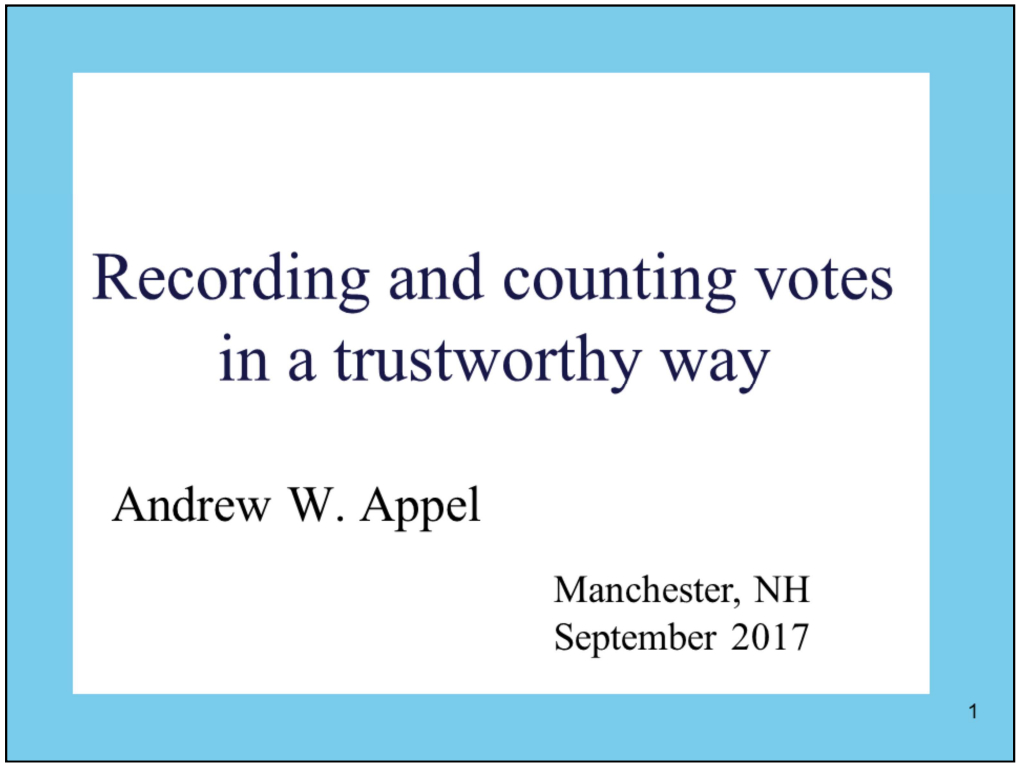


When voters go to the polls, how can they trust that their votes will be recorded accurately, counted accurately, and aggregated accurately? I will address the technological and organizational answers to that question.

This is a summary of my testimony before the Presidential Commission on Election Integrity, in Manchester, New Hampshire, September 12, 2017. By background, I am a computer scientist with expertise in computer security and formal verification of software. But for the last 15 years I have also studied, and written about, elections and voting technology.

Andrew W. Appel

Professor of Computer Science

Princeton University

What a voting protocol needs

- Allows each person to vote (just) once
- Accurately records the votes
- Accurately counts the votes
- Voter can be sure her vote is counted, without trusting the other side's people
  - Even if the other side's people are election officials!
- Secrecy
  - Can't learn how a person voted

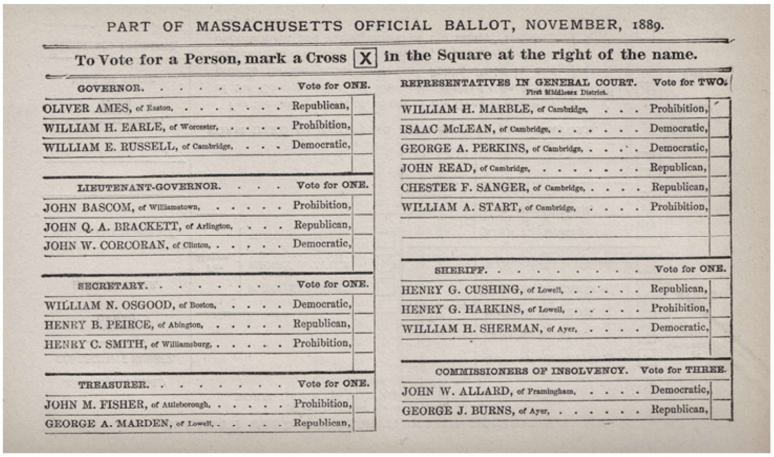
2

Every eligible voter should be allowed to cast one vote – but not more than one! Starting around 1890 in the U.S., voter registration combined with sign-in in the polling place (using "pollbooks") ensures that. Then, each vote should be counted – exactly once! Then, totals from each polling place or ballot box should be added up — correctly!

To make things even more challenging, in the U.S. we have the secret ballot. That's because, throughout the 19th century and even into the 20th century, there were many abuses: without the secret ballot, if a worker didn't vote the "right way" he might lose his job, if a small businessman didn't vote "the right way" he might lose customers, if a householder didn't vote "the right way" he might lose garbage collection and street repairs. Now, we take the secret ballot for granted—but it does make it harder to design an accurate and trustworthy election system.

The "Australian Ballot"

adopted in U.S.A around 1890



PART OF MASSACHUSETTS OFFICIAL BALLOT, NOVEMBER, 1889.

To Vote for a Person, mark a Cross [X] in the Square at the right of the name.

GOVERNOR. . . . . Vote for ONE.

OLIVER AMES, of Easton, ... Republican,
WILLIAM H. EARLE, of Worcester, ... Prohibition,
WILLIAM E. RUSSELL, of Cambridge, . . . Democratic,

LIEUTENANT-GOVERNOR. . . . Vote for ONE.

JOHN BASCOM, of Williamstown, ... Prohibition,
JOHN Q. A. BRACKETT, of Arlington, . . . Republican,
JOHN W. CORCORAN, of Clinton, ... Democratic,

SECRETARY. . . . . Vote for ONE.

