User Study of the Improved Helios Voting System Interfaces

Fatih Karayumak, Michaela Kauer, M. Maina Olembo, Tobias Volk and Melanie Volkamer
Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
Darmstadt, Germany
Email: name.surname@cased.de

***Abstract*—There is increasing interest in cryptographic verifiability in remote electronic voting schemes. Helios is one example of an open-source implementation. In previous work, we proposed an improved version of the original Helios interface in version 3.1 for vote casting and individual verifiability. We now test this interface in a mock mayoral election set up with 34 users. Users are given instructions and fill out questionnaires before and after the vote casting process. Data on mouse movements and time is collected and a modified helmet with eye tracking lenses is used to capture eye movement data. The study shows that the interface is easy to use while people have difficulty understanding the motivation for and the concept of verifiability.**

I. Introduction

Internet voting has for many years attracted the attention of the general public, election officials and security researchers among others. Remote internet voting systems have been used in actual elections for a couple of years in some countries on different levels like in Estonia and Switzerland. Those election officials that enable remote e-voting rarely use verifiable voting protocols proposed by the security community, instead opting for black box systems which need to be trusted.

There is a move towards using cryptographically verifiable schemes to enable voters and the public verify that votes are cast as intended, stored as cast (both constitute individual verifiability) and tallied as stored (universal verifiability). This is as a result of changes in legislature, for example in Germany [1], as well as a push by the general public. There already exist very promising cryptographically verifiable voting schemes, like Helios [3] and Civitas [7]. While security analyses of these schemes have been undertaken, their usability and practicability has in the past been neglected. The core of our research is making verifiable remote e-voting systems user friendly, practical, and understandable. We focus on the Helios voting system as it has been implemented including user interfaces.

In previous work, [12], we carried out a usability analysis of Helios using the cognitive walkthrough approach and concluded that the Helios interface is not yet ready for use by average voters. Specifically, the individual verifiability process is long and tedious and may result in a voter either not verifying their vote, or failing to complete the vote casting process. We proposed new interfaces to improve the usability of the vote casting and individual verifiability process. Our focus is on the cast as intended aspect of individual verifiability. This is most important as all other steps can be done by an external party without breaking election secrecy.

In this paper we present the findings of a preliminary user study undertaken to evaluate the proposed new interfaces for Helios. The election is a mock mayoral election in Darmstadt, Germany. We present related work (Section II) and later briefly introduce Helios version 3.1 before discussing the suggested improvements (Section III). The methodology and details of the user study are next (Section IV), and the results are presented and analysed thereafter (Section V). General findings deduced from the results, conclusions and future work are proposed in Section VI. The appendices contain screenshots of the interfaces, user instructions, and the questionnaires.

II. Related Work

A few studies on the usability of e-voting systems have been undertaken. Non-remote and non-verifiable e-voting systems have been analysed for example in [4], [8], [9] and [10]. The usability of verifiable e-voting devices used in polling stations has been of interest e.g. in [15], Prêt à Voter is analysed, and in [13], DualVote. In [2] and [11], voting systems providing voter verifiable paper audit trails have been analysed regarding their usability and corresponding analysis has been undertaken for ballot scanning techniques in e.g. [6]. The usability of Helios version 1.0 has already been assessed in [14]. There the authors set up a mock student government election, and had twenty voters participate to verify and cast a vote. They found that the Helios version 1.0 user interface was not user friendly. We used their results for improving the interface in [12] and extended their questionnaire for the study we conducted.

III. Helios Voting System and Improved Interfaces

Helios is an open-source, cryptographically verifiable remote electronic voting system implemented and presented by Ben Adida [3]. It is currently available in version 3.1[1]. It requires that a voter's web browser has Java Script enabled. Communication is secured by SSL and voter authentication is secret-based.

Ballot preparation and casting is based on Benaloh's Simple Verifiable Voting Protocol [5] and Benaloh's challenge. Ballot preparation is separate from ballot casting which allows any

[1] www.heliosvoting.org

This work has been published in the First Workshop on Socio-Technical Aspects in Security and Trust (STAST), 2011. IEEE 2011 ISBN 978-1-4577-1181-7.
DOI: http://dx.doi.org/10.1109/STAST.2011.6059254

interested party (and not only voters) to view and fill out a ballot for an election. Their vote will be encrypted (locally) and the system commits to this encryption by creating and displaying a hash of the ciphertext (the so called verification code). One can then choose to verify this vote, to ensure that it has been encrypted correctly and thus verify the step 'cast as intended'. When the voting system is challenged, an independent entity receives the plaintext and the random value used for encryption. This entity generates the ciphertext on its own as well as the corresponding hash value. This is displayed together with the plaintext vote. The user needs to verify whether this matches the actual candidate selected and the earlier displayed verification code. Once a vote is verified, it has to be re-encrypted to ensure voter privacy.

