Why is Online Voting Still Largely a Black Box?*

Michael Kirsten[0000−0001−9816−1504], Melanie Volkamer[0000−0003−2674−4043],
and Bernhard Beckert[0000−0002−9672−3291]

KASTEL Security Research Labs, Karlsruhe Institute of Technology (KIT),
76131 Karlsruhe, Germany
kirsten@kit.edu, melanie.volkamer@kit.edu, beckert@kit.edu

Abstract. Online elections and polls are increasingly gaining ground. Since the beginning of the pandemic, many associations, companies and agencies opted for online elections at some point. Yet, most of these elections use online voting systems that are a black box for voters, even though the current state of research offers cryptographic means that would allow voters to detect potential manipulations, e.g., by methods for end-to-end (E2E) verifiability. In this paper, we report on qualitative exploratory research to determine the reasons for this situation. We evaluate responses from a panel at a national conference in Germany by specialists from official agencies, industry, and academia, whom we asked why election organizers still largely opt for systems that are not verifiable and how this could be changed. We furthermore present an exploratory study in which we asked program committee members from relevant international conferences to assess the obtained panel responses on their accuracy, relevance, and completeness. Finally, we discuss possible next steps for strengthening our findings and how to implement them to see more verifiable voting systems being used in the future.

Keywords: Online voting · Black-box systems · Panel discussion · Qualitative exploratory study.

1 Introduction

Digitization in our society is on the rise and at the latest with the pandemic, the demand for remote applications over the Internet has increased significantly. A notable example are online voting and polling systems, which are increasingly gaining ground. Despite the increasing popularity and rapid dissemination, the employed systems are oftentimes opaque and apply outdated cryptographic standards. However, the state of research nowadays (and particularly in Germany – see [2]) offers cryptographic means for end-to-end (E2E) verifiability that allow to retrace individual votes through the election process in a way that both vote secrecy is ensured and voters can detect manipulations. As already the results from non-electronic elections are regularly getting challenged and audited publicly,

* This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

we find it startling that online elections do not undergo comparable scrutiny and many election organizers still accept opaque black-box systems. Albeit the research community for electronic voting is very active, their transfer into practice appears limited as current online voting systems badly lag behind the current state of research – again, in particular, in Germany.

Our interest are the reasons for this gap and how they can be overcome, with a focus on election organizers and their considerations against or in favor of black-box voting systems. In this paper, we take the first step toward scientifically examining the reasons and explore actions to address them by using qualitative data analysis techniques. Through qualitative evaluation of a specialist panel with seven members from official agencies, industry, and academia, and a qualitative online survey with responses by 10 experts from program committees within the research community, we explore two main research questions:

1) What reasons and arguments do stakeholders and experts consider accurate or relevant for organizers to decide for using black-box online voting systems?
2) What actions do stakeholders and experts propose and consider feasible or relevant to lead organizers to use E2E-verifiable online voting systems?

Our study resulted in a list of reasons that serve as arguments for election organizers to keep using black-box online voting systems, as well as recommendations on actions to lead them towards using end-to-end verifiable systems.

2 Related Work

To the best of our knowledge, this is the first systematic research on why black-box voting systems are used. There is, however, research on the general case for online voting without specifically addressing system transparency [5]. Moreover, multiple works studied voters' subjective perceptions for online voting [1,4] and their mental models, trust and understanding of online voting and voter verification [6–8,10,11]. Besides user studies, Teague addresses the general arguments and problems regarding the current situation of e-voting systems and formulates corresponding research challenges [9].

3 Background and Overview

3.1 End-to-End Verifiability

The common security notion for voting systems of *end-to-end verifiability* (E2E-V) is concerned with providing convincing evidence as built-in functionality. Such a functionality ensures that each individual voter can themselves monitor the integrity of the election [3]. From one end to the other, this comprises that voters can independently verify (a) that their votes are correctly recorded (*cast as intended*), (b) that the representation of their vote is correctly collected in the tally (*collected as cast*), and (c) that every well-formed and collected vote is correctly included in the tally (*tallied as collected*).