WILLIAM N. OSGOOD, of Boston, ... Democratic,
HENRY B. PEIRCE, of Abington, ... Republican,
HENRY C. SMITH, of Williamsburg, ... Prohibition,

TREASURER. . . . . Vote for ONE.

JOHN M. FISHER, of Attleborough, ... Prohibition,
GEORGE A. MARDEN, of Lowell, ... Republican,

REPRESENTATIVES IN GENERAL COURT. Vote for TWO.
First Middlesex District.

WILLIAM H. MARBLE, of Cambridge, . . . Prohibition,
ISAAC McLEAN, of Cambridge, ... Democratic,
GEORGE A. PERKINS, of Cambridge, ... Democratic,
JOHN READ, of Cambridge, ... Republican,
CHESTER F. SANGER, of Cambridge, ... Republican,
WILLIAM A. START, of Cambridge, ... Prohibition,

SHERIFF. . . . . Vote for ONE.

HENRY G. CUSHING, of Lowell, ... Republican,
HENRY G. HARKINS, of Lowell, ... Prohibition,
WILLIAM H. SHERMAN, of Ayer, ... Democratic,

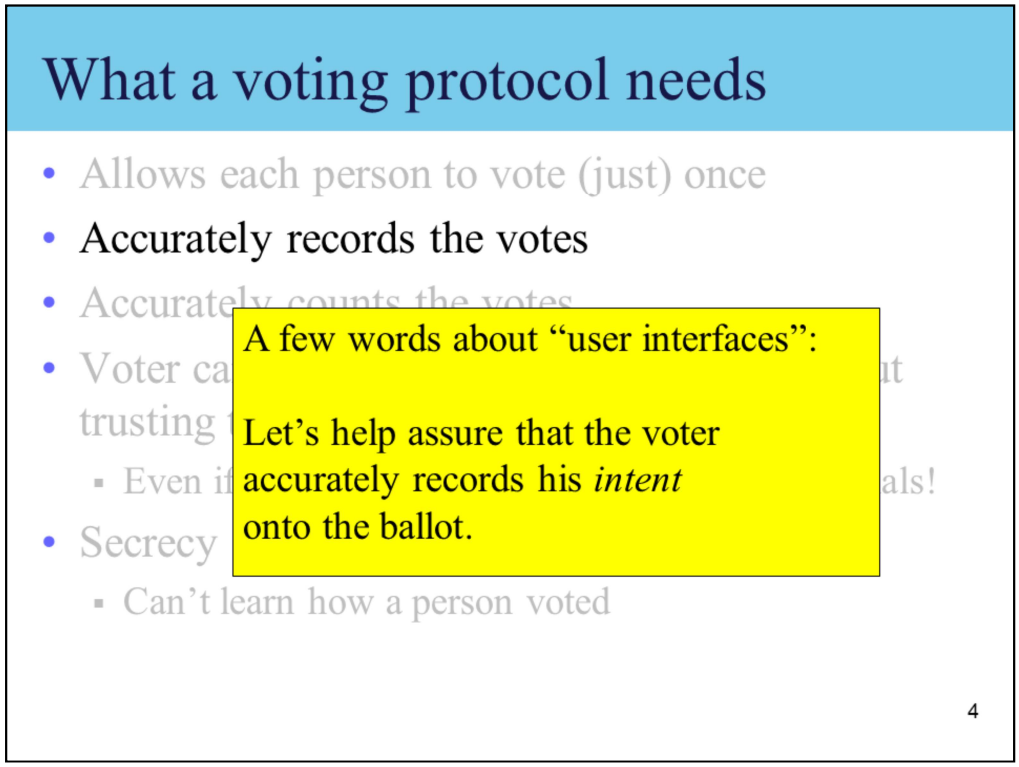
COMMISSIONERS OF INSOLVENCY. Vote for THREE.

JOHN W. ALLARD, of Framingham, ... Democratic,
GEORGE J. BURNS, of Ayer, ... Republican,

From *ELEMENTS OF CIVIL GOVERNMENT*
by ALEX. L. PETERMAN, Kentucky State College, 1891

3

We take for granted that a ballot looks something like this. But before it was invented, in the late 19th century, people voted by just telling the election judge who they wanted to vote for. Or, they voted by writing down the names of their candidates on a piece of paper. Or by bringing a paper ballot with them preprinted with the names of the candidates they wanted. Or, unfortunately, by bringing a whole stack of paper ballots and trying to get away with inserting them all into the ballot box. The "Australian Ballot", where all the candidates are printed onto the ballot and the voter just marks an X, was an important technological invention. The preprinted ballots are in the possession of the poll workers, and they hand out just one blank ballot to each voter.

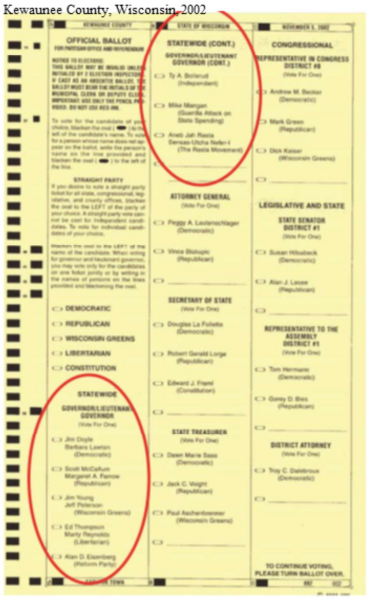


If the layout of the ballot isn't designed very well, or the technology for voting is clumsy and counterintuitive, then the voters may not properly translate their *intent* onto the ballot paper or onto the touchscreen. I'll give a couple examples of ballot-design failures.