This process can be repeated an arbitrary number of times. Once satisfied with the correctness of the encryption, the voter can proceed to finally cast their encrypted vote[2]. Here the voter is authenticated and their vote captured. Note, obviously, this last step is possible only for authorized voters. In the context of usability and understandability it is relevant to note that one cannot cast a verified vote. The verification code belonging to the vote that is cast cannot be used to verify that the vote has been cast as intended (i.e. properly encrypted), while it can be used to verify that the vote has been stored as cast. This can be done by the voter (or someone on behalf of the voter) visiting the election web page at the end of the election period where all verification codes of cast votes are displayed. Further techniques implemented to verify that all stored votes are properly tallied are not discussed here because we focus only on the 'cast as intended' step in our study.

In [12], we carried out a cognitive walkthrough on version 3.1 of Helios. Based on our findings we proposed improvements to the Helios interfaces and processes while assuming a different setting from the one provided by the Helios web page. This includes using postal mail instead of email to distribute voting credentials[3], running only one election which makes the reference to particular election IDs unnecessary, and integrating several different institutions to handle the verification. Fig. 1 shows the individual verifiability process in the original version and Fig. 2 in our improved version to give the reader an idea of this work.

We made several general usability improvements like integrating back and forward buttons in the interface and improving the menu bar, e.g. in Fig. 12 and utilising consistent wording. In addition, we suggested the following: The election letter contains a URL for the voter to directly access the vote casting website while in the original version, the voter would click a link in the email and first be directed to a web page with potentially confusing instructions. In addition, the letter contains SSL certificate information of the voting server as well as of the institutions' servers accessible for verification

[2]The idea is that the Java Script never knows whether voters opt for verifiability or not and therefore need to behave properly.

[3]Assuming a reliable postal mail system, this is a secure way of distributing login credentials as average email systems without encryption can easily be compromised. Users may also be more familiar with this approach.

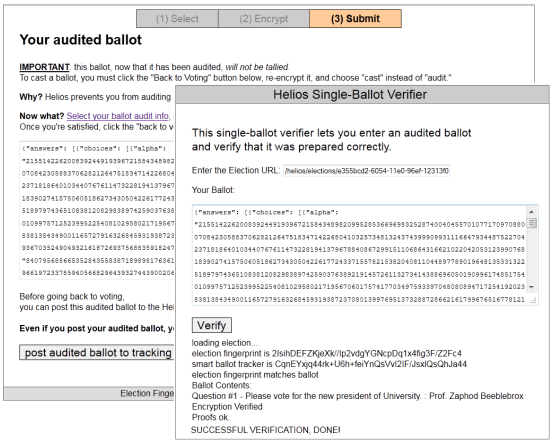

Fig. 1. Verifiability Process

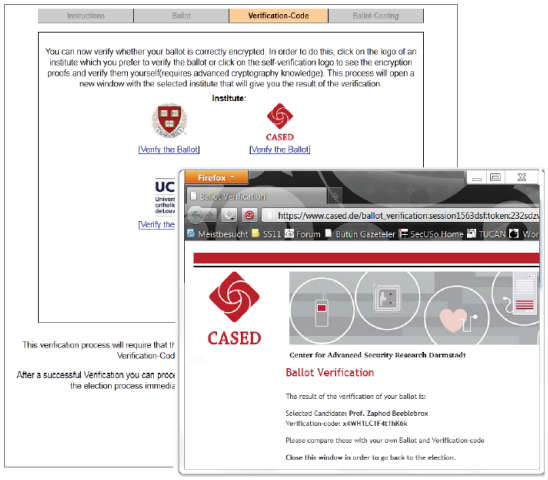

Fig. 2. Verifiability Institutions and Results

purposes (see Fig.10). We modified the text in the letter and the instructions on all interfaces and in particular on the first page (refer to Fig. 11). The main contribution is the simplification of the verification process (compare to Fig. 1 and Fig. 2). In this context we also proposed to shorten the verification code and improved the instructions in particular by explaining the purpose of this verification code, what exactly needs to be compared, and that it changes after the voter verifies their vote due to privacy issues (refer to Fig. 13). Finally, the confirmation and authentication process has been simplified (refer to Fig. 14) and the final page provides instructions for the next step to verify whether the vote has been stored as cast (refer to Fig. 15).

IV. Evaluation of the Improved Helios Interfaces

The main purpose of the user study was to evaluate whether the vote casting and the individual verification step in terms of cast as intended was user friendly and whether all voters who want to verify are able to do so.

The election used is a mock mayoral election in Darmstadt. The questionnaires and interaction with the voters were

originally in German and are translated into English, whereas the screen interfaces proposed in [12] were translated from English to German. We integrated several institutions namely the Federal Agency for Security in Information Technology (BSI), our university, our security research institute (CASED) and the TÜV-IT as we assumed these would be more familiar to the participants. In addition, the option for self-verification based on the provided data was not made available as voters were most likely not able to write their own verification program in the short time given. The final page has been modified as we only test the cast as intended aspect of individual verifiability.

The interfaces were re-written from scratch as a server-side web application because it was easier to implement the desired changes including extensive logging of the users' actions, since every page in the voting system was fetched from the web server. The original look and feel was retained. However, the server side logging does not provide information regarding people having printed or saved the verification code on the computer. To ensure quality of the implementation and the interface design, several versions were evaluated in small pre-tests before the study started.