E2E-V requires furthermore that it is possible to check the list for those voters who cast ballots, such that no *ballot-box stuffing* can occur, i.e., no additional votes are added to the collection (*eligibility verifiability*). The first two monitoring mechanisms are also commonly classified as *individual verifiability* since an individual voter can verify their own vote, and the third one as *universal verifiability* since the collection of votes can be verified as a whole.

More advanced security mechanisms based on E2E-verifiability also provide *accountability*, e.g., *collection accountability* denotes that, once a voter detects that their vote has not been collected as cast or intended within the vote-casting protocol, they obtain evidence that is convincing to an independent party in order to demonstrate that their vote has not been correctly collected. Yet, when aiming to provide accountability, there is a likely trade-off with the confidentiality requirement of coercion resistance, since the voter might be forced to present the obtained evidence to convince a (malicious) coercer.

3.2 Black-Box System

For this paper, we consider a black-box voting system (in short, a *black-box system*) as a system which does not provide voters with any functionality that allows them to verify that their votes are tallied as intended, cast, or collected. In such an opaque system, voters rely, in particular for election integrity, on strong trust assumptions such as: (a) They need to trust the election operating service to be trustworthy. (b) They also need to trust that neither their vote casting device nor the election server infrastructure is corrupted.

3.3 Overview

We present the panelists' responses on our two questions in Section 4. Further, we present and analyze the results of our survey and qualitative study with e-voting experts' considerations in Section 5. Finally, we provide a small discussion in Section 6 and conclude in Section 7.

4 Panel Responses from Specialists

4.1 Composition and Setup

We organized a one-hour panel discussion on the topic of "Why do election organizers decide to (only) use black-box online voting systems?" as part of the German national security conference *Sicherheit* on April 7th, 2022. The conference *Sicherheit* is steered by the special interest group *Security* (*Fachbereich Sicherheit*) within the German Informatics Society (GI – *Gesellschaft für Informatik*). The panel was composed of seven specialists from Karlsruhe Institute of Technology (KIT), Heilbronn University of Applied Sciences, IT University of Copenhagen (ITU), the Federal Office for Information Security (BSI – Bundesamt für Sicherheit in der Informationstechnik), University of Koblenz, and POLYAS

GmbH – a German commercial vendor and provider of online elections –, with a moderator from Karlsruhe Institute of Technology (KIT). Each of the panelists from academia had experience with talking to election organizers about securing elections and in particular verifiable systems.

The panel started with an introduction and some technical background by the moderator,[1] followed by short leading statements prepared by each of the panelists beforehand in response to the topic question. Thereon, after the panelists answered questions from the audience for about 30 minutes, the panelists were asked about their ideas regarding possible actions to get election organizers to use end-to-end verifiable online voting systems. Afterwards, again, the audience could asked questions.

In the following, we categorize, summarize, and explain both the leading statements as well as the actions proposed by the panelists.

4.2 Arguments on Current Election Organizers' Motivation

We have organized and sorted the panelists' statements on why election organizers still largely decide to use black-box online voting systems. Note that, when we use phrases such as "election organizers argue [. . .]", this does not mean that we interviewed election organizers, but that the panelists mentioned this from their own experience. The same holds when we talk about voters. We both provide the mentioned potential explanation and comment on it.

Transparency Dismissal. Election organizers argue that the stakes in their elections, e.g., for a university students' committee, are not as high as, e.g., for general parliamentary elections at national level, and hence they say the requirements should be allowed to be lower. For this reason, particularly verifiability mechanisms might not be needed.

With this distinction between different election scenarios, organizers dismiss arguments against opaque electronic voting systems and court decisions, that demand elections to have at least some degree of publicity or transparency. Effectively, no matter which kind or scenario of election is conducted, it is unclear how to handle complaints about suspected manipulations of the election result if the system does not provide any means of verifiability.