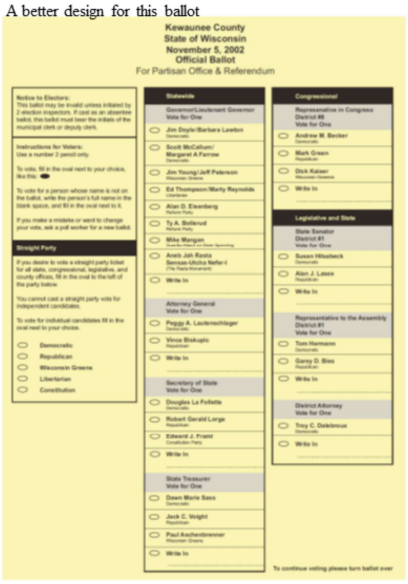
Misleading ballot design

can cause voters to waste their vote

Kewaunee County, Wisconsin 2002



A better design for this ballot



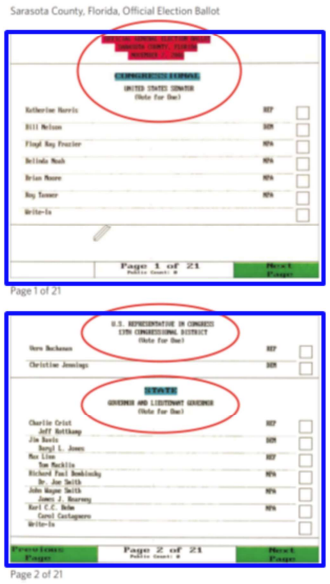
5

Images from: Better Ballots, by Lawrence Norden, David Kimball, Whitney Quesenbery, and Margaret Chen, 2008.

In this ballot at left, from Kewaunee County, Wisconsin in 2002, there are 8 candidates for Governor. That list of 8 starts near the bottom of the first column and continues at the top of the second column. Hundreds of voters misunderstood, and thought that there was a 5-person race in the first column, and a 3-person race in the second column; and those voters marked a candidate in each of those two contests. That meant they *overvoted* in the Governor contest, and therefore their choice didn't count.

A proposed better design for this ballot is shown at right. It has many typographical improvements that make it easier for voters to read and understand. In particular, it doesn't split the Governor candidates into two parts.

Touchscreens can also have ballot-design problems



Sarasota, Florida, November 2006:

21-screen ballot, one contest per page,

except that **this** page had **2** contests.

Many voters didn't notice to vote in this congressional race –

more undervotes than the margin of victory.

6

In Sarasota, Florida in 2006, using touchscreen voting machines, there were so many contests on the ballot that it took 21 pages of touchscreen to show all the contests. But the ballot designers chose to put two contests on one page, as shown at the bottom of this slide. The race for U.S. House of Representatives, with only two candidates, took up so little space on the screen that hundreds of voters didn't notice it was there, and didn't cast a vote for Congress. That's bad design—if there's one contest per page, then they should have stuck to that consistently, to avoid confusing voters.

Good ballot design is not an accident

Good election administers use "best practices" in ballot design.

From: Center for Civic Design, civicdesign.org

7

User-interface design experts, such as the authors of the "Better Ballots" report cited on the previous page, and such as the authors of the booklets shown here, have developed guidelines and methods that election administrators can use in preparing ballots. Many professional election administrators in the U.S. are aware of these concepts, and are enthusiastic to improve the readability and usability of their ballot designs.

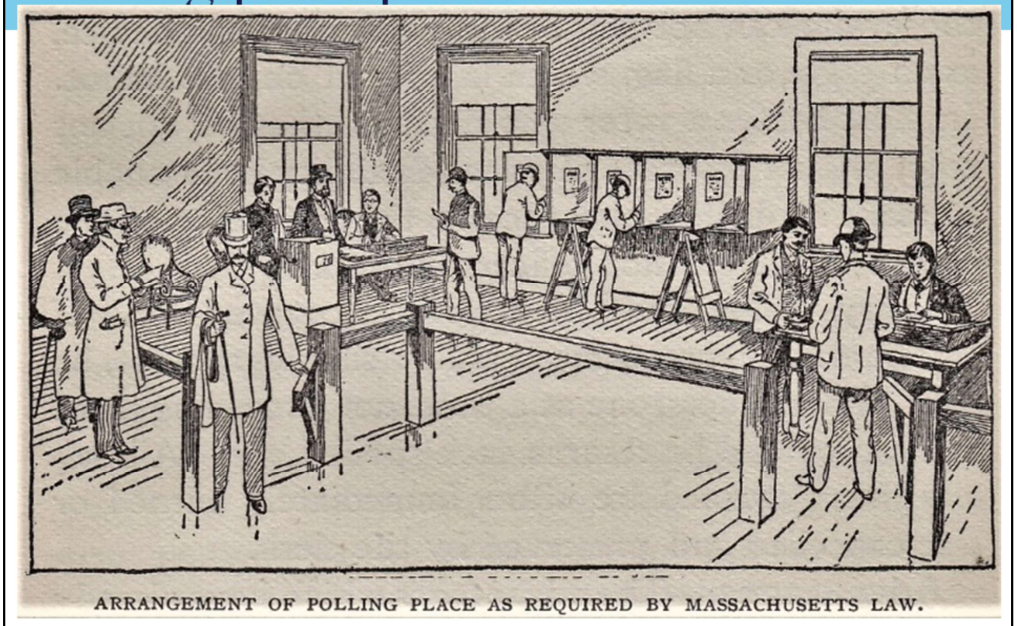
What a voting protocol needs

- Allows each person to vote (just) once
- Accurately records the votes
- Accurately counts the votes
- Voter can be sure her vote is counted, without trusting the other side's people
  - Even if the other side's people are election officials!
- Secrecy
  - Can't learn how a person voted

8

Ballot design is a part of "Accurately records the votes." But how are all these other criteria ensured?