We opted for a lab test as opposed to a field study so as to have full control over the test environment. Additionally, the setup of a laboratory study allowed us to collect additional data, like videos with eye-tracking, and thereby gave a deeper insight into the usability of Helios and into the users' understanding of verifiable e-voting. The lab used was a room set up with a computer for the user to cast their vote and answer a web-based questionnaire. The computer was configured to allow the participants to browse any other web page and not just the voting web pages. Only the voting and the verification pages were redirected to our own server.

A modified bicycle helmet with eye tracking lenses was connected to a separate laptop. This was first configured for each participant prior to their beginning the process. Not all users had this eye movement data collected due to configuration challenges. The eye tracking enabled us to check whether participants really verified the codes character by character and the videos were used to evaluate if participants printed or saved the verification code.

Participation was invited from both technical and non-technical users. Recruitment was by word of mouth invitation and compensation was in the form of a USB memory stick with the institution's logo. There were 34 participants, half female and half male. The average age was 28.5. The youngest was 18, the oldest, 47 years old[4]. 22 (65%) of the participants had a technical background, deduced from one question asked to the participants (scale of 1-5 where 5 indicates very high technical understanding; we categorised 1-3 as non-technical and 4-5 as technical background). All participants were fluent in German.

The average duration of each test was 30 minutes (including time to configure the helmet). The participants first answered a questionnaire with general questions on age, gender and computer knowledge (Table I). Next they used the voting system for the first time, with no guidance and no information on verifiability[5]. After the vote was cast or the process was aborted by the user, they then answered a second questionnaire on their opinion about the system (Table II). The user was then given instructions (Appendix B) for the vote casting and verification process. They were explicitly instructed to use the verification function of the system, and then they used the voting system once again to cast a vote. By entering the authentication tokens and finally casting their vote, they were done. Upon completion, users filled out an exit questionnaire (Table III). Besides questions on the general usability of the voting system and the individual verifiability there were also questions on users' concerns over the security of the voting website. We considered their awareness of phishing attacks as well as use of SSL certificates to authenticate websites. Finally we sought to determine what wording is appropriate and readily identifiable to users in the context of verifiability in remote e-voting.

V. Results

In this section, we provide the results of the study regarding usability and understandability as well as the participants' opinion about eBanking and eVoting in general.

A. eBanking/eVoting

Only five participants (14%) do not use eBanking, while two out of these five would like to use Internet voting for any type of elections (although they do not see a need for eBanking). The remaining three would not like to use Internet voting (either at all or at least not for parliamentary elections). Eleven participants out of the 29 eBanking users do not want to use Internet voting at all and justified this with general open security issues. One stated that the Internet is in general not secure (although this participant indicated that they use eBanking). Participants in favor of Internet voting saw benefits in its flexibility, ease of use, fast results, and greater convenience compared to postal voting. Participants tended to compare Internet Voting to postal voting.

B. General usability

After the first test run the users were asked to rate the user friendliness of the voting system. Various statements were presented to the users, which could be rated on a 7-point scale from "do not agree at all" to "fully agree". The result is rather positive (see Fig. 3[6] for results).

Almost all users were able to successfully cast their vote in the first test run (without instructions) and the second test run (with instructions). Only one user aborted the voting process, because he did not trust the verification mechanism.

[4]As this is a preliminary study, we do not analyse usability and accessibility issues for the elderly and this will be considered in future work.

[5]Our assumption was that also in real elections, it cannot be assumed that people are aware of the new features of a newly introduced voting channel.

[6]For all these figures, 1 means "do not agree at all" and 7 "fully agree".

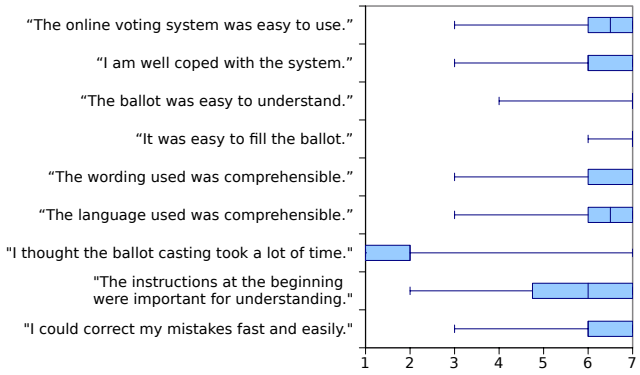

Fig. 3. Rating of User friendliness

We started measuring the time taken as soon as the participant opened the website of the voting system and stopped when the participant had successfully cast their vote. In the first test run users needed 3.8 minutes on average, 5.6 in the second run. Most users found the time required for the voting process acceptable (see also Fig 3).

C. Who is interested in verifying?

In the first test run, the verification function was used by 20 of 34 participants (59%), 59% of those with a technical background and 58% of those without, opted to verify. There is no correlation between the technical skills of the participants and the fact that they opted for verification in the first test run. In the second test run, the verification function was used by 32 of 34 participants (94%). This was expected, since it was suggested in the instructions. It was however surprising that not all participants verified their vote.

