Nothing Comes for Free: How Much Usability Can You Sacrifice for Security?

Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, Melanie Volkamer

This article appears in IEEE Security & Privacy (Volume: 15, Issue: 3, 2017), pp. 24-29

Abstract

A widely discussed issue in Internet voting is the secure platform problem: ensuring vote secrecy and/or vote integrity in the presence of compromised voting devices. A well-known approach to address this issue is code voting. Code voting systems differ regarding their security level: some ensure either vote secrecy or vote integrity, while others ensure both. However, these systems potentially impair usability, as voters have to enter and/or compare random codes, rather than just selecting their preferred candidate. This might negatively affect voters' attitude towards the adoption of Internet voting. Therefore, it is important to determine to which extent voters would sacrifice usability for security. To determine this tradeoff between usability and security, we conducted a pilot user study among university students in the university elections setting, and a quantitative analysis. Our findings reveal that voters would sacrifice approximately 26 points (scale 0-100) of usability given a system with higher security.

1 Introduction

Due to the widespread usage of Internet technology, Internet voting has become a topic of extensive research. However, before Internet voting could be adopted on a large scale in practice, a number of challenges have to be addressed, such that the fundamental election principles (namely, general, free, secret, equal and direct vote for the elections in Europe[1]) are ensured. One of the most prevalent challenges is to ensure the security requirements of vote secrecy and vote integrity that are deduced from these elections principles[2]. The worldwide infection rates of personal computers above 33%[3] makes it even more crucial to ensure vote secrecy and vote integrity in the presence of compromised voting devices (voters' personal computers). This challenge is also known as the secure platform problem.

Over the last years, the research community has proposed a number of possible solutions to the secure platform problem. Most of these solutions trace back to code voting approach, originally introduced by Chaum[4]. Generally, the idea behind code voting approaches is that election authorities provide voters with so called code sheets that are distributed via postal mail. In order to cast a vote, voters enter the voting code assigned to their preferred candidate and/or party. Upon receiving the voting code, election authorities acknowledge its receipt by sending to the voters a so-called confirmation code. At this step voters are encouraged to compare the received confirmation code, displayed by their voting device, with the confirmation code on their code sheet. Given the fact that potentially compromised voting devices do neither know valid voting codes, other than the one entered by the voters, nor the relation between voting codes and candidates, both vote secrecy and vote integrity are ensured against such devices. Nevertheless, the security gains come at the cost of usability losses: Voters have to enter and compare random codes, rather than just selecting (clicking) their preferred candidate and/or party from a given list. The competition between security and usability is well-known, and both of these aspects are of fundamental importance to the acceptance of new voting technologies[5]. However, to the best of our knowledge, it remains unknown to which extent voters are ready to trade usability for security. Note that determining this trade-off has a very high practical relevance, as it would allow decision makers to identify the adequate Internet voting system with respect to their election setting.

Consequently, the present work aims to close this gap. Thereby, we conducted a user study in the context of the university elections at Technische Universität Darmstadt, where three different voting systems were considered: One that is vulnerable to compromised voting devices (secure platform problem) and two code voting systems, which provide different levels of security. 23 participants took part in the study. Participants were required to cast a vote by using all three systems. After casting their vote with each of the systems, participants filled in the system usability scale (SUS[6]) questionnaire. Then, participants were required to indicate which system they would prefer to use in the real university elections. Finally, in order to identify the trade-off between security and usability, i.e. to derive a quantitative model that describes how much usability voters are willing to sacrifice for using a system with higher security, we conducted a multinomial logit analysis. The rest of this work is structured as follows: Section 2 introduces our methodology. In section 3 we present and discuss our findings. Last, but not least, section 4 summarizes the findings of this work and provides future work directions.

2 Methodology

In the following we describe the context, the considered voting systems and the study design.

2.1 Context

The TU Darmstadt considers the introduction of Internet voting for the university elections. Given these circumstances, we decided to conduct the user study in the context of the university elections. We think that the findings of our study would be beneficial for the respective decision makers. University elections at TU Darmstadt are held annually and comprise four individual races, namely the department council, the student council, university assembly and student parliament. In the elections for the department and student council, voters can select up to three candidates. For the student parliament and the university assembly, voters can select one party.

2.2 Voting Systems

For the user study we developed three mock-up systems, which were developed according to the university's corporate design. In the following we describe the vote casting process and discuss the security properties for each system.

