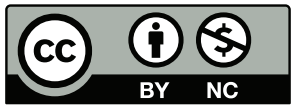
Risks of Computers: Voting Machines



Voting Systems and Computers

- There is a long history of problems (or perceived problems) with voting systems
- Technology has frequently been invoked to solve the problems
- Over the years, many different kinds of voting machines
- Elections are process-driven and often highly partisan

Requirements

- Accuracy
- Voter privacy
- Resistant to fraud
- Resistant to error
- Resistant to information leakage
- Usable by voters
- Usable by handicapped voters
- More. . .

Participants

- Voters
- Election boards (usually county-run, but following state standards)
- Poll workers
- Poll watchers from political parties
- Courts (state and federal)
- News media

Processes (Simplified!)

- Voter registration
- Distribution of the eligible voter rolls
- Zeroing the counting mechanism
- Voter verification at the polls—and must handle challenges
- ☞ Voter must be given the right ballot
- Casting a vote
- "Closing the polls"
- Quick count and reporting
- Preservation of the ballots
- The official count
- Recounts

Voter Registration

- How is registration data stored?
- Hard copy? (I once had problems voting because the cards were alphabetized incorrectly)
- Computers? What about software bugs? Backups?
- What about typographical errors in someone's name? Suffixes like "Jr." or "III"? Name collisions?

Zeroing the Count

(Public domain photo, Wikipedia)

- Must show that no votes are recorded before the polls open
- Transparent or translucent ballot boxes; sometimes opened and showed to everyone
- Poll workers—and watchers—verify the counters on mechanical voting machines
- Print a “zero tape” on an electronic voting machine

Voter Verification

- How do you find a voter?
- Software?
- What if the software is buggy?
- What if the system crashes?
- What about network links in “vote anywhere” jurisdictions?
- What about exception processing?

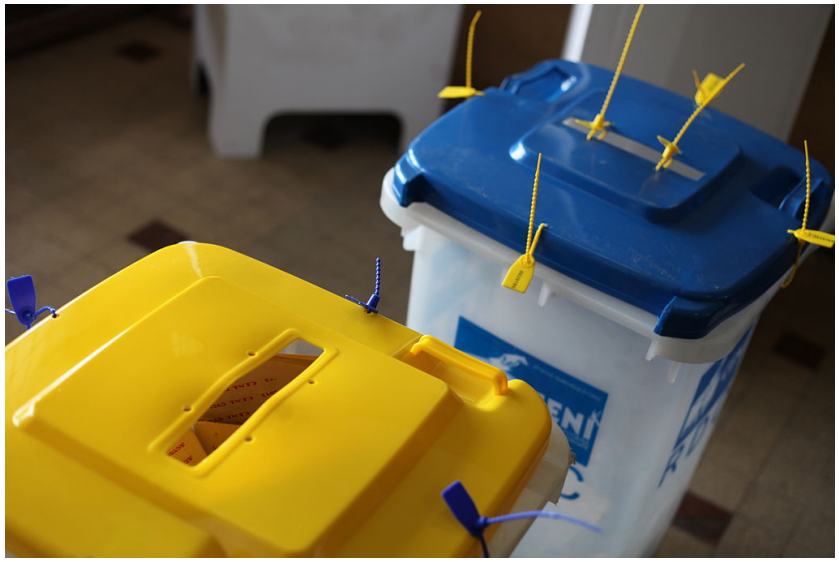
Exception Processing

- There are strict—and complicated—processes for verifying and recording each voter
- Sometimes, there's an exception: someone who isn't listed but claims to be registered, or perhaps gets a court order allowing them to vote
- What is the process? Does the software support it?
- Example: some electronic polling books produce a magnetic card with the proper ballot for that voter. Can it handle an unlisted voter?
- Computers are inflexible!

Casting a Vote

- Paper—it's pretty easy, though people can get it wrong
- (There are strict legal requirements for valid ballots)
- Mechanical machines: move levers; move large lever to vote
- Punch cards—but watch out for hanging chads
- Electronic: many different ways. . .
  - Press physical buttons under ballot labels
  - Use a touch screen, repeatedly
  - Mark paper ballots and immediately feed to an optical scanner
- Internet voting?
- Many problems in this space—more shortly

Closing the Polls



(Photo by MONUSCO, a UN agency)

- Must show that no votes are recorded after the polls close
- Seal the ballot boxes in a verifiable way
- Lock the actuating mechanism on mechanical voting machines
- Run the software that prints the vote totals to paper tapes and disables further voting

