# Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability

Oksana Kulyk, Melanie Volkamer

Karlsruhe Institute of Technology, Karlsruhe, Germany

**Abstract.** A well-known issue in electronic voting is the risk of manipulation of the cast vote. For countering this risk, a number of methods have been proposed that enable the voter to verify that their cast vote actually represents their intention, the so-called *cast-as-intended verification*. Yet, the empirical studies on the voter's behaviour towards using these methods show that often only a small amount of voters attempts the verification or succeeds in performing it. Poor usability of the verification procedure has been often named as the main reason for such a failure of the voters to verify. Research into human factors in other security domains, however, reveals other reasons aside from poor usability, that hinder the proper adoption of security practices among end users. In this paper we discuss these factors with respect to their applicability to cast-as-intended verification. Our results indicate, that many of these factors are potentially relevant in the electronic voting context, too. Correspondingly, we conclude that additional measures aside from ensuring the usability of the cast as intended verification mechanisms are required in order to make sure that the voters successfully verify the integrity of their votes. As such, corresponding mechanisms are proposed.

## 1 Introduction

Remote e-voting over the Internet can solve many problems. Voters from abroad are included more easily as well as voters with disabilities. Furthermore, voting from wherever Internet is available gains attraction since a polling station does not have to be visited during particular hours and day(s). Although there are many benefits, remote Internet voting channels introduce new possibilities for adversaries that aim to maliciously influence the outcome of the election directly by changing votes or indirectly by breaking vote privacy. Therefore, Internet voting systems introduce new challenges. One of these challenges is the so-called trusted platform problem: Since the voting device typically is a voter's device, e.g. computer, laptop, tablet, or smartphone, this device is beyond the control capabilities of the election authorities and of the provider of the Internet

voting system. Hence, an adversary might take control over voters' devices to maliciously manipulate the outcome of the election. Another challenge is to detect a malicious vote casting software. In this case an adversary would manipulate the vote casting software in a way that votes would be changed before storing them in the electronic ballot box.

Previous research on electronic voting resulted in numerous proposals for addressing these challenges. While some of the proposals focus on ensuring the security of the voting devices via trusted platform module [26], most of the state-of-the-art research is dedicated on proposing techniques that enable voters to verify that their vote has been sent to the voting system without being manipulated by the voting device or the vote casting software (i.e. providing *cast-as-intended verifiability*). These proposals include cryptographic protocols, as well as ready-to-use implementations of corresponding cryptographic protocols within deployed voting systems. However, even if the system provides the possibility to verify that the voters' choices have been encoded correctly, it is not guaranteed that voters actually make use of this functionality. In particular, the available statistics of elections using Internet voting systems demonstrate that a very small percentage of all voters actually verifies [4, 10]. One of the reasons for such a low number is the fact that verifying is not usable enough, too complicated, and confusing for the voters.

Outside of electronic voting, the research of human factors in security mechanisms has identified and studied various factors besides the usability of security mechanisms that prevent users from protecting their security and privacy by applying corresponding mechanisms. Whether these factors are applicable for verifying votes has not been considered in electronic voting research, yet. Thus, the goal of this paper is to analyze whether selected human factors identified for security mechanisms in general, are applicable for the security mechanism 'cast as intended' verification. We focus on the following directions:

**General factors:** We discuss the relevance of corresponding factors such as lack of awareness risks identified for security and privacy mechanism in [27]. We decided to go for this paper as the factors are identified based on an interview study and a literature review. We discuss the applicability of their factors for cast as intended verification.

**Psychological factors related to social engineering attacks:** We discuss the factors identified for success of social engineering attacks in other cyber security contexts, i.e. the adversary relying on the victim's tendencies to obey the authority. In our discussion we rely on [31]. The authors derived factors via an empirical study.

**Attacks focusing on the user interfaces:** We discuss how an adversary can modify interfaces in a way that the security mechanism disappears or gets very un-usable.

We show, that most of these factors are applicable for 'cast as intended verifiability'. As such, while the usability of the proposed solutions plays an important role, other factors such as the lack of awareness of security threats need to be addressed. Furthermore, we discuss the implications from these findings for the future of electronic voting.

## 2 Background and Related Work

In this section, we describe previous work on cast-as-intended verification methods and the research on human factors in the verification.

