ThreeBallot Analysis

Greg Belote, Harvey Jones, Jason Juang

Outline

- ThreeBallot Background
- Usability Tests
- In-Class Test

ThreeBallot

- Proposed in 2006 by Ron Rivest
- Design Criteria
  - Match security properties of cryptographic systems
  - Publicly-verifiable
  - Simple
  - Scalable

Sample Multiballot

What is your favorite video game system?	What is your favorite video game system?	What is your favorite video game system?
○ Playstation III	● Playstation III	○ Playstation III
● Nintendo Wii	○ Nintendo Wii	○ Nintendo Wii
○ XBox 360	● XBox 360	○ XBox 360
○ PlayStation Portable	○ PlayStation Portable	● PlayStation Portable
○ Nintendo DS	● Nintendo DS	○ Nintendo DS
● Other	● Other	○ Other
Best baseball team?	**Best baseball team?**	**Best baseball team?**
○ Yankees	○ Yankees	● Yankees
● Red Sox	● Red Sox	○ Red Sox
○ Pat Buchanan	● Pat Buchanan	○ Pat Buchanan
Ballot ID: 212010336	Ballot ID: 240232886	Ballot ID: 623451381
END OF BALLOT	END OF BALLOT	END OF BALLOT

Criticisms of ThreeBallot

- Complexity
  - Non-intuitive rules
  - High time demands on voters and on poll workers
- Privacy
  - Charlie Strauss' ballot reconstruction
- Security

Questions

- How robust is it against attacks on privacy, and on the election results?
- How usable is the system as designed?
- Could computers make it better?
- Would people trust this system?

Usability Tests

- Implemented a computer-based ThreeBallot Machine
- Assigned half of the voters to computer, half to paper (88 ballots cast)
- Surveyed voters about their understanding of the system

Usability Results

- Voters were initially intimidated
- Voters required assistance
- Voters were angry when overvotes required that the ballot be redone
- Some questioned need for such a complex system

Usability Results

- Voters were more comfortable voting by computer
- 16 of 51 paper ballots were initially rejected
  - 12 got it right the second time
  - 1 got frustrated and left
- 1 of 36 computer voters misclicked and had to try again

Post-vote Survey Results

- 50% would use it in a federal election
- 70% believed ThreeBallot is secret and secure

- 58 of 64 correctly identified a valid ballot
- 59 of 64 correctly labeled an overvoted ballot as invalid
- 19 of 49 at EC correctly labeled a legal abstention as valid

In-Class Mock Election

- Held in class on Monday, December 4
- Offered incentives
  - Selling a vote
  - Creating a fraudulent bulletin board
  - Discrediting a fraudulent bulletin board

In-Class Results

- Vote selling
  - 4 out of 18 succeeded
- Scanner malfunction
  - One negative vote for “other”
- Election throwing
  - One adversary was able to change winners of all races.

The Yoyoverse

- Gather all the receipt numbers you can
- Reconstruct triples that have to be connected
  - 6 of 18 were reconstructed
- Match ID numbers to known receipts
- Profit!

Reconstruction Results

- Stata: 25 of 29 reconstructed
  - 19-bit ballots
- EC: 0 of 58 reconstructed
  - 14-bit ballots

Conclusion

- Initial intimidation, but most get it after a few minutes of explanation
  - Special cases still confusing
  - About a third of voters got the first ballot wrong
  - Computers help, but with security tradeoff
- Reconstruction attacks are bad for privacy and for security
- Pre-printed IDs are easy to memorize
  - Complex IDs hurt transparency
  - Long IDs don't help