JeDEM 14(1): 72-85, 2022
ISSN 2075-9517
http://www.jedem.org
Date of submission: 27.07.2021
Date of acceptance: 03.11.2021
Article DOI: 10.29379/jedem.v14i1.673

Towards Identifying Social Factors behind (In)Efficiency of Voting Security Measures

Jan Willemson

ORCID Nr: 0000-0002-6290-2099
Cybernetica, Tartu, Estonia, jan.willemson@cyber.ee

Abstract: In this paper, we take a look at some standard requirements set to voting, and measures to achieve them. We argue that while the measures themselves are typically technical or organizational, their (in)efficiency is often determined by social factors. As the requirements set to voting are contradictory, every society will have to make trade-offs between them. Our analysis shows that one reason why some potential vulnerabilities are perceived as acceptable residual risks in some societies may be that, there simply is no tradition of abusing these vulnerabilities in this particular society. We identify a number of societal parameters, categorize them and study their effect on the (perceived) security of the respective measures.

Keywords: Voting, security, social factors

Acknowledgements: This paper has been supported by the Estonian Research Council under grant number PRG920. The author is grateful to the anonymous reviewers and professor Robert Krimmer for their valuable feedback and comments in the process of preparing the manuscript.

1. Introduction

Even though the overall goal of voting (to adequately reflect the social preferences) is easy to state, the task of actually building a system that achieves this turns out to be tricky. Historic experience has revealed many aspects that can go wrong with elections. In the process of learning from these errors, a number of requirements have been developed in an attempt to capture the properties that democratic elections should possess.

The list of such requirements is not completely universal and varies somewhat from source to source (see e.g. (Cetinkaya, 2008; Heiberg & Willemson, 2014a; Mitrou et al., 2002; Schryen, 2004)). But of course, there is also a significant overlap, typically including the following items.

- *Eligibility* – only eligible voters are allowed to cast a vote.
- *Generality* – all eligible voters have a chance to vote.
- *Uniformity* – all the voters are equal (often every voter has exactly one vote).

- *Freedom* – each voter can vote according to her free will.
- *Correctness* – election result is correctly calculated on the basis of the cast votes.
- *Availability, usability, and accessibility* – voting methods are readily available to and usable by all the voters, including disabled persons.

The above list is declarative, and every community/society has to decide what is the best way of implementing them. In this process, it is often the case that these requirements imply others. For example, in the case of paper voting, freedom is typically achieved via vote *secrecy*, assuming that if a potential coercer does not learn how she voted, she can not influence the voter. The correctness and generality requirements imply the need for *verifiability*, whereas eligibility checking and uniformity can be implemented via voter *identification*.

All of these properties, in turn, need some technical or organizational measures to be applied. To allow for proper verification of the tally, some sort of audit trails are needed, and there must be some auditors to check them. Ideally, every voter could act as an auditor, being able to at least verify that her own vote has been counted correctly. On the other hand, this verification should not result in a strong repeatedly presentable evidence (a *receipt*) of the vote as otherwise it could be used in coercive scenarios (e.g. vote-selling) to violate voting freedom. We see that some requirements set to voting are, at least, partially contradictory, so it is important to find a balanced trade-off between them.

The optimal placement of this balance largely depends on the community/society where the elections are held. Thus, the main research question we study in this paper can be stated as follows.

What are the societal parameters that determine whether a given security measure is efficient in achieving a given target requirement of voting?

To seek possible answers to this question, we follow an exploratory approach. Our study is based on the observations made in the course of our work on electronic voting conducted over the past decade. There are a number of case studies from around the world that have contributed to the current treatment, either via our direct involvement, or in the form of a literature review.

Following the three high-level properties identified above, the paper is also divided into three main sections. We will start with the treatment of privacy and coercion resistance issues in Section 2, addressing the voting freedom requirement. Next, in Section 3 we look at some voter identification issues rising from the eligibility and uniformity requirements. Section 4 will be devoted to various aspects of verifiability necessary to guarantee the integrity-related requirements of correctness and generality. The parameters identified in the course of the analysis will be reviewed and classified as a part of the discussion in Section 5. Finally, Section 6 will draw some conclusions and set directions for future research.