### 2.1 Methods for Cast-as-Intended Verification

A number of methods for cast-as-intended verification have been proposed in the literature. The most prominent examples of methods used in voting systems are as follows (see also [8] for a more detailed taxonomy):

**Decryption-Based:** In order to verify that her vote was encrypted and cast correctly, the voter uses a second device (the so-called verifier) such as a smartphone. The randomness used for encrypting the vote is transferred from the voting device to the verifier. The verifier uses the randomness to encrypt each one of the available voting options and compare the resulting ciphertexts with the encrypted vote sent to the voting server. As soon as the match is identified for one of the voting options, the verifier outputs the corresponding voting option to the voter, who in turn verifies that the option matches her intent. This approach, in particular, is used in the Estonian system [9].

**Challenge-or-Cast:** A variant of the decryption-based method, the challenge-or-cast verification also requires using an external verifier, which is either a second device [19], a website of the trusted institution [19] or software running on the voter's device [2]. The main difference to the decryption-based approach is that after the vote is encrypted and the encrypted vote is output to the voter, the voter chooses either to cast it or to challenge the voting system. In case the voter chooses to challenge, the randomness and the chosen voting option are transferred to the verifier. The verifier encrypts the voting option using the randomness and outputs the resulting ciphertext to the voter, who finally has to compare the

ciphertext with the encrypted vote output by the voting client. Once challenged, the vote cannot be cast, and the voter has to start the vote casting process again. The challenge-or-cast approach is used in the Helios system [2].

**Return Codes:** In this approach the verification relies on code sheets, distributed to the voter via an out of band channel (e.g. traditional mail), see e.g. [5]. The code sheets contain a list of voting options with a unique code assigned to each option. After casting the vote, the voting system outputs a so-called return code, which the voter has to compare with the code on their code sheet for their chosen option. This approach, in particular, is used in the Neuchatel voting system [7].

### 2.2 Human Factors in Cast-as-Intended Verifiability

A number of works explore the human factors involved in the cast-as-intended verification. These works, in particular, focus on the following research questions: whether the verification process itself is effective (i.e. whether the voters are capable of performing the verification if they choose to do so), and whether the mental models of the voters are accurate (i.e. whether the voters understand the concept of verification well enough to be motivated to verify). The usability in terms of effectiveness of the cast-as-intended verification has been the focus of various studies. As such, the study in [6] evaluated the usability of the Norwegian Internet Voting system, identifying usability shortcomings in the verification process. Similarly, the usability of cast-as-intended verification in the Helios voting system has been evaluated in several studies [1, 11, 15, 29], revealing that many of the study participants were not able to perform the verification successfully. Various modifications of the verification process in Helios have furthermore been investigated via a user study [15], revealing that although these modifications managed to improve the usability of the original proposal, further problems remain that prevent the participants from successfully verifying. The studies conducted by Acemyan et al. [1] furthermore evaluated the usability of the Pret a Voter and Scantegrity II voting systems, concluding that the usability of the verification in these systems was poor as well. The usability of various approaches for cast-as-intended verifiability has been investigated by Marky et al. [16] via an expert evaluation approach based on cognitive walkthrough method. The investigation revealed a number of assumptions on voter capabilities, such as the ability of the voters to compare random-looking strings of characters, cruical for ensuring the security of the investigated approaches. Other studies focused on the mental models of voters regarding verifiability

in electronic voting. As such, the study of Olembo et al. [22] identified five groups of mental models (Trusting, No Knowledge, Observer, Personal Involvement and Matching), revealing that the voter's understanding of verifiability is often lacking and thus preventing the voters from performing the verification. The follow-up study [21] furthermore evaluated the effect of diverse messages in motivating the voters to verify, revealing further misconceptions regarding the verification process, prevalent among the voters and preventing them from verifying, such as beliefs that their experience as a computer user is enough to protect against possible vote manipulation. Further misconceptions prevalent among the voters regarding the verification were revealed by the study of Schneider et al. [23], i.e. the belief that the verification is only needed to safeguard against voter's own mistakes (such as accidentally choosing the wrong candidate) as opposed to malicious vote manipulation.

## 3 General Factors

The factors preventing end users from adopting secure behaviour and from using available solutions for security and privacy protection have been investigated in various contexts, such as smartphones [27] or password managers [3]. These works have shown, that while many of the investigated solutions lack in usability, there are other factors no less important for end user to adopt these solutions. As a systematization of these factors, a model has been proposed by Volkamer et al. [27], distinguishing between the different factors that the developers of security mechanisms need to address. These factors are: *lack of awareness*, *lack of concern*, *lack of self-efficacy*, *lack of compulsion* and *lack of perseverance*. In this section, we elaborate on each factor and its possible implications in the electronic voting context for cast-as-intended verification.