Polling place procedures 1890

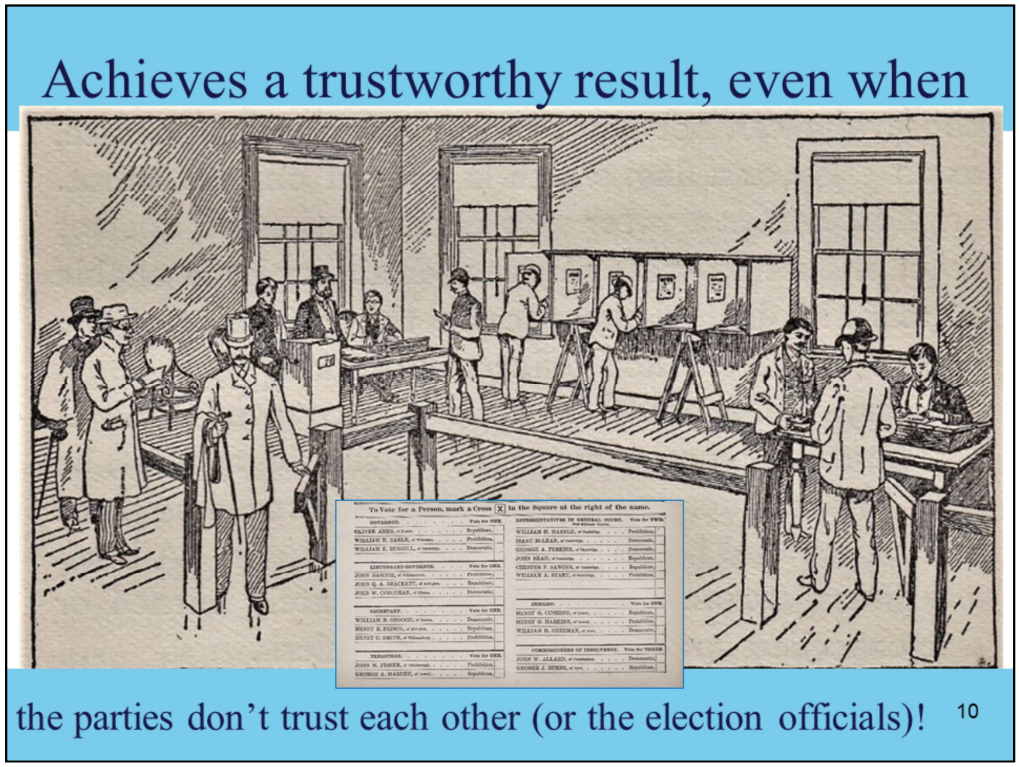


ARRANGEMENT OF POLLING PLACE AS REQUIRED BY MASSACHUSETTS LAW.

From PETERMAN 1891

Here's how, at least traditionally in the U.S. in the 20th century. You can see at right, the voter is signing in at the pollbook. Two election workers, or an election worker and a pollwatcher, are there behind the desk, checking for his name in the pollbook and matching his signature. Then they hand him a ballot, which he takes to the booths at center to mark in private, with nobody looking over his shoulder. Then he brings it to the ballot box—and look how many people are watching that ballot box, to make sure no unauthorized ballots are dropped in! You can just make out the curved lever on the left side of the ballot box; when the pollworker pulls that lever, it opens up the slot on the ballot box, *and* it rings a bell, so that everybody in the room can hear when a ballot is dropped in the box. That helps prevent cheating. And some people will cheat if they can—that's why there are all these safeguards.

There's nothing very surprising in this picture. We take it for granted that this is the way you organize a polling place. But it had to be *invented*, in response to the abuses of the 19th century.



When you put together the Australian Ballot, marked by the voter with an X, with pollbooks and voting booths and a ballot box that's watched by witnesses from both parties, you get a system that works pretty well.

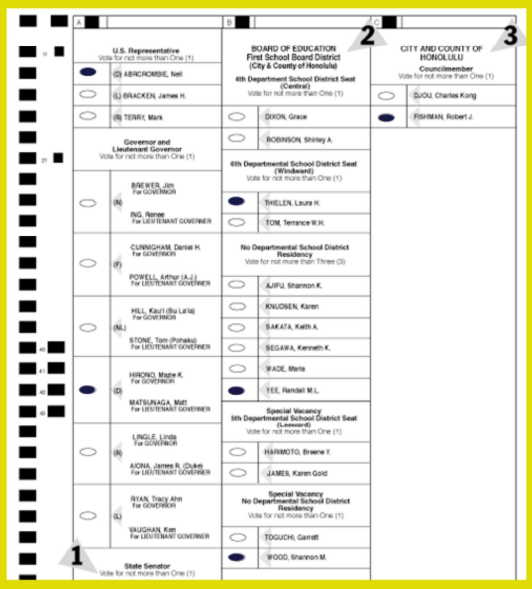
Hand-counted paper ballots

- On the whole, a good system
- Works well in many countries
  - where there's just one contest on the ballot
- **In U.S. elections, has a major flaw:**
  - **So many contests to count**
  - **hand counting difficult to do accurately**
  - difficult to find volunteers from both (all!) parties to supervise against cheating

11

But even by 1900, people noticed that it's hard to count paper ballots by hand. Actually, in Europe or Canada, it's not so hard, because in their parliamentary, nonfederal systems they have elections with only one contest on the ballot. And then you can count by hand, by just sorting the ballot papers into one pile for each candidate, and counting up the piles. But in an American election, there are many contests on the same ballot: President, Senator, Congressman, Governor, State Senator, State Rep., Mayor, Councilman, School Board, Dogcatcher, Judge retentions, propositions. To count those, at 8pm after a long election day, is hard to do consistently and accurately. So already by 1900 people were trying to design machines to count votes.

Precinct-count optical-scan



12

Optical-scan balloting was introduced in the U.S. about 1970. By the 1980s, precinct-count optical scan was already in use in some places. In the precinct-count system, the voter marks the ballot and feeds it directly into the scanner in the polling place. The computer (in the white box on top) counts the votes, and the ballot drops into a sealed ballot box (the blue box at bottom). With well designed ballots, precinct-count optical scan has proved to be a very accurate and trustworthy way of voting.

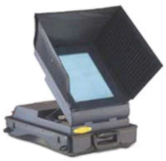
Touch screens:

Direct-Recording Electronic

Shouptronic, 1980

Sequoia, 1987

Votronic, 1991



Sequoia, 2000

Diebold, 2002

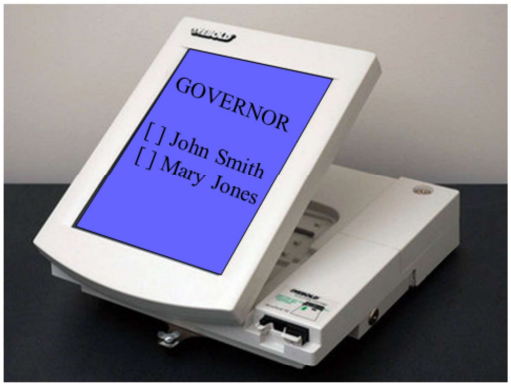
13

In the 1980s and 1990s, voting-machine vendors developed "direct-recording electronic" (DRE) voting computers. In this system, the voters indicate their choices on a touchscreen (or some other input device), and the computer records and counts the vote in its internal memory, and/or in an electronic memory cartridge. There's no paper record of the vote (but see note below). At the closing of the polls, the machine can print a cash-register-tape printout of the results; this along with the memory cartridge are transported to a central place for aggregation (adding up all the per-machine totals).

