Paper Audit Trails and Voters' Privacy Concerns

Jurlind Budurushi, Simon Stockhardt, Marcel Woide, and Melanie Volkamer

TU Darmstadt / CASED
name.surname@cased.de

Abstract. Advances in information technology have simplified many processes in our lives. However, in many cases trust issues arise when new technology is introduced, and voting is one prominent example. To increase voters' trust, current e-voting systems provide paper audit trails (PATs) which enable automatic tally and/or manual audit of the election result. PATs may contain only the encrypted vote or the plaintext vote in human-readable and/or machine-readable format. Previous studies report voter privacy concerns with PATs containing additional information (e.g. QR-Codes) other than the human-readable plaintext vote. However, omitting such PATs negatively influences security and/or efficiency. Hence, to address these concerns we applied the coping and threat appraisal principles of the protection motivation theory in the communication process. We evaluated them in separate surveys focused on the EasyVote system [15]. Results show that the coping appraisal is more promising than the threat appraisal approach. While our findings provide novel directions on addressing privacy concerns in the e-voting context, corresponding limitations need to be considered for future user studies.

Keywords: electronic voting, paper audit trails, privacy, user study

1 Introduction

The introduction and the continuous advances in information technology have simplified many processes in our lives, for example traveling has become much easier because of navigation systems. Recently, voting has also joined the family of the processes improved by information technology, as a large number of electronic voting systems have been proposed and are already in use for legally binding polling station elections, for instance in the US. However, in many cases (including voting) trust issues arise when new technology is introduced. In order to increase voters' trust and detect malicious voting systems, many of these proposals provide voters with paper audit trails (PATs) of their cast votes. PATs are used for tallying and/or auditing the election result and remain in a ballot box in the polling station.[1] PATs differ from system to system and they may

[1] For example, in [5] and [6] voters can take copies of their PATs and audit the election result independent form time and place.

contain: only the encrypted vote [5], the encrypted permutation of candidates together with the position of the selected candidate [6], the plaintext vote in a human-readable format [17], or the plaintext vote in a human-readable and a machine-readable (e.g. QR-Code [14] and [15], or RFID chip [16]) format.

Beside enabling the detection of malicious voting systems, PATs also enable an automatic tallying of cast votes. Thus, less time and human resources are required. However, previous studies [3] and [10] report that voters have concerns regarding vote secrecy, when PATs with additional information (e.g. encryption of the vote or a QR-Code that encodes the plaintext vote) other than the plaintext vote are used. Voters are concerned that this information might reveal their selections, i.e. voters believe that the encryption helps others to guess their selections, or that the QR-Code contains a time stamp of their cast vote. Hence, enabling voters to verify (i.e. detect a malicious voting system), decreases their trust regarding vote secrecy.

Refraining from PATs with additional information is not in the interest of security and/or efficiency, therefore our goal is to identify an adequate approach to address these concerns. In order to achieve our goal, we use the protection motivation theory [12] as the underlying theoretical foundation. Thereby, we focus on its two key principles, namely the coping and the threat appraisal. Respectively, we developed two approaches: The first approach, which is based on the coping appraisal, provides a technical solution. While based on the threat appraisal, the second approach describes the necessary effort an attacker needs in order to violate vote secrecy. We evaluated both approaches in a user study with two online surveys, and focused on the EasyVote system proposed by Volkamer et al. [15]. We report the findings from our user study and analyzed the impact of both approaches regarding voters' privacy concerns. The coping appraisal approach is more promising than the threat appraisal approach. However, the two approaches provide new and important insights into addressing voters' privacy concerns and how these concerns can be positively influenced (decreased) to increase voters' trust regarding new voting technology.

This work is structured as follows: In section 2 we briefly introduce the EasyVote system. Section 3 provides an overview of voters' privacy concerns reported in previous studies. Section 4 presents the methodology and describes the design of the user study. In section 5 we present the results. Section 6 summarizes our findings and provides directions for future research.

2 The EasyVote Voting System

The EasyVote system proposed by Volkamer et al. [15] focuses on voting challenges introduced by complex ballots and voting rules, e.g., some local elections in Germany or parliamentary elections in Belgium. Many other electronic voting systems, for example [2], [4], [14] and [16], are based on the same general concepts. We only describe here the voting phase, and omit the description of the tallying phase which is beyond the scope of this paper.