### 3.1 Lack of Awareness

According to [27], many users don't see a need to use security mechanisms simply because they are unaware of potential risks in general and specific attacks related to the corresponding mechanism.

This factor is likely to influence the likelihood that voters use the cast as intended verification mechanisms: Voters might be simply unaware of possible risks of vote manipulation that the cast as intended verification mechanism can protect against. As far as we are aware of, neither mass media nor election organizers communicate such risks. While a lot of

recent media attention has been dedicated to the potential manipulations of election results with means of cyber warfare (see e.g. [33]), the discussion focused on the manipulation of components of the voting system in controlled environment, e.g. the voting machines at the polling place. The dangers to the manipulation of the vote casting software on voters' individual devices, however, has not been the focus of attention. On the opposite, several studies on voters' perception of verifiability in electronic voting [22, 23] have shown that participants' first thought is that the election management boards are responsible to select a 'secure' system and prevent manipulations. Thus, unless the voters understand the inherent necessity of verifiability for the security of voting systems, it is not very likely that they actually verify their vote.

### 3.2 Lack of Concern

The next identified factor is the perception regarding security and privacy risks, that while people are aware in general that these risks exist, they do not present a great concern for them personally. For instance, they are aware of phishing attacks in general but are not concerned that a phisher may attack them personally. As such, the users tend to believe, that (1) they are not important enough to become a target of the adversary, or that (2) e.g. they have nothing to hide, therefore, they should not be concerned if someone hacks into their phone. The lack of concern of end users is often misguided due to underestimating the value of personal data and overestimating the effort from hackers or service providers required to collect it or install malware, and it can – at least partially – be rationally explained: Indeed, it is not unreasonable to assume that the private communication of regular citizens is of less interest to hackers, than the private communication of high-profile politicians .

So in case of the trusted device problem, one should be careful in explaining this problem to voters. In case it is purely that voters' devices might have malware installed (not necessary for the election, but in general), the 'lack of concern' factor might be applicable for electronic voting, too. Voters might consider them as not important enough that someone installs malware on their device in general. Some of the voters therefore might conclude, that the probability of them becoming a victim of the hacker attack is low. As a consequence they are not very likely to apply cast as intended verification mechanisms.

If voters are made aware that it is important to verify to make sure their vote cannot be manipulated (using voting specific attacks) without the manipulation being detected, the applicability of the 'lack of concern'

factor depends on voters' understanding of demographic elections. In democratic societies, the value of each vote counts equally[1], therefore, any citizen is equally likely to be targeted for vote manipulation, regardless of their social status. It is therefore reasonable to assume that the importance of one's vote is self-evident to many of those who choose to participate in the election (otherwise they would abstain)[2].

### 3.3 Lack of Self-Efficacy

The next identified factor that prevents users from adopting these solutions is the non-accessibility of the security mechanisms. As such, while the users might be aware about the risks to their security and privacy and even be concerned about the corresponding threats, they don't apply corresponding security mechanisms as they have only an abstract idea about the security mechanisms and as such (1) either consider them as being to complex for them to be used or (2) as being too ineffective (2a) against really powerful players like Google or national security agencies, or (2b) as they still need to relay on third parties taking care of their security duties (thus feeling helpless). Thus, users without technical knowledge do not have the confidence that they can apply these countermeasures effectively and/ore that the measures they can take only slightly increase the security. As a consequence they don't use the security mechanisms.

The 'lack of self-efficacy' is also applicable for the voting context and in particular for the cast as intended verification mechanisms: Voters' might not properly be aware of the mechanisms as such, they might consider it as too complicated and being afraid that they cannot properly apply it. The complexity of the verification process can furthermore discourage the voters from verifying. As shown in Section 2, it is well-known that many of the existing voting systems fail to provide such simplicity, hence, the voters might feel overwhelmed even before they attempt the verification.

Furthermore, they may consider the mechanisms as too ineffective as taking the steps is useless if others are not taken by the voting system company, the election management boards, and the crypto experts who for instance take care of other verification issues including eligibility verification as well as the system's availability. Furthermore, voters may

[1] While there might be inequalities between the weight votes from different districts in some political systems, e.g. via so-called gerrymandering, the equality still holds among the voters within a district.