After the polls close, the machine can print out a list of every vote cast, from its internal memory; but that's not the same as a paper ballot that the voters can see, and if the computer is wrong (by accident or cheating), then the paper is just a printout of those wrong numbers.

Some DRE voting computers (in about 3 states of the U.S.) are outfitted with a "Voter Verified Paper Audit Trail" that the voters *can* see before they cast their vote, and that drops into a sealed ballot box that can be recounted by hand. That's an important check on the computer memory; but it still has many problems: most voters don't understand what that printout is for; and they don't check it very reliably; the thermal paper ("cash register tape") is hard to recount by hand. Better technology is now available, for example, voters that are unable to use pen-and-paper can use touch-screen Ballot Marking Devices (BMDs) that can produce optical-scan ballots to be counted by op-scan voting machines.

Ballot definition files



14

How does the computer program in the voting machine "know" what candidates are on the ballot? The answer is that there is a "ballot definition file" prepared by election administrators, listing all the contests and candidates.

Election Management computer

Ballot Definition Cartridge

15

The election administrator (a county employee, or a contractor, etc.) uses software on an ordinary laptop or desktop computer to prepare the ballot definition file. Then the ballot definition is written to a removable memory cartridge (like a thumbdrive, or some similar technology). This is the "ballot definition cartridge."

Ballot definition files

Insert memory card
into the PCMCIA
slot of a voting machine

16

The ballot definition cartridge is then inserted into a slot on the voting machine. Here, you can see that the slot is down low on the right-hand side. Now the voting computer is ready for election day.

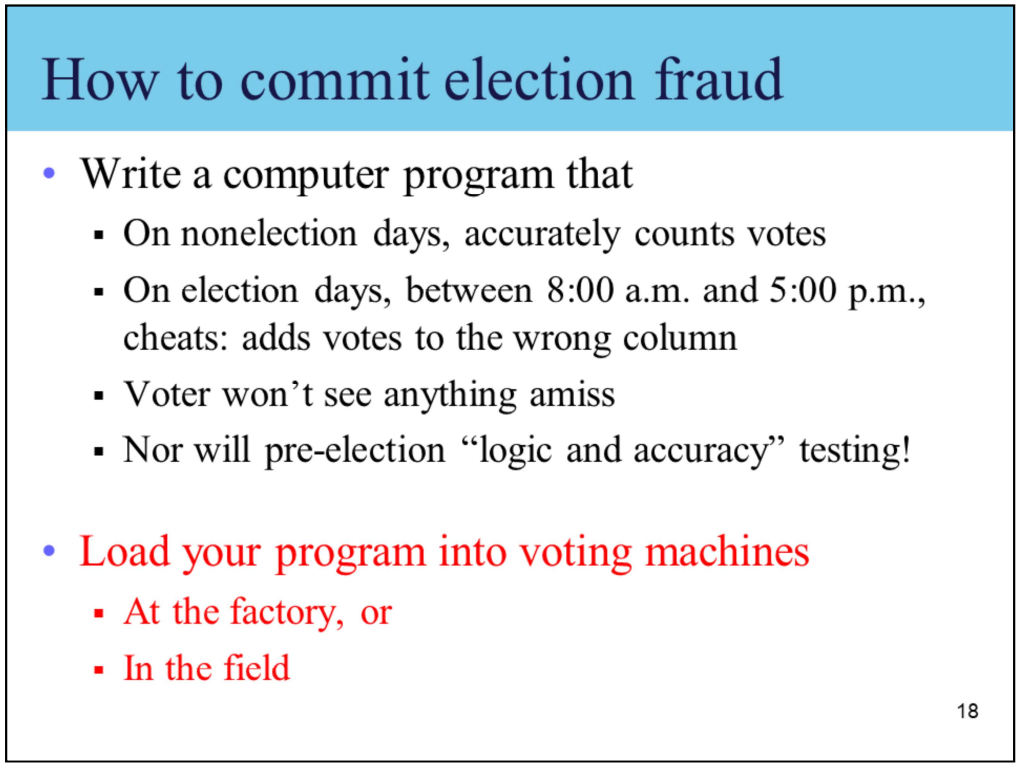
Fundamental flaw of voting computers:

Whoever programs the computer,

decides what election results are reported by the computer program inside the voting machine