Ballot Box Seals

(Australian Government Department of Foreign Affairs and Trade)

(Photo by MONUSCO, a UN agency)

Quick Count

- Reporters want the totals *immediately*
- Paper ballots take a long time to count
- (That's one reason Americans prefer voting machines; another is the length and complexity of the ballots)
- Precincts send the immediate results to the local election board: phone calls, faxes, dial-up modems, more

Errors in the Quick Count

- It's easy to misread the numbers
- Handwriting errors in manual processes
- Data entry errors
- Arithmetic errors
- Buggy tallying software

Showing That All Votes were Counted

Photo by Dave Kopel; used by permission. (http:

//volokh.com/2008/03/22/taiwan-presidential-election-results-and-process/)

Preserving the Ballots

- The official count takes longer, and is done with more care
- Goal: try to eliminate the errors in the quick count
- Also: handle absentee ballots and provisional ballots
- This is the count that really matters
- So: recount the paper ballots, reread the mechanical counters, and—for electronic voting machines—use the data recorded on the memory cards

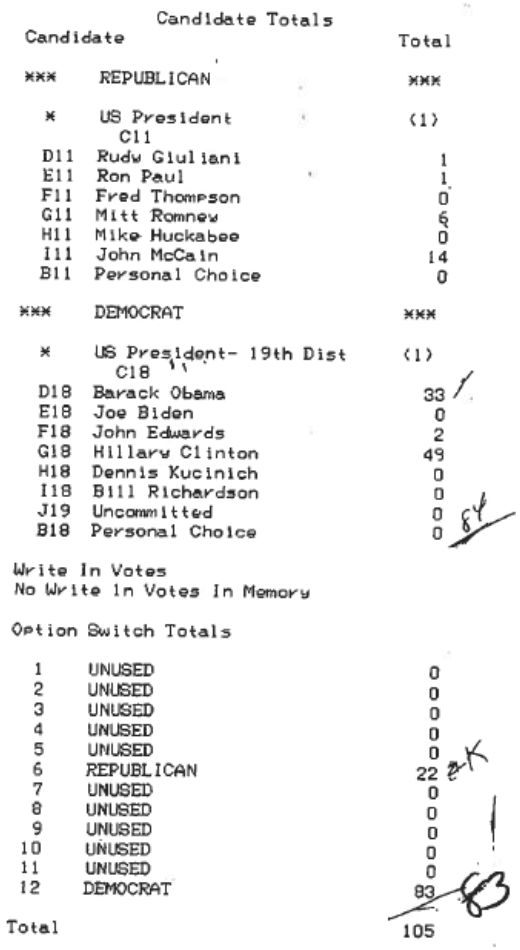
Errors. . .

- The quick count printouts from some voting machines *should* be the same as what's on the memory cards.
- Not always. . .
- In 2008, Ed Felten found a precinct where the tapes showed 280 Democratic voters, and 95 votes for Obama
- The memory cards showed 279 and 94
- But the tapes should just be a printout of what's on the memory card!
- The discrepancy was never satisfactorily explained. There was no independent investigation.
- (The vendor attributed a previous discrepancy to operators pressing buttons they shouldn't have. There are other errors that can't be explained that way.)

Recounts

- With paper ballots, a recount makes lots of sense
- With mechanical machines, you can eliminate errors in reading the counters or transcribing the figures
- With electronic machines, you're just running the same software again—there's no independent check

Englewood Voting Machine Tape



Candidate Totals

Candidate		Total
***	REPUBLICAN	***
*	US President C11	(1)
D11	Rudy Giuliani	1
E11	Ron Paul	1
F11	Fred Thompson	0
G11	Mitt Romney	6
H11	Mike Huckabee	0
I11	John McCain	14
B11	Personal Choice	0
***	DEMOCRAT	***
*	US President- 19th Dist C18	(1)
D18	Barack Obama	33
E18	Joe Biden	0
F18	John Edwards	2
G18	Hillary Clinton	49
H18	Dennis Kucinich	0
I18	Bill Richardson	0
J19	Uncommitted	0
B18	Personal Choice	0

Write In Votes
No Write In Votes In Memory

Option Switch Totals

1	UNUSED	0
2	UNUSED	0
3	UNUSED	0
4	UNUSED	0
5	UNUSED	0
6	REPUBLICAN	22
7	UNUSED	0
8	UNUSED	0
9	UNUSED	0
10	UNUSED	0
11	UNUSED	0
12	DEMOCRAT	83
Total		105

- The per-candidate totals show 84 Democratic votes and 22 Republican votes
- The ballot selection totals show 83 Democratic votes and 22 Republican votes
- Why the discrepancy?
- (From `https://freedom-to-tinker.com/blog/felten/nj-election-discrepancies-worse-previous`

What's the Problem?