[2] Note, however, that the issue might be less clear within the countries that have mandatory voting, as some voters might vote in order to avoid penalty rather than believing that their vote has an effect on society.

consider the mechanisms as useless as the cast as intended mechanism might not offer protection against a very powerful adversary (e.g. the one who can break the cryptography behind the method, or corrupt both the voter and the verification device). They might not see that the mechanisms still provide a level of security sufficient for many cases.

### 3.4 Lack of Compulsion

Lack of compulsion has been identified as another factor in preventing the adoption of security mechanisms: Even if the users recognise that there is some value in these mechanisms, this perceived value is still outweighed by the costs of adopting the mechanisms, such as time, effort, but also possible financial costs. For example, inconvenience caused by these mechanisms, e.g. by having to input the password in order to unlock the smartphone each time one wants to use it, or the performance drop caused by installing an antivirus, have been commonly named by the users who decided against using these protection measures.

With respect to the applicability of this factor for cast-as-intended verification mechanisms, it is important to mention that elections don't happen too often, even in countries with relatively frequent elections such as Switzerland. Even if there are elections every three months this is not as often as unlocking a smartphone. So time might on the one hand not play such an important role. On the other hand most people when thinking of casting their vote online, think of a simple solution such as logging in, selecting a candidate, confirming the candidate and that's it, compared to shopping online. These issues were shown by previous studies to be prevalent among existing voting systems, as described in Section 2. Such mental models about vote casting processes make the factor 'lack of compulsion' applicable for cast as intended verification mechanisms in particular in cases the steps should be repeated several times as required with the Benaloh Challenge. However, previous studies show that the voters would be ready to use systems that require more time and effort from the voter for both vote casting and verifying, if these systems provide a higher level of security and this higher level of security is made transparent to them [13]. What has not been studied – to the best of our knowledge – whether voters would be willing to take any costs for verifying (e.g. a special device).

### 3.5 Lack of Perseverance

The last identified factor addresses the lack of perseverance: i.e., even among the users who are generally willing to adopt more secure behaviour, many still get side-tracked and therefore fail to make such behaviour as long-term habit in their daily life. One of the named reasons in the security context is the fear of social pressure and of appearing paranoid by paying too much attention to security.

As the verification procedure is meant to be performed by each voter on her own, one can presume that the social pressure aspects are less likely to play a role in the voters' desire to verify their votes. Yet, if the attitude prevalent in the society is that the verification option only exists to appease the minority of most concerned voters, and the rest do not need to verify – an attitude which presence was confirmed by previous studies [23] – this could negatively affect the voters desire to verify.

## 4 Psychological Factors

In the field of security, a number of attacks have arised, that aim to 'manipulate' the end users or administrators via deception techniques known as social engineering. The previous research by Workman [31, 32] identifies the following psychological factors contributing to the success of such attacks: *trust*, *normative commitment*, *continuance commitment*, *affective commitment* and *obedience of authority*. In this section, we briefly explain the identified psychological factors and discuss their applicability in the context of cast as intended verification to execute corresponding social engineering attacks.

### 4.1 Trust

The first psychological factor is the willingness of users to trust: Many of the attacks relying on social engineering exploit the general willingness of the user to trust. As such, the adversary attempts to appear trustworthy to their victims, for example, by pretending to be someone from their social circle, so that the victim would comply with the attacker's request, such as granting the adversary access to the system.

In the context of electronic voting, trust would be gained in case the adversary spoofs the email address of either the election management board, the party the candidate is a member of or in favour of, or some other parties being officially involved in the process such as the vendors, international observers, or the security experts. Having this in mind very

easy deployable social engineering attacks are of interests, i.e. sending so called phishing emails reminding people to vote but including the slightly change URL in the email. Depending on the voting system in place the phisher would be successful with this approach or not. It is most likely that this approach is only successful in combination with others (see e.g. Section 5).

The willingness of the voters to trust the adversary can be particularly exploited in the systems that rely on external verifiers. Such systems, in particular, include either explicitly delegating the verification to a third trusted party [19, 24], or letting the voter to choose and install the verification software from such a party [19]. In case an adversary manages to masquerade themselves as a trusted third-party to the voters, they can subvert the verification of these voters. Thus, the voter believes to verify with the support of a trustworthy party but actually the verifier is not trustworthy. Actually, in this case voters would adopt the mechanisms but it would not mean that their vote cannot be altered.

