Poster: Usable Verifiable Remote Electronic Voting - Usability Analysis of the Helios System

{Fatih Karayumak, Michaela Kauer, Maina M. Olembo, Melanie Volkamer}
CASED, TU Darmstadt
Mornewegstrasse 32
Darmstadt, Germany
Name.Surname@cased.de

1. INTRODUCTION

Internet voting has for many years attracted the attention of the general public, election officials and security researchers. However, only very few remote internet voting systems have been used in actual elections. Those election officials that enabled remote electronic voting rarely use voting protocols proposed by the security and cryptography community, instead opting for black box systems that need to be trusted as it is not possible for the public to verify the election in any terms. On the research side there already exist very promising end to end verifiable voting schemes (that incorporate both individual and universal verifiability), like Helios and Civitas. From a cryptographic perspective the main challenge is to find an appropriate balance between verifiability, anonymity and coercion resistance while ideally ensuring all three to a particular extent. The usability and practicability of these schemes has in the past been neglected. Many protocols are too complex for average voters to interact with or even understand the underlying concepts. As a result of this, voters will neither accept such systems nor opt to verify their votes. This would also mean that the system then is not much more secure than an easy-to-use black box system. In our research we focus on making verifiable remote e-voting systems user friendly and practical. We focus on the Helios voting system as it is the only one that has been implemented including user interfaces. In previous work [4], we conducted a usability analysis of Helios version 3.0 based on the cognitive walkthrough approach while focusing on vote casting and the individual verifiability. Based on the findings we proposed new interfaces. We recently conducted a lab study on these improved interfaces. In this abstract we describe the result of the cognitive walkthrough in terms of the improved interfaces and processes. We also propose the setup of the lab study and a first overview of the expected results. Results will be presented in greater detail during the oral poster presentation.

2. RELATED WORK

A few studies on the usability of e-voting sytems have been undertaken: Non-remote and non-verifiable e-voting in e.g. [3]; verifiable e-voting devices used in polling stations where the verifiability is mostly implemented by a paper audit trail e.g. in [7], as well as scan based approaches e.g. in [2]. The NIST special publication [5] also defines usability and accessibility requirements for electronic voting systems. The usability of Helios version 1.0 has been assessed in [6]. The authors set up a mock student election with twenty voters participating. Their findings were that the interfaces were not user friendly at all.

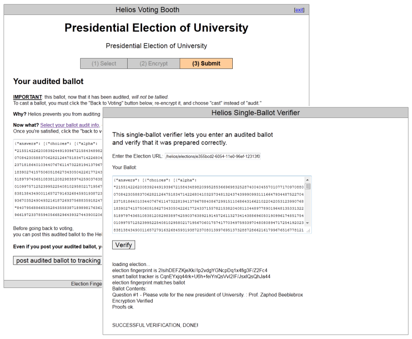
3. THE HELIOS VOTING SYSTEM

Helios is an open-source, end to end verifiable remote electronic voting system implemented and presented by Ben Adida [1]. It is currently available in Version 3.1 [1]. Running Helios requires that a voter's web browser has Javascript enabled. Communication is secured by SSL. Voter authentication is secret-based (received via email). A key feature in its operation is the separation of ballot preparation from ballot casting. This is done in order to provide individual verifiability and secrecy for the voter and allow anyone to challenge the system regarding the cast as intended aspect of individual verifiability. As a result the voter only authenticates at the end of the vote casting process. Due to this fact, everyone is able to make a candidate selection, encrypt it and verify that Helios has encrypted their choice correctly. Once voters are satisfied with the accuracy they are prompted to authenticate themselves in order to cast the vote. The next relevant property when analysing usability of the system is that voters cannot verify the final vote that they choose to cast due to secrecy concerns.

4. IMPROVED USER INTERFACES

With a team of usability experts and e-voting experts, we carried out a cognitive walkthrough on the current version [4]. The e-voting experts had an understanding of the details of the underlying voting protocol. Based on our findings we suggested improvements to the Helios interfaces and processes. In order to give the reader an impression of the improvements, Fig. 1 shows the individual verifiability process in the original version and Fig. 2 in our improved version. We made several general usability improvements (such as back and forward buttons and use of consistent wording) which are not discussed here. In addition, the following improvements were suggested: Voters receive voting information and credentials by postal mail instead via email. This is a more secure way of distributing login credentials and an approach users may be more familiar with. This letter contains a link to access the vote casting website whereas in the original email the voter was first directed to a confusing election web page where they found instructions. We changed the instructions on the first page. After having encrypted the ballot, a verification code is displayed. We shortened this

[1] www.heliosvoting.org



Helios Voting Booth [exit]

Presidential Election of University

Presidential Election of University

(1) Select | (2) Encrypt | (3) Submit

Your audited ballot

IMPORTANT: this ballot, now that it has been audited, *will not be tallied*.
To cast a ballot, you must click the "Back to Voting" button below, re-encrypt it, and choose "cast" instead of "audit."

Why? Helios prevents you from auditing

Now what? Select your ballot audit info,
Once you're satisfied, click the "back to v

Before going back to voting,
you can post this audited ballot to the Hel

Even if you post your audited ballot, y

post audited ballot to tracking

Election Finge

Helios Single-Ballot Verifier

This single-ballot verifier lets you enter an audited ballot
and verify that it was prepared correctly.