2. Privacy and coercion resistance

Throughout human history, the role of privacy in society and in the case of voting, in particular, has changed significantly. For example in the US, before the mid-19th century, voting was seen as a part

of participating in public affairs, and as such, was performed publicly. Voting happened either by saying one's preference out loud or submitting a visually easy-to-distinguish ticket.

Of course, this allowed for different kinds of coercive practices. The candidates used to 'treat' the voters by going to a local pub and leaving a few dollars there for everyone to get drinks (Brent, 2006). Offering a dollar or two personally "for the trouble of voting" was also commonplace. In some instances, political leaders even agreed across party lines to standardize bribery practices and prices (Wasley, 2016).

As an alternative point of view, show-of-hands voting can also be seen as a strong measure to ensure public verifiability of the tally. Because of this desirable property, public voting as a legislative mechanism has survived till our days in two Swiss cantons, Appenzell Innerrhoden and Glarus (Moeckli, 1987; Reinisch & Parkinson, 2007). Comparing this to the US case study above we can conclude that public voting is only feasible in communities where coercive practices are rare. Thus, the tendency for coercion is the first societal parameter we have to consider when deciding how well public voting, as a tally integrity protection measure, works.

As a number of societies struggled with coercion, the idea of voting by a secret ballot started to emerge. The first proposals and early try-outs go back to the 17th-18th century, but it took a long time and many political discussions until secret voting became universally accepted. Finally, it got sustainably implemented in mid-19th century Australia together with other related innovations (like ballot sheets being printed not by the candidates, but the election organizer) (Brent, 2006).

Voting in the privacy of a booth, served mankind well for over a century despite occasional clever attacks, like the Italian attack where the voter is required to vote in a pre-determined pattern (Di Cosmo, 2007), or chain voting (Benaloh, 2007). A more recent problem is that, the voter can provide strong proof of her vote if she wants to. Using easily accessible technology, it is possible to take a photo or a video of oneself, together with the filled ballot sheet (so-called *stemfie* (Hammelburg, 2015)) inside the polling booth.

In a way, the voter becomes an attacker from the system's point of view. Is violating one's own ballot secrecy legal or illegal? The answer depends on the country. Stemfies are legally banned in e.g. Belgium[1], but a judge in the Netherlands has ruled that "… although the disadvantages of 'stemfies' were in his eyes bigger than the advantages, the Election law does not prohibit them" (Loeber, 2014).

From here we obtain a social parameter, that needs to be taken into account when deciding whether polling booth, as an anti-coercion measure is efficient or not. The parameter expresses the level, to which extent deliberately proving one's preferences are spread in the society, and how much is this perceived as a threat. If stemfies are feared of being used as facilitators in large-scale coercion attacks, society has no choice but to ban them. On the other hand, if this fear remains below a certain threshold, society may choose to value personal freedom (including the freedom of openly stating one's preferences) more highly.

[1] https://www.thebulletin.be/stemfie-not-allowed-belgium

An additional factor in this consideration is the recent emergence of new covert side-channel attacks against paper voting (Krips et al., 2018, 2019; Toreini et al., 2017). For the time being, these attacks are on the level of lab experiments. However, as is the case with the security of many systems, the privacy guarantees provided by a voting booth tend to decrease in time. In the future, there will be a moment when communities will have to decide whether paper voting in a polling station offers sufficient coercion mitigation or not.

In the case of remote voting, the threat of coercion naturally applies as well, but the mitigation measures must differ in this case, as creating a physically controlled voting environment is not possible.

The first option is to do nothing about it and hope that not too much coercion occurs. This is yet another societal assumption that, of course has to be validated in the community where remote voting is to be implemented. For example, group influence was studied on the US state of Oregon that introduced total vote-by-mail general elections in 1996. About 30% of the interviewed voters reported that someone else (typically a family member) was present while they were filling their ballots, but only about half a percent said that they would have voted differently without this presence (Schaffer, 2014). This can be interpreted as evidence that remote voting in an uncontrolled environment does not necessarily have too much impact on voting freedom.

An even more illustrative example of a society, where the threat of in-person coercion in case of remote voting is efficiently ignored can be seen in Switzerland. The Swiss Post voting protocol specification (Swiss Post, 2021) is heavily concerned with the verifiability aspects. Coercion as a possible attack is, however, completely missing from the threat model.

On the other hand, there are many countries around the world where family voting happens even in polling stations (Schaffer, 2014). Postal voting would not probably do much to alleviate this problem either.