Voting phase. The voter first identifies herself to the poll workers, similar to traditional paper-based system. Afterwards, the voter enters the voting booth and uses the electronic voting device to prepare her ballot. When the voter confirms her selections, the electronic voting device starts the printing process and all electronic data are deleted, i.e. all voter's selections.[2] The printout (PAT), which contains voter's selections, consists of two parts: a human-readable and a machine-readable (a QR-Code) part, see Figure 1.[3] The voter verifies that the human-readable part contains the made on the electronic voting device. Finally, the voter leaves the voting booth and deposits the folded printout into the ballot box.

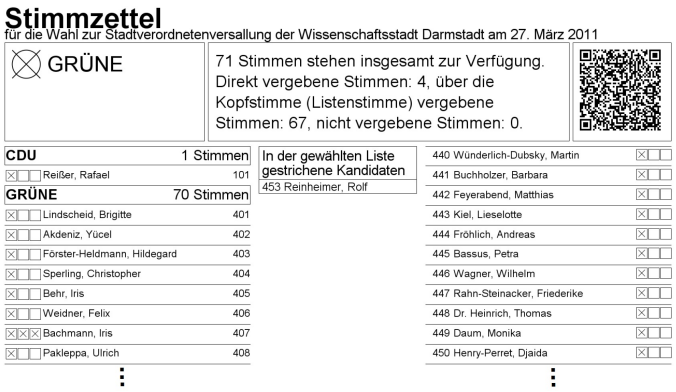

Fig. 1. The EasyVote paper ballot (printout/PAT).

3 Privacy Concerns in previous Studies

The studies conducted by Budurushi et al. [3] and Llewellyn et al. [10] showed that voters have concerns regarding privacy of their votes, when PATs containing information other than the plaintext vote are used [3] and [10]. Llewellyn et al. [10] conducted a user study at the University of Surrey, UK in June/July 2011. The user study was repeated five times. In each repetition, which consisted of six sequentially rounds, took part 12 different participants. The electronic voting system used in the user study implemented the system proposed by Ryan et al. [11]. The goal of this user study was to evaluate voters' understanding regarding privacy of the vote and the subsequent impact on verifiable voting

[2] Note that here voter's selections are deleted from the vote casting software, i.e. on the software level.

[3] The machine-readable part (the QR-Code) contains the exact information as the human-readable part and enables an automatic tallying of the printouts. Further, if two voters select the same candidates the QR-Codes are identical.

technologies. In the user study participants cast a vote in a fictitious election, and were additionally required to select on the ballot (receipt) whether they wish to "post" their receipt (anonymously) on the bulletin board. Afterwards, participants (including themselves) attempted to guess the selection of every participant, independent whether or not that participant published her receipt. Participants who chose to post their receipts received a reward of £1. Further, for each correct guess the participant received a reward of £.50 and lost an amount of £.50 for every participant who correctly guessed her selection. The economic incentives revealed participants' understanding of the security mechanisms, i.e. privacy of the vote. Thus, in case a participant was confident that the receipt does not reveal any information on her selection, she would always post her ballot in each and every round. Otherwise, she would not publish her receipt. In the study 23 out of 60 participants did not post their receipts in at least one round, i.e. were concerned regarding privacy of the vote.

Budurushi et al. [3] report about the results of a test election, which was combined with an exit survey and took place alongside the university elections at Technische Universität Darmstadt in June 2013. The electronic voting system used in the user study implemented the EasyVote system proposed by Volkamer et al. [15]. The general goals of this study were: 1) To evaluate the system from a technical and practical perspective; 2) To find out participants' (voters) perception regarding privacy of the vote. In order to measure participants' perception with respect to privacy, of the vote, the exit survey contained two specific items: First, the statement, "I think that vote secrecy might be violated by the use of the QR-Code.". Thereby, participants indicated their agreement with this statement on a five-point Likert scale anchored in "strongly disagree" and "strongly agree". Second, a text box where participants could justify their selections. In the study 79 out of 198 participants were concerned regarding privacy of the vote due to the use of QR-Codes. Further, the most comprehensive justification whose parts include most of all other justifications, was the following: "In the election poll workers recorded names on the electoral register, sequentially. In addition to my selections, the time and the sequential order of vote casting can be stored on the QR-Code.".

4 User Study

In this section we describe the different approaches (two online surveys) which were used in order to increase voters' trust and decrease voters' privacy concerns with respect to PATs that contain additional information (e.g. encryption of the vote or a QR-Code that encodes the plaintext vote) other than the human-readable plaintext vote. We also report about recruiting and sampling of participants.