### 4.2 Normative Commitment

The second identified factor is called 'normative commitment'. The social engineering attacks exploiting normative commitments rely on the person's feeling of obligation towards the attacker, for example, by offering a pay-off to the victim in exchange for a favor for the attacker, e.g. as part of a game to see whether people provide passwords for a chocolate bar.

In the context of electronic voting, an example of attacks relying on normative commitment would be vote buying. It remains, however, an open question, whether social engineering attacks exploiting the normative commitment factor in the context of verification specifically are possible. It looks like, this factor is not an issue for the adoption of cast as intended verification.

### 4.3 Continuance Commitment

The attacks exploiting the continuance commitment factors, according to [31], rely on the costs and benefits of an action as perceived by the victims. As such, these attacks aim to persuade the victims, that the effort required to take precautionary security measures (a) outweighs the risks that these measures are designed to protect against and (b) in particular because taking security measures comes with increased privacy risks.

In the context of electronic voting, the attacker might want to exploit the fact, that the verification procedures require additional effort from

the voters, and persuade the voters into not verifying by downplaying the risks of vote manipulation. As such, the attacker might convince the voters that the voting system is trustworthy enough without the need of additional verification, or that there is no need to verify for each voter and it is enough that the security experts do verify. The question here is how to distribute this information. The success rate clearly depends on the measures taken to make sure voters understand the importance of the cast as intended verification mechanism.

Another measure the adversary can take is hyperbolising the costs of the verification to the voters. As such, the attacker can rely on lack of voters' knowledge about the security properties of the verification procedure and convince the voters that performing this procedure leads to certain security risks. An example of such an attack would be convincing the voters that as soon as they verify, the voting system will know how they voted, leading to loss or decreasing the level of vote privacy. Not having a cryptography background makes it likely to believe in this. For example, in case the return codes are used for the verification, the voter might think that it is impossible for the system to output the right return code without knowing how the voter has voted. With challenge-or-cast verification which uses an external verifier, the voter might think that the verifier knows the option chosen by the voter, without realising that only the challenged vote (which might be different from the actual cast vote) is revealed to the verifier.

### 4.4 Affective Commitment

Attacks exploiting affective commitment rely on the feeling of emotional ties of the victim with the group the attacker claims to represent. Such attacks, in particular, can be performed via social networks, whereby the attacker might try to pretend to be someone connected to the victim's social circle and persuade the victim into divulging private information.

In the context of electronic voting, the attacker might try to exploit the positive attitudes of the voters towards the groups that advocate using the proposed voting system, such as the state or the political parties who proclaim themselves to be in favor of electronic voting. In such a scenario, an adversary might manage to convince the voters that they do not need to verify their vote, since they do not doubt the integrity of the system. Such attacks can be particularly successful if the voters who choose to cast their vote electronically already tend to have more trust in the government than the voters who prefer more traditional means – a correlation that has been supported by some of the previous studies [18].

### 4.5 Obedience of Authority

Many of the social engineering attacks involve the attacker taking the role of the person of authority to the victim, with the goal to make the victim to comply to the attacker's requests.

In the context of electronic voting, attacks exploiting the voters' obedience towards authority would be based on voter coercion, e.g. as threats from an authority figure to vote in a specific way. It is, however, to be determined, to which extent the verification process can be targeted.

## 5 Attacks Focusing on the User Interfaces

Providing means for cast-as-intended verification, implementing them via usable interfaces and addressing the above mentioned factors, however, is not sufficient for reliable election results. Even if the original interfaces are usable, an adversary could manipulate them in a malicious way in order to prevent the voter to carry out verification successfully. These attacks can exploit two possibilities: modifying the design of the verification interface, or modifying the verification process as displayed to the voter.

*Modifying the Design.* Poor usability of the design of the verification can lead to voters failing to perform the verification, for example, by not knowing which button to click, as shown by previous studies [11, 15]. As such, a number of heuristics for developing usable interfaces has been developed, in the field of human-computer interaction in general [20] (e.g. providing sufficient feedback and status information to the user), as well as in security context specifically [14] (e.g. presenting the security-relevant information in an abstract way instead of confronting the user with technical descriptions). Following these heuristics, hence, the developers of voting system interfaces can potentially improve the voters' capabilities for performing the verification successfully and reduce the time and effort required from the voters to do so. On the other hand, an adversary controlling the voting software can modify interfaces in the opposite direction, deliberately making the verification non-usable, for example, by making the important elements on the web page less visible to the voters or even blocking them entirely. Such an attack would be unnoticed by the voters, unless they had the chance to familiarise themselves with the interfaces earlier.