In the questionnaire after the first test run, six people stated that they did not verify at all, 14 claimed to have verified once, six twice, three three times, and five four times. The real number of verifications carried out is different, looking at the number of visited institution websites in the logfiles: 14 people did not verify at all, eight once, five twice, four three times, two four times, and one person verified five times[7]. Seven people who claimed to have verified at least once did not verify at all (compare to Fig 4). These people likely confused "verifying" with double checking that the ballot was correctly filled. The other 27 people correctly estimated, with some minor deviations, the number of times they verified their vote.

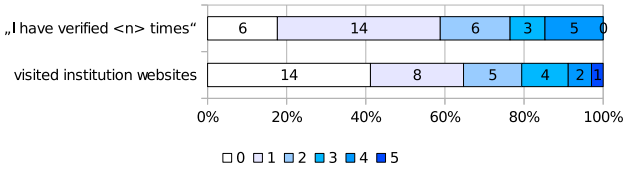

Fig. 4. Number of Verifications as Claimed vs. Actual Verifications

[7]Note, verifying x times means that the vote was re-encrypted $x-1$ times, i.e., one went back to the corresponding interface (from Fig. 2 to Fig. 13).

Two participants who claimed to have verified - but actually did not according to the log files - went to the verification page with the institution logos, but did not visit any institution website to do an actual verification. These two participants are therefore also counted as not having verified. From the videos, it can be seen that some participants compared the verification codes only by having a quick overview, and not on a character-by-character basis while others compared character-by-character. 29 of the 34 participants stated that they would prefer to have a system that enables verifiability. However, only 24 of the 34 participants believe that such a system is more secure than one without. Four of the five people that were in favor of a system without verifiability had a technical background and were concerned with privacy issues ("The institutions can see my vote!"), found the procedure to be too cumbersome ("Writing down a new security code each time annoys me.") or thought that "normal" people would find it to be too cumbersome. However, only one of the participants without a technical background preferred a system without verification, finding it too complicated. The others seemed to be fine with the verification, and thought that the added security would be worth the extra effort.

D. Do people have enough information to properly verify and cast their vote?

16 of the 34 participants stated that the provided information was not enough. One participant stated that proceeding with vote casting was possible even though he/she did not read the information on the first screen. People categorised as having a non-technical background complained about too much information in particular on the first page while the other group wanted more detailed information, e.g. papers, security proofs, statements from other institutions about the security of the voting system, e.t.c. Only one of the 20 participants who chose to verify in the first test run stated that they did not notice that the verification code changed after their having verified the encryption. In the second test run another participant (who did not verify in the first test run) did not notice the change in the verification code. The other 31 of the 32 participants who verified in the second test run noticed the change. Only eight of the 34 participants stated after the second test run that it was not clear to them that they needed to compare the verification code and their selection on the verification page from the selected institute. All people who stated they were aware that this was necessary did compare the values as well according to their own statement. Almost all participants (33 of the 34) understood that the vote had not been cast after having been properly verified. 31 of 34 participants agreed that it is necessary to introduce the concept of verifiability before applying such a system for legally binding elections.

E. Which is the preferred type of verification?

Of the 20 participants who went for the verification in the first test run, 17 (85%) wrote down the hash values, nine (45%) saved them to a file, and only four (20%) printed them (multiple methods can be used at the same time). In the second

test run, the participants were asked to try out all methods for storing the hash values. In the questionnaire after the second test run they were asked which method they preferred. 21 (62%) of the 34 participants preferred to write down the hash values, ten (29%) preferred saving to a file, and three (9%) preferred printing. From the videos made during the study it can be seen that some people were a bit confused while trying to save the hash values to a file and retrieve them again. This is likely caused by the fact that the software configuration on the computer used by the participants was not the same as the configuration of their computers at home. Most participants did not use the printing method, including in the second test run, where this was explicitly suggested in the instructions. Probably the participants thought that this method would be too cumbersome.

F. Do people understand why they need to verify and what they verify?

The tested verification only ensures that the vote is correctly cast, however participants had slightly less trust in this than in the proper tallying. It would be expected that the trust level in proper tallying is lower than in correct vote casting. However, there was no significant difference in the responses to the two questions, which indicates that it was not clear for the participants that these are actually two different concepts while they had only the chance to verify the first of these two steps.

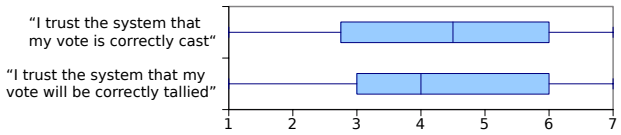

Fig. 5. User Confidence in Correctness of the Voting Process (All)

From Fig. 6 and Fig. 7, it can be seen that participants with a technical background tend to trust the system less than those without. This is likely caused by the fact that the system did not present information about technical details.