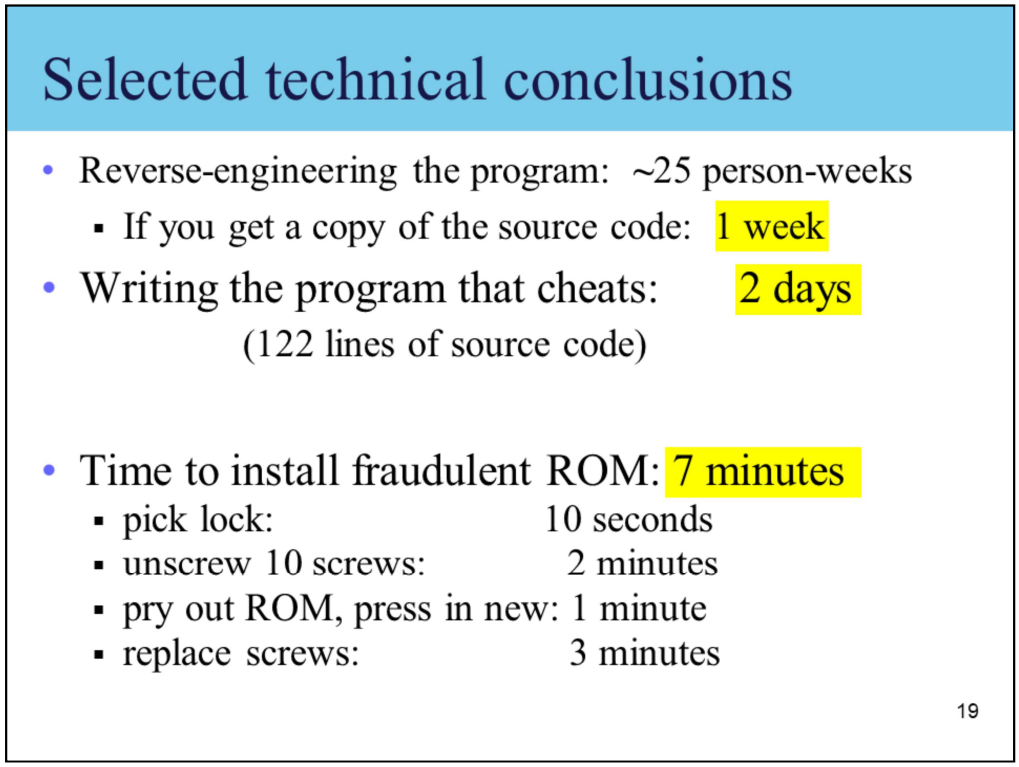
17

'nuff said.



Suppose someone wants to steal an election by hacking a voting machine. They can replace the legitimate vote-counting program inside the voting computer, with a fraudulent program that deliberately miscounts the votes. If you were doing this, you wouldn't make it *always* cheat, because the election administrators sometimes test the machines, before the election, by casting a few votes and then seeing the total. This is called "logic and accuracy testing," or LATA. LATA is good for some things—for example, making sure that the touchscreen isn't miscalibrated, or that the ballot definition is generally OK.

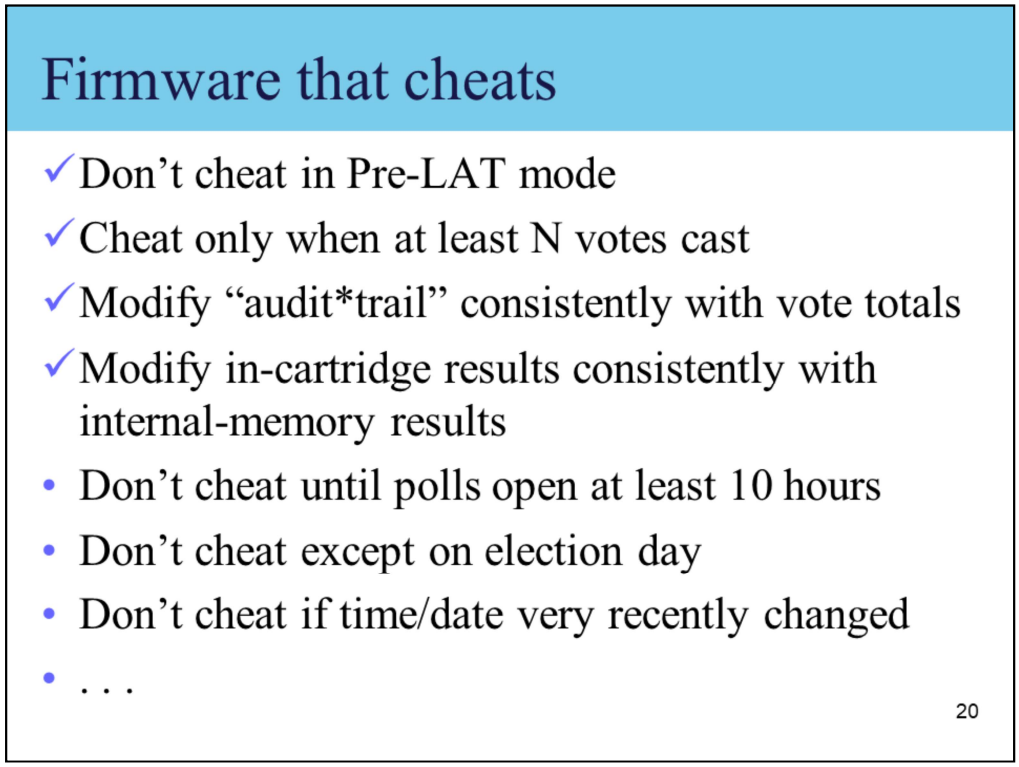
BUT, it's easy to make a cheating vote-stealing program that isn't detected by logic and accuracy testing! Every voting machine (just like any other kind of computer) has an internal clock, so it knows when it's election day. So you just make your cheating program cheat only on election day, after 8am. Since the LATA is done *before* election day, the cheating program will be on its "best behavior" when LATA is done.



In connection with my expert-witness testimony in a court case in New Jersey (2008-2009), I did a forensic examination of New Jersey's "AVC Advantage" voting machines. As part of that study, I wrote a vote-stealing program. First, my team had to understand how the legitimate program works, before modifying it to cheat. This is called "reverse engineering." We tried it two ways: first, without the "source code," and second, with the "source code." It's much easier with the source code, of course, but either way it's well within the capabilities of a moderately qualified hacker.

Then, writing the vote-stealing program is easy—it took just a couple of days to write and test.

By the way, don't try this at home! It's a felony to install vote-stealing programs into a government owned voting machine that will be used in an election. I did mine as part of a court-ordered forensic study, inside a secure building at the New Jersey State Police headquarters. But an election hacker wouldn't have that kind of respect for the law.



Here are some things my vote-stealing program did, so as to avoid detection. Basically, it waits until 8pm when the pollworker turns the key to shut down the election and print out the results. Just before printing out the results, my program shifts 20% of the votes from candidate A to candidate B. The computer program stores the votes redundantly in two different memories, so my program makes sure to cheat in both memories. The computer program has an "audit trail" in its electronic memory that's supposedly some sort of protection, so my computer program changes the audit too!

By the way, the Ballot Definition File has each candidate listed with his/her party affiliation (Democrat or Republican). So if you want to steal votes generically in favor of one party or the other, it's easy to program that up. Once you install that program in the voting computer, it will steal votes in election after election for many years to come.