Voter Unawareness. Trust or distrust of voters in systems is most likely based on examinations and testimony by experts, control and inspection bodies, official agencies, certificates etc. It is less likely based on the voters' understanding of the inner workings of the voting systems. This phenomenon is similar to people who drive a car and are not interested in the inner parts of the car's engine, instead they let the car be checked on a regular basis.

[1] The main purpose consisted in introducing the comparison of black-box and verifiable voting systems to the audience.

As a consequence of a missing understanding of the inner workings, voters are typically unaware of specific risks concerning voting systems that may compromise the whole election and not (only) individual ballots. There is no reason for them to complain about black-box systems or to ask for alternatives.

Justification Avoidance. The development of voting systems inherently involves the need to compromise at least some degree of secrecy in favor of some integrity or vice versa. However, justifications or explanations for a particular compromise require technical understanding and potentially scare people who may feel overwhelmed and overestimate the true risks. Election organizers want to avoid this potential for more distrust and suspicion among voters, and instead opt for black-box systems or mechanisms that do usually not require any technical understanding. In order to avoid debates for mitigating the voters' suspicions, the organizers instead use (black-box) systems that – as they require little technical understanding – appear "shiny" and clean, as most voters do not ask for justifications or explanations.

Complicated Usability. The implementation of verifiability mechanisms is challenging and hard to get right, which often results in complicated mechanisms with which the voters are not familiar. Election organizers then opt for black-box solutions, in order to avoid the problems or difficulties involved with making verifiability mechanisms usable or explain their usage.

Cost-Efficiency Focus. Market economy oftentimes focuses on efficiency and saving costs instead of factors that do not directly translate to such quantitative measures, e.g., security. For example, easy-to-use software might get a higher priority than more secure software with potentially poorer usability, since the better usability avoids a costly telephone hotline. Election organizers hence do not account as much for security concerns that cannot be quantified as easily, but prioritize concerns for which there are foreseeable costs, e.g., by choosing an easy-to-use black-box system with inferior security.

Complex Decision. The choice of a suitable product is complex as there are many vendors and products with various functional and security features, and decision-makers usually lack the time, budget, capacity, and the personnel to evaluate the options and decide on a product. Election organizers have an "easier" decision with black-box solutions that are directly advertised by the vendors.

Missing Orientation. Organizers need orientation to make the right decision, e.g., regarding the decisions of other election organizers, their experiences with available systems, standards or certificates, legal requirements, and court decisions. As long as a working system is perceived as "safe enough", an organizer needs a good justification for changing the system, and the current situation mostly comprises black-box systems.

4.3 Action Proposals to Change Election Organizers' Motivation.

We organized and sorted the panelists' proposed actions that they believe could lead election organizers to E2E-verifiable electronic voting systems as follows:

Active Marketing. The community and vendors should actively propose verifiable voting systems and undertake marketing measures for usable verifiable systems to actively spread the word. This creates competition among vendors and generally makes organizers aware that verifiable systems are a viable option.

Requirement Catalogs. Official agencies and institutions need to set up requirement catalogs that demand E2E-verifiability and that are practical to be demanded from election organizers. Consequently, these could turn into official recommendations, give orientation, and communicate expectations to both vendors and election organizers, e.g., by notable national agencies.

Lawmaker Awareness. The community should raise awareness among lawmakers so that they can make their assessments on the basis of the right criteria, e.g., when evaluating court cases. Once the lawmakers adopt the right criteria, there is an incentive to set similar and comparable standards that can be enforced for all publicly-employed voting systems.

Standards Enforcement. The lawmaker should set and enforce standards and regulations for secure and usable verifiable online voting systems. Clear and strict regulations should replace a vague reliance on the market and its potentially harmful dynamics, so that systems must comprise a certain level of transparency. Such levels could be the technical realization of official requirements or recommendations, and hence be incorporated by national or international standards such as the common criteria.

