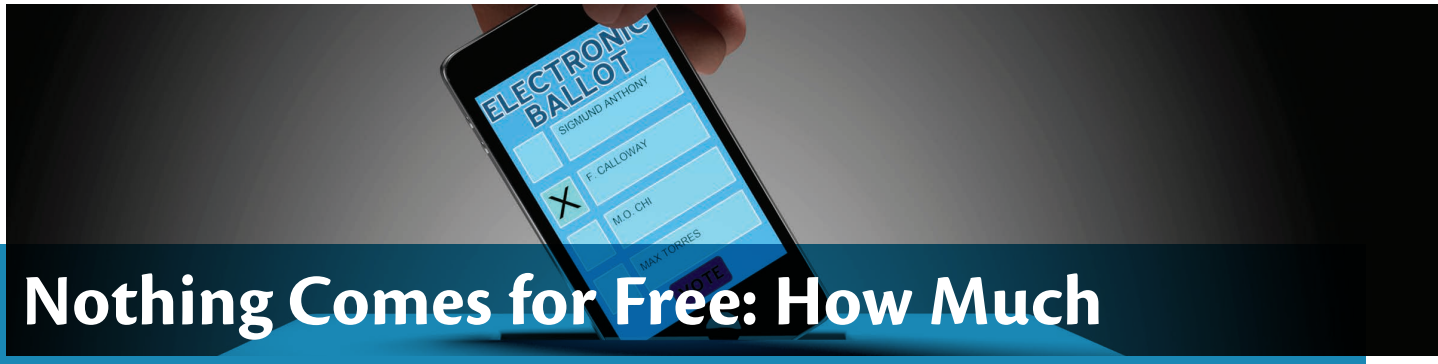

Nothing Comes for Free: How Much Usability Can You Sacrifice for Security?

Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer |
Technische Universität Darmstadt

Code voting systems differ in security: some ensure either vote secrecy or vote integrity, while others ensure both. However, these systems potentially impair usability, which might negatively affect voters' attitudes toward Internet voting. To determine the security–usability tradeoff, the authors conducted a pilot user study examining voters in a university elections setting.

Owing to the widespread use of Internet technology, Internet voting has become a topic of extensive research. However, before Internet voting can be adopted on a large scale in practice, many challenges must be addressed so that fundamental election principles (namely, general, free, secret, equal, and direct voting for European elections[1]) are ensured. One prevalent challenge is to ensure the security requirements of vote secrecy and integrity that are deduced from these election principles.[2] The worldwide infection rate of PCs is above 33 percent, making it even more crucial to ensure vote secrecy and integrity in the presence of compromised voting devices (voters' PCs).[3] This challenge is also called the *secure platform problem*.

Over the past 16 years, the research community has proposed several possible solutions to the secure platform problem. Many solutions are based on the *code voting approach*, originally introduced by David Chaum.[4] Generally, the idea behind code voting approaches is that election authorities provide voters with "code sheets" via postal mail. To cast a vote, voters enter the voting code assigned to their preferred candidate and/or party. On receiving the voting code, election authorities acknowledge its receipt by sending the voters a confirmation code. Voters are encouraged to compare the received confirmation code, displayed by their voting device, with the confirmation code on their code sheet. Because potentially compromised voting devices don't know valid voting codes, or the relation between voting codes and candidates, both vote secrecy and integrity are ensured.

Nevertheless, the security gains come at the cost of usability losses: voters must enter and compare random codes rather than just select 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 fundamental to users' acceptance of new voting technologies.[5] However, to the best of our knowledge, it remains unknown to what extent voters are ready to trade usability for security. Note that determining this tradeoff has a very high practical relevance, as it would allow decision makers to identify the appropriate Internet voting system with respect to their election setting. To close this gap of knowledge of the tradeoff between security and usability acceptable by voters, we conducted a user study in

 Copublished by the IEEE Computer and Reliability Societies

the context of Technische Universität (TU) Darmstadt elections.

Methodology

We created mock-ups of three different voting systems: one that's vulnerable to compromised voting devices (secure platform problem) and two code voting systems with different security levels. Twenty-three participants took part in the study. Participants were required to cast a vote using all three systems. After casting a vote using each system, participants filled in the system usability scale (SUS) questionnaire.[6] Then, participants were required to indicate which system they would prefer to use in real university elections. Finally, to identify the tradeoff between security and usability—that is, 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.

Races

University elections at TU Darmstadt are held annually and comprise four individual races: department council, student council, university assembly, and student parliament. In the elections for department and student councils, voters can select up to three candidates. For the student parliament and the university assembly, voters can select one party.

