Verification, auditing and evidence

if we didn’t notice anything wrong, is the election outcome right?

Vanessa Teague
Dept of Computing and Information Systems, The University of Melbourne

Based on joint work with Craig Burton, Chris Culnane, Steve Schneider & Peter Ryan
We’ll begin with a short survey

https://www.surveymonkey.com/r/verifiableCheating

Please be honest
it’s important we get the right answer

I cheated on my

☐ Finals
☐ Taxes
☐ Spouse
☐ Other (write in)______________
End-to-end Verifiability is easy

- Just need a public list of names & votes

<table>
<thead>
<tr>
<th>Name</th>
<th>Letter</th>
<th>Cheated On My</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ABBOTT</td>
<td>A.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>ACEVEDO</td>
<td>B.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>ACOSTA</td>
<td>C.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>ADAMS</td>
<td>D.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>ADKINS</td>
<td>E.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>AGUILAR</td>
<td>F.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>AGUIRRE</td>
<td>G.</td>
<td>I cheated on my</td>
<td></td>
</tr>
<tr>
<td>ALEXANDER</td>
<td>H.</td>
<td>I cheated on my</td>
<td></td>
</tr>
</tbody>
</table>
Verifiability with privacy is hard

- Privacy is important
  - You shouldn’t be able to prove how you voted even if you want to (Benaloh ’94)

- End-to-end verifiability with privacy is hard
Verifiability is important

• NSW iVote really wasn’t verifiable
• About 4,000 people successfully verified
• How many tried to verify but failed?
Public evidence of the right result from secret votes

The Australian ballot

Jury voting disks
(Athenian Agora, Ca. 300 BCE)

French urne électorale

Risk-limiting audits

Philip Stark and Ron Rivest, reproduced from Ars Technica with permission.
End-to-end Verifiability

• End-to-end verifiable systems with privacy
  – Scantegrity II / Remotegrity
    • Local election in Takoma Pk, MD
  – Helios
    • IACR elections
  – Wombat
  – Benaloh’s simple voter-verifiable elections
  – Demos
  – StarVote
  – etc.
Victorian vVote: end-to-end verifiable pollsite e-voting

Vic State Election 2014

- From supervised polling places in London and Victoria
- Pre-poll voting

- Organized by Craig Burton, Victorian Electoral Commission,
- Led by Steve Schneider, U Surrey
- Implemented by Chris Culnane, U Surrey
- Design by Culnane, Heather, Schneider, Ryan, T.
Victorian vVote: end-to-end verifiable pollsite e-voting

Vic State Election 2014
1121 votes

• Based on Prêt à Voter
• Voters take home a copy of their vote (encrypted)
• Encrypted votes are posted on the web
  – Shuffled & decrypted with proof
• Scrutineers check the right votes go into the paper count
• GPL code on bitbucket
Victorian vVote: end-to-end verifiable pollsite e-voting

Vic State Election 2014
1121 votes from supervised polling places

Vote; Receipt

Electoral Commission
Vote Server

Vote application provides various mathematical proofs of integrity. Please note that for privacy reasons, some of the provided (for example if there was only one vote taken in that race). There are two options for verification:

1. To verify the entire electronic voting run, please download this package:

   ALL VOTES.ZIP
   (50MB)

   Contains: allvotes.csv, all proofs, vVote verifier Batch file, Readme.txt

2. To verify an individual race, please select below. Each zip file is 42MB and contains the vVote verifier.exe and Readme.txt:

   - Albert Park District.zip
   - Altona District.zip
   - Bayswater District.zip
• How do you know that
  – Your vote is cast as you intended?
  – Your vote is included as cast?
  – All the votes are properly decrypted and tallied?
Prêt à voter

- Uses pre-prepared paper ballot forms
- The candidate list is randomised for each ballot form.
- Information defining the candidate list is encrypted in an “onion” value printed on each ballot form.
  - Actually, we print a serial number that points to the encrypted values in a public table

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>$rJ9*mn4R&amp;8</td>
</tr>
<tr>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Chequered</td>
<td></td>
</tr>
<tr>
<td>Fuzzy</td>
<td></td>
</tr>
<tr>
<td>Cross</td>
<td></td>
</tr>
</tbody>
</table>
• Each voter can challenge as many ballots as they like
  – And get a proof that the onion matches the candidate list
  – Then don’t use that ballot
• Vote on an unchallenged one
  – So you can’t prove how you voted
Prêt à voter: voting

- Fill in the boxes
- Use a computer to help
- Check its printout
  - Against candidate list
- Shred candidate list
- Computer uploads vote
  - Same info as printout
- Take printout home
  - Doesn’t reveal vote
There’s a public website listing all the receipts
  – More precisely, there’s a “bulletin board” which is a public website augmented with some evidence that everyone sees the same data

Find yours

Verify proof of shuffle & decryption
Public evidence of the right result from secret votes

The Australian ballot

French urne électorale

Risk-limiting audits

vVote

Jury voting disks
(Athenian Agora, Ca. 300 BCE)
End-to-end verifiable polsise voting: practicalities

- Evidenced transfer of right votes from overseas, interstate, long time intervals
  - Where paper evidence is difficult
- Getting people to verify is hard
Could we do that securely from home via the Internet?

• No
• Secure Internet voting is an unsolved problem. End-to-end verifiability is necessary, but
• Still unsolved in practice:
  – Authentication (both ways)
  – Malware
    • Privacy/coercion
    • Difficulty of verification
  – Dos, ballot stuffing, ...
1. Election outcomes must include evidence that they're correct.

2. Secure Internet voting is unsolved:
   • Authentication,
   • usable/quantifiable verification,
   • coercion resistance, DoS, ...

3. End-to-end verifiability could make secure pollsite e-voting much more flexible
Questions?