4.1 Online Surveys

Both surveys shared the same general structure and differed only in the part that addressed voters' privacy concerns. Thus, the general structure of the sur-

veys was the following: First participants were asked if they would cast their vote electronically in the upcoming federal election in September 2013. Second, participants were asked if they know what is a QR-Code. In the third question, participants were asked if they have a QR-Code reader application on their smartphone. Then, participants were provided with the survey's specific approach. In addition the surveys collected some demographic data (gender, age and education degree).

4.2 Recruiting and Sampling

The participants were recruited via E-Mail and social networks, for example Facebook. In the first survey participated 99 subjects (38 female, 61 male). 38 participants were between 18 and 25 years old, 41 participants were between 26 and 35 years old, 8 participants were between 36 and 45 years old, 10 participants were between 46 and 60 years old, and 2 participants were older than 60 years. The education level was as follows: 1 participant had a secondary school certificate, 13 had an advanced technical certificate, 34 had a general qualification for university entrance, 14 had a bachelor degree, 29 had a master degree or equivalent like diploma, 3 had a Ph.D. and 5 had an alternative educational degree.

In the second survey participated 94 subjects. There were 61 male and 33 female participants. 44 participants were between 18 and 25 years old, 26 participants were between 26 and 35 years old, 8 participants were between 36 and 45 years old, 14 participants were between 46 and 60 years old, and 2 participants were older than 60 years. The participants' education levels were the followings: 8 participant had a secondary school certificate, 11 had an advanced technical certificate, 38 had a general qualification for university entrance, 18 had a bachelor degree, 12 had a master degree or equivalent like diploma, 4 had a Ph.D. and 3 had an alternative educational degree. Note that difference of the education level between both groups was not significant.

4.3 Approaches to address Participants' Privacy Concerns

In order to address participants' privacy concerns we used the protection motivation theory [12]. This theory, which predicts participants behavior when confronted with a threat and has been applied to other security contexts e.g. [8] and [9], but not electronic voting, provides the foundation for our approaches. For further information regarding the protection motivation theory, refer to [1] and [7].

First Approach: Coping Appraisal After the initial questions participants were first confronted with a summary of the concerns that was deduced from the results of the study conducted by Budurushi et al. [3]. The concern statement in the survey was the following: "In the election poll workers recorded names on the electoral register, sequentially. In addition to my selections, the time and the

sequential order of vote casting can be stored on the QR-Code.": Then, participants were confronted with a technical approach: First, the approach requires that in the pre-voting phase one ore more trustworthy authorities generate sample PATs, i.e. all possible QR-Codes that can be generated in an election.[4] These sample QR-Codes encode only the corresponding selected candidate(s) and no other information like a time stamp or the sequential order of cast votes. Second, to ensure privacy of the vote, i.e. to detect a malicious voting system that has included additional information in the QR-Codes rather than only voter selections, all QR-Codes generated in the voting phase have to be compared with the sample QR-Codes.

Participants were asked to rank different comparison procedures according to their preference. This ranking included also the option, which enabled participants to indicate that this approach does not ensure privacy of the vote. The ranking contained the following items:

A: Voters have a specific application on their smartphone that compares the generated QR-Codes with the sample QR-Codes.
B: A trustworthy, external institution, for example the German Federal Office for Information Security or OSCE/ODHIR, compare all generated QR-Codes with the sample QR-Codes.
C: A combination of both procedures, namely A and B, is provided.
D: The approach does not ensure vote privacy. QR-Codes have to be removed.

In the next step participants were asked if they would use the electronic voting system in the upcoming federal election. To answer this question, participants could chose all or none of the items from the ranking. Finally, participants had to justify the comparison procedure they had ranked in the first position.

Second Approach: Threat Appraisal In this approach participants were confronted with the description of a possible attack to violate vote privacy. After the initial questions the survey described the voting process step by step for both the electronic voting system and the paper-based system.[5] Then, participants were confronted with a specific attack with respect to each systems. From an abstract perspective both attacks described adversaries' capabilities, i.e. the necessary effort an adversary needs for violating privacy of the vote. These are the sequential steps of the attacks presented to the participants:

Attack steps in the electronic voting system.

1. The attacker needs to get access and manipulate the electronic voting system (the voting device or the printer) such that timestamps are encoded on the QR-Codes.

[4] Note that this approach is only feasible for "simple" elections.
[5] In this survey we did not include the privacy concerns regarding the electronic voting system that were identified in [3], because they are covered in the corresponding attack.