Voting Systems

For the user study, we created three mock-up systems, which were developed according to the university's corporate design.

System A. The vote-casting process in system A is very simple and intuitive. Voters make their choice by selecting the preferred candidate from the candidate list on the voting website.

They then review and confirm their candidate choice, just like reviewing and confirming a purchase in an online shopping basket. Finally, voters receive a confirmation message that their vote has been successfully cast.

Although simple in usage, system A fails to ensure vote secrecy and integrity in the presence of compromised voting devices. A compromised voting device could learn a voter's candidate choice, violating vote secrecy, or it could send a vote for another candidate or simply drop the vote, violating vote integrity.

System B. The vote-casting process in system B differs slightly from system A. Prior to casting a vote, voters receive a code sheet, with a unique code sheet ID. On this sheet, each candidate has a unique confirmation code (see Figure 1). The confirmation codes on each code sheet are known only to the respective voter and the voting authorities.

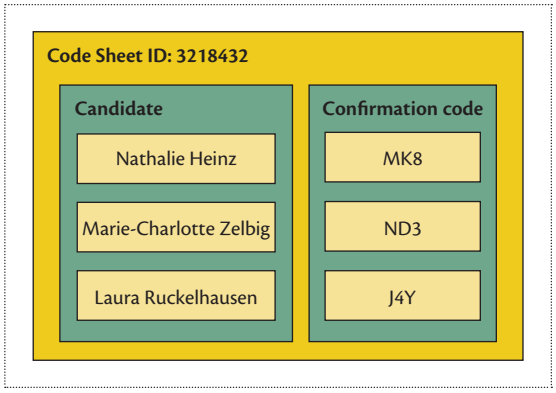

Figure 1. A simplified depiction of a code sheet for system B.

Analogously to system A, voters cast a vote by selecting their preferred candidate from the candidate list, reviewing and confirming their choice. After casting their vote, they receive a confirmation message that their vote has been cast successfully. In addition, this message contains a confirmation code. Voters are encouraged to compare the received confirmation code with the confirmation code assigned to their 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, a voter could detect such misbehavior. Because confirmation codes are secretly shared among the voter and the voting authorities, a compromised device can't obtain the voter's expected confirmation code. As such, as opposed to system A, system B protects vote integrity against a compromised voting device. A similar approach has 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.

System C. The third system, system C, further modifies the vote-casting process. Similar to system B, voters get a unique code sheet. However, these code sheets are constructed differently: 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 confirmation codes are known only to the respective voter and the voting authorities.

To cast a vote, voters enter the voting code assigned to their preferred candidate on the code sheet. Analogously to system B, after casting their vote, voters receive a confirmation message and a confirmation code, which they are required to compare with the confirmation code on their code sheet.

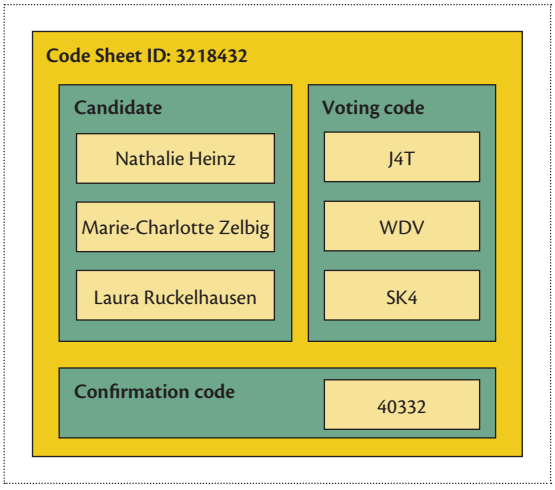

Figure 2. A simplified depiction of a code sheet in system C.

The purpose of the voting codes is to enhance security, more specifically to ensure vote secrecy against a compromised voting device. Because the link between candidates and voting codes is secretly shared among the voter and the voting authorities, the voting device doesn't 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 integrity in the presence of a compromised voting device. Peter Y.A. Ryan and his colleagues as well as Jurlind Budurushi and his colleagues have proposed a similar approach.[8,9]

Study Design

Here, we describe the participant selection process and sampling and the five parts of our study's procedure.

Participants: recruitment, incentives, and sampling. We recruited participants via personal contact, email, and flyers. Because we conducted the study in the context of the university elections, our participants were either students or employees at TU Darmstadt. No incentives were provided; participation was purely voluntary. In total, 23 participants (11 female and 12 male) between the ages of 18 and 35 took part in the study.

