The Risks of Electronic Voting

Dan Wallach
Rice University

Collaborators:
Tadayoshi Kohno (UCSD)
Aviel D. Rubin (Johns Hopkins)
Adam Stubblefield (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.
Human factors issues
Mechanical flaws

Bush

Gore
Ugly failure modes

Ballot stuffing
- Absentee (mail-in) votes from deceased voters
- 100% of votes in Oregon are mail-in!

Post-election ballot tampering
- Fraudulent behavior by election officials

Bribery or coercion
Traditional anonymous voting

- One paper card per office, list of candidates
  - Easy to count (just make two piles)
  - Easy to recount
  - Used in most countries
Mechanical voting systems

Odometer-style rotors inside

- Hidden during election
- Visible after election

Post-election...

- Machines impounded
- Can be inspected for fraud
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

- 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
Accuracy of voting systems

- California recall election (October 2003), residual vote rate
  - Percentage of "incomplete" / undervoted ballots (source: Rebecca Mercuri)

![Bar chart showing residual vote rate for different voting systems](chart.png)
Reliance on certification

Independent Testing Authorities

- Allowed to see the code
  - Nobody else allowed to look
- Certify satisfaction of FEC standards
- Required by many states

Result: “Faith-based voting”
Trust issues

- All code **must** be correct
  - No fall-back position if code is buggy
- No independent verification that code works
  - Should voting machines be closed source?
    - Alternative: Government pays for 3rd party developer
    - Give source code away to everybody (Australia)
Can a DRE system employee throw the election?

- Is it technically feasible?
  - Yes

- Would there be any evidence?
  - Probably not

- “Logic and accuracy tests”?
  - Easily faked
Trusted Computing Base

- Essential concept when doing a security analysis
  - The portion of the system that must be secure
  - Smaller TCB $\implies$ more secure system
DRE has a much larger TCB

- In-house software developers
- Pre-election storage of machines
- Pre or post-election manipulation of storage cards
- Hand recounting removes software from TCB
How to build e-voting correctly

- Option 1: Print onto plain paper
  - Deposit in ballot box
  - Accessible interface
  - Inside: normal inkjet printer

(AccuPoll AVS1000)
How to build e-voting correctly

- Option 2: Print onto existing optical-scan ballots
  - Accessible interface
  - Only need one per precinct

(ES&S Automark)
Ballot under glass

- Option 3: Brazilian urnas
  - Ballot under glass
  - Voters type number for candidate

- Recently cancelled (unclear why)

→ “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.
Track Record for DRE in U.S.?

- Diebold AccuVote-TS Adopted by Georgia for Nov. 2002 election

- But then something interesting happened...
Bev Harris’ findings

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
Diebold’s smart card protocol

Terminal

My password is (8 bytes)

Card

“Okay”

Are you valid?

“Yup”

Cancel yourself, please.

“Okay”
Administrator cards

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

Terminal

What kind of card are you?

"Administrator"

Card

What's the secret PIN?

"1234"

What's the secret PIN?

"1234"
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...
#define DESKEY
    ((des_key*)"F2654hD4")

- One key for every voting machine, everywhere
- Doug Jones (Iowa official) found this in 1997!
  - Bug still exists in early 2004
  - Fixed now?
How else not to encrypt data

DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize, DESKEY, NULL, DES_ENCRYPT);

- Initialization vector is always zero
- Encryption is deterministic
- Vulnerable to chosen-plaintext attacks
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
Software process

- Assorted bad practices
  - #ifdef 0 / #ifdef XXX / #ifdef LOUISIANA

- Poor documentation
  - No evidence of (useful) high-level design docs
    - Nothing checked into the archive
    - No comments quoting from design docs
      - Some quotes from algorithms textbooks
  - Numerous complex functions without comments

- Code quality well below any “high assurance” system
Thoughts

- Our democracy is depending on these machines!

- Election officials rely on independent testing authorities (ITAs)
  - Diebold certified despite its poor design
  - Raises questions about other vendors

- Vendors don’t understand computer security

- Features vs. security
  - Adding wireless capabilities to voting terminals?
Impact of our work

- Our results confirmed by several independent studies
- California, Nevada, some others will require voter-verifiable audit trails
- Holt bill pending in U.S. Congress (H.R. 2239)
  - Requires voter-verifiable audit trail
- U.S. military cancelled SERVE
  - Paperless, Internet-based voting system
What you can do

Think globally, act locally
  ● Every state is different
  ● Often, every county is different

Read any policy & procedure docs
  ● Machine storage & maintenance?
  ● Offer to help improve policies

Be an election judge
Get to know your representatives
If they’re still using DREs

Leadership Council on Civil Rights / Brennan Center Report (www.civilrights.org)

Recommendations for Nov. 2004
● Independent audits
● Better policies and procedures
● Parallel testing
● Etc.
Conclusion

- Paperless DRE voting systems are unacceptable
  - “Security through obscurity” arguments are fallacious
  - Independent certification is (currently) meaningless
  - Best today: precinct-based optical scan

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

- Our study of Diebold’s system
  http://avirubin.com/vote/

- More about voter-verifiable audit trails
  http://www.verifiedvoting.org/

- See also, Bev Harris
  http://www.blackboxvoting.com/
How do you like my Halloween costume?

Sorry—what are you supposed to be, exactly?

Something truly terrifying. I'll give you a hint—

I'm prone to technical glitches. I have huge security flaws, and I leave absolutely no paper trail—

Give up? I'm certainly stumped!

And the companies that make me are owned and operated by intensely partisan Republicans!

I'm a touch screen voting machine! Bwah ha ha ha ha ha!

See, the point is, this is a really scary threat to democracy—

Yeah, yeah, I got that part.

I'm going to be a ghost!