Enhanced Secure Interface for a Portable E-Voting Terminal

André Zúquete
IEETA / University of Aveiro
Portugal
One advantage of e-voting is the “voting anywhere” paradigm possibly using untrusted computers (e.g. cyber-caffes).

Portable, personal TCB for the REVS e-voting system [WRAITS07]
- Smart card and FINREAD terminal with human I/O interface
- May be used with any host computer
  - Hosts provide Internet access to REVS electoral servers
  - A voter interacts only with his TCB
Problem: FINREAD terminal limitations

- Used to securely present questions & answers to the voter
  - Ballot questions (for correctness)
  - Answers (for secrecy)
- FINREAD output display is small
  - Only 4 lines of 80 characters
- Global ballot view is an issue
  - With long ballots
  - With many answers per question
Objective

- Enhance the output capabilities of the TCB without compromising voters’ security
  - Voters’ answers must remain secret to the TCB
  - Ballot questions must be correctly presented to voters
Contribution:

Enhanced, secure TCB interface

- Secure cooperation with hosting computers
  - The hosting computer presents an image of the ballot to the voter
    - Enhanced interface, global view of the ballot
  - The image should not disclose voter’s choices
    - Secrecy / privacy
  - The image should allow the voter to detect relevant modifications introduced by the hosting computer
    - Correctness (of Q&A)
Non-disclosure of voters' choices

- The image presented by the hosting computer does not contain voter's choices
  - They are presented at the FINREAD display
  - Possible answers and choices are linked by numbers

Are you understanding this?
- Yes
- No
Non-disclosure of voters’ choices: Expressing multiple votes

Preferred domestic animals?

- Cat
- Fish
- Dog
- Bird

Screen image

Preferred domestic animals?

0) 1) Cat 2) Fish 3) Dog 4) Bird

Vote = 1 3
Non-disclosure of voters’ choices: Expressing values in ranges

Best year of your life? 18
1: Do you like this interface?
0) 1) Yes 2) No

Vote = 1 (65)

2: What are your preferred background colours?
0) 1) Red 2) Blue 3) Green 4) Gray

3: Rate this interface from 0 (bad) to 100
0) NO ANSWER (1) ANSWER
Authentication of ballot images

- Ballot images must be visually authenticated by voters
  - To prevent hosting computers from changing the ballot
- Authentication with feedback
  - The ballot is displayed with some highlighted details
  - The voter checks them details with the FINREAD terminal
  - Active feedback
    - The voter inputs the highlighted details in the FINREAD terminal
    - The FINREAD produces an OK/NOK authentication result
  - Passive feedback
    - The FINREAD terminal presents the highlighted details
    - The voter visually checks the match
- We chose colours for highlighting feedback characters
Feedback with colours:
Examples of active / passive feedback

1: Do you like this interface?
0) 1) Yes 2) No

Vote = 1
Red = 1Dolonts)

Vote = 1
Red = 1Dolent)\textgreater\textbackslash{}sN
Feedback with colours:
Undetectable tampering is possible

<table>
<thead>
<tr>
<th>1: Do you like this interface?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0) 1) Yes 2) No</td>
</tr>
</tbody>
</table>

1: Do you like this interface?
0) 1) No 2) Yes

1: Do you hate this interface?
0) 1) Yes 2) No
Feedback with colours:
Reduction of tampering success probability

1: Do you like this interface?
0) 1) Yes 2) No

Solution adopted for N feedback colours
- Feedback is given with 2 colours (out of N)
  - One for the question, one for the answer
  - Possibly equal
- Text is divided in blocks of N characters
  - All N colours are randomly used in each block
- Voter can shuffle colours in the FINREAD terminal
  - Without changing the presented image

Vote = 1
Green = :uehnef
Red = 0YN
Security & usability analysis (1/2)

- **Voter privacy**
  - Displayed images do not convey personal choices
  - Voter privacy is kept

- **Image authentication**
  - Colour handling is an issue
    - More colours, more security, less usability
    - More feedback colours, more security, less usability
  - Compromise
    - Less possible number of colours, 2 feedback strings
    - Tampering is possible
      - But the success probability is low
      - It can be arbitrarily reduced with feedback shuffling
Feedback validation

- Passive validation is more convenient
  - But more prone to human errors
  - Careless voters may be deceived
  - Voters have to do error management

- Active feedback is less convenient
  - But it becomes very hard to deceived voters
  - FINREAD terminal can do some error management
Preliminary usability experiences

- A prototype demonstrator was developed
  - Java applet
  - Passive feedback, adjustable colour palette
- Usability: lessons learned
  - Extensive colour scattering reduces readability
    - Solution: aggregation
    - Aggregates of characters with the same colour instead of single characters
  - Long questions/answers require many colours
    - For producing short feedback strings in the FINREAD
    - Visual colour separation becomes a problem
  - Colour blind people have natural difficulties
    - Personal tuning of the colour palette may help them
Conclusions

- The secure, enhanced interface relies on two different displays
  - One protected (FINREAD terminal)
    - Shows small amounts of information (choices & feedback strings)
  - One insecure (hosting computer display)
    - Shows an image of the ballot
- Visual authentication of ballots with colours
  - Randomly coloured feedback characters
  - Feedback strings may be shuffled
    - For improving confidence in the authentication
- Colour-based authentication is not trivial for voters
  - Unusual task
    - High cognitive workload
    - Usability tests must be performed to evaluate it
  - Training / personal tuning may reduce the cognitive workload