Study procedure. The study consisted of five parts. In the first part, participants were introduced to the fictive research goal—to test the voting systems that are being considered for future university elections. Next, participants were required to read and sign the consent form to participate in the study. Participants could leave the study at any point without providing a reason; however, all participants completed the study. Then, participants were provided login credentials. It's important to note that, to ensure participants' privacy, we required them to vote by following a voting agenda, that is, to vote for a predefined candidate and party.

In the second part, participants were provided with voting instructions for system A. After casting their votes using system A, they filled in the SUS questionnaire. Next, they were introduced to a vulnerability of system A, namely that it fails to ensure a vote's integrity in the presence of a compromised voting device, and that system B was developed to address this vulnerability.

In the third part, participants were provided with voting instructions for system B. They then cast their vote using system B and filled in the SUS questionnaire. Afterward, they 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 disclosed vulnerabilities.

In the fourth part, participants were provided with voting instructions for system C. After casting their vote using system C, they were again required to fill in the SUS questionnaire. Then, participants were asked to indicate and explain which of the three systems they would prefer using for future university elections.

The final part consisted of participant debriefing: they were introduced to the study's actual goal—that it aimed to evaluate the tradeoff between usability and security that the participants were willing to make, and that none of the systems was actually considered for the university's elections.

Results and Discussion

We first consider the results with respect to each system's usability evaluation, then provide an overview of the participants' preferred system.

Usability

To assess each system's usability, we evaluated the SUS questionnaires according to Jeff Sauro's method, presented in Figure 3.[10] Our evaluation revealed a significant difference (both according to a Wilcoxon signed rank test and a sample t-test,[11] $p < 0.001$) in the usability score between systems A and C as well as between systems B and C. We identified a less significant difference between systems A and B ($p = 0.06$ for the Wilcoxon test and $p = 0.05$ for the t-test). It's not surprising that the usability score for system C was significantly lower than for both systems A and B, because to cast a vote with system C, participants were required to enter a specific voting code, rather than just selecting their preferred candidate. Furthermore, it's interesting that the difference between systems A and B was less significant, even though they differ slightly in the vote-casting process, wherein system B participants are required to compare the confirmation code. Last but not least, our

findings might be somewhat susceptible to the learning effect due to our study design. This means that a greater difference might be identified regarding usability scores between the systems.

System of choice and arguments. Figure 4 depicts participants' choice with respect to their preferred voting system. The findings reveal that the majority of the participants, 15 out of 23, preferred system C to cast a vote, even though it performed worst in usability. When asked, via an open question in the questionnaire, to explain why they would prefer this particular system, participants' most mentioned argument 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 system, because there was a voting code and a confirmation code. Since names of candidates were not shown, eavesdropping on 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.

From the remaining participants, three chose system A and five chose system B. The participants who chose system A mentioned that they aren't concerned about the secrecy and integrity of their vote in the context of university elections:

> The university elections [are] 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 systems 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 who chose system B mentioned that they aren't concerned about vote secrecy, but rather integrity:

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

It's worth mentioning that one participant held the opinion that increasing the complexity of the voting process fostered his feeling that the process was correct:

> 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.

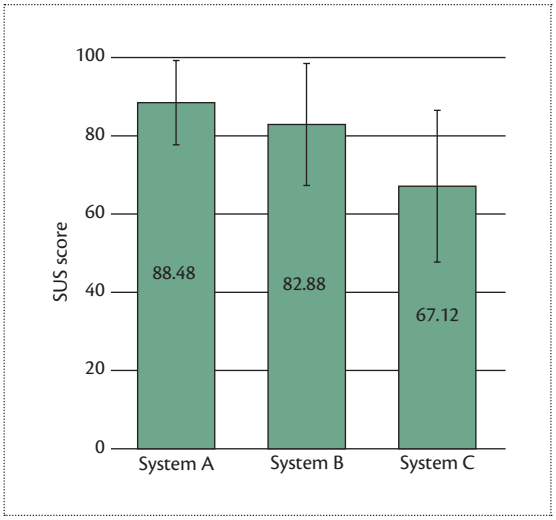

Figure 3. Average system usability scale (SUS) scores and their standard deviation for each voting system.