On 1990's era voting machines, you had to replace some ROM chips to install cheating software

(This machine is still used in NJ, LA, PA)

21

Then, to install that vote-stealing program in the AVC Advantage voting machine, I picked the lock on the back door of the machine. That's easy, it's a cheapo lock; I'm not at all an expert lock-picker, but I can pick this lock in about 10 seconds. Then I unscrew 10 screws on the panel that covers the motherboard. You can see the motherboard here, it's green. Those four computer chips with the white labels on them, hold the computer program that runs the election. Just replacing one of them, at lower right, is enough to install my vote-stealing program. The whole process takes about 7 minutes, using a screwdriver.

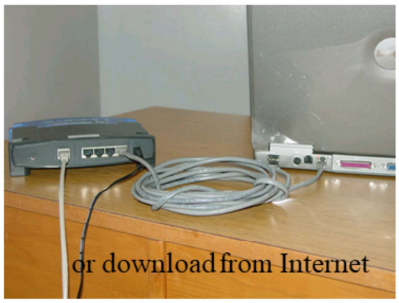
By the way, you might think that the state could install some tamper-evident security seals, and that would prevent the crooks from getting in there. But you would be wrong! Supposedly "tamper-evident" seals don't provide much protection. See my paper, "Security Seals on Voting Machines: A Case Study," by Andrew W. Appel. *ACM Transactions on Information and System Security,* vol. 14, no. 2, pages 18:1--18:29, September 2011.

On more "modern" voting computers,

How do you replace the software?

Load it from CD-ROM,

or USB

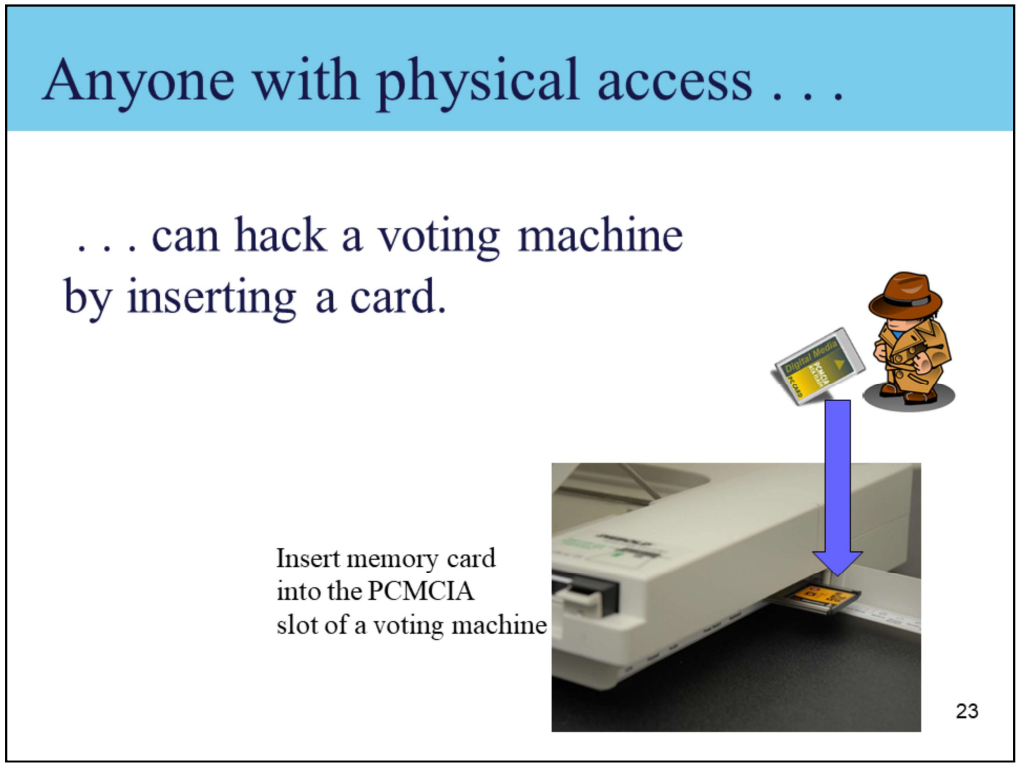


or download from Internet

Or, insert memory card into the PCMCIA slot of a voting machine

22

On most voting computers these days, you don't need a screwdriver to replace the vote-counting program. It's loaded in on a memory card, a removable media like a thumbdrive or the equivalent. In fact, on most voting machines, you use the same memory-card slot where the Ballot Definition Cartridge is inserted. If you put a card into that slot, that *instead* of the ballot definition, has a new vote-counting program, then the computer will replace its old vote-counting program with your new one.



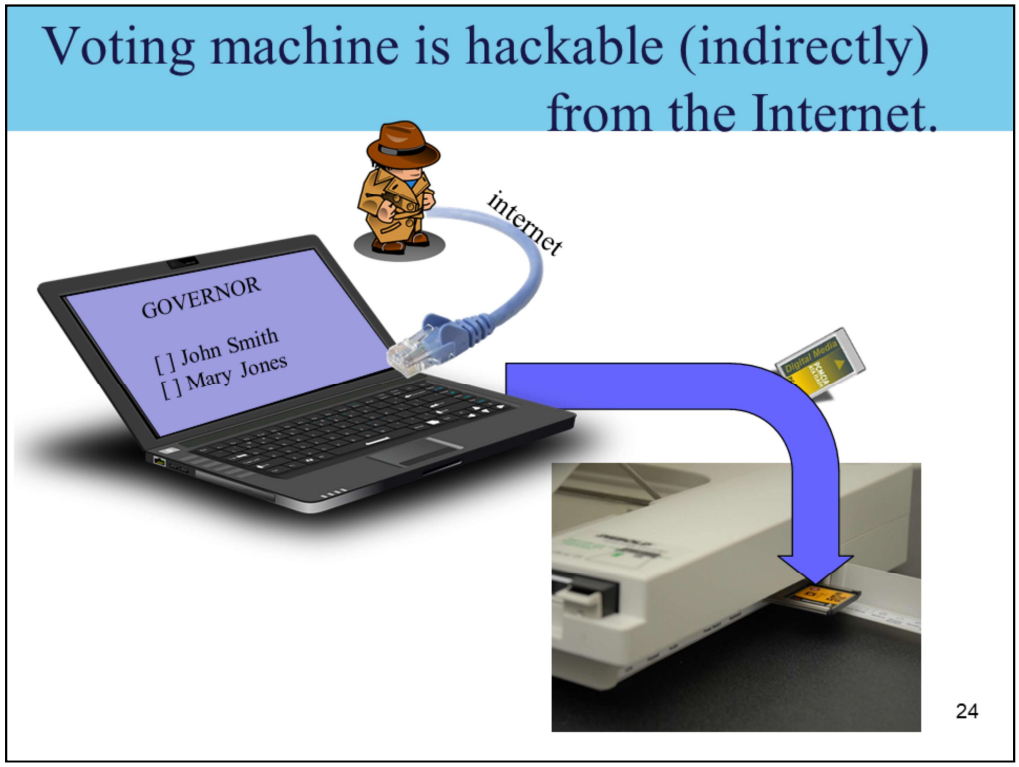
And therefore, if you can get unobserved access to a voting machine for just a minute or so, you can install vote-stealing software into it.