Trust Level Communication. In order to make an informed decision, vendors or other agencies should provide clear-cut comparisons of available systems and why or how, i.e., under which trust assumptions, they can or cannot be trusted. By this measure, election organizers are given orientation and they can align their choices with the needs, budget, and their capabilities for the election at-hand, so that they are also able to justify their decision before courts and clearly communicate the specific trust assumptions to other involved parties, e.g., interested voters, political parties, etc. As a result, election organizers gain a better orientation towards the most suitable system.

Interface Implementation. For a better usability and a more fine-grained and informed decision of election organizers, vendors should implement and offer common software interfaces and modules, e.g., one module for counting the votes, one for verifying them, etc. Such systems are more transparent and can both simplify the decision for election organizers and give them better orientation.

Voter Awareness. The community should raise awareness among voters so that they themselves pressure election organizers to use and vendors to provide end-to-end verifiable online voting systems.

5 Exploratory Study for Response Evaluation

5.1 Composition and Setup

We carried out a short qualitative exploratory online survey with 62 members of international program committees and a return of 10 completed questionnaires. We sent emails to 62 members of the program committees of the *First International Workshop on Election Infrastructure Security* (EIS 2022) as well as the tracks on *Governance of E-Voting* and *Election and Practical Experiences* at the *Seventh International Joint Conference on Electronic Voting* (E-Vote-ID 2022) between June 16 and June 23, 2022. In that email, we provided a short description and motivation of our study, the procedure of our survey, stated that participation is anonymous and can be canceled at any moment, explained the intended use of the received responses, and included a link to our anonymous survey on the platform *SoSci Survey*. This survey platform adheres to strict data privacy requirements to ensure the participants' anonymity. In the beginning of the questionnaire, every participant was given information on the study, its intended use, the information that the survey is completely anonymous and can be canceled at any moment, and then had to actively confirm their consent to participate in the study. At the end of the questionnaire, we provided our contact information to allow inquiries about the study by the participants.

Within the survey, we presented summaries of the seven leading statements and seven proposed actions by the panelists at *Sicherheit 2022*. For the arguments, we asked whether the participants consider any of them wrong or irrelevant, and for the proposed actions, whether they consider any of them infeasible or irrelevant. For both lists, we asked the participants whether they think that any relevant points are missing and, if so, which ones they think are missing.

5.2 Evaluation Methodology

After the one-week survey period, we received valid responses from ten participants, who spent on average about 13 minutes on our survey. We organized all responses that addressed the election organizers by the categories of the panelists' statements or into new categories where appropriate. Therein, we identified three new arguments and three new proposals for actions. From the survey responses, we could also add new aspects to two of the panelists' arguments and four of the panelists' proposed actions. In the following, we summarize the responses from the survey participants regarding their evaluations and amendments to the panelists' arguments and action proposals.

5.3 Arguments on Current Election Organizers' Motivation

Seven of the participants felt that most of the panel arguments are very much aligned with their own experiences and communication with election officials, and overall agreed with our arguments.

Accuracy or Relevance. Regarding accuracy or relevance of the arguments from the panel, four survey participants addressed the argument of voter unawareness. Two of them stated that they do not consider the voters' unawareness a current argument for election organizers to opt for black-box voting systems. They elaborated that voters are generally not the relevant group to advocate policies on specific technologies. Another two participants had the additional opinion that voters are already sufficiently aware of potential threats of election manipulations and the benefits of systems with verifiability mechanisms.

Moreover, two participants replied that the arguments of justification avoidance and focus on cost efficiency are effectively wrong arguments. They did not question their relevance for the decisions by election organizers, however. The stated reason for the inaccuracy of justification avoidance was that voters generally appreciate the fact that they are provided an option to verify the election result, or that they know that, e.g., election officials have such procedures in place, which likely compensates or eliminates potential distrust or suspicion that could arise from technical justifications or explanations. Regarding the focus on cost efficiency, they stated that favoring a black-box solution in order to save costs fails to account for potential fallout costs in case an actual election manipulation is happening or disinformation about alleged manipulations is being spread.

Further Aspects for the Arguments. Moreover, the participants also provided both new aspects to given arguments and new arguments that were not yet stated by the panelists. They had the following three further aspects to our arguments.