Remote electronic voting can, in principle, offer a wider range of measures against coercion. There are many approaches proposed in the literature; see Kulyk and Neumann (Kulyk & Neumann, 2020) for a comprehensive overview. They divide the proposed approaches into the following broad categories.

- Using fake credentials, the method pioneered by Juels, Catalano and Jakobsson in their seminal paper (Juels et al., 2010).
- Vote updating as done in the Estonian system, or in the variant of Helios proposed by Kulyk, Teague and Volkamer (Kulyk et al., 2015).
- Masking-based schemes where the voter is provided with a masking commitment which she can use to cast the correct vote, or change to submit a coerced vote.

There are also, other schemes not falling into these categories, most notably Selene that uses trapdoor commitments for tracking votes on the bulletin board (Ryan et al., 2016).

A general problem with the majority of the proposed schemes is their usability (Krips & Willemson, 2019; Kulyk & Neumann, 2020; Neto et al., 2018; Zollinger, 2020). From here we can extract the next societal parameter – readiness of the citizens to accept decreased usability in order to counter a problem that they did not cause.

However, there is another aspect to countering coercion with the above methods. Namely, using fake credentials, changing one's vote after the coercer has left, opening a trapdoor commitment to a wrong vote, etc., potentially involves lying. It would be for the greater good of voting freedom, but it would still be lying. To which extent the voters would be ready to do it, again depends on the overall level of civic responsibility in the society.

It is hard, to directly estimate to which extent would citizens of a particular country, be ready to act to protect democratic values. There are several contradictory aspects influencing this readiness. On one hand, there is the general level of perceived truthfulness of people varying from country to country. Data from the European Social Survey run in 2012 suggests that, people from the Nordic countries are expected to act more truthfully compared to, say, Eastern Europeans (Kwiatkowska, 2015).

On the other hand, lying to protect one's rights (in this case, freedom of voting) presumes a high level of civic competence. One way to estimate this is the civic competence composite indicator (CCCI-2), see e.g. Hoskins *et al.* (Hoskins et al., 2015, 2011). As the name suggests, the indicator is a weighted mix of various civic competence measures. For example, it contains a component called "Knowledge and skills for democracy". When this component was measured for youth in various European democracies, Nordic countries scored higher, whereas Eastern European and Balkan countries scored lower (Hoskins et al., 2015).

3. Voter identification

As mentioned in Section 1, a possible solution to the eligibility checking and uniformity problems is voter identification. Being a natural, and well-established mechanism in many countries, the ability to identify the citizens is not actually as universal as one might hope in the 21st century.

This transition was accompanied by a lot of controversies, with the proponents claiming to fight electoral fraud, and the opponents arguing that voter impersonation is a very rare problem while disenfranchising minority groups, who do not have valid ID-s, is a much more serious violation (Barreto et al., 2007; Sobel & Smith, 2009).

The debate over the effects of enforcing stricter ID requirements is still ongoing, with some evidence supporting both the claims that introducing such barriers hurts voter turnout (Hershey, 2009; Wolf, 2007) and that it does not (Cantoni & Pons, 2019; Mycoff et al., 2009). One way or another, this case is an example of a conflict between the requirements of generality and eligibility. Apparently, in the US, the person's right to vote is traditionally valued more than resistance against potential voter impersonation attacks. An important reason why such a choice may be perceived as secure in society is the historical experience assuring that impersonation has not been much of an issue.

In the case of online communication and applications (chatrooms, social media, etc.) assuming fake identities is a common practice (Elovici et al., 2014; Ramalingam & Chinnaiah, 2018). Even more, it is easy to automate the creation of many fictional characters (Chu et al., 2010). Thus, in the case of Internet voting, we can not simply hope that impersonation would not take place, and must rely on strong mechanisms of voter identification instead.

From the viewpoint of our current research, we obtain another societal parameter, measuring how widespread voter impersonation is. The magnitude of this parameter, determines how urgently strong voter identification is required in the community.