2.2.1 System A

The vote casting process with System A is very simple and intuitive. The voter makes her choice by selecting her preferred candidate from the candidate list on the voting website. She then reviews and confirms her candidate choice, just like reviewing and confirming her purchase in the shopping basket. Finally, the voter receives a confirmation message that her vote has been successfully cast.

While being simple in usage, System A fails to ensure vote secrecy and vote integrity in the presence of compromised voting devices. On the one hand, a compromised voting device could learn the voter's candidate choice, i.e. violates vote secrecy. On the other hand, a compromised voting device could send a vote for another candidate or simply drop the vote, i.e. a violation of vote integrity.

2.2.2 System B

The vote casting process with System B is slightly different in comparison to system A. Prior to casting her vote, the voter receives a unique code sheet (i.e. having a unique code sheet ID), where a unique confirmation code is assigned to each candidate, see Figure 1. The confirmation codes on each code sheet are known only to the respective voter and the voting authorities.

fig1

Figure 1: A simplified depiction of a code sheet for System B.

Analogously to System A, the voter casts her vote by selecting her preferred candidate from the candidate list, reviewing and confirming her choice. After casting her vote, the voter receives a confirmation message that her vote has been successfully cast. In addition, this message contains a confirmation code. The voter is encouraged to compare the received confirmation code with the confirmation code assigned to her chosen candidate on the code sheet.

The deployment of confirmation codes enhances the security in comparison to System A. If a compromised voting device alters or drops the vote, the voter would detect such misbehaviour. Given the fact that confirmation codes are secretly shared among the voter and the voting authorities, a compromised device is not capable of obtaining the confirmation code expected by the voter. As such, as opposed to System A, vote integrity is protected in System B against a compromised voting device. A similar approach has also been used for the Norwegian parliamentary election[7]. Note, however, that a compromised voting device can still violate vote secrecy in System B by learning the voters' input choice.

2.2.3 System C

The third system, System C, further modifies the vote casting process. Similar to System B, the voters also get a unique code sheet. These code sheets, however, are constructed in a different way, namely they contain a unique voting code for each candidate, and a single confirmation code for the entire code sheet, see Figure 2. The voting and the confirmation codes are known only to the respective voter and the voting authorities.

fig2

Figure 2: A simplified depiction of a code sheet in System C.

In order to cast a vote, the voter enters the voting code that is assigned to her prefered candidate on the code sheet.

Analogously to System B, after casting her vote, the voter receives a confirmation message and a confirmation code, which she is required to compare with the confirmation code on her code sheet.

The purpose of the voting codes is to enhance security, more specifically to ensure vote secrecy against a compromised voting device. As the link between candidates and voting codes is secretly shared among the voter and the voting authorities, the voting device does not learn anything about the voter's choice by seeing entered voting codes. In combination with the use of confirmation codes, System C ensures vote secrecy and vote integrity in the presence of compromised voting device. A similar approach has been proposed by Ryan et al[8] and by Budurushi et al[9].

2.3 Study Design

2.3.1 Participants: Recruitment, Incentives and Sampling

Participants were recruited by personal contact, e-mail and flyers. As we conducted the study in the context of the university elections, our participants were members of TU Darmstadt. No incentives were provided, thus participation was purely voluntary. In total twenty-three participants (11 female, 12 male), between the ages of 18-35 years, took part in the study.

2.3.2 Study Procedure

The study consisted of five parts. In the first part participants were introduced to the fictive research goal, namely to test the voting systems that are considered to be used for the next university elections. Next, participants were required to read and sign the consent form for participating in the study. Participants could leave the study at any point in time without providing a reason, however, all of the participants completed the study. Afterwards, participants were provided their login credentials. It is important to note that to ensure participants' privacy, we required them to vote by following a voting agenda, i.e. to vote for a pre-defined candidate and party.

In the second part participants were provided with voting instructions for System A. After casting their votes by using System A, participants filled in the SUS (System Usability Scale) questionnaire[6]. Next, participants were introduced to one of the vulnerabilities of System A, namely that this system fails to ensure integrity of the vote in the presence of compromised voting devices, and that System B has been developed to address this vulnerability. In the third part participants were provided with voting instructions for System B. Further, they cast their vote by using System B and filled in the SUS questionnaire. Afterwards, participants were introduced to a security vulnerability common to both systems A and B, namely that a compromised voting device might violate vote secrecy. They were further told that System C addresses both vulnerabilities, namely the violation of vote secrecy and integrity. In the final part participants were provided with voting instructions for System C. After casting their vote by using System C, they were also required to fill in the SUS questionnaire. Last but not least, participants were asked to indicate and explain which of the three systems they would use for the next university elections. In the last part participants debriefing took place, i. e. participants were introduced to the actual goal of the study, namely, that the study aimed at evaluating the trade-off between usability and security that the participants were willing to make, and that none of the systems was actually considered for the university elections.