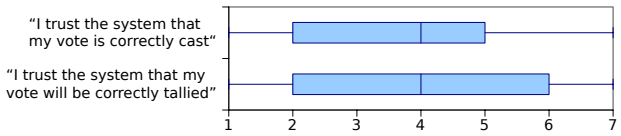

Fig. 6. User Confidence in Correctness of the Voting Process (Tech)

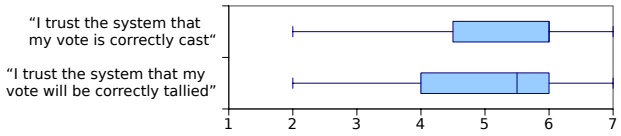

Fig. 7. User Confidence in Correctness of the Voting Process (Non-tech)

One typical statement was "System was easy to use (for vote casting and also verification) but I did not understand the idea of the verification code". Participants also complained that it was unclear why they should trust the verification procedure while they cannot trust the main voting system which makes the verification necessary. Others did not understand that they can verify test ballots, but not the one that is to be cast. Surprisingly, only four of the 24 participants who believe that such a system is more secure than one without verification believe that this is only true if all voters verify while the others agree that it is not necessary that everyone verifies. While this is true it is unclear why the participants agree on this.

G. Do participants worry about the vote secrecy issues arising from the verification of the encryption?

According to Fig. 8 twelve of the 20 people who really verified and 14 of the 28 who claimed to have verified in the first test run worried about the fact that they could see their vote at the institution website in clear text, and that the institution could see what they have voted for (which is not true, since the ballot can still be changed and is re-encrypted afterwards). Furthermore, from the statements some participants made, it became obvious that the concept of re-encryption and correspondingly the reason for the new verification code was not clear to them. The 32 participants that did the verification in the second test run were asked whether it was clear to them that the ballot is re-encrypted after a verification. 26 (81%) answered with yes. However, 19 (73%) of those still answered that they were irritated by the fact that their verification code changed. This is another indication that most participants did not fully understand the reason behind the re-encryption.

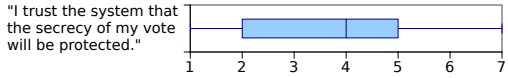

Fig. 8. User Confidence in the Vote Secrecy Protection

Only two (10%) of the 20 participants who verified their selection in the first test run modified the selection after having verified a test vote. This changed in the second test run, where 27 (84%) of the 32 participants who verified changed their vote. This was expected, since changing the vote was part of the instructions. One person also thought that it might be possible to somehow derive the ballot from the hash (which is not possible since it is a hash function/value). It was assumed that this is the way the institutions get the information about the ballot and consequently the participant worried that others could do the same. Of interest also was the statement of one participant, who was not afraid of seeing the selection of the institution web page, saying that he/she knows that this institution is well known for its high data protection standards.

H. Are voters irritated when logging in for the first time at the end of the vote casting?

One half of the participants was irritated, the other not, as shown in Fig. 9. Typical web services require the users to

log in before they can do anything useful, so this might be irritating to them.

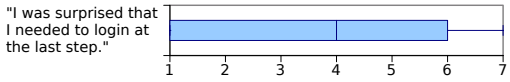

Fig. 9. User Irritation by Delayed Login

Some participants stated that they are in particular surprised that they could verify without being authenticated.

I. Type of institute

The participants had the choice of four different institutes for the verification. Most participants were content with this selection of institutes. One participant demanded a larger selection, but did not suggest institutes that could be added. In the first test run 14 participants used BSI, 12 CASED, 13 TU Darmstadt, and six TÜV IT, for verification (in the second run: 37 BSI, 39 CASED, 31 TU Darmstadt, and 24 TÜV IT).

J. Do people verify the SSL certificate?

77% of the technically experienced users did not verify the SSL certificates, although 82% claim to be able to verify an SSL certificate. Almost all of the participants that did verify the certificate did so only for the voting system itself, and not the institution websites. Only one participant also verified the certificates of the institution websites. Almost all participants that verified the certificates (with one exception) claimed to also verify the e-banking SSL certificates. None of the technically inexperienced users verified the SSL certificates. Some of the participants with a technical background who did not verify the SSL certificates in the first test run did so in the second test run, although there were no explicit instructions to do so. Most likely the questions about SSL in the questionnaire after the first test run caused the participants to give more attention to this in the second test run. Almost all of those who did verify the SSL certificates also thought that there was a secure connection to the election server, one person still was not sure although he verified the certificates. About half of those who did not verify said that there was a secure connection, simply because HTTPS was used and the browser did not give any warnings. One person said that the websites looked “official”.

VI. Conclusion and Future Work

As a summary of the results, one can state that the user friendliness of the system has reached an acceptable level and in particular has been improved compared to version 1.0 and the results from [14]. However, most participants neither understood the need for verification nor the reason why the final vote to be cast could not be verified. The whole idea seemed to scare them regarding voters’ privacy. While this overall result was not that surprising there were two specific statements that were surprising, namely: The fact that people worried about the institutes knowing how they voted; and in particular the statement of one participant who was afraid that from the hash value (named verification code) everyone who is familiar with cryptography is able to deduce votes from the verification code like the verifications intuitions do to be able to display the plaintext vote (what is not true as the verification institutions get the plaintext information already from the Java Script). After having reviewed the interfaces again we agree on required improvements regarding explanations of the concept of test ballots for arbitrary votes that can be verified. This is currently not explained before seeing the first verification code. Actually, it is surprising that participants did not complain that they were not informed before.