If voter identification is weak and impersonation is perceived as a threat, trade-offs with other requirements may be considered. For example, in order to counter the risk of casting the vote on behalf of another voter, several countries have made trade-offs with vote secrecy. 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.[2]

Ballot numbering in the UK has been criticised several times by OSCE/ODIHR (*United Kingdom of Great Britain and Northern Ireland. General election 5 May 2005. OSCE/ODIHR Assessment Mission Report*, 2005; *United Kingdom of Great Britain and Northern Ireland. General election 6 May 2010. OSCE/ODIHR Election Assessment Mission Report*, 2010; *United Kingdom of Great Britain and Northern Ireland. General election 7 May 2015. OSCE/ODIHR Election Expert Team Final Report*, 2015), 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" (*United Kingdom of Great Britain and Northern Ireland. General election 5 May 2005. OSCE/ODIHR Assessment Mission Report*, 2005).

4. Verification

One can argue that, out of the requirements listed in Section 1, correctness is the most central one. As a result, many of the measures implemented in voting ceremonies are targeted towards ensuring or verifying the respective properties.

There are several aspects that one may want to verify. The voter may want to check that the ballot she sent into the (physical or virtual) ballot box adequately reflects her preference (*cast-as-intended*). After the voter let the ballot go off her hands, it should stay in the ballot box in an unmodified way (*recorded-as-cast*). And, last but not least, we want to be convinced that the ballots coming from all the boxes indeed give rise to the officially declared tally (*tallied-as-recorded*).

The next questions to answer now are: who exactly could verify these claims, what kind of competencies do they need and what motivation do they have to engage in the verification processes?

The question of the verifier in the first case (cast-as-intended) is straightforward. Since the vote privacy requirement demands her preference to be known only to the voter herself, it is the voter

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

who should perform this kind of verification. However, this already assumes a certain level of competence from the members of the electorate.

There are various paper ballot designs used around the world, with many having complex structures and filling-in rules. In extreme cases, this may result in more than 10% of ballots being filled incorrectly simply because the voters are incapable of following the rules, see e.g. Pachón *et al.* (Pachón et al., 2017). The same paper also states the respective societal parameter – the degree of political sophistication, which is connected to the level of general information the electorate has.

In the case of electronic voting, things are potentially a bit better as the machine can assist the voter in checking whether the ballot rules are followed. On the other hand, the machine can also be an attacker, showing the voter one ballot on the screen, while quietly recording something else behind the scenes. It is especially problematic when there is no paper audit trail, e.g. in the case of remote electronic voting (Heiberg et al., n.d.).

There are a few methods proposed against this problem, e.g. Benaloh-style challenges to audit-xor-cast the vote as implemented in the Helios system (Adida, 2008), or opening the vote cryptogram on a different device as done in Estonia (Heiberg & Willemson, 2014b). However, all such methods require the voter to do something extra to counter a threat she perhaps can not fully comprehend, nor feels responsible for.

As a result, not too many voters tend to perform vote verification steps. E.g. statistics from the Estonian elections shows that, the percentage of verified votes ranges between 3.4 and 5.3 (Solvak, 2020). On the positive side, the study by Olembo *et al.* shows that, educating the voters by specifically crafted messages can increase the intent to verify (Olembo et al., 2014). Again, we see that the level of voter awareness as a social parameter plays a crucial role in how well individual vote verification mechanisms work.

System-side verification is a different matter. In the case of paper voting, the number of ballot sheets may reach millions – far outside the capability of one person to recount. There are statistical methods allowing to gain high assurance in the correctness of the count by only re-examining a fraction of the ballots, e.g. risk-limiting audits (Lindeman & Stark, 2012).

However, whether and how such methods translate to public acceptance of the election results is an entirely different question. It has been consistently observed that supporters of the losing parties perceive elections as more fraudulent (see e.g. Kernell and Mullinix (Kernell & Mullinix, 2018) for an overview). No mathematical proof is likely to change this perception. Citing Donald Trump from the 2016 US presidential rally: "I will totally accept the results of this great and historic presidential election – if I win." This translates to the level of trust citizens have in the election organizer (and perhaps in the state institutions in general), which constitutes the next social parameter influencing the perceived security of elections.

US presidential elections of 2020 underlined the importance of this parameter yet again. As the initial 700,000 vote lead in Pennsylvania started to shrink when absentee ballots were processed, the sitting president Donald Trump made allegations against the impartiality of the vote-counting staff,

accusing them of fraud[3]. Of course it is possible to recount the ballots independently, but the inherent need to trust the counters remains. In a strongly polarised society (which the US as of 2020 seems to have been), counter partiality claims are hard to deal with. Even though the courts rejected the majority of such claims in the US, the people not liking this decision still initiated civil unrest[4]. Thus, paper voting is no magic bullet against the insufficient trust.