2. The attacker must be physically present in the polling station to record the name and time of voters casting their vote.
3. The attacker needs to have access to the QR-Codes (PATs) in order to violate vote privacy. This can only be done after the public tallying phase: either during transport or by accessing the storage room in the corresponding municipality.[6]

Attack steps in the paper-based system.

1. The attacker needs to attach a unique identifier to each paper ballot. This identifier should not be visible to the human eye.
2. Then, the attacker must be physically present in the polling station to keep track which voter gets which paper ballot.
3. Similar to the electronic voting system.

Afterwards, participants were asked to indicate which of the systems is more vulnerable with respect to the corresponding attack, and justify their selection. Then, participants had to indicate their understanding of the described attacks and their agreement that these attacks are possible in practice, on a five-point Likert scale anchored in "strongly disagree" and "strongly disagree". Further, participants had to answer six questions which evaluated their perception of vulnerability and risk with respect to the electronic voting and the paper-based system. The last question in the second survey required participants to indicate if they would cast their vote with the electronic voting system.

Note that we intentionally repeated this question in order to evaluate the impact of the approach regarding participants' security behavior and compare both surveys. In the first survey this question was implicitly asked, while participants chose their preferred option to cast a vote with the electronic voting system.

5 Results

In this section we report the results of our user study. The results of each survey are presented separately. We first present the results of the first survey (technical approach), and then the results of the second survey (attack to violate privacy of the vote).

In the first survey 51 out of 99 participants would cast their vote electronically in the upcoming federal election in September 2013. 81 out of 99 participants knew what a QR-Code is, and 44 of all participants had a QR-Code reader application on their smartphone. Table 1 presents the ranking of the different comparison procedures according to the participants' preference.

The option that was ranked on the first place by most of the participants, namely 51 out of 99, is D. However after the survey, 90 participants would cast

[6] In this work we address the parliamentary elections in Germany. Thereby, the tallying process is public, and votes are physically stored at most six month before the upcoming election. Thus, this needs to be considered when designing user studies.

Ranking	A: Smartphone application	B: Trustworthy, external institution	C: A and B	D: No QR-Code
1	9	18	21	51
2	21	27	42	9
3	29	41	21	8
4	40	13	15	31

Table 1. Ranking of the comparison procedures by number of participants.

a vote with the electronic voting system in the upcoming elections if at least one of the options (A, B, C and D) is provided. Thereby, 26 out of 90 participants would cast a vote only if the QR-Code is removed This means that about 64 out of 90 participants would cast a vote with the electronic voting system if option A, B or C is provided. Furthermore, from the 26 participants, seven stated in the beginning of the survey that they would cast a vote with the electronic voting system, and 19 would not. Finally, only nine out of 99 participants would not cast a vote with the electronic voting system. Thereof, five had stated at the beginning of the survey that they would not cast a vote with the electronic voting system, and four that they would.

In the second survey 59 out of 94 participants would cast their vote electronically in the upcoming federal election in September 2013. 72 out of 94 participants knew what a QR-Code is, and 45 of all participants had a QR-Code reader application on their smartphone. At the end of the survey 60 participants would cast their vote electronically. Thereof, stated six in the beginning of the survey that they would not do so. Further, 34 would not cast their vote electronically, while five of them stated the contrary in the beginning. 82 out of the 94 participants understood the attack description regarding the electronic voting system, while 84 out of all participants understood the attack regarding the paper-based system. Further, 30 out of 94 participants agreed that the electronic voting system is vulnerable with respect to the described attack. Thereof, 10 had stated in the beginning of the survey that they would cast their vote electronically, while at the end of the survey only seven of them would still accept the "risk". In contrast, 38 out of 94 participants agreed, or strongly agreed that the electronic voting system is not vulnerable with respect to the corresponding attack. In comparison only 12 out of 94 participants agreed that the paper-based voting system is vulnerable to the described attack, while 58 did not agree. From the 12 participants that agreed, nine of them would like to cast a vote with the electronic voting system.