Transparency Dismissal. Additionally to dismissing transparency demands due to other election scenarios, participants stated a believe among some organizers that smaller jurisdictions may not have the budget, capacity or capability to offer any meaningful form of transparency or verifiability and should be excused from it. Hence, they do not find the objective of verifiability, end-to-end or not, viable or worth pursuing at all for reasons of insufficient budget or capacity.

Justification Avoidance. Other than choosing black-box systems to avoid justifications that could raise suspicions, participants added that the property of being nontransparent with no explanations is sometimes considered to be a security guarantee in itself. A potential reason might be that potential attackers can also not exploit explanations of the system for attacking or manipulating an election.

Missing Orientation. Additionally to, e.g., legal requirements that give no orientation for the decision on an online voting system, local laws oftentimes do not formulate any sensible requirements for voting systems and hence even allow virtually any technology. Therefore, more than just missing orientation, such laws do not even provide any incentive, not even for black-box systems.

Further Arguments. The participants also provided the following two new arguments that make election organizers opt for black-box systems.

Potential Misuse. Organizers of elections are interested in an orderly procedures and that elections cannot be discredited. However, the data produced by non-black-box systems with the objective of proving integrity of the vote could also potentially be misused to abusively discredit an election. Depending on the specifics of the verification mechanism, even sound verification data could be used in combination with a false pretense of having voted for a different candidate or by exchanging verification data with other voters. Election organizers might be scared on how to resolve such situations, especially when verification mechanisms do not entail accountability or conflict resolution, so that the only solution might consist in a repeated election, which election organizers generally want to avoid.

Blind Trust in Technology. Some vendors promote that technology is generally unbiased, flawless and secure, and electronic systems should be generally trusted more than human integrity. In the extreme, this favors any technological solution over any human intervention, no matter the actual trustworthiness of the employed technology. This is sometimes used to argue that any human intervention in elections should be avoided and electronic elections are generally cleaner. As a result, election organizers do not raise concerns about opaque black-box systems and the benefits of transparent systems are not even discussed.

5.4 Action Proposals to Change Election Organizers' Motivation

Six participants agreed with the proposed actions, but replied that especially the actions for raising awareness are rather unclear and challenging in their specifics.

Feasibility or Relevance. Regarding relevance of the proposed actions, nine participants agreed with the actions, but we received mixed replies on their feasibility. In the following, we provide more details on the participants' points.

Many participants generally considered raising awareness, e.g., among voters, lawmakers, etc. to be a key factor, but stated that it is generally unclear what this specifically comprises. One participant stated that voters are already sufficiently aware and appreciative of verifiable systems if these are implemented and communicated "the right way", and another participant said that awareness can easily change if experts share insights in the process, and subsequently more experts become vocal which then convinces the public, as experts generally do not like black-box systems. Yet another participant stated that raising awareness is only likely to be effective with actually problematic results or events in practice. One participant assessed the proposal to implement common interfaces and modules to be on the outer limit of feasibility, mentioning that success stories for such actions are sparse, and that it might be hard or even infeasible to agree on specific common interfaces or modules. Regarding the proposal to give clear-cut comparisons of trust assumptions for available systems, one participant addressed that this only works if viable alternatives exist. For no viable options, clear-cut descriptions of trust assumptions may simply scare people with no way to act.

Moreover, we received feedback by one participant that our question conveyed a, not necessarily accurate, dichotomy between black-box systems and E2E-verifiable systems. More specifically, end-to-end-verifiable systems could also be perceived to be a version of black-box systems, since voters might also need to trust engineers who themselves defined the verification process.

Further Aspects for the Proposed Actions. The participants provided two new aspects for our given proposals and also four new proposals for actions that might lead election organizers to use end-to-end verifiable online voting systems. We describe the new aspects for the respective actions in the following.

Requirement Catalogs. Setting up requirement catalogs that demand E2E verifiability is deemed a promising measure. However, the requirements should also be defined in an understandable way to be understood by non-engineers and are hence easier to develop, even without a deep technical understanding.

