Usability of Verifiability in Helios

Maina Olembo, Fatih Karayumak, Michaela Kauer, Melanie Volkamer

8th August, 2011
Overview

- Why usability of verifiability in remote EVoting

- Review of Helios
  - Vote Casting Process
  - Sample Interfaces

- Improving Helios Interfaces
  - Cognitive Walkthrough
  - Improved Interfaces
  - User Study

- Future Work and Conclusion
Overview

- Why usability of verifiability in remote EVoting
Verifiability (Definition)

→ Verifiability requires extra effort from voters
`Not every voter needs to verify’

True, but:

Any voter who wants to verify should be able to

&

Voters should not be confused by the option to verify
Objective

Analysing and improving usability of

Helios E2E verifiable remote EVoting system

while focusing on voter verifiability
Overview

- Review of Helios
  - Vote Casting Process
  - Sample Interfaces
About Helios

- Proposed by Ben Adida
- Open-source system
- Applies Benaloh’s simple verifiable voting protocol for voter verifiability
- Used in legally binding elections
  - in academic contexts: UCL, Princeton
  - election for IACR
Helios Vote Casting Process

Trigger

- Voter receives invitation-to-vote email
  - Voter clicks on URL to access Voting Booth
    - Voter reads Instructions and clicks Start button
      - Voter makes candidate selection
        - System encrypts (or re-encrypts) vote
          - Cast or Verify?
            - Cast
              - Voter logs in
            - Verify
              - Voter verifies smart ballot tracker on bulletin board
                - System gives confirmation message
                  - Voter confirms identify to Cast Vote
                    - System verifies and gives voter result
Overview

- Sample Interfaces
Voter selects whether to cast or verify

Presidential Election of University

Your ballot was successfully encrypted

Please keep a record of your smart ballot tracker [print] [email]:

CqnEYxjq44rk+U6h+fieiYnQsVvI2IF/Jsx1QsQhJa44

To protect your privacy:
- Helios has not yet asked for your identity.
- Once you click “Proceed”, Helios will remember only your encrypted vote.
- Thus, only you know your vote.

Proceed to Cast

Audit [optional]
If you choose, you can audit your ballot and reveal how your choices were encrypted.
You will then be guided to re-encrypt your choices for final casting.

Verify Encryption

Election Fingerprint: 2IsihDEFZKjeXlk/Ip2vdgYGNcpDqlx4fig3F/Z2Fc4

help!
Sample Helios Interfaces (2)

Select audit info  
Open verifier window  
Copy information
Sample Helios Interfaces (3)

Paste

Verify

Review results
Sample Helios Interfaces (4)

Select next steps
Overview

- Improving Helios Interfaces
  - Cognitive Walkthrough
Cognitive Walkthrough

- Usability inspection method
- A psychology, usability expert and computer scientists
  - Usability expert – no background in EVoting systems
  - Security and EVoting experts familiar with techniques employed

- Analyzed the vote casting and verifiability procedures

- Assessed the interfaces from voter’s perspective

- Considered
  - Actions required for vote casting and verifying a vote
  - Confusing aspects
Findings

Interchanging use of terms

Audit/verify

Inadequate emphasis placed on verifying

Voter may be confused by additional steps

Voter seeking help has to send an email

Impractical

Verifiability process is confusing

Mathematical proofs can be overwhelming to average voter
Copy and paste may be prone to error
Smart ballot tracker long, difficult to compare
Overview

- Improved Interfaces
Clear instructions

To authenticate servers

Dear...

You are registered on the electoral roll. For this election you will use a secure online voting system that uses verification codes. These codes will help you understand the correctness of this election.

You can vote on the election web-page [www.election.university.com](http://www.election.university.com) on 27 March 2011 between 9:00 a.m. and 6:00 p.m. Here you can also get further information about the execution of this election.

To check your eligibility to vote, you will be required to authenticate yourself with a username and a password.

Your username: <User-Name>
Your password: <Password>

Please don’t share this information with anyone.