Electronic voting has the potential to shift the balance here. One does not need to spend many person-years to add millions of digital votes, this can be done in an instant by a computer. Assuming there is a bulletin board from where everyone can download the votes and count them independently, making claims of miscounting, hopefully, becomes harder. If nothing else, there will be an efficient resolution mechanism in case of conflicting claims.

However, the technical details are not necessarily straightforward. In order to prove the recorded-as-cast property, together with the eligibility and uniformity requirements, the bulletin board should provide some sort of vote authenticity assurance. One way of doing this is letting the voters digitally sign their (encrypted) votes. Such a solution brings along a new problem – the community should have a reliable public-key infrastructure in place, with all the citizens having the means and ability to use it. This assumption translates to a societal parameter measuring the country's readiness for using digital signatures, or some other form of strong authentication.

Putting all the votes on the bulletin board in an encrypted form helps to protect the vote privacy, but publicly verifiable signatures may still bring along certain forms of coercion, as the coercer may want to influence his subject to simply abstain from elections. If this is perceived as a threat in society (which is yet another parameter in the view of our study), using a public bulletin board with publicly verifiable signatures is not an option. There are possible alternatives (e.g. non-public bulletin board or pseudonymized signatures), but they will have their own trade-offs, which we leave as a subject for future research.

After the authenticity of the votes is verified, they need to be tallied. One can not simply decrypt them since this would reveal how everyone voted. To counter this problem, there are two general approaches used in electronic voting – mixing the votes before individual decryption, and homomorphic tallying, adding the votes under encryption before decrypting just the final result.

Both of these approaches make heavy use of cryptography. As the mixing, homomorphic tallying or decryption applications can potentially lie, too, they have to be built in a way that they produce mathematical proofs of correct operation. On one hand, these proofs can be verified by independent observers, but on the other hand, these proofs add complexity to the cryptographic machinery.

As a result, the selection of people being able to understand and verify all the components is limited to a few highly trained professionals. Even if there are several of them, all being independent and agreeing that the cryptographic proofs check out, this may be insufficient to translate into public

[3] https://www.dallasnews.com/news/elections/2020/11/05/with-biden-one-state-from-presidency-trump-demands-stop-the-count/

[4] https://www.theguardian.com/us-news/2021/jan/06/us-capitol-lockdown-senate-trump-supporters-protesters-police

acceptance. Whether it does or not depends on yet another societal parameter – to what extent does the community feel comfortable relying on experts.

5. Discussion

In the paper, we have identified the following societal parameters that some voting security mechanisms rely on:

1. tendency for coercion,
2. the level to which extent deliberately proving one's preferences are spread in the society,
3. readiness of the citizens to accept decreased usability in order to counter a problem that they did not cause,
4. how wide-spread is voter impersonation,
5. the degree of political sophistication and general awareness of the electorate,
6. the level of trust citizens have in the election organizer,
7. readiness to use strong authentication means (e.g. digital signatures),
8. the level to which forced abstention is perceived as a threat,
9. readiness to accept expert opinions.

We do not claim that this list is exhaustive, but it allows us to identify some more general categories of parameters that need an assessment before deciding on the elections' protection mechanisms.

- **Coercive behaviour** (parameters 1, 2, 8): Fighting against coercion has traditionally involved relying on some form of voter privacy, but privacy, in turn, is at least in partial conflict with verifiability (Chevallier-Mames et al., 2010). Thus, the level of coercion (and its perception as a threat) in the society determines how strong verification mechanisms can be implemented.
- **Voter identification** (parameters 4, 7): Being able to reliably identify voters mitigates several threats related to voter impersonation, double voting, etc. However, this assumes extra infrastructure from the society which may not be available for various (e.g. historic) reasons.
- **Voter awareness** (parameters 3, 5): In order to achieve all the desired goals of the elections, its rules may be rather complex. This complexity may manifest itself for the voter in the structure of the ballot, the need to take extra actions to ensure vote integrity, etc. Readiness to accept this complexity (and perhaps some decrease in usability) determines how elaborate properties of the voting system can be targeted in the given community.
- **Trust issues** (parameters 6, 9): General elections are a huge undertaking and no single person can manage it alone. This brings along an inherent need to rely on someone else to provide eligibility verification, (re)count the votes, check cryptographic proofs, etc. At the end of the

day, the level of assurance the society gets in the fairness of elections depends on, to which extent are its members ready to trust authorities and experts in the field. If this trust is not there, getting election results accepted in society is impossible.