Currently, we see two different ways to address the problem of not understanding the concept of verifiability. One could provide interfaces where only experts who understand the purpose of verifiability will most likely opt for it while others will cast their vote while not really noticing that there is a possibility to verify. However, what would remain is the information about the verification code which needs to be displayed to everyone. This is the approach chosen by the designers of Helios. We criticised this in [12] as then most voters do not opt for the verification and thus do not have an equal chance to secure their vote by verifying test votes and challenging the system.

Another option would be to have a campaign running before the election with such a system explaining the need for verification and how it works on an abstract level. By doing so, a lot of the information provided on the interface could be provided during the campaign. Note, when explaining verifiability, it is important not to bias people about this new system or about the fact that past elections might have had a problem because verifiability was not provided in the same way as in the new system. One way to test whether this helps would be to produce a very short video which would be shown to participants of a user study before they use the system and see whether this aids understanding. By doing so one could try to use metaphors to explain encryption, for example, that verification is only possible when opening an envelope and correspondingly afterwards a new one is required because the old envelope is unusable. In order to realise this approach, a cooperation with those in marketing research would be desirable in order to sell the benefits of verifiable electronic voting systems. Both alternatives need to be discussed with voters, legal scientists and psychologists/social scientists and is left as future work.

The study also shows that it is necessary to better understand the users’ model about verification. Thus, future work also includes interviews with people about their idea of verification. This result will also help to produce a short video as proposed, that is understandable.

Besides this we learned several lessons from this study:

- It might be helpful to exclude people from a user test who are against electronic voting, in turn, it might be of high interest to have interviews with these people to identify main concerns.
- There is a need to clearly explain that the motivation is to replace postal voting with Internet voting because

if not people comment on either the benefits of using Internet voting instead of going to the polling stations or they refer to the general problems of remote voting (like family voting). While both are interesting to read, they do not serve as input to solve the problems addressed by the study.

- It is important to try to get participants that have really cast their votes in the election you use as mockup for the user test. This might make it easier to give them a feeling their real vote needs to be properly included in the tally. Some participants stated this time that one might be more motivated to go for extra steps for verifying and checking the codes more properly when there is a legally binding election rather than just a user study.

Besides these improvements to the user study and the idea of producing a video explaining the concept of verifiability, we see some potential to further improve the technology. For example, an application for mobile phones with integrated cameras enabling the user to take a photo of the hash values and the encryption in Quick-Response (QR) or two-dimensional code format and run the verification on an app on the handset. Regarding, the second step of individual verifiability, we plan to enable voters to send the verification code of their final vote to one or several of the trusted institutes to take care that the vote is stored and tallied.

As people obviously also do not verify HTTPS certificates and as probably many are also not able to do so, future work will include this challenge as well. Note, if people do not verify the certificate of the institutes they select for verification the whole process is meaningless. Thus, a first step would be to use extended validation certificates and inform the voter to confirm validity by, at the very least, for example checking that the browser shows the green bar.

Acknowledgment

This work was supported by CASED and Micromata.

References

[1] Bundesverfassungsgericht (BVerfG) In: German Federal Court Decisions, Urteil des Zweiten Senats, 2 BvC 3/07 pp. 1-163.

[2] A Study of Vote Verification Technology Conducted for the Maryland State Board of Elections Part II: Usability Study. Technical report, CAPC Report on Vote Verification Systems, 2006.

[3] B. Adida. Helios: Web-based Open-Audit Voting. In *Proceedings of the 17th Symposium on Security*, pages 335 – 348, Berkeley, CA, USA, 2008. Usenix Association.

[4] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi. Electronic Voting System Usability Issues. In *CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 145–152, New York, NY, USA, 2003. ACM.

[5] J. Benaloh. Simple Verifiable Elections. In *EVT'06: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2006. USENIX Association.

[6] M. D. Byrne, K. K. Greene, and S. P. Everett. Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines. In *CHI '07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 171–180, New York, NY, USA, 2007. ACM.

[7] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: Toward a Secure Voting System. *Security and Privacy, IEEE Symposium on*, 0:354–368, 2008.

[8] F. G. Conrad, B. B. Bederson, B. Lewis, E. Peytcheva, M. W. Traugott, M. J. Hanmer, P. S. Herrnson, and R. G. Niemi. Electronic Voting Eliminates Hanging Chads but Introduces New Usability Challenges. *Int. J. Hum.-Comput. Stud.*, 67:111–124, January 2009.

[9] S. P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. PhD thesis, RICE UNIVERSITY, 2007.

[10] P. S. Herrnson, B. B. Bederson, B. Lee, P. L. Francia, R. M. Sherman, F. G. Conrad, M. Traugott, and R. G. Niemi. Early Appraisals of Electronic Voting. *Soc. Sci. Comput. Rev.*, 23(3):274–292, 2005.