*Modifying the Procedure.* In case the voters are not aware of the proper verification procedure, an adversary might use this lack of knowledge

and alter the procedure. This concerns the steps after a voter chooses to verify. As such, in systems that require the voter to explicitly start the verification (e.g. Helios), the adversary could display a success message direct after the voter clicks on the "Verify-"Button. In case the voter does not know what to expect, she would assume a successful verification procedure although, she has not verified at all. A similar attack can be conducted on the systems that integrate the verification into the vote casting process, namely, the systems based on return codes. As such, an adversary can display a finalization message directly after vote casting. If the voter does not know that a return code is expected, they would not perform the verification.

## 6 General Discussion and Conclusion

In this section we describe the implication of the results from the previous chapters, proposing countermeasures to adress the derived factors and outlining further possible directions of future work.

### 6.1 Countermeasures

The presented research in human factors in security shows clearly, even if the voting system provides means for cast-as-intended verifiability and the steps are even usable, a number of factors can prevent voters from verifying. Hence, measures for addressing these factors should be taken. We describe the necessary steps in this section and discuss possible consequences of applying these steps. An overview of the proposed countermeasures and the factors they address is provided on Figure 1.

*Raising Awareness for Risks and the Verification Procedures to Mitigate the Risks.* As shown in Section 3.1, the voters' lack of awareness of possible vote manipulation can prevent them from verifying their vote. Furthermore, as shown in Section 4.3 an adversary can try to deliberately downplay the risks, thus convincing the voters that the verification is not necessary. Hence, measures should be taken to ensure that the voters are aware about the possibility of vote manipulation via compromised voting client software or vote casting platform.

Note, confronting the voters with the risks of manipulated votes and the fact that only by verifying, these risks can be mitigated effectively, a plausible reaction would be that this particular electronic voting system should not be used and the election management board should only use a

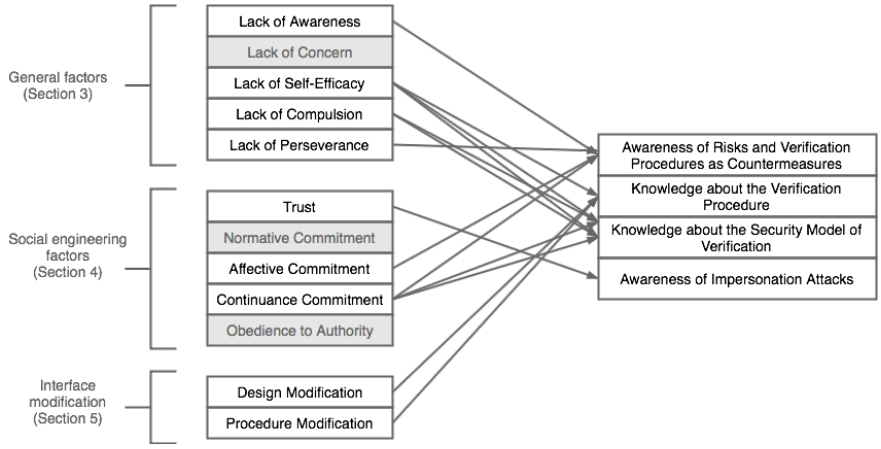


**Fig. 1.** The countermeasures addressing the factors outlined in Sections 3 to 5. The factors with questionable relevance for the electronic voting context are greyed out.

system which is secure enough without making voters taking care of its security. Thus, it might also be necessary to make voters aware that it is impossible to have a voting system, including paper-based voting, which is totally free of the vote manipulation risk. On the other hand, verifiability has been identified as a measure to increase trust in the voting system in previous research [25, 28]. Furthermore, empiricial studies show that the voters who are concerned about the security of electronic voting would be more willing to trust the system if it provides verifiability possibilities such as personalised codes on each ballot (note that other commonly used approaches for cast-as-intended verifiability were not mentioned in the study) [17]. Hence, further investigations on the reactions of voters once they are made aware of risks of manipulating votes and corresponding verifiability countermeasures are needed.

The knowledge of security provided by the verification can furthermore be helpful to offset the potential usability problems of the verification. In the current state of research, verification procedure requires extra steps from the voter. As discussed in previous chapters, this additional effort becomes a danger if it prevents the voters from verifying, either because they are generally unwilling to dedicate too much effort (Section 3.4), or actively discouraged by the adversary to do so (Section 4.3). While the time and effort required for the verification can sometimes be minimized via usability improvements, often the additional steps in the verification are are inevitable in order to ensure the security of the verification. As mentioned in Section 3.4, previous studies show that the voters are ready

to accept the additional effort if they understand the security benefits it brings. Hence, while generally the verification processes should be designed to be as efficient as possible, an appropriate trade-off with security should be carefully considered and communicated to the voters.