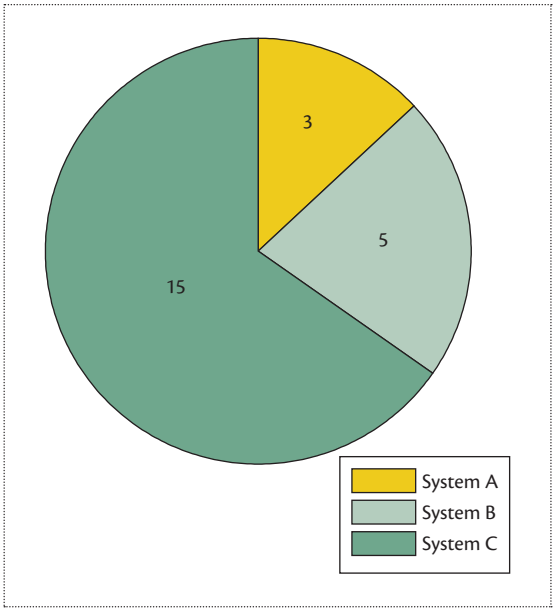

Figure 4. Number of participants who chose each system.

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

Usability versus Security

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

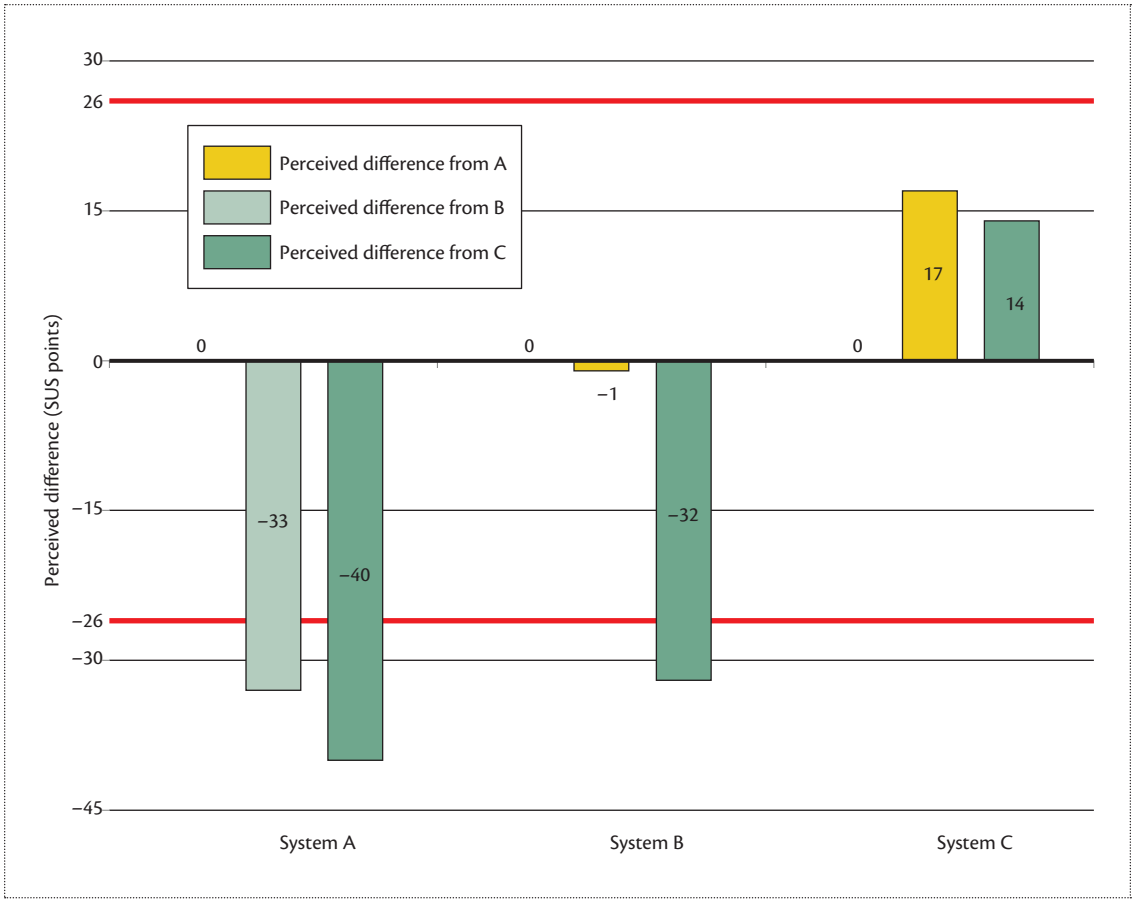

Figure 5. Perceived usability difference between voters' preferred system and other systems. Voters choose more secure systems unless they perceive that usability has decreased more than approximately 26 SUS points.

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

Our analysis revealed that both security and usability were significant factors ($p < 0.001$ and $p < 0.05$, respectively) for choosing the preferred system.