[11] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, and M. Traugott. The Importance of Usability Testing of Voting Systems. In *EVT'06: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*, pages 3–3, Berkeley, CA, USA, 2006. USENIX Association.

[12] F. Karayumak, M. Kauer, M. M. Olembo, and M. Volkamer. Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System. In *Proceedings of the 2011 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2011.

[13] D. Macnamara, T. Scully, J. P. Gibson, F. Carmody, K. Oakley, and Q. Elizabeth. DualVote: Addressing Usability and Verifiability Issues in Electronic Voting Systems. In *Conference for E-Democracy and Open Government (CeDEM11)*, 2011.

[14] J. Weber and U. Hengartner. Usability Study of the Open Audit Voting System Helios. www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf, 2009.

[15] M. Winckler, R. Bernhaupt, P. Palanque, D. Lundin, K. Leach, P. Y. Ryan, E. Alberdi, and L. Strigini. Assessing the Usability of Open Verifiable E-voting Systems: A Trial with the System Prêt à Voter. In *Proceedings of ICE-GOV 2009, pp. 281-296.*, 2009.

Appendix

A. Screenshots of Improved Interfaces

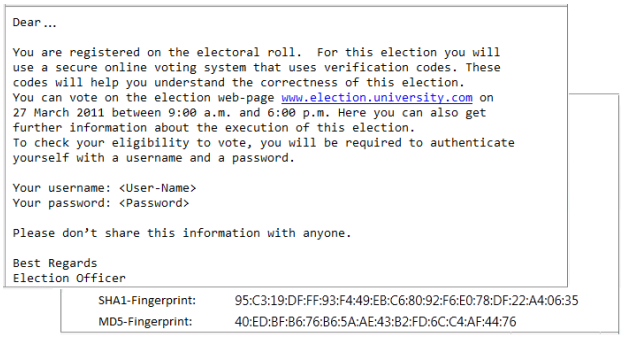

Fig. 10. Invitation to Vote Letter

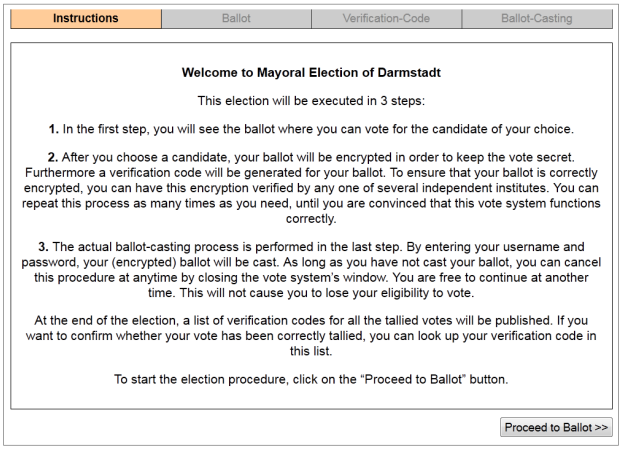

Fig. 11. Instructions to the Voter

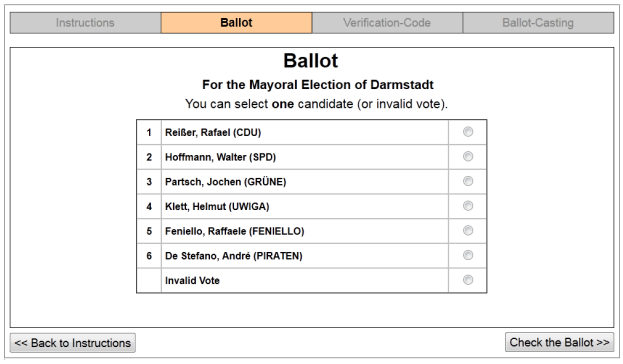

Fig. 12. Ballot with Candidate Information

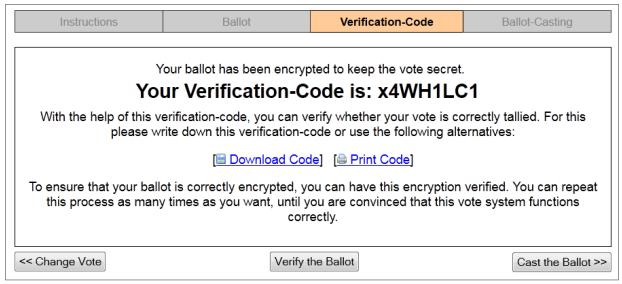

Fig. 13. Verification Code

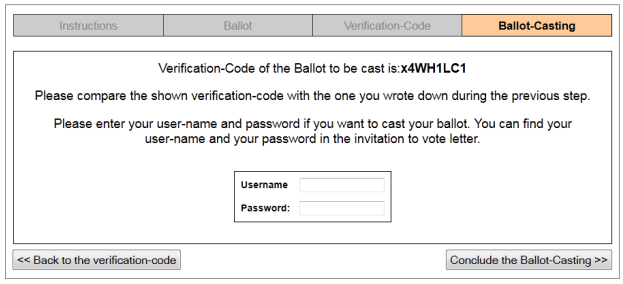

Fig. 14. Voter Login Page

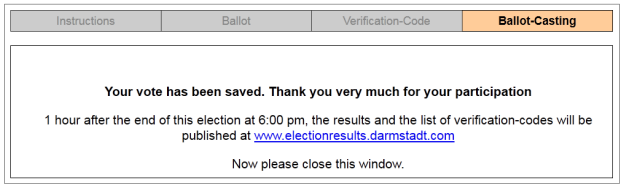

Fig. 15. Ballot Cast Successfully

B. Instructions for Second Test Run

1) Choose a candidate and encrypt the choice but do not cast your ballot, yet.
2) Change your choice to another candidate and re-encrypt your choice.
3) Write the Verification-number on a piece of paper.
4) Let the encrypted ballot be verified by an institute.
5) Finish the verification and proceed with the election.
6) Repeat the 2. and the 5. Steps several times (at least twice). Change here the chosen candidate and try all of the proposed Methods to verify the verification-code(write-down, download, print).
7) Change your ballot one last time. Choose the candidate for whom you are willing to vote (it does not need to be the candidate for whom you are willing to vote in an actual election).
8) Click on the 'cast the ballot' and give your username and password in the next page.

C. User Study Questionnaire

TABLE I
PRETEST QUESTIONNAIRE

How old are you?	Age: — old
What is your gender?	Male/ Female
What is your education level?	No degree/ Middle school/ High school/ BA/ MA
How often do you use the Internet actively?	Less than an hour in a day/ 1-3 Hours/ 4-8 Hours/ 9-10 Hours/ More than 10 hours in a day
How do you assess your own computer & internet knowledge?	Very low/ low/ average/ high/ very high
Do you use home banking?	Yes/ No
Why do you or do not you use home banking?	*text*
Would you vote in the future over the Internet?	Yes, generally/ Only if I am traveling abroad/ Only for non-parliament elections/ Not at all
Please justify your answer shortly.	*text*

TABLE II
FIRST QUESTIONNAIRE AFTER VOTING

