some computer to write server installation disks? Good, then we say we can attack that one. Or you say that you rely on SHA-256 hashes to prove integrity of these images? Excellent, then we can implement our own phony hash application. It does not matter if

[6] `http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/`
[7] `https://www.cryptocoinsnews.com/blockchain-voting-used-by-danish-political-party/`
[8] `http://www.bitcongress.org/`
[9] `https://followmyvote.com/`
[10] `http://www.unchain.voting/`

you record all the server installation on the video and put it up on YouTube for everyone to watch, there will always be something happening behind the scenes before you start filming, and that's what we are claiming to attack.

So all in all, the struggle goes over the trust base. What you do not usually read in the papers such as [18] is that the trust base of paper voting has a much more complex structure than the one of, say, voting over Internet. You implicitly trust all the people who count the votes to do their job correctly, you trust the paper manufacturers that they have not included tiny identifying marks on the ballots, you trust the storage facility owner that some of the packages with ballots do not mysteriously disappear, etc.

It is true that Internet voting concentrates a lot of trust around relatively few components (like central servers and their administrators). Hence the attackers have clear targets and can expect relatively larger effects if their attacks succeed [13].

On the other hand, such a trust concentration makes the crucial components of Internet voting also easier to guard. For example background checks of server administrators have to be very thorough, but there is only a rather limited number of them.

At the same time, the number of people involved in hand counting easily reaches tens of thousands of individuals for large elections. There is some redundancy in the form of recounting, but there is a limit to that, too. Hence, in order to manipulate the election result, an attacker has to bribe far less than 10,000 people. Even worse, the number of subsets of counting officials that may give rise to undetected fraud is huge, and no-one is able to check all of them for honesty.

Stating it otherwise, the problem of one person being unable to check the count of millions of ballots does not go away that easily. As a solution, risk-limiting audits proposed by Philip Stark have recently become very popular [19]. The underlying idea is simple – using a predefined correctness threshold, a statistical sample of ballots is selected and manually recounted. If the threshold is not met, more ballots are selected, etc. In the worst case, this method may end up selecting all the ballots, but hopefully it will finish much earlier. For example, after EU Parliament elections in Denmark, risk-limiting auditing was used and only 1903 ballots were required to be studied to obtain 99.9% confidence level [20].

Does this mean that risk-limiting audits reduce our trust assumptions? Not really. In order to perform the statistical test, a random sample needs to be generated. This means that we need to trust (= can attack) the random number generator and manipulate it to give us the seed that the attacker needs to prove that his version of the count is correct.

People preparing the Danish 2014 audit actually thought about this problem and established a dice-throwing ceremony that determined the seed. The ceremony was also recorded and the video was made publicly available.

However, the "I claim to attack what's behind the scenes" approach still applies. We do not know how many attempts of filming this video were made

until a suitable random seed was generated. We do not know where the dice came from and whether they were fair or not. So all of a sudden, the dice manufacturer and supplier are added to the trust base. Is this really what people had in mind when introducing post-election statistical auditing? Not necessarily.

When comparing the trust bases of paper and Internet voting, the comparison ultimately boils down to the questions like which one is harder to manipulate without detection – dice or SHA-256 hash implementation? The answer is far from being straightforward or clear.

6 Cost vs. benefit

Even though many of the risks of Internet voting are not new and have accepted analogues in paper-based systems, this is not true universally. The two are fundamentally different as a horse and a train, even though they serve the same purpose.

However, when emphasising threats posed by remote electronic voting, many esteemed researchers including Rivest *et al.* [8] and Springall, Halderman *et al.* [18] present the situation in a biased light.

Namely, they concentrate on *cost* (in terms of potential problems) instead of a more balanced *cost-benefit* analysis. Following similar reasoning, it would never make sense to invest any money, take a plane or even go outside, since these actions involve risks. However, in reality we do all of those things, because we estimate the gains exceeding the potential losses.

When taking such decisions, we can rarely rely on precise scientific measurement. Often the scale for such a measure can not even be properly defined. Is it riskier to starve to death or catch a flu while shopping for food? Is it worse to leave more people without a convenient voting method or to risk that a hostile neighbouring country hacks its way into your government? There is no single answer. In fact, the answer depends on subjective risk estimation, and this differs from country to county, from person to person.

Coming back to the Estonian context, there definitely is a big neighbouring country with its clear geopolitical agenda. However, would hacking the Internet voting system be the easiest way to achieve its goals? Again, there is no clear answer. But the author argues that bribing local politicians or using overwhelming military power (and hoping that NATO is willing to give up Estonia, avoiding World War III) are still good alternatives to consider.

