What Do We Do Next?

Notes and comments on the past 2 days

Douglas W. Jones
Department of Computer Science
University of Iowa
Iowa City, Iowa
jones@cs.uiowa.edu

supported, in part, by NSF
Grant CNS-05243

Cut the hype!

- End-to-End voting is a game changer!
  - Cast as intended – a big human factors problem
  - VVPAT fails largely because of this
  - Explaining what End-to-End does and VVPAT doesn't is not that easy
- No trust required!
  - Really? I must trust the cryptosystem
  - I must trust that only the custodians have the keys
  - I must trust that the ballot printer didn't keep copies

Campaign to ban Homomorphism

(A fictional California-style ballot initiative)

No government funds shall be spent to teach or advocate homomorphism, homomorphic relationships, or any topics dealing with homomorphism in any school, college or university. Government funds shall not be used to print or otherwise disseminate any materials containing the words homomorphic or homomorphism.

Seriously

- Encryption, homomorphic encryption and mix nets, are very difficult to explain.
- We need to learn how to explain these, not just to college freshmen, but to the losers.
- We have made progress since 2002.

Chaum, West 2002

By way of critique:

- Ron Rivest's presentation was at an appropriate level for the public, but did not cover enough technical detail to help an E2E election observer.
- Josh Beneloh's presentation presented some detail, but above the level of many election observers.

Terminology

We need to be careful not to convert these to insider terms, with definitions different from what the words themselves say.

- End to End
- Receipt Free

We need to be aware that the law tends to radically redefine terminology.

- Firmware – software running in the polling place
- Secret Ballot – Washington claims this with postal ballots and few voters per ballot style

Which End is Which?

- Usual presentation of end-to-end voting
  - End 1: Voter intent (or an approximation of it)
  - End 2: Election result
- These ends are critical
- But there are other ends
  - End 3: Generate codebook (very first step)
  - End 4: Post election forensics (post certification)
- Some of these are new with electronic voting!

Observability

- For a classic paper ballot election with precinct count, as in British parliamentary elections:
    - Observation at the polling place between poll opening and completion of the count is key
    - Observers conduct parallel count and canvass
    - Casual observation by voters frequently suffices
- For End-to-End voting:
    - Must observe key creation
    - Must observe chain of custody of ballots
    - Casual observation not applicable to these

Voter Intent

- End to End systems do not capture intent
  - They assume intent can be captured
  - They let you verify encrypted vote was counted
  - They are no better than DRE at intent capture
  - Some are worse (added indirection – Punchscan)
- Intent capture is a human factors problem
- Election margins of 1% are common
  - In this context, 98% accuracy is not good enough

The International Angle

- We tend to ignore international law in the US
- Secret ballot rights in the US are eroding
  - We don't need secrecy because we're pretty honest
- If we allow weak secrecy to be entrenched
  - We are at risk if we ever become less civil
  - We set a bad example for less civil countries
- We must remember that we (the US and europe) set the standard for democratic elections worldwide.

Aside

Publicly Verifiable Randomness

Originally for selecting precincts to audit
Can use same idea for E2E challenge

- Dill-Wagner proposal:
  - 10-sided dice, participants can each roll a digit
  - Reroll dice if outside required range
- My proposal
  - Each participant provides sealed random value.
  - Unseal and sum mod desired range.
  - If any participant was random and uniformly distributed over the range, so is the sum.
- These work if participants fit in one room

Aside

Z-Base-32

- Base-32 code for human transcribed bignums
  - Type `o`, `O` or `0`, they're all zeros
  - Type `i`, `I`, `l`, `L` or `1`, they're all ones
- I first encountered this encoding in RIES
  - Authorization to vote sent by post, bignum must be transcribed into RIES as authorization to vote.
- Base 32 lets you encode error detecting code
  - Reduce impact of typos in vote authorizations
  - Reduce impact of typos in voter verification