The above categories are not independent. For example, the interplay between the voter's awareness concerning the system details, and the level of trust she is willing to place into the system, is a complicated one. de Visser *et al.* argue that the trust level should be balanced (calibrated) between over- and under trust, and provide empirical evidence that it is possible to achieve this balance by an appropriate informational strategy (Visser et al., n.d.). Sacha *et al.* (Sacha et al., 2016) show how the awareness classification by Skeels *et al.* (Skeels et al., 2010) in terms of uncertainty, can be used to understand the mechanisms behind the formation of this balance. In particular, Skeels *et al.* identify *Unidentified Unknowns* as the most critical kind of misinformation, resulting in misalignment between the system's actual features and their human perception.

The relationship between voter awareness and trust in the case of (electronic) voting, has not been studied deeply to the best of our knowledge. However, we expect this to be a fascinating research avenue. As the requirements set to voting have many potential conflicts (Wilson, 2019), raising awareness in the voting system unavoidably raises awareness in such conflicts as well. How this impacts the users' trust in voting mechanisms remains the subject for future studies.

6. Conclusions and further work

Organizing vote collection and later tallying the results are just a few technical aspects of elections. The real challenge is, to convince the public (and especially the losing parties!) in the correctness of the results. This includes, proving that there were no attacks significant enough to change the final distribution of the elected seats. As the number and variation of the potential attacks is extensive, this is no easy task.

An additional layer of difficulty is introduced by inherently conflicting requirements that elections have (mostly vote privacy vs. verifiability, but sometimes also vote privacy vs. impersonation resistance, or eligibility vs. generality). Hence, for every voting system, there exists a security definition under which this system is not secure.

This in turn, means that the community or society where elections are run must make some trade-offs between these requirements. The properties that the selected voting system does not fully achieve are essentially residual risks that the community has to accept.

However, the nature of risks to accept may differ significantly between communities. There are a number of historical and societal factors that influence this decision. In this paper, we have identified a number of such factors and provided their initial classification. A general tendency that emerges from our analysis is that communities are more willing to accept risks associated with attacks that are rare in their environment.

There may be many reasons behind this rarity, but often they simply come down to tradition. Stating it otherwise – there may be known and even openly talked about vulnerabilities in the system, but if there are not too many attacks against them, the society is still willing to accept the overall system as secure.

Conversely, if society is not ready to compromise on any of the requirements, setting up a voting system that would produce a universally accepted result becomes impossible. Clearly stating and communicating the assumptions and trade-offs made between the requirements is an important step towards greater transparency of elections, as a societal representation mechanism. The question of how to do this, without causing misunderstanding in society, is still open and requires future treatment.

Also, the list of parameters identified in the current paper is not exhaustive, and we plan to extend it in the course of future research. At this stage, it is unclear even, how to determine the completeness of this process. Connected to this objective is, obtaining quantitative estimations for the identified parameters. One way or another, expert validation will need to be conducted, to both complete the parameter list and evaluate the corresponding values.

References

Adida, B. (2008). Helios: Web-based Open-Audit Voting. *Proceedings of the 17th USENIX Security Symposium*, 335–348. http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdfX.

Barreto, M. A., Nuno, S. A., & Sanchez, G. R. (2007). Voter ID requirements and the disenfranchisements of Latino, Black and Asian voters. *Annual Meeting of the American Political Science Association, Chicago, Illinois*, *30*.

Benaloh, J. (2007). Ballot Casting Assurance via Voter-Initiated Poll Station Auditing. *Proceedings of Evt'07*.

Brent, P. (2006). The Australian ballot: Not the secret ballot. *Australian Journal of Political Science*, *41*(1), 39–50.

Cantoni, E., & Pons, V. (2019). *Strict ID Laws Don't Stop Voters: Evidence from a US Nationwide Panel, 2008–2016*. National Bureau of Economic Research.

Cetinkaya, O. (2008). Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract). *Proceedings ARES 2008*, 1451–1456.