Furthermore, as discussed in Section 3.5, the perception of the society, that the verification is unnecessary unless one is particularly concerned about the risks of vote manipulation, can hinder the voters' readiness to verify. As discussed in Section 4.4, the adversary can exploit such a societal attitude by persuading the voter, that as long as they are willing to trust the government or the groups in favor of introducing electronic voting, they should not verify. It is therefore important to ensure, that the voters understand the general importance of verification as a stepstone into ensuring the integrity of democratic institutions without perceiving the need to verify as mistrust in the institutions.

*Educating about Procedure.* Once they are aware of the need of verifiability and the need for them to take actions it is necessary to explain the procedure to them (in order to increase the level of self-efficacy, see Section 3.3. However, they should know that one possible adversary strategy is to modify the interfaces to make it less likely that voters verify (Section 5). They should know whom to contact in case they detect a modification.

*Explaining Security Model.* The voter's lack of knowledge about the security that the verification provides can furthermore hinder them from verifying, if they believe that the verification is either futile or dangerous (see Section 4.3). Hence, education measures are needed that explain the security model of the verification and address potential misconceptions .

*Raise Awareness of Impersonation Attacks.* It is furthermore important to make voters aware of possible social engineering attacks that involve the adversary impersonating a trustworthy entity to the voter (see Section 4.1). As such, the voter should be able to detect whether their communication with the voting system is genuine. If the voter have the option to select a trusted third party to perform the verification on their behalf, the trustworthiness of such a party should be clearly communicated to them, ideally with an option to validate it from an independent source. For this, further research into trust communication is required.

### 6.2 Future Work

While ensuring cast-as-intended verifiability is a crucial step towards the security of electronic voting, it is not enough to prevent election

manipulation on its own. As such, measures towards protecting against server-side attacks have to be implemented, which is, however, out of scope of this work.

The factors and countermeasures outlined in the paper focus on the voters who are generally willing to follow the voting protocol, or at least do not actively try to violate it. Hence, we did not consider the issue of vote buying, where the adversary does not try to deceive a law-abiding voter, but the voter willingly collaborates with the adversary instead. As the issue of vote buying is crucial in electronic voting, particularly, in remote voting, we consider the consideration of vote buying from a human-centered perspective an important part of future work.

As consider the cast-as-intended verifiability in Internet voting, while some of our results are likely to be transferred to other channels of electronic voting, the specific scenarios, such as polling-place voting machines, remain the topic for the future work. Furthermore, as the security of electronic voting and paper-based voting (polling place or postal) has been the topic of previous research [12, 30], it would also be possible to compare the security issues related to human factor and voter verifiability between these two voting channels.

## References


1. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Usability of voter verifiable, end-to-end voting systems: Baseline data for helios, prêt à voter, and scantegrity ii. The USENIX Journal of Election Technology and Systems 2(3), 26–56 (2014)
2. Adida, B.: Helios: Web-based open-audit voting. In: USENIX security symposium. vol. 17, pp. 335–348. USENIX Association (2008)
3. Alkaldi, N., Renaud, K.: Why do people adopt, or reject, smartphone password managers? In: 1st European Workshop on Usable Security (EuroUSEC) (2016)
4. Brightwell, I., Cucurull, J., Galindo, D., Guasch, S.: An overview of the ivote 2015 voting system. Tech. rep. New South Wales Electoral Commission (2015)
5. Budurushi, J., Neumann, S., Olembo, M.M., Volkamer, M.: Pretty understandable democracy-a secure and understandable internet voting scheme. In: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. pp. 198–207. IEEE (2013)
6. Fuglerud, K.S., Røssvoll, T.H.: An evaluation of web-based voting usability and accessibility. Universal Access in the Information Society 11(4), 359–373 (2012)
7. Galindo, D., Guasch, S., Puiggali, J.: 2015 neuchâtel's cast-as-intended verification mechanism. In: VoteID 2015: 5th International Conference on E-Voting and Identity. pp. 3–18. Springer (Sep 2015)
8. Guasch Castelló, S.: Individual Verifiability in Electronic Voting. Ph.D. thesis, Universitat Politécnica de Catalunya (2016)
9. Heiberg, S., Martens, T., Vinkel, P., Willemson, J.: Improving the verifiability of the estonian internet voting scheme. In: International Joint Conference on Electronic Voting. pp. 92–107. Springer (2016)