Trust Level Communication. The comparison of systems on their trust levels should also specifically address how they still preserve the vote secrecy and protect against vote buying and voter intimidation. This comparison should be on a level that is understandable to the average voter without a degree in engineering.

Further Action Proposals. The participants also provided the following four new proposals to lead election organizers towards using E2E-verifiable online voting systems. In the following, the new actions are described.

Society Awareness. As much as participants assessed raising awareness to be essential, they identified that, e.g., voters rarely advocate for policies regarding specific technologies. Therefore, they considered it to be more important to raise awareness among the general society, media, other stakeholders, and political parties in general, i.e., not only those directly involved in lawmaking. This action addresses the proposals for raising awareness among voters and among lawmakers, but targets the society and media as a whole.

Cost Reduction. The development of voting systems that provide E2E-verifiability, especially with good usability, is not promoted by the market and may generally be costly. Especially as market dynamics usually prioritizes saving costs, it is sensible to reduce the development costs for such systems, for example with subsidies from official institutions, politics, or agencies.

Pilots and Demonstrations. Advertising E2E-verifiable systems can have a high impact, but also organizers or other stakeholders could get active and, e.g., do pilots and demonstrations of usable E2E-verifiable systems. This can be a first step before election organizers generally opt for such solutions. The action could be started with kiosk versions, before allowing voters to bring their own devices.

Public Auditing. Since examinations and testimony by experts typically have a great impact on the voters' trust or distrust, it might be beneficial if end-to-end-verifiable systems are publicly audited by experts. This might also lead to election organizers becoming more aware of end-to-end-verifiable systems.

6 Discussion

Our findings provide a catalog of reasons why election organizers largely opt to use opaque black-box systems for online elections and possible actions to encounter their arguments and lead them to use E2E-verifiable systems. One notable observation is that many laws on online voting systems do not provide any sensible requirements and are largely deficient. Actions to provide already a minimum of suitable requirements integrated in respective regulations and laws could already resolve arguments such as dismissing transparency requirements or avoiding justifications. Other arguments such as complicated usability or missing orientation should be encountered by actions that provide practical experiences and better comparability of available systems. Here, we received valuable proposals, e.g., to start by doing pilots and demonstrations as well as getting experts to do public audits of those systems. When such actions lead to more systems on the market, other arguments such as complex decisions and a focus on cost-efficiency could become easier to resolve. Some of the provided arguments do not specifically address voting systems, but software systems and security issues in general. Problems with software security might also become less problematic by proposed actions such as understandable requirement catalogs and raising awareness in the society and for stakeholders. For voting systems, there are actually already official recommendations, e.g., by the *Council of Europe*. However, our findings suggest that stricter requirements might be necessary. Yet, it should be noted that our survey only addressed experts. For substantiating our findings, other stakeholders such as officials, vendors, or election organizers should also be addressed specifically.

7 Conclusion

Within this paper, we addressed our hypothesis that most election organizers choose online voting systems wich are a black box for voters, even though established cryptographic mechanisms allow voters to detect potential manipulations by methods for end-to-end verifiability.

7.1 Summary

We examined the conjectures why election organizers decide on using black-box voting systems and explored actions to address them by using qualitative data analysis techniques, evaluating a specialist panel with members from official agencies, industry, and academia, and a qualitative survey with experts from program committees of the research community. Our study resulted in a list of reasons that serve as arguments for election organizers to keep using black-box voting systems, as well as recommendations on actions to lead them towards using end-to-end verifiable systems. Based on our findings, we developed recommendations for organizers to improve the current situation of online voting systems.

7.2 Outlook

This paper provides a first step toward scientifically examining the current situation of online voting systems by using qualitative data analysis techniques. However, for fostering our findings, it would be interesting to conduct quantitative studies with more participants and possibly different stakeholders, e.g., by talking to election officials. Moreover, we observed mixed results on awareness and how to raise it. For this matter, it would be interesting to establish mental models to better understand the situation regarding awareness and differences across different stakeholder groups. Finally, as we also gathered a list of recommended actions, both further evaluations should be done to substantiate those proposals and experiments should be done for actually putting them into practice, maybe first with simulations and mock-ups.