The online-voting-system was easy to use, I am well coped with the system, The ballot was easy to understand, It was easy to fill the ballot, I thought the ballot casting took a lot of time, I trust the system that my vote is correctly cast, I trust the system that my vote will be correctly tallied, I trust the system that the secrecy of my vote will be protected, The instructions at the beginning were important for understanding, The wording used was comprehensible, The language used was comprehensible, I could correct my mistakes fast and easily, I was surprised that I needed to login at the last step	Please rate the following statements (do not agree at all - fully agree)
Do you have any other comments/ suggestions to improve the system?	*text*
How many times did you verify your (encrypted) ballot, before you cast it?	I verified — times.
If you verified your ballot, why? If not, why?	text
The verification-code, did you ...	write down?/save in the computer?/ print it out?
Which institute did you choose to verify your ballot?	BSI/CASED/TU Darmstadt/TÜV IT
Would you choose other institutes? If so, which ones?	
Did you change your vote, after you verified it?	Yes/ No
Have you had any concerns about the secrecy of your vote when you saw your vote on the site of the verifier?	Yes/ No
If so, why? If not, why not?	*text*
Did you realise that you received a new verification-code after the verification?	Yes/ No
Would you say that there existed a secure connection to the election-server?	Yes/ No
If so, why? If not, why not?	*text*
Do you know what SSL is and how you can verify a SSL-Certificate?	Yes, No
Did you verify the SSL certificate?	Yes, for the voting system/Yes, for the external-institute/ Yes, for both/ No
Do you verify the SSL certificate for home-banking?	Yes/ No/ I do not use home-banking

TABLE III
FINAL QUESTIONNAIRE

Would you use a system with or without verification?	Yes/ No
Which method do you prefer to preserve your verification-code?	Write down/ save/ print
Do you believe that a system with verification possibility is more secure than a system without it?	Yes/ No
If you answered "yes" for the previous question: Do you believe that it still applies if not all the voters use this mechanism to verify their ballots?	Yes/ No
Why do you think a system with verification is more secure or why it would not be?	*text*
Were you aware that you needed to compare the verification-code and your vote on the external site of the institute?	Yes/ No
If yes: Did you compare?	Yes/ No
Were you aware that you needed to compare the verification-code and your vote on the login-page?	Yes/No
If yes: Did you compare?	*text*
Did you change your ballot after you verified it once?	Yes/ No
Do you find it confusing to receive a new verification-code after the verification?	Yes/ No
Was it clear for you that the ballot was not cast after the successful verification of the encrypted ballot?	Yes/ No
Was it clear for you that the ballot needed to be re-encrypted after the successful verification of the encrypted ballot?	Yes/ No
Did you realise that you received a new verification-code after the verification?	Yes/ No
Was the information lacking for you?	Yes/ No
If yes, which one?	*text*
Do you find the word "verification-code" appropriate?	Yes/No
If not, which term would you prefer?	*text*
Were there any terms which were unclear for you? If so, which were these?	*text*
Do you find it necessary to inform the voter about verifiability before using the system?	Yes/ No
Do you have general comments on the voting-system or this study?	*text*