- Software can be buggy
- Vendors consider their source code proprietary, and have often blocked investigations
- There is nothing else to check on a recount: the software is the software is the software

Errors!

- There is a long history of errors with DRE voting systems
- The NJ election tapes
- “Fleeing voters”: voter who don’t press the ”cast my vote” button
- Cuyahoga, OH: none of the vote-tallying counts agreed
- NC: a 12-bit counter overflowed in a large precinct
- Many more. . .

Counting Software is Also Buggy

- Bernalillo County, NM: in-person voters used DRE machines; absentee ballots used optical mark cards
- On Election Day in 2000, the absentee ballots appeared to go for Gore
- That was odd—in that jurisdiction, absentee ballots tend to skew Republican
- The problem: the counting program didn't handle the "straight ticket" option
- The elections supervisor: the software was buggy
- The vendor: he programmed it incorrectly

Why Use DRE Machines?

- They're cheaper and mechanically more reliable
- Blind voters can cast ballots without assistance
- Other handicaps are also more easily accommodated
- They report results very quickly

Evaluations

- To my knowledge, *every* independent evaluation of DRE machines has found serious flaws
- Bad crypto, poor design, no voter privacy, buggy software, susceptibility to viruses, and more
- California even decertified many

Physical Security

- If voting equipment isn't properly safeguarded, tampering can occur
- *Chain of custody must be maintained throughout the election process*
- Paper ballot boxes can be stuffed, before, during, or after voting
- Tamper with the gears and cams on mechanical machines
- Reprogram electronic voting machines
- There are supposed to be security seals, but they're easy to bypass

☞ It's much easier to introduce subtle, unauditable flaws

Pacman!

(Photo courtesy Alex Halderman)

- These machines are generally have their programming on a compact flash card
- There's supposed to be a security seal—but those are easy to bypass
- Alex Halderman and his students reprogrammed a voting machine to be a Pacman game
- `https://www.youtube.com/watch?v=TpMDCArdzwA`

Pre-Election Voting Machine Storage, Princeton, 2008

(Photos courtesy Ed Felten)

Current Standards

- Most places are moving to optical mark ballots that are scanned immediately
- Voters can verify that their ballots were read correctly, and there are pieces of paper for hand recounts
- But: do voters actually check the scan results? Not really. . .

Other Ideas

- Internet voting
- Cryptographically verified voting

Internet Voting

- It's software, with all that implies
- It's running on ordinary PCs with ordinary Web browsers
- (Washington, DC, ran a trial election that way, and challenged people to break it. Halderman and his students made it play the U. Michigan fight song when people cast ballots.)
- Imagine an electoral virus
- Imagine one written by a country that wanted to influence another country's elections
- What about authentication? Coercion? Usability?

Cryptographic Schemes

- Use fancy cryptography to cast and tally votes
- Anyone can look at the published (cryptographic) vote totals and verify that their vote was counted
- No one else can tell who voted for whom
- But—it's still all done with software

We Can Build ATMs; What's Different About Voting?

- ATMs have audit logs, cameras, etc.—but for voting, we need privacy
- Consumers get bank statements—but there's no receipt for your votes
- Transactions can be checked and (if necessary) rolled back—but we rarely rerun elections
- Banks will spend more money than elections boards will. . .

Breaking News: Virginia Decertifies AVS WinVote DRE Machines

- Runs Windows XP Embedded, but with no patches since 2004
- (The system was too old for some standard security tools!)
- Uses WiFi with WEP—and an unchangeable password of “abcde”, and you can’t disable WiFi without disabling the voting software
- Lots of ports open—including disk-sharing. It’s a WiFi file server!
- Administrator password hardwired to “admin”
- The database password is hardwired to “shoup”, the previous company name
- The USB ports are only marginally protected
- Source: `http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf`

Conclusions

- With current technology, DRE machines are not nearly good enough
- We need a voter-verifiable audit trail
- We also need one that people will actually check
- The security and correctness of a voting system is a systems problem: you have to get them all right
- Very few security or software engineering peope have any confidence in today's electronic voting systems