6 Discussion and Future Work

The results show that in the first approach a considerable number of participants still have privacy concerns, because some of them would only cast a vote if the QR-Code is removed, and others chose to not do so only after the survey. The

percentage of participants that have privacy concerns is smaller compared to the study conducted by Budurushi et al. [3], 21% v.s. 39.9% respectively, however not sufficient in the context of electronic voting. Furthermore, half of the participants that were "against" electronic voting in the beginning of the survey, are willing to cast a vote electronically if they have an application on their smartphone that verifies the content of the QR-Code, or a trustworthy, external institution verifies the content of QR-Codes, or both procedures are provided. This shows that the first approach is a promising method towards increasing voters' trust and decreasing voters' privacy concerns with respect to PATs with additional information or more generally regarding new voting technologies. In contrast, the second approach has a lower impact on participants' security behavior, as no significant changes were identified before and after the survey. Hence, this indicates that the coping appraisal has a higher impact on security behavior than the threat appraisal. However, the results of the second approach reflect the current participants' perception regarding new voting technologies in general, i.e. their insecurity towards understanding and perception of the corresponding risks.

Our findings provide novel directions on addressing privacy concerns in the context of electronic voting. However, both approaches to address voters' privacy concerns are tailored to the EasyVote system [15]. Furthermore, we are aware that the sample does not represent the entire population. These limitations need to be considered for the design of future user studies. Nevertheless, the results of this work lead future work in many different directions. In particular, more research is needed to better understand voters' mental models regarding trust and privacy concerns with respect to new voting technologies. The coping appraisal seems a promising method, however more research is needed in order to improve this method in the context of electronic voting.

Acknowledgements

This paper has been developed within the project 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen - which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation). We would like to thank everyone who supported us by participating in the user study.

References

1. Anderson, C., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. J. MIS Q. 34, 613–643 (2010)
2. Ben-Nun, J., Fahri, N., Llewellyn, M., Riva, B., Rosen, A., Ta-Shma, A., Wikström, D.: A New Implementation of a Dual (Paper and Cryptographic) Voting System. In: Kripp, M., Volkamer, M., Rüddiger, G. (eds.) EVOTE 2012. LNI, vol. 205, pp. 315–329. GI (2012)

3. Budurushi, J., Volkamer, M.: Implementing and evaluating a software-independent voting system for polling station elections. J. JISA (Special Issue on Electronic Voting) (accepted, to appear in April 2014)
4. Board of Elections City of New York: Ballot Marking Device, http://www.votethenewwayny.com/en/using-the-new-voting-system.
5. Chaum, D.: Secret-Ballot Receipts: True Voter-Verifiable Elections. In: Schneider F. (eds.) IEEE S&P 2004. IEEE, vol. 2, pp. 38–47. (2004)
6. Chaum, D., Ryan, P. Y., Schneider, S.: A Practical Voter-Verifiable Election Scheme. In: De Capitani di Vimercati, S., Syverson, P., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 118–139. Springer (2005)
7. Floyd, D., Prentice-Dunn., S., Rogers, D.: A Meta-Analysis of Research on Protection Motivation Theory. J. JASP. 30, 407–429 (2000)
8. Johnston, A. C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. J. MISQ. 34, 548–566 (2010)
9. Lee, Y., Larsen, K. R.: Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. J. EJIS. 18, 177–187 (2009)
10. Llewellyn, M., Schneider, S., Xia, Z., Culnane, C., Heather, J., Ryan, P. Y., Srinivasan, S.: Testing Voters' Understanding of a Security Mechanism Used in Verifiable Voting. J. JETS. 1, 53–61 (2013)
11. Ryan, P. Y., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à Voter: a Voter-Verifiable Voting System. In: IEEE Transactions on Information Forensics and Security (Special Issue on Electronic Voting), vol. 4(4), pp. 662–673. IEEE (2009)
12. Rogers, R.: A Protection Motivation Theory of Fear Appeals and Attitude Change. J. Journal of Psychology: Interdisciplinary and Applied. 9, 93–114 (1975)
13. Rivest, R., Wack, J.: On the notion of "software independence" in voting systems. Technical report, Information Techonolgy Laboratroy, National Institute of Standards and Technology (2006)
14. Vegas, C.: The New Belgian E-voting System. In: Kripp, M., Volkamer, M., Rüddiger, G. (eds.) EVOTE 2012. LNI, vol. 205, pp. 199–211. GI (2012)
15. Volkamer, M., Budurushi, J., Demirel, D.: Vote Casting Device with VV-SV-PAT for Elections with Complicated Ballot Papers. In: Grimm, R., Schneider, S., Volkamer, M., Weldemariam, K. (eds.) REVOTE 2011. IEEE, pp. 1–8. Publisher (2011)
16. Vot.ar, http://www.vot-ar.com.ar/en/system-votation/
17. VOTE-TRAKKER, http://www.avantetech.com/products/elections/dre/