Enter the Election URL: /helios/elections/e355bcd2-6054-11e0-96ef-12313f0

Your Ballot:

```
{"answers": [{"choices": [{"alpha":
"2155142262008392449193967215843489820995285366969832528740040455701077170970880
07084230588370628212647518347142268041032573481324374399909931116647934487522704
23718186401034407676114732281941379678840867299151106864316621022042053123990768
18390274157506051862734305042261772433715578215382040811044897789019648135331322
51897974365108381208298389742590376389219145726113273414388696050190996174851754
01099757125239952254081029580217195670601757417703497593397048080894717254192023
83813843490011657279163268459319387237080139976951373288728662161799676516778121
```

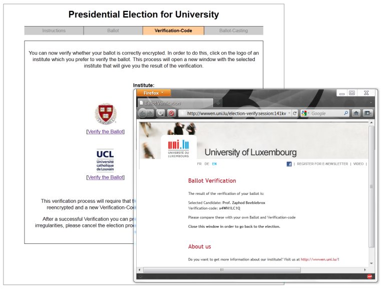
Verify

loading election...
election fingerprint is 2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4
smart ballot tracker is CqnEYxjq44rk+U6h+feiYnQsVvI2IF/JsxlQsQhJa44
election fingerprint matches ballot
Ballot Contents:
Question #1 - Please vote for the new president of University. : Prof. Zaphod Beeblebrox
Encryption Verified
Proofs ok.

SUCCESSFUL VERIFICATION, DONE!

Figure 1: Verifiability Process

hash value based on a security analysis of what is required for a four day Internet voting election. The instructions have been improved in particular by explaining the purpose for this verification code. The most dramatic change was to the verification process. Here, if the voters opt to verify the ballot, a new webpage is displayed containing different trusted institutions to carry out the verifiability. They will select one of these institutions to verify their ballot. The results of the verification will be displayed in a separate window displaying a web page hosted by the corresponding institute (Fig. 2). The text on these pages has been improved also as it was not clear in the original interfaces that 'proofs ok' is clear feedback for the voter. In this context the fact that a new verification code is generated and displayed after the verification is highlighted in the improved version. Finally, the confirmation and authentication process has been simplified.



Presidential Election for University

Instructions | Ballot | Verification-Code | Ballot-Casting

You can now verify whether your ballot is correctly encrypted. In order to do this, click on the logo of an institute which you prefer to verify the ballot. This process will open a new window with the selected institute that will give you the result of the verification.

Institute:

[Verify the Ballot]

[Verify the Ballot]

This verification process will require that t
reencrypted and a new Verification-Co

After a successful Verification you can pr
irregularities, please cancel the election pro

Firefox
Ballot Verification
http://wwwen.uni.lu/election-verify:session:141kv
Google
uni.lu
UNIVERSITÉ DU LUXEMBOURG
University of Luxembourg
FR DE EN
REGISTER FOR E-NEWSLETTER | VIDEO
UCL
Université catholique de Louvain

Ballot Verification

The result of the verification of your ballot is:

Selected Candidate: Prof. Zaphod Beeblebrox
Verification-code: x4WH1LC1Q

Please compare these with your own Ballot and Verification-code

Close this window in order to go back to the election.

About us

Do you want to get more information about our institute? Visit us at http://wwwen.uni.lu/!

Figure 2: Verifiability Institutions and Results.

5. USER STUDY SETTING

A mock mayoral election was set up and participation was invited from both technical and non-technical users. Recruitment was by word of mouth invitation in and around a university campus. We recruited thirty users, fifteen with a technical background in that they either have studied some aspect of computing at university level or use computers on a regular basis, for example for online shopping and e-banking. No monetary compensation was given to the participants. They however received a USB memory stick with the institution's logo. The lab used was a room set up with a computer for the user to cast their vote and answer a web-based questionnaire. A modified bicycle helmet with eye tracking lens was connected to a separate laptop. First, the user answered an initial questionnaire with general questions such as age, gender and computer knowledge. Next they used the voting system for the first time, unguided. After the vote was cast or the process was aborted by the user, they answered a second questionnaire to give their opinion about the system. After this the voter was given instructions on how to interact with the voting system. Finally upon completion, the users filled out an exit questionnaire. Besides questions on the general usability of the voting system and the individual verifiability there are also questions on users' concerns over the security of the voting website and the voting system both regarding the secrecy and the integrity of their vote. Finally we include questions to determine which wording is appropriate and readily identifiable to the users' in the context of verifiability in remote e-voting. The eye-tracking helmet enables us to view the points on the screen that users paid attention to as well as to check whether users really compared the verification code written down with the displayed one. One result so far is that the technical participants raised complaints about a lack of detailed information while some of the non-technical ones could not understand why the system itself was not secure enough and why their own effort to verify something was required. Here, it should be mentioned that we did not provide any information about verifiable electronic voting systems to the participants of the user study beforehand.

6. REFERENCES

[1] 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.

[2] 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.

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

[4] F. Karayumak, M. Kauer, M. M. Olembo, and M. Volkamer. Usability analysis of helios - an open source verifiable remote electronic voting system.

[5] S. Laskowski, M. Autry, J. Cugini, W. Killam, and J. Yen. Improving the usability and accessibility of voting systems and products nist special publication. 2004.

[6] 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.

[7] M. Winckler, R. Bernhaupt, P. Palanque, D. Lundin, K. Leach, P. Ryan, E. Alberdi, and L. Strigini. Assessing the usability of open verifiable e-voting systems: a trial with the system prt voter. In *Proceedings of ICE-GOV 2009, pp. 281-296.*, 2009.