Acknowledgments. The authors would like to thank the participants in the panel discussion as well as the anonymous participants in the exploratory study.

References

1. Alvarez, R.M., Levin, I., Pomares, J., Leiras, M.: Voting made safe and easy: The impact of e-voting on citizen perceptions. Political Science Research and Methods **1**(1) (2013). https://doi.org/10.1017/psrm.2013.2
2. Beckert, B., Budurushi, J., Grunwald, A., Krimmer, R., Kulyk, O., Küsters, R., Mayer, A., Müller-Quade, J., Neumann, S., Volkamer, M.: Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen. Tech. rep., Karlsruhe Institute of Technology (KIT) (2021). https://doi.org/10.5445/IR/1000137300
3. Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y.A., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public evidence from secret ballots. In: Krimmer, R., Volkamer, M., Binder, N.B., Kersting, N., Pereira, O., Schürmann, C. (eds.) Second International Joint Conference on Electronic Voting (E-Vote-ID 2017). Lecture Notes in Computer Science, vol. 10615. Springer (2017). https://doi.org/10.1007/978-3-319-68687-5_6
4. Kersting, N., Baldersheim, H. (eds.): Electronic Voting and Democracy: A Comparative Analysis. Palgrave Macmillan (2004). https://doi.org/10.1057/9780230523531

5. Licht, N., Duenas-Cid, D., Krivonosova, I., Krimmer, R.: To i-vote or not to i-vote: Drivers and barriers to the implementation of internet voting. In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Kulyk, O., Rønne, P.B., Solvak, M., Germann, M. (eds.) 6th International Joint Conference on Electronic Voting (E-Vote-ID 2021). Lecture Notes in Computer Science, vol. 12900. Springer (2021). https://doi.org/10.1007/978-3-030-86942-7_7
6. Marky, K., Gerber, P., Günther, S., Khamis, M., Fries, M., Mühlhäuser, M.: Investigating State-of-the-Art practices for fostering subjective trust in online voting through interviews. In: 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA (2022), https://www.usenix.org/conference/usenixsecurity22/presentation/marky
7. Olembo, M.M., Bartsch, S., Volkamer, M.: Mental models of verifiability in voting. In: Heather, J., Schneider, S.A., Teague, V. (eds.) 4th International Conference on E-Voting and Identify (VoteID 2013). Lecture Notes in Computer Science, vol. 7985. Springer (2013). https://doi.org/10.1007/978-3-642-39185-9_9
8. Solvak, M.: Does vote verification work: Usage and impact of confidence building technology in internet voting. In: Krimmer, R., Volkamer, M., Beckert, B., Küsters, R., Kulyk, O., Duenas-Cid, D., Solvak, M. (eds.) 5th International Joint Conference on Electronic Voting (E-Vote-ID 2020). Lecture Notes in Computer Science, vol. 12455. Springer (2020). https://doi.org/10.1007/978-3-030-60347-2_14
9. Teague, V.: Which e-voting problems do we need to solve? In: Malkin, T., Peikert, C. (eds.) 41st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2021). Lecture Notes in Computer Science, vol. 12825. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_1
10. Zollinger, M., Distler, V., Rønne, P.B., Ryan, P.Y.A., Lallemand, C., Koenig, V.: User experience design for e-voting: How mental models align with security mechanisms. CoRR **abs/2105.14901** (2021), https://arxiv.org/abs/2105.14901
11. Zollinger, M., Estaji, E., Ryan, P.Y.A., Marky, K.: "just for the sake of transparency": Exploring voter mental models of verifiability. In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Kulyk, O., Rønne, P.B., Solvak, M., Germann, M. (eds.) 6th International Joint Conference on Electronic Voting (E-Vote-ID 2021). Lecture Notes in Computer Science, vol. 12900. Springer (2021). https://doi.org/10.1007/978-3-030-86942-7_11