Chevallier-Mames, B., Fouque, P.-A., Pointcheval, D., Stern, J., & Traoré, J. (2010). On Some Incompatible Properties of Voting Schemes. In *Towards Trustworthy Elections: New Directions in Electronic Voting* (pp. 191–199). Springer.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010). Who is Tweeting on Twitter: Human, Bot, or Cyborg? *Proceedings of the 26th Annual Computer Security Applications Conference*, 21–30.

Di Cosmo, R. (2007). *On privacy and anonymity in electronic and non electronic voting: the ballot-as-signature attack.*

Elovici, Y., Fire, M., Herzberg, A., & Shulman, H. (2014). Ethical considerations when employing fake identities in online social networks for research. *Science and Engineering Ethics*, *20*(4), 1027–1043.

Hammelburg, E. (2015). #Stemfie: Reconceptualising liveness in the era of social media. *TMG Journal for Media History*, *18*(1), 85–100.

Heiberg, S., Laud, P., & Willemson, J. (n.d.). The Application of I-Voting for Estonian Parliamentary Elections of 2011. *Proceedings of Voteid 2011*, *7187*, 208–223.

Heiberg, S., & Willemson, J. (2014a). Modeling threats of a voting method. In *Design, development, and use of secure electronic voting systems* (pp. 128–148). IGI Global.

Heiberg, S., & Willemson, J. (2014b). Verifiable internet voting in Estonia. *Proceedings of EVOTE 2014*, 1–8.

Hershey, M. R. (2009). What we know about voter-id laws, registration, and turnout. *PS: Political Science and Politics*, *42*(1), 87–91.

Hoskins, B. L., Barber, C., Van Nijlen, D., & Villalba, E. (2011). Comparing Civic Competence among European Youth: Composite and Domain-Specific Indicators Using IEA Civic Education Study Data. *Comp. Ed. Review*, *55*(1), 082–110.

Hoskins, B., Saisana, M., & Villalba, C. M. H. (2015). Civic Competence of Youth in Europe: Measuring Cross National Variation Through the Creation of a Composite Indicator. *Social Indicators Research*, *123*(2), 431–457.

Juels, A., Catalano, D., & Jakobsson, M. (2010). Coercion-resistant electronic elections. *Towards Trustworthy Elections, New Directions in Electronic Voting*, *6000*, 37–63.

Kernell, G., & Mullinix, K. J. (2018). Winners, Losers, and Perceptions of Vote (Mis)Counting. *Int. J. Of Public Opinion Research*, *31*(1), 1–24.

Krips, K., & Willemson, J. (2019). On Practical Aspects of Coercion-Resistant Remote Voting Systems. *E-Vote-Id 2019*, *11759*, 216–232.

Krips, K., Willemson, J., & Värv, S. (2018). Implementing an audio side channel for paper voting. *E-Vote-Id 2018*, *11143*, 132–145.

Krips, K., Willemson, J., & Värv, S. (2019). Is your vote overheard? A new scalable side-channel attack against paper voting. *EuroS&P 2019*, 621–634.

Kulyk, O., & Neumann, S. (2020). Human Factors in Coercion Resistant InternetVoting – A Review of Existing Solutions and Open Challenges. *Proceedings of E-Vote-Id 2020*, 189–204.

Kulyk, O., Teague, V., & Volkamer, M. (2015). Extending helios towards private eligibility verifiability. *E-Voting and Identity*, *9269*, 57–73.

Kwiatkowska, A. (2015). *The small and big deceptions: In psychology and evolutionary sciences perspective* (pp. 46–72). Wydawnictwo Uniwersytetu Rzeszowskiego.

Lindeman, M., & Stark, P. B. (2012). A Gentle Introduction to Risk-Limiting Audits. *IEEE Secur. Priv.*, *10*(5), 42–49.

Loeber, L. (2014). E-voting in the Netherlands; past, current, future. *Proceedings of Evote 2014. TUT Press, Tallinn*, 43–46.

Mitrou, L., Gritzalis, D., & Katsikas, S. K. (2002). Revisiting Legal and Regulatory Requirements for Secure E-Voting. *Security in the Information Society: Visions and Perspectives, IFIP TC11 Sec2002*, *214*, 469–480.

Moeckli, S. (1987). Die schweizerischen Landsgemeinde-Demokratien. Paul Haupt.

