Usability of End-to-End Verifiable E-Voting Schemes

Karola Marky
SECUSO

- Security, Usability und Society
- Research group at TU Darmstadt
- Human Centered Security
- Interdisciplinary team
Motivation

Were is my vote?

Solution: End-to-end verifiability
End-to-end Verifiability

- **Cast-as-intended**
  Cast vote corresponds to the voter’s intent

- **Recorded-as-cast**
  Recorded vote matches the cast vote

- **Tallied-as-recorded**
  All recorded votes are correctly included in the result
Cast-as-intended Verifiability (C-a-I)

- „Decryption“
  - E.g. Estonian system
- Challenge or cast
  - E.g. Benaloh Challenge
- Return Codes
  - E.g. Pretty Good Privacy
- Tracking Codes
  - E.g. Selene
Impact of Usability

- Attacker alters vote in secret
- Voting platform alters vote in secret
- Voting platform might malfunction

- Bad usability of C-a-I leads to
  - More successful attacks
  - Inaccurate election results
Usability (ISO 9241-11)

- **Effectiveness**
  Ability of users to complete their task.

- **Efficiency**
  Extent to which users consume resources to perform their task.

- **Satisfaction**
  Level of satisfaction users experience in performing their task.
Benaloh Challenge
User Study
Benaloh Challenge

Voter

Observer

Voting Device

Verifier

Ballot Box

Veriﬁcation

Vote Casting
3 Approaches

- Differences in the transfer of verification data
- Differences in the degree of voter involvement

1. Manual (Copy and Paste)
2. Automatic
3. Mobile (Scan of QR code)
Study Scenario

- German Federal Election 2017
- Verifier
  - BSI
  - OSCE
- Verification devices
  - Android App

3 Voting Websites

Demo-Session
After workshop
Study Design

- Lab study: 95 participants
- Between subjects
- Lab devices
- First-time voters: 17-22 years old
Procedure

- Explanation of the study
- Declaration of consent
Procedure

- Demographic questions:
  - Age
  - Gender
  - Occupation
  - Voting experience
Procedure

- Internet voting document incl. login data
- Instructions
  - Mark party „SPD“
  - Verify vote using website / app
  - Mark party „GRÜNE“
  - Cast vote
Procedure

- Screen recording of devices
- Logging of time by software
- Observation
Procedure

- SUS questionnaire
- Additional questions
Collected Data: Effectiveness

- Completion rate
  - Share of subjects that verified successfully
- Determined by screenrecordings

![Bar chart showing completion rates for Manual, Automatic, and Mobile methods.](chart.png)
Collected Data: Efficiency

- Completion times:
  - Duration of the first successful verification
  - Logs by the software
  - Screenrecordings

![Box plots comparing completion times for Mobile, Automatic, and Manual methods.](image)
Collected Data: Satisfaction

- System Usability Scale
  - 10 item questionnaire
  - SUS score from 0 up to 100

![Box plot showing SUS scores for Mobile Device, Automatic, and Manual methods.]
Collected Data: Additional

- Would you use the presented Internet voting system in a real Bundestag election?
- Would you use the presented verification option in a real Bundestag election?
- If you answered the question above affirmatively, how often would you perform verification?
- Did you experience any problems during vote verification?
- Did you experience any problems during vote casting?
## Study Results

<table>
<thead>
<tr>
<th></th>
<th>Automatic</th>
<th>Mobile</th>
<th>Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø – SUS</td>
<td>75,4</td>
<td>79,4</td>
<td>75,8</td>
</tr>
<tr>
<td>Completion rate</td>
<td>61,3 %</td>
<td>81,25 %</td>
<td>81,25 %</td>
</tr>
<tr>
<td>Ø – Time</td>
<td>131 s</td>
<td>47 s</td>
<td>61 s</td>
</tr>
</tbody>
</table>

Automatic is better than manual
Mobile is better than manual
Lessons Learned – Motivation

- Participants have to be motivated to execute a task
- Usability does not include motivation

**Motivation important**
- Cover story
  - Less biases
  - Personal relevance

**Motivation not important**
- Instructions
  - Ensure execution
Lessons Learned – Vote Privacy

- Concerns the votes of the study participants
- Recording and observation break vote privacy

Vote privacy needed

No recording

- Other measures

Vote privacy not needed

Recording

- Option instructed
- Trivial question
Lessons Learned - Effectiveness

- Actual comparison of data hardly detectable
  - Screenrecordings are not sufficient
  - Self reporting not reliable

Eye-Tracking

Manipulation
Next Steps

- Long-term goal: Further research on c-a-i usability
- Next step: Evaluation of code voting vs. Benaloh
- Next-next step: Evaluation of other c-a-i approaches
  - Literature search for cast-as-intended approaches
  - Overview of available approaches
  - Classification of approaches
Discussion

- Mixing of understandability and usability
  - How can those concepts be separated?