3 Results and Discussion

In this section we present and discuss the findings of our study as follows: We first consider the results with respect to the usability evaluation of each system. Then, we provide an overview regarding participants' choice of their preferred system and summarize their arguments. Further, we evaluate the trade-off between usability and security that our participants were willing to make.

3.1 Usability

In order to assess the usability of each system we evaluated the SUS questionnaires according to the method described by Sauro[10], presented in Figure 3. Our evaluation revealed a significant difference (both according to Wilcoxon signed rank test and one sample t-test[11], $p < .001$) in the usability score between systems A and C, as well as between systems B and C. A less significant difference was identified between systems A and B ($p = 0.063$ for the Wilcoxon test, and $p = 0.052$ for the t-test). It is not surprising that usability score of System C was significantly lower than both System A and B, because to cast a vote with System C participants are required to enter a specific voting code, rather than just selecting their preferred candidate. Furthermore, it is interesting that the difference between System A and B was found to be less significant, even though they slightly differ in the vote casting process, namely in System B participants are required to compare the confirmation code. Last but not least, our findings might be slightly susceptible towards the learning effect due to the adopted study design. This means that a greater difference might be identified regarding usability scores between the systems.

fig3

Figure 3: Average usability scores and their standard deviation for each one of the systems.

3.2 System of Choice and Arguments

Figure 4 depicts participants' choice with respect to their preferred voting system. The findings presented in Figure 4 reveal that the majority of the participants, namely 15 out of 23, indicated System C as their choice of preference to cast a vote, even though it performed worst regarding usability. Thereby, when asked to explain why they would prefer this particular system via an open question in the questionnaire, the most mentioned argument by the participants was the higher level of security,

"*Due to the high security measures, throughout the election I feel more secure.*"

"*I felt most secure when using the third voting systems, because there was a voting code and a confirmation code. Since names of candidates were not shown, eavesdropping my vote is made more complicated. At the same time, the use [of codes] remains simple, but for inexperienced users, not choosing the names might cause problems.*"

fig4

Figure 4: Number of participants who chose each one of the systems.

From the remaining participants, three chose to use System A and five chose to use System B. Thereby, the participants that chose System A mentioned that they are not concerned about the secrecy and integrity of their vote in the context of university elections,

"...The university elections is not so important for me, if someone knows how I voted. I think that I would rather quickly cast my vote in such elections, and therefore the extra effort required by System B and C is unnecessary."

"...It's the simplest and quickest to use. The security aspect is for me as a user not important. It should be secured in the background such that I am not directly involved."

Participants that chose system B mentioned that they are not concerned about vote secrecy, but rather integrity,

"...Not unnecessarily complex, it does not matter who sees who voted for whom."

It is worth mentioning that one participant holds the opinion that increasing the complexity of the voting process fosters his feeling of the process' correctness.

"*... the multiple security layers suggest that the election is conducted correctly, because it does not only require simple clicking. But I did not understand what the confirmation code served for.*"

Note that these arguments might differ in other elections settings, for instance local or federal elections.

3.3 Usability vs. Security

In order to evaluate the trade-off between security and usability, we conducted a multinomial logit analysis (using mlogit package in R[12]), where we measured a relative impact of security and usability on participants' preferences with respect to the choice of their preferred system.

Based on the security requirements vote secrecy and vote integrity, we measured security on a scale from 0 to 2. System A, which protected neither one of these requirements, was assigned score 0. System B, which protected only one of them, was assigned score 1. System C, which protected both requirements, was assigned score 2. Furthermore, to measure usability we used the respective scores calculated in section 3.2, refer to Figure 3.

Our analysis reveals that both security and usability were significant factors (with significance of $p < .001$ and $p < .05$ respectively) for choosing the preferred system.

By calculating the relative coefficients of these factors, security and usability, it can be concluded, according to the model derived from our analysis, that voters would be ready to sacrifice on average approximately 26 points on usability (on a scale 0 to 100) for using a system which provides higher security. The finding suggests, that the voters would prefer System B to System A, as well as System C to System B, as long as the difference in usability scores is no more than approximately 26 points on usability.