10. Heiberg, S., Parsovs, A., Willemson, J.: Log analysis of estonian internet voting 2013–2014. In: International Conference on E-Voting and Identity. pp. 19–34. Springer (2015)
11. Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability analysis of helios-an open source verifiable remote electronic voting system. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections EVT/WOTE '11 (2011)
12. Krimmer, R., Volkamer, M.: Bits or paper? comparing remote electronic voting to postal voting. In: EGOV (Workshops and Posters). pp. 225–232 (2005)
13. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: How much usability can you sacrifice for security? IEEE Security & Privacy 15(3), 24–29 (2017)
14. tom Markotten, D.G.: User-centered security engineering. In: Proceedings of the 4th EurOpen/USENIX Conference–NordU2002 (2002)
15. Marky, K., Kulyk, O., Renaud, K., Volkamer, M.: What did i really vote for? In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. p. 176. ACM (2018)
16. Marky, K., Kulyk, O., Volkamer, M.: Comparative usability evaluation of cast-as-intended verification approaches in internet voting. In: SICHERHEIT 2018. pp. 197–208. Gesellschaft für Informatik e.V. (2018)
17. Milic, T., McArdle, M., Serdült, U.: Haltungen und bedürfnisse der schweizer bevölkerung zu e-voting. Tech. rep., Aarau: Zentrum für Demokratie Aarau (2016), https://doi.org/10.5167/uzh-127938
18. Nemeslaki, A., Aranyossy, M., Sasvári, P.: Could on-line voting boost desire to vote?–technology acceptance perceptions of young hungarian citizens. Government Information Quarterly 33(4), 705–714 (2016)
19. Neumann, S., Olembo, M.M., Renaud, K., Volkamer, M.: Helios verification: To alleviate, or to nominate: Is that the question, or shall we have both? In: International Conference on Electronic Government and the Information Systems Perspective. pp. 246–260. Springer (2014)
20. Nielsen, J.: Enhancing the explanatory power of usability heuristics. In: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. pp. 152–158. ACM (1994)
21. Olembo, M.M., Renaud, K., Bartsch, S., Volkamer, M.: Voter, what message will motivate you to verify your vote. In: Workshop on Usable Security, USEC (2014)
22. Olembo, M.M., Bartsch, S., Volkamer, M.: Mental models of verifiability in voting. In: International Conference on E-Voting and Identity. pp. 142–155. Springer (2013)
23. Schneider, S., Llewellyn, M., Culnane, C., Heather, J., Srinivasan, S., Xia, Z.: Focus group views on pret a voter 1.0. In: Requirements Engineering for Electronic Voting Systems (REVOTE), 2011 International Workshop on. pp. 56–65. IEEE (2011)
24. Simpson, R., Storer, T.: Third-party verifiable voting systems: Addressing motivation and incentives in e-voting. Journal of Information Security and Applications (2017)
25. Spycher, O., Volkamer, M., Koenig, R.: Transparency and technical measures to establish trust in norwegian internet voting. In: International Conference on E-Voting and Identity. pp. 19–35. Springer (2011)
26. Volkamer, M., Alkassar, A., Sadeghi, A.R., Schulz, S.: Enabling the application of open systems like pcs for online voting. In: Proc. of Workshop on Frontiers in Electronic Elections (2006)
27. Volkamer, M., Renaud, K., Kulyk, O., Emeröz, S.: A socio-technical investigation into smartphone security. In: International Workshop on Security and Trust Management. pp. 265–273. Springer (2015)

28. Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. pp. 1–10. ACM (2011)
29. Weber, J.L., Hengartner, U.: Usability study of the open audit voting system helios. http://www.jannaweber.com/wpcontent/ uploads/2009/09/858Helios.pdf (2009)
30. Willemson, J.: Bits or paper: Which should get to carry your vote? Journal of Information Security and Applications 38, 124–131 (2018)
31. Workman, M.: Gaining access with social engineering: An empirical study of the threat. Information Systems Security 16(6), 315–331 (2007)
32. Workman, M.: Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the Association for Information Science and Technology 59(4), 662–674 (2008)
33. Zetter, K.: The myth of the hacker-proof voting machine. https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html (2018), online; accessed: 15-May-2018