More importantly, as said above, we also need to look at the potential benefits. One of the clearest gains of Internet voting is solving the absentee problem. In 2001, Ron Rivest wrote:

> *In my opinion, however, by allowing such an increase in absentee voting we have sacrificed too much security for the sake of voter convenience. While voters should certainly be allowed to vote by absentee ballot in cases of need, allowing voting by absentee ballot merely for convenience seems wrong-headed. I would prefer seeing Voting Day instituted as a national*

holiday to seeing the widespread adoption of unsupervised absentee or remote electronic voting. [16]

These words nicely illustrate the way people lived just 15 years ago. However, the world has changed a lot since then. Moving abroad is not a matter of convenience, but for many of us it is a need to find a job. For instance, according to Eurostat, on January 1st 2016, in EU there were 19.3 million persons who had been born in a different EU Member State from the one where they were resident.[11] It is unrealistic to assume that all those people would move back to their country of origin just for the voting day. The question that the above-cited researchers [18, 16, 8] conveniently ignore is how should these people vote.

One way or another, overseas voters must be given the means to exercise their civil right and duty. In US, this is done under the Uniformed and Overseas Citizens Absentee Voting Act. As of 2016, 32 states out of 50 states allow some form of electronic transmission of ballots over the Internet [12] like downloading, filling and submitting PDF forms via fax or e-mail.[12]

Security of this method is, on the other hand, still comparable to 19-century postal voting. Strength of authentication is questionable, transmission lines are vulnerable to tampering and voter coercion is insufficiently addressed.

As long as absentee voting is marginal, these problems may be ignored, but this is no more the case. Despite its researcher-backed rhetoric, even US is doing vote transmission over the Internet, and there is in fact no real alternative (see [14] for a further discussion on the comparison of Internet and postal voting).

There are also benefits in Internet voting for the people who have not migrated, but have stayed. In many parts of the world (including Estonia), a strong drive towards urbanisation can be observed. A lot of people move to bigger cities, because the infrastructure is much better there, the salaries are higher, etc. The remaining population in rural areas is no more sufficient to justify running the schools, cultural centres, shops, post offices, etc. As a result, many of these institutions have been closed down recently in rural Estonia.

An unfortunate side effect for elections is that in such places, there is no more location to put the polling station into. Also, there are no more school teachers who used to act as polling station workers. The only alternative is to travel a relatively long distance to a county capital to cast a vote, and the cost of this is the higher, the further away the voters live.

A recent study by Solvak and Vassil [17] has shown that in Estonia, the probability of being an Internet voter reaches over 50% as soon as the round trip duration to the polling station increases over 30 minutes. Following Rivest, we can declare all the people who do not undertake this trip as being too convenience-oriented, but the sad fact is that decrease in rural population has also made public transportation considerably less available in those areas, making participation in paper elections simply too costly.

---

[11] `http://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics`

[12] `https://www.sec.state.ma.us/ele/elemil/milidx.htm`

All in all, we see that compared to the conventional alternative, casting votes over Internet increases availability and (if done properly) also security of absentee voting. Additionally, it decreases the cost of participation in elections, allowing to make the whole process more accessible for example in rural areas.

7 Conclusions

Voting on paper and by using the assistance of machines are two very different things. Hence, their risk and trust models differ also by a fair margin; in fact to an extent where comparing them becomes very complicated.

With paper voting, security assumptions are largely social (a person is able to mark the ballot correctly, another person is able/willing to count it the intended way, a third person verifies the counting fairly, a fourth one keeps a good guard of the key for a ballot storage facility, etc.). In case of machine (and especially Internet) voting, digital threats become prominent. The more a voting system relies on electronic means, the more an attacker is able to utilise scalability of digital attacks.

Mankind has been relying on voting with paper medium for centuries. Its properties and potential vulnerabilities are considered to be known and threats are considered as mitigated to an acceptable level by the current legislation.

Electronic means of communications and data processing are only a few decades old. We have not yet seen all the evil that can be done with them, and hence we tend to over-estimate the risks compared to what we feel comfortable with.

Unfortunately, there is no *a priory* measure for the margin of this over-estimation. The only reliable way to see which problems occur in practice and how severe they are is to try the whole system out live.

Yes, there are risks involved, but these are inevitable if we want to move the state of the art forward. Recall the loss of two British Overseas Airways Corporation Comet airliners in 1954 [7]. These planes were revolutionary in their own time, having some of the first commercial jet engines, pressurised cabins, etc. Yet, they came crashing down. The reason established after a long series of tests was that microscopic production defects were amplified in the corners of the rectangular doors and windows. Thanks to that study, airplane windows now have round corners.

Would it have been possible to predict those crashes? Theoretically, yes – mathematical methods required to model stresses in surfaces had been developed by that time already. But in practice there are so many aspects to consider that ultimately the deployment in a real environment is what determines what is important and what is not.

Of course, this does not mean that we should leave all the known vulnerabilities wide open for everyone to exploit. But waiting until the implementation is theoretically perfect is not an option either. Requirements set to elections in general are contradictory in nature (like vote secrecy vs full auditability), so there will always exist a security definition according to which a given system is

not secure. Likewise, there will always be some parts of the setup that the voter will have to trust as given, and hence critically-minded researchers will have an eternal chance to write papers about breaking them.