To illustrate this finding, consider when our study participants were ready to use a system with higher security and when not. For instance, refer to second column in Figure 5, participants who preferred System C (higher security) to B (lower security) evaluated C to be only 14 points less usable than B. On the contrary, participants who preferred System B to C evaluated C to be 32 points less usable.

fig5

Figure 5: Perceived usability difference between preferred system and other voting systems. Voters choose more secure systems unless they perceive usability decreases above approximately 26 SUS points.

4 Conclusion

In this paper we report about the extent to which voters are ready to sacrifice usability for higher security assurances. We found out that voters prefer systems with higher security assurance, unless security gains come at the cost of more than approximately 26 usability points (scale 0-100) on average.

Note that as common for user study, our study is not free of limitations: The participants in our study were university members, and therefore not representative of the larger voting population. Furthermore, we focused on the secure platform problem, while Internet voting faces further security challenges, which include preventing voter coercion and implementing the principle of separation of duties. A further limitation of our study is that the usability scores that the participants gave were their perceived scores, probably biased by the study design (in particular, the learning effect). However, as the goal of the study was to find out the trade-off between security and usability as perceived by the participants, that they were ready to make, we consider the results of the study appropriate for this goal.

While our findings provide important baseline data and novel directions on determining the trade-off between usability and security, further investigations are necessary to address the limitations of the reported study, and generalize our findings.

References

1. Bundestag. “Election principles (Article 38 I GG)”. Online: https://staatsrecht.honikel.de/en/bundestag.htm, last accessed on 1.09.2016.

2. Neumann, Stephan. “Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements“. PhD Thesis. *Technische Universität Darmstadt, 2016. URL: http://tuprints.ulb.tu-darmstadt.de/5375/.*

3. Panda Security. “PandaLabs Quaterly Report Q1 2016”. Online: http://www.pandasecurity.com/mediacenter/src/uploads/2016/05/Pandalabs-2016-T1-EN-LR.pdf, last accessed on 1.09.2016.

4. Chaum, David. "Surevote: technical overview." *Proceedings of the workshop on trustworthy elections (WOTE’01)*. 2001.

5. Volkamer, Melanie, Oliver Spycher, and Eric Dubuis. "Measures to establish trust in internet voting." *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*. ACM, 2011.

6. Brooke, John. "SUS-A quick and dirty usability scale." *Usability evaluation in industry* 189.194 (1996): 4-7.

7. Gjøsteen, Kristian. "The norwegian internet voting protocol." *International Conference on E-Voting and Identity*. Springer Berlin Heidelberg, 2011.

8. Ryan, Peter YA, and Vanessa Teague. "Pretty good democracy." *International Workshop on Security Protocols*. Springer Berlin Heidelberg, 2009.

9. Budurushi, Jurlind, et al. "Pretty understandable democracy-a secure and understandable internet voting scheme." *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*. IEEE, 2013.

10. Sauro, Jeff. "Measuring usability with the system usability scale (SUS)." (2011). Online: http://www.measuringu.com/sus.php, last accessed on 1.09.2016

11. Crawley, M. J. “The R Book. [s.l.]”. 2012. *Wiley*. Retrieved from http://onlinelibrary.wiley.com/book/10.1002/9781118448908

12. Croissant, Yves. "Estimation of multinomial logit models in R: The mlogit Packages." (2012). *R package version 0.2-2.* Online: http://cran.r-project.org/web/packages/mlogit/vignettes/mlogit.pdf, last accessed on 1.09.2016.

Appendix

We include the raw data of SUS scores[6] that resulted from our study. Note, that in some of the cases the participant's answer to a questionnaire item was ambiguous, hence, we included the decimal point to indicate, that the participants placed her mark between two suggested answers.

Participant ID	I think that I would like to use this system frequently			I found the system unnecessarily complex			I thought the system was easy to use			I think that I would need the support of a technical person to be able to use this system			I found the various functions in this system were well integrated.			I thought there was too much inconsistency in this system.			I would imagine that most people would learn to use this system very quickly.			I found the system very cumbersome to use.			I felt very confident using the system.			I needed to learn a lot of things before I could get going with this system.		
	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
1	5	4	3	2	4	4	5	4	3	2	1	4	4	5	3	2	2	2	5	5	3	2	1	3	5	5	3	2	1	2
2	5	5	5	1	4	4	5	5	5	1	1	1	5	5	5	4	3	3	5	5	5	1	1	1	5	5	5	1	1	1
3	5	5	5	2	4	2	5	4	3	1	1	3	4	4	5	1	1	1	4	4	3	2	2	4	5	5	5	1	1	1
4	2	4	4	3	4	3	3	4	3	3	2	5	4	4	4	2	2	2	4	4	4	2	4	3	4	4	2	2	2	4
5	5	5	5	1	1	1	4	4	4	1	1	1	5	5	5	1	4	4	5	4	5	1	1	3	5	5	5	1	1	4
6	3	3	3	1	1	1	5	4	4	1	1	1	5	5	5	1	1	1	5	4	4	1	1	1	5	4	4	1	1	1