- Measuring of effectiveness
  - Are there other approaches to completion rates?

- Challenges in evaluation
  - Are there further challenges not mentioned in this presentation?
Backup Slides
Benaloh Challenge
Benaloh Challenge

Voter

Voting Device

Verifier

Ballot Box
Benaloh Challenge

Voter → Choice → Voting Device → Verifier → Ballot Box
Benaloh Challenge

\[ \text{Encryption Check-Code} = \text{Hash(Enc(Choice, Random))} \]
Benaloh Challenge

Voter

Choice

Check-Code

Voting Device

Encryption Check-Code = $Hash(Enc(Option, Random))$

Verifier

Ballot Box
Benaloh Challenge

\[ \text{Encryption Check-Code} = \text{Hash}(\text{Enc(Option, Random)}) \]
Benaloh Challenge

\[ \text{Encryption Check-Code} = \text{Hash(Enc(Choice, Random))} \]
Benaloh Challenge

Encryption Check-Code = Hash(Enc(Choice, Random))
Benaloh Challenge

Verification

Vote Casting

Voter

Observer

Voting Device

Verifier

Ballot Box
Code Voting
PUD

Code Sheet

<table>
<thead>
<tr>
<th>ID: 34919</th>
<th>ID: 34919</th>
<th>ID: 34919</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred Rubble</td>
<td>28502</td>
<td>93448</td>
</tr>
<tr>
<td>John Citizen</td>
<td>23983</td>
<td>62104</td>
</tr>
<tr>
<td>Jane Doe</td>
<td>45982</td>
<td>12937</td>
</tr>
<tr>
<td>Mary Hill</td>
<td>83410</td>
<td>89129</td>
</tr>
<tr>
<td>Joe Smith</td>
<td>29311</td>
<td>13812</td>
</tr>
<tr>
<td>–</td>
<td>94340</td>
<td>83429</td>
</tr>
</tbody>
</table>

Voter

Voting Device

Ballot Box
PUD

Code Sheet

<table>
<thead>
<tr>
<th>ID: 34919</th>
<th>ID: 34919</th>
<th>ID: 34919</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred Rubble</td>
<td>28502</td>
<td>93448</td>
</tr>
<tr>
<td>John Citizen</td>
<td>23983</td>
<td>62104</td>
</tr>
<tr>
<td>Jane Doe</td>
<td>45982</td>
<td>12937</td>
</tr>
<tr>
<td>Mary Hill</td>
<td>83410</td>
<td>89129</td>
</tr>
<tr>
<td>Joe Smith</td>
<td>29311</td>
<td>13812</td>
</tr>
<tr>
<td>–</td>
<td>94340</td>
<td>83429</td>
</tr>
</tbody>
</table>

Voter

83410 89129

Voting Device

Enc(83410 89129)

Ballot Box
PUD

Code Sheet

<table>
<thead>
<tr>
<th>ID: 34919</th>
<th>ID: 34919</th>
<th>ID: 34919</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred Rubble</td>
<td>28502</td>
<td>93448</td>
</tr>
<tr>
<td>John Citizen</td>
<td>23983</td>
<td>62104</td>
</tr>
<tr>
<td>Jane Doe</td>
<td>45982</td>
<td>12937</td>
</tr>
<tr>
<td>Mary Hill</td>
<td>83410</td>
<td>89129</td>
</tr>
<tr>
<td>Joe Smith</td>
<td>29311</td>
<td>13812</td>
</tr>
<tr>
<td>—</td>
<td>94340</td>
<td>83429</td>
</tr>
</tbody>
</table>

Voter

83410 89129
94340 83429

Voting Device

Enc(83410 89129)
94340 83429

Ballot Box