Some Thoughts on Electronic Voting

Ronald L. Rivest

MIT CSAIL

DIMACS Voting Workshop
May 26, 2004
"What's one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one and one?"

"I don't know," said Alice. "I lost count."
Outline

- 12 “debatable propositions”
- A “pedagogical variant” of Chaum’s voting proposal
12 Debatable Propositions

- We give some “propositions” worth consideration and debate.
- These are arbitrarily phrased, so as not to imply support, one way or the other.
- We give a couple of pro/con arguments each way for each proposition.
- “Sometimes I’ve believed as many as six impossible things before breakfast.” (White Queen)
1. Voting in private is not important

- **Pro:**
  - If so, why do we allow such widespread use of absentee ballots or vote-by-mail??
  - Threats affecting large number of vote counts are more important.

- **Con:**
  - Voter privacy is necessary to defeat coercion and vote-selling.
  - History of voting shows privacy to be important.
2. Voting fraud is rare

- **Pro:**
  - Few convicted of voting fraud
  - Problems in manipulation of registration seem much more prevalent.

- **Con:**
  - *Absence of evidence is not evidence of absence.*
    “We’ve never seen a problem” does not mean problems don’t exist!
  - Maybe unsuccessful voting fraud is rare.
3. Voter is not a computer

- **Pro:**
  - *Gee, this seems obvious.*

- **Con:**
  - Much existing cryptographic voting literature assumes otherwise.
  - Someday voters will have their own “trusted computing base” (a cell phone?) that can act on their behalf in a trustworthy manner...
4. Voting by machine is “proxy voting”

◆ Pro:
  - Gee, this seems obvious.

◆ Con:
  - Well, we don’t consider a pencil a “proxy” for the voter, do we?
  - Is a DRE (or a computer) more like a pencil or more like a corruptible person?
5. We must “trust the machines”

- **Pro:**
  - It’s either that, or back to #2 pencils…
  - Because we can

- **Con:**
  - Why outsource our elections to vendors?
  - Necessity has not been demonstrated; good audit and controls seem possible
  - Because we can’t
6. Trustworthy software is possible

- **Pro:**
  - We fly in planes, don’t we?

- **Con:**
  - Planes have no field-upgradable software.
  - Avionics software is enormously expensive. (DO178B regulations)
  - Insider threat less serious for planes.
7. Code review is sufficient

- **Pro:**
  - Gee, it’s what we’re doing now…
  - Open source could make this even better…

- **Con:**
  - Need to trust compiler, and even that’s not enough (Ken Thompson)
  - Undecidable in general
  - Very hard even in simple cases:
    » Does this program ever refuse to let someone vote? :
      * On input n (e.g. n is the blank ballot, as an integer)
      * While n>1: if n even n ← n/2 else n ← 3x+1
      * Proceed to ordinary voting code…
    » It is an *unsolved problem* even for this program!
8. Testing is sufficient

◆ **Pro:**
  - As long as voting machine can’t tell if it is being used “for real”, it can’t cheat.

◆ **Con:**
  - Easy for an accomplice to “signal” software that it is being used “for real”.
  - Sufficiently extensive parallel testing is very expensive.
9. Paper is necessary

`I think I should understand that better,' Alice said very politely, `if I had it written down: but I can't quite follow it as you say it.'

Pro:
- Without (voter-verified) paper ballot, voter doesn't really know how he voted.
- Without paper output, voting machine isn't committed to any particular behavior or action.
- Electronics can't audit itself (at least, if made by same manufacturer...)

Con:
- Same investment can yield equivalent results in other ways...
10. Transparency helps security

- **Pro:**
  - Publishing source code, lists of voters, ballot images, etc. seems like a good idea

- **Con:**
  - Not easy to do and protect voter privacy.
  - Giving voters more chances to complain can cause more problems than it solves.
11. We’ll see fewer close elections

- **Pro:**
  - Populations are growing

- **Con:**
  - Sophisticated polling allows candidates’ resources to be spent efficiently, narrowing margins in close states.
12. If it’s close, it doesn’t matter

◆ Pro:
  - No matter which way it goes, about the same number of voters are unhappy.
  - “Which road do I take?” asked Alice.
    “Where do you want to go?” said the cat.
    “I don’t know…” said Alice.
    “Then it doesn’t matter!” said the cat.

◆ Con:
  - Rule by minority is not democracy!
A pedagogical variant of Chaum’s voting proposal

- Used in my class this spring as introductory example, before going into details of Chaum’s and Neff’s schemes.
- Captures many significant features, but not all; some problems/concerns not well handled.
- Intended to be simpler to explain and understand than full versions.
- Related to Jakobsson/Juels/Rivest mix-net scheme.
- Little novelty here; main ideas (e.g. cut and choose) already present in Chaum’s scheme.
Pedagogical variant (overview)

- Voting machine produces ciphertext that is encryption of voter’s ballot.
- Ciphertext posted on bulletin board as “official cast ballot” (electronic).
- Voter given receipt copy of ciphertext.
- Voter given evidence that ciphertext correctly encodes his intended choices.
- Ciphertexts “mixed” for anonymity.
- Ciphertexts decrypted and counted.
Pedagogical variant (details)

- Voter $V_i$ prepares ballot $B_i$
- Machine prints and signs $B_i$, $C_i$, $D_i$, $r_i$, $s_i$ and gives them to voter.
  $C_i$ is encryption of $B_i$ (randomization $r_i$)
  $D_i$ is re-encryption of $C_i$ (randomization $s_i$)
- If voter doesn’t like $B_i$, he starts over.
- Voter destroys either $r_i$ or $s_i$, and keeps the other information as evidence (paper).
- Voting machine signs and posts ($V_i$, $D_i$,”final”), and gives (paper) receipt copy to voter.
- Final $D_i$’s mixed up (mixnet), decrypted, and counted.
Pedagogical variant (details)

El-Gamal encryption and re-encryption:

\[ C_i = (g^{ri}, B_i^r y^{ri}) \]
\[ D_i = (g^{ri+s_i}, B_i^r y^{ri+s_i}) \]

- Voter keeps only one link as evidence (similar to Jakobsson/Juels/Rivest, or Chaum)
- Voting machine can cheat undetectably with probability at most 1/2 per vote.
- Voter can check evidence on exit.
- Signed \( B_i \)’s are easy to get...
- Can add “visual crypto” to hide \( B_i \)’s...
Pedagogical variant (summary)

- Official ballot is *electronic ciphertext*.
- Voter’s *receipt* allows him to ensure his ballot is counted.
- Voter’s *evidence* supports claim that ballot captures his intended vote.
- Schemes such as these (Chaum / Neff) provide an interesting degree of “end-to-end” security...
“Begin at the beginning,” the King said gravely, “and go on until you come to the end, then stop.”
(The End)