7	5	5	4	1	1	4	5	5	2	1	1	3	5	5	5	1	1	2	5	5	2	1	1	4	4	5	5	1	1	3
8	4	4	4	2	2	2	4	4	4	1	1	1	4	4	4	1	1	1	5	4	3	1	1	1	4	4	4	1	1	1
9	4	4	3	1	1	2	5	5	3	1	1	1	5	4	5	1	1	1	5	5	1	1	1	4	5	5	3	1	1	3
10	5	5	5	1	1	2	5	5	4	1	1	1	5	5	5	1	1	1	5	5	4	1	1	2	5	5	5	1	1	2
11	4	5	3	1	1	2	5	5	3	1	1	2	4	4	4	1	1	1	5	5	3	1	1	4	5	5	4	1	1	1
12	5	5	5	1	1	1	5	5	5	1	1	1	5	5	5	1	1	1	5	5	5	1	1	1	5	5	5	1	1	1
13	5	5	2	1	1	4	5	5	2	1	1	3	5	5	3	1	1	2	5	5	1	1	1	5	5	5	2	1	1	4
14	5	5	5	1	1	2	5	5	4	1	2	3	5	5	4	2	2	2	5	5	4	1	2	2	2	5	5	1	1	2
15	4	3	3	1	3	5	5	4	3	1	5	1	4	3	2	1	2	2	4	4	5	1	4	5	2	3	3	1	4	1
16	4	2	1	2	2	1	5	2	1	1	3	5	5	1	1	4	1	5	5	1	1	1	2	5	5	4	2	1	3	2
17	2	3	3	1	2	3	5	4	3	1	1	1	5	5	4	1	1	1	5	5	4	1	1	3	3	3	3	1	1	2
18	3	1	3	1	1	1	5	5	3	1	1	1	4	1	5	3	1	1	5	5	5	1	1	1	5	1	4	1	1	3
19	5	5	4	1	1	2	5	4	3	1	1	1	4	4	4	1	2	1	4	4	3	1	1	3	4	4,5	5	2	1	2
20	4	3	3	2	4	4	4	3	2	1	1	1	4	4	4	2	2	2	4	3	3	2	4	4	3	2	2	1	2	1
21	5	5	5	1	4	4	5	5	5	1	1	1	5	5	5	1	1	1	5	5	5	1	2	3	4	5	4	1	1	1
22	3	5	5	2	1	2	3	3	2	1	1	1	3	3	3	2	2	2	3	3	3	3	2	3	2	4	5	1	1	2
23	5	5	3	1	2	4	5	5	3	5	1	1	4	4	3	2	2	3	2	2	1	1	2	4	2	4	2	1	1	2

Authors Biographies

Oksana Kulyk (oksana.kulyk@secuso.org) is doctoral researcher at the Center for Research in Security and Privacy at Technische Universität Darmstadt. Her research focuses on secure, usable and verifiable electronic voting systems. She leads the research in the area of electronic voting in the research group Security, Usability, and Society (SECUSO).

Stephan Neumann (stephan.neumann@secuso.org) is postdoctoral researcher at the Center for Research in Security and Privacy at Technische Universität Darmstadt. His research focuses on usable secure digital communication and the security of electronic voting systems. He is the area head of secure digital communication in the research group Security, Usability, and Society (SECUSO).

Jurlind Budurushi (jurlind.budurushi@secuso.org) is postdoctoral researcher at the Center for Research in Security and Privacy at Technische Universität Darmstadt. His research focuses on security and privacy delegation, and the security of electronic voting systems. He is the area head of privacy in the research group Security, Usability, and Society (SECUSO).

Melanie Volkamer (melanie.volkamer@secuso.org) is professor for Usable Privacy and Security at the University of Karlstad (Sweden) and professor (Kooperationsprofessor) at the Technische Universität Darmstadt. She is the head of the research group Security, Usability, and Society (SECUSO).