But let's remember that this holds true universally and not only for electronic voting. The only aspect where paper voting is really superior to its electronic sibling is its centuries-long head start. But if we do not give electronic voting a chance, we will also miss all the opportunities of increased accessibility, lowered cost of participation and fully repeatable counting which, contrary to the paper voting, really is doable by everyone.

I'd like to conclude the paper with a thought by the creator of Helios Internet voting system Ben Adida who stated during the panel of EVT/WOTE'11 conference:

> *Internet Voting is terrifying, but it may be inevitable.*

Indeed, the world has changed a lot in recent years. People move around freely and we can not assume any more that all of our citizens are born, live their lives and die in close proximity of the polling station. As a result, absentee voting is going from an exception to a rule.

So instead of attacking the inevitable, let's concentrate on making it as secure as possible by introducing strong cryptographic authentication tokens, improving digital ballot box integrity and developing verifiability techniques.

And last but not least – let's remember that personal security is largely a *feeling* that can be supported by voter education and positive experience. Our children will not question Internet voting the way we do, since for them it will have always been existing.

Acknowledgements

The author is grateful to Melanie Volkamer, Sven Heiberg and Arnis Paršovs for useful and inspiring discussions.

The research leading to these results has received funding from the European Regional Development Fund through Estonian Centre of Excellence in ICT Research (EXCITE) and the Estonian Research Council under Institutional Research Grant IUT27-1.

References

1. United Kingdom of Great Britain and Northern Ireland. General election 5 May 2005. OSCE/ODIHR Assessment Mission Report (May 2005), `http://www.osce.org/odihr/elections/uk/16204`
2. United Kingdom of Great Britain and Northern Ireland. General election 6 May 2010. OSCE/ODIHR Election Assessment Mission Report (May 2010), `http://www.osce.org/odihr/elections/69072`

3. Part E – Verifying and counting the votes. UK Parliamentary general election in Great Britain on 7 May 2015: guidance for (Acting) Returning Officers (May 2015), http://www.electoralcommission.org.uk/__data/assets/pdf_file/0006/175389/Part-E-Verifying-and-counting-the-votes.pdf
4. United Kingdom of Great Britain and Northern Ireland. General election 7 May 2015. OSCE/ODIHR Election Expert Team Final Report (May 2015), http://www.osce.org/odihr/elections/uk/174081
5. Calandrino, J.A., Clarkson, W., Felten, E.W.: Some consequences of paper fingerprinting for elections. In: EVT/WOTE (2009)
6. Culnane, C., Schneider, S.: A peered bulletin board for robust use in verifiable voting systems. In: Computer Security Foundations Symposium (CSF), 2014 IEEE 27th. pp. 169–183. IEEE (2014)
7. Fearon, P.: The growth of aviation in Britain. Journal of Contemporary History 20(1), 21–40 (1985)
8. Gerck, E., Neff, C.A., Rivest, R.L., Rubin, A.D., Yung, M.: The business of electronic voting. In: Financial Cryptography 2001. LNCS, vol. 2339, pp. 243–268. Springer (2002)
9. Goggin, S.N., Byrne, M.D., Gilbert, J.E.: Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence. Election Law Journal 11(1), 36–51 (2012)
10. Heiberg, S., Laud, P., Willemson, J.: The application of i-voting for Estonian parliamentary elections of 2011. In: E-Voting and Identity, LNCS, vol. 7187, pp. 208–223. Springer (2011)
11. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: Electronic Voting: Verifying the Vote (EVOTE), 2014 6th International Conference on. pp. 1–8. IEEE (2014)
12. Horwitz, S.: More than 30 states offer online voting, but experts warn it isn't secure. The Washington Post (May 17th 2016)
13. Jefferson, D.: If I Can Shop and Bank Online, Why Cant I Vote Online? , https://www.verifiedvoting.org/resources/internet-voting/vote-online/
14. Krimmer, R., Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In: Electronic Government – Workshop and Poster Proceedings of the Fourth International EGOV Conference. pp. 225–232 (2005)
15. Noizat, P.: Blockchain electronic vote. In: Lee Kuo Chuen, D. (ed.) Handbook of Digital Currency. Elsevier (2015), chapter 22
16. Rivest, R.L.: Electronic voting. In: Financial Cryptography. vol. 1, pp. 243–268 (2001)
17. Solvak, M., Vassil, K.: E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 – 2015). Johan Skytte Institute of Political Studies, University of Tartu (2016)
18. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J.A.: Security analysis of the Estonian internet voting system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 703–715. ACM (2014)
19. Stark, P.B.: Conservative statistical post-election audits. The Annals of Applied Statistics pp. 550–581 (2008)
20. Stark, P.B., Teague, V.: Verifiable european elections: Risk-limiting audits for dhondt and its relatives. USENIX Journal of Election Technology and Systems (JETS) 1, 18–39 (2014)
21. Yasinsac, A., Bishop, M.: The dynamics of counting and recounting votes. Security & Privacy, IEEE 6(3), 22–29 (2008)