By calculating the relative coefficients of these factors (security and usability), we can conclude that voters would be ready to sacrifice on average 26 points on usability (on a scale from 0 to 100) for a system that provides higher security, according to the model derived from our analysis. The finding suggests that 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.

To illustrate this finding, consider when our study participants were willing to use a system with higher security and when they weren't. For instance, in the 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.

Limitations

Note that our study isn't free of limitations: the study participants were university students or employees and, therefore, not representative of the larger voting population. Furthermore, we focused on the secure platform problem, whereas Internet voting faces further security challenges, including preventing voter coercion and implementing the principle of separation of duties. A further limitation of our study is that the usability scores the participants gave were their perceived scores, probably biased by the study design (in particular, the learning effect). However, the study's goal was to discover the tradeoff between security and usability that participants were willing to make, so we consider the study results appropriate for this goal.

Although our findings provide important baseline data and novel directions on determining the tradeoff between usability and security, further investigations must address the study's limitations and generalize its findings. ■

Acknowledgments

The research that led to these results was funded by a project in the Hessen ModellProjekte framework (HA project 435/14-25) and financed by Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz, Förderlinie 3: KMU-Verbundvorhaben (State Offensive for the Development of Scientific and Economic Excellence).

References

1. "Election Principles (Article 38 I GG)," Bundestag, Basic Law for the Federal Republic of Germany, *Federal Law Gazette Part III*, classification no. 100-1, as amended by Article 1 of the Act of 23 Dec. 2014 (*Federal Law Gazette I*, p. 2438); www.gesetze-im-internet.de/englisch_gg/englisch_gg.html.
2. S. Neumann, "Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements," PhD thesis, Computer Science Dept., Technische Universität Darmstadt, 2016; tuprints.ulb.tu-darmstadt.de/5375.
3. *PandaLabs Quarterly Report Q1 2016*, tech. report Q1 2106, Panda Security, 2016; www.pandasecurity.com/mediacenter/src/uploads/2016/05/Pandalabs-2016-T1-EN-LR.pdf.
4. D. Chaum, "SureVote: Technical Overview," *Proc. Workshop Trustworthy Elections* (WOTE 01), 2001; www.iavoss.org/mirror/wote01/pdfs/surevote.pdf.
5. M. Volkamer, O. Spycher, and E. Dubuis, "Measures to Establish Trust in Internet Voting," *Proc. 5th Int'l Conf. Theory and Practice of Electronic Governance* (ICEGOV 11), 2011, pp. 1–10.
6. J. Brooke, "SUS—A Quick and Dirty Usability Scale," *Usability Evaluation in Industry*, CRC Press, 1996, pp. 4–7.
7. K. Gjøsteen, "The Norwegian Internet Voting Protocol," *Proc. 3rd Int'l Conf. E-Voting and Identity* (VoteID 11), 2011, pp. 1–18.
8. P.Y.A. Ryan and V. Teague, "Pretty Good Democracy," *Int'l Workshop Security Protocols*, Springer, LNCS 7028, 2009, pp. 111–130.
9. J. Budurushi et al., "Pretty Understandable Democracy—A Secure and Understandable Internet Voting Scheme," *Proc. 8th IEEE Conf. Availability, Reliability and Security* (ARES 13), 2013; doi:10.1109/ARES.2013.27.
10. J. Sauro, "Measuring Usability with the System Usability Scale (SUS)," MeasuringU blog, 2 Feb. 2011; www.measuringu.com/sus.php.
11. M.J. Crawley, *The R Book*, 2nd ed., Wiley, 2012.
12. Y. Croissant, "Estimation of Multinomial Logit Models in R: The mlogit Packages," R Project, 2012; cran.r-project.org/web/packages/mlogit/vignettes/mlogit.pdf.

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

Stephan Neumann is a postdoctoral researcher at the Center for Research in Security and Privacy at TU Darmstadt. His research focuses on usable secure digital communication and the security of electronic voting systems. He's the area head of secure digital communication in SECUSO. Contact him at stephan.neumann@secuso.org.

Jurlind Budurushi is a postdoctoral researcher at the Center for Research in Security and Privacy at TU Darmstadt. His research focuses on security and privacy delegation and electronic voting system security. He's the area head of privacy in SECUSO. Contact him at jurlind.budurushi@secuso.org.

Melanie Volkamer is professor of usable privacy and security at the University of Karlstad as well as a professor at TU Darmstadt. She's the head of SECUSO. Contact her at melanie.volkamer@secuso.org.