Best Regards
Election Officer

Improved Interfaces (2)

**Presidential Election for University**

Instructions to voters

1. In the first step, you will see the ballot where you can vote for the candidate of your choice.

2. After you choose a candidate, your ballot will be encrypted in order to keep the vote secret. Furthermore, a verification code will be generated for your ballot. To ensure that your ballot is correctly encrypted, you can have this encryption verified by any one of several independent institutes. You can repeat this process as many times as you need, until you are convinced that this vote system functions correctly.

3. The actual ballot-casting process is performed in the last step. By entering your username and password, your (encrypted) ballot will be cast. As long as you have not cast your ballot, you can cancel this procedure at anytime by closing the vote system’s window. You are free to continue at another time. This will not cause you to lose your eligibility to vote.

At the end of the election, a list of verification codes for all the tallied votes will be published. If you want to confirm whether your vote has been correctly tallied, you can look up your verification code in this list.

To start the election procedure, click on the “Proceed to Ballot” button.

**Added verifiability step**
Improved Interfaces (3)

Presidential Election for University

Ballot
For the Presidential Election of University

You can select one candidate (or invalid vote).

1. Prof. Ford Prefect
2. Prof. Zaphod Beeblebrox
3. Prof. Tricia McMillan

Invalid Vote

Provide invalid vote option

Back and Forward Buttons

<< Back to Instructions

Check the Ballot >>
Improved Interfaces (4)

Your Verification-Code is: x4WH1LC1F4t1hK6k

Your ballot has been encrypted to keep the vote secret.

With the help of this verification-code, you can verify whether your vote is correctly tallied. For this please write down this verification-code or use the following alternatives:

Options for voter

To ensure that your ballot is correctly encrypted, you can have this encryption verified. You can repeat this process as many times as you want, until you are convinced that this vote system functions correctly.

Shortened verification code
Improved Interfaces (5)

Trusted institutions for verification
Improved Interfaces (6)

Simplified results

EVT/WOTE | Maina Olembo | 8th and 9th August, 2011
Improved Interfaces (7)

Explanation for voter

Your Verification-Code is: x4WH1LC1F4t1hK6k

Attention: Your Verification-code has been changed, because it has been re-encrypted. The previous verification-code is therefore invalid.

With the help of this Verification-code, you can control whether your vote has been correctly tallied. In order to do this please write down this verification-code or use the following alternatives:

[Download Code] [Print Code]

To ensure that your ballot is correctly encrypted, you can have this encryption verified. You can repeat this process as many times as you want, until you are convinced that this vote system functions correctly.
Presidential Election for University

Verification-Code of the Ballot to be cast is: x4W1LC1F4t1hK6k

Please compare the shown verification-code with the one you wrote down during the previous step.

Please enter your user-name and password if you want to cast your ballot. You can find your user-name and your password in the invitation to vote letter.

Username
Password:

<< Back to the verification-code

Conclude the Ballot-Casting >>
Presidential Election for University

Your vote has been saved. Thank you very much for your participation

1 hour after the end of this election at 6:00 pm, the results and the list of verification-codes will be published at [www.electionresults.university.com](http://www.electionresults.university.com)

Now please close this window.
Comparison

- Old Interfaces
  - Total # mouse clicks to *cast a vote* - 9
  - Total # mouse clicks to *verify a vote* - 8

- New Interfaces
  - Total # mouse clicks to *cast a vote* - 7
  - Total # mouse clicks to *verify a vote* - 3
Overview

- User Study
User Study

- Tested usability of new interfaces with 34 users

- Lab set up

- Two runs; voters given instructions after first run

Findings:

- Voters find the new interfaces usable

- Voters need more assistance to understand concept of verifiability

Results in STAST2011
Overview

- Future Work and Conclusion
Future Work

- Adequate length for the verification code
- More user-friendly techniques for verifiability, e.g. QR codes
- Interview potential voters for their understanding of verifiability
- Short video to explain concept of verifiability to voters
- Integrate metaphors
- Investigate how to assist voters to authenticate voting servers
Conclusion

- Investigated usability of verifiability in Helios
- Analysed current interfaces using cognitive walkthrough technique
- Developed alternative interfaces for Helios
- Evaluated new interfaces in a user study [STAST2011]
- Usability of verifiability processes still requires further research
The End

Thank you for your attention

Any Questions?