The Risks of Electronic Voting

Prof. Dan Wallach
Department of Computer Science
Rice University

Joint work with Tadayoshi Kohno (UC San Diego), Adam Stubblefield and Aviel Rubin (Johns Hopkins)

Perception vs. reality

- Voter feels that
  - Vote was counted
  - Vote was private
  - Nobody else can vote more than once
  - Nobody can alter others’ votes
- People believe that the machine works correctly
  - These have to do with perception

It is also important that these perceptions are true.

Many potential failure modes

Ugly failure modes

- Ballot stuffing
  - Absentee votes from deceased voters
  - 100% of votes in Oregon are mail-in!
- Post-election ballot tampering
  - Fraudulent behavior by election officials
- Bribery or coercion
Optical sense systems

- Comparable to punch cards
  - Human-factors issues
  - Possible to hand-recount
  - High accuracy

What about e-voting?

- Several different forms
  - Internet voting (used on many college campuses)
  - Computerized voting machines (DRE)

Obvious benefits

- Better human factors
  - Can check for “overvoting”
  - Can review for mistakes
  - Accessible interfaces (no need for helpers)

- It’s new
  - No antiquated machinery
  - Non-traditional election styles
    - Condorcet voting, approval voting, IRV, etc.

Obvious flaws

- Indication to voter that vote is recorded?
  - No paper to drop in ballot box
  - No satisfying thunk from mechanical gears

- Why should you trust that the computer worked?
  - Same argument made by accessibility community
    - Why should you trust a human helper?
  - No voter-visible evidence
How to build e-voting correctly

- Add a card printer to voting machine
  - Get card
  - Insert card
  - Select candidates
  - Print
- Card printed in English
- Voter can read card
- Drop in a box

⇒ “Voter-verifiable audit trail”

And in Brazil…

- Electronic voting since early 90’s
- Paper built-in for newest systems
- Type number for your candidate
- Screen shows picture
- Paper held behind glass – verifiable, but not touchable

⇒ “Mercuri method”

Benefits of a hybrid system

- Human factors benefits via computer input
- Fast computer counting
  - “Estimated results”
- Useful re-counting
  - Computer (OCR)
  - Human
- No vendor trust needed
- No vendor lock-in
  - Standardize cards, fonts, etc.

What about Diebold?

- Established vendor
  - Optical sense systems
  - New DRE systems
- Adopted by Georgia for Nov. 2002 election

- But then something interesting happened…
Some Diebold problems

- March 18, 2003: Bev Harris announces:
  - Open FTP site from Diebold with many GB of data
  - Source code, sample ballots, etc.
- July 8, 2003: Security holes with GEMS
  - Uses Microsoft Access
  - Audit logs can be bypassed
  - All users have the same password (“password”)
    ➔ If it’s online, it’s editable by anybody

Our findings

- Smart card issues
- Incorrect use of cryptography
- General software engineering notes

Smart cards

- Voting terminals are offline during the election
- Voter gets “voter card” after authentication
- Insert card
- Vote
- Machine cancels card

- Other cards
  - “Ender card”
  - Administrator card

Smart card protocol

Terminal ➔ My password is (8 bytes) ➔ Card

Are you valid?
  ➔ “Yup”
  ➔ Cancel yourself, please.
  ➔ “Okay”
Administrator cards

- Administrator / ender cards require a PIN
  - End election
  - Print records
  - Etc.

Administrator card protocol

Malicious poll workers?

- Private access to voting machines / storage cards?
- Before election, rearrange the order of the candidates
  - Votes are recorded by their order, not by name
    - Candidate #1 got 5 votes
    - Candidate #2 got 3 votes
  - Change the order → change who gets credited
  - Come back at the end of the day to fix it
- Voting machines can never be left alone!

Cryptography

- After election is closed, voting terminals phone home
  - Fast “preliminary” tabulation of voting results
- Data also hand-carried via memory card
- Encryption to protect data confidentiality…
How *not* to encrypt data

```c
#define DESKEY ((des_key*)"F2654hD4")
```

- One key for every voting machine, everywhere
- Doug Jones found this five years ago!
  - Still not fixed

If the crypto fails...

- Plaintext data has votes *in the order they were cast*
  - Trace votes to who cast them
  - Vote buying / voter coercion is now possible
- Active adversary can modify the data
  - Confuse preliminary totals
  - Threat to storage cards (in transit and post-delivery)

Software engineering

- Software written in C++, runs on WinCE
  - Some effort to prevent buffer overflows
  - In public filings, Diebold has admitted problems
- Code quality well below any “high assurance” system

Thoughts

- Our democracy is depending on these machines!
- Election officials don’t realize what they’re buying
- Vendors don’t understand security
- Features vs. security
  - Adding wireless capabilities to voting terminals?
Yes, punch cards need to go...

Conclusion

- Paperless DRE voting systems are unacceptable
  - “Security through obscurity” arguments are fallacious
  - Certification is (currently) meaningless

Everything worked fine in our last election.
How do you know?