Mycoff, J. D., Wagner, M. W., & Wilson, D. C. (2009). The empirical effects of voter-ID laws: Present or absent? *PS: Political Science and Politics*, *42*(1), 121–126.

Neto, A. S., Leite, M., Araújo, R., Mota, M. P., Neto, N. C. S., & Traoré, J. (2018). Usability Considerations For Coercion-Resistant Election Systems. *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, 40:1–40:10.

Olembo, M. M., Renaud, K., Bartsch, S., & Volkamer, M. (2014). Voter, what message will motivate you to verify your vote? *Workshop on Usable Security, Usec*.

Pachón, M., Carroll, R., & Barragán, H. (2017). Ballot design and invalid votes: Evidence from Colombia. *Electoral Studies*, *48*, 98–110.

Ramalingam, D., & Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165–177.

Reinisch, C., & Parkinson, J. (2007). *Swiss Landsgemeinden: a deliberative democratic evaluation of two outdoor parliaments*.

Ryan, P. Y. A., Rønne, P. B., & Iovino, V. (2016). Selene: Voting with transparent verifiability and coercion-mitigation. *FC 2016 International Workshops, Bitcoin, Voting, and Wahc*, *9604*, 176–192.

Sacha, D., Senaratne, H., Kwon, B. C., Ellis, G. P., & Keim, D. A. (2016). The role of uncertainty, awareness, and trust in visual analytics. *IEEE Trans. Vis. Comput. Graph.*, *22*(1), 240–249.

Schaffer, F. C. (2014). Not-So-Individual Voting: Patriarchal Control and Familial Hedging in Political Elections around the World. *Journal of Women, Politics & Policy*, *35*(4), 349–378.

Schryen, G. (2004). Security Aspects of Internet Voting. *Proceedings of Hicss-37*.

Skeels, M. M., Lee, B., Smith, G., & Robertson, G. G. (2010). Revealing uncertainty for information visualization. *Information Visualization*, *9*(1), 70–81.

Sobel, R., & Smith, R. E. (2009). Voter-ID laws discourage participation, particularly among minorities, and trigger a constitutional remedy in lost representation. *PS: Political Science and Politics*, *42*(1), 107–110.

Solvak, M. (2020). Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. *Proceedings of E-Vote-Id 2020*, *12455*, 213–228.

Swiss Post. (2021). *Protocol of the Swiss Post Voting System, Version 0.9.8*.

Toreini, E., Shahandashti, S. F., & Hao, F. (2017). Texture to the rescue: Practical paper fingerprinting based on texture patterns. *ACM Trans. Priv. Secur.*, *20*(3), 9:1–9:29.

United Kingdom of Great Britain and Northern Ireland. General election 5 May 2005. OSCE/ODIHR Assessment Mission Report. (2005).

United Kingdom of Great Britain and Northern Ireland. General election 6 May 2010. OSCE/ODIHR Election Assessment Mission Report. (2010).

United Kingdom of Great Britain and Northern Ireland. General election 7 May 2015. OSCE/ODIHR Election Expert Team Final Report. (2015).

Visser, E. J. de, Cohen, M. S., Freedy, A., & Parasuraman, R. (n.d.). A design methodology for trust cue calibration in cognitive agents. *Proceedings of VAMR HCI 2014*, *8525*, 251–262.

Wasley, P. (2016). Back When Everyone Knew How You Voted. *Humanities*, *37*(4).

Wilson, A. (2019). Modeling Requirements Conflicts in Secret Ballot Elections. *Proceedings of E-Vote-Id 2019, Taltech Press*, 171–186.

Wolf, R. (2007). Study: Stricter Voting ID Rules Hurt'04 Turnout. *USA Today*, *19*.

Zollinger, M.-L. (2020). *From secure to usable and verifiable voting schemes* [PhD thesis, University of Luxembourg]. http://hdl.handle.net/10993/44422X.

About the author

Jan Willemson

Jan Willemson defended his PhD in computer science at Tartu University, Estonia, in 2002. He has been working at Cybernetica as a researcher since 1998, specializing in information security and cryptography. His areas of interest include risk analysis of heterogeneous systems, secure multi-party computations, e-government solutions and security aspects of Internet voting. He has authored more than 60 research papers published in international journals and conferences.