Between elections, voting machines are stored in warehouses. County employees have access to them, to perform maintenance such as replacing batteries. I'm sure 99.9% of those public servants are trustworthy and of the highest integrity. But we organize our elections so you shouldn't have to trust every single election worker. That's why there are witnesses in the polling places, and witnesses to recounts, and so on.

Right before an election, voting machines are delivered to the polling places: school gymnasiums, firehouses, churches, town-hall lobbies. There, in many cases, they are left unattended and unsecured. Anyone could get access to those machines and stick in a cartridge.

And what about *after* an election, before the voting machines are collected from the polling places? Hacking them at that point won't change the election that just happened, but it will make the machine cheat in the *next* elections, for years to come.

To steal a big election, the attacker would have to install cheating software in many voting machines, not just one. But surely that's well within the capabilities of a corrupt political machine—or even a freelance criminal who steals votes in favor of a candidate who's not even aware of the fraud.



An election administrator may say, "our voting machines don't connect to a network, so they can't be hacked from the Internet." That's not true: even if a voting machine has no network connector, it *can* be hacked from the Internet.

And here's how to hack a voting machine from the Internet. The attacker hacks in to the election administrator's network, and gains access to the computer used for programming Ballot Definition Files. He hacks that computer so that, in addition to putting Ballot Definitions into the removable cartridge, the election management system computer also writes a fraudulent vote-counting (vote-stealing) program to the cartridge. The computer will put the vote-stealing program into every Ballot Definition cartridge destined for every voting machine. Then, when that cartridge is loaded into the voting machine, before the election, it will be installing the vote-stealing program.

This attack was first demonstrated in 2006, on a real voting machine:

Security Analysis of the Diebold AccuVote-TS Voting Machine, by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07),* August 2007.

Conclusion: hackability of voting computers

Computers connected to the Internet, *even indirectly,* can be vulnerable to hacking.

Election officials should use good security practices to make their computers *less vulnerable,* but there is no way to make them *invulnerable.*

Therefore we should run our elections in a way that can detect and correct for computer hacking, without having to put all our trust in computers.

25

And therefore,

Don't use paperless touch-screen voting computers!

They are a *fatally flawed* technology.

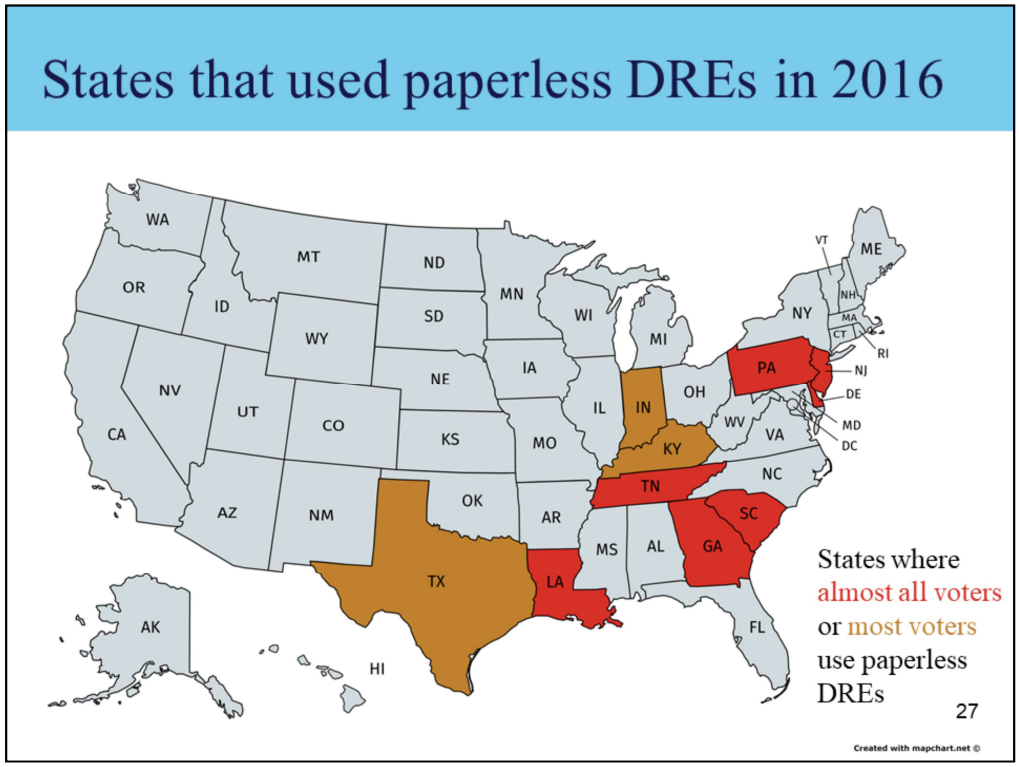
And actually, everybody knows this now:

Only a few states still use them.

One by one, states are switching to optical-scan.

Since 2004, no states have switched *to* paperless voting.

26



About 10 states still use paperless direct-recording electronic (DRE) "touchscreen" voting computers, for most or all of their voters. Two or three states use touchscreen DREs with a "voter verified paper audit trail," which is not quite as bad. About 37 states use optical-scan balloting for almost all their voters.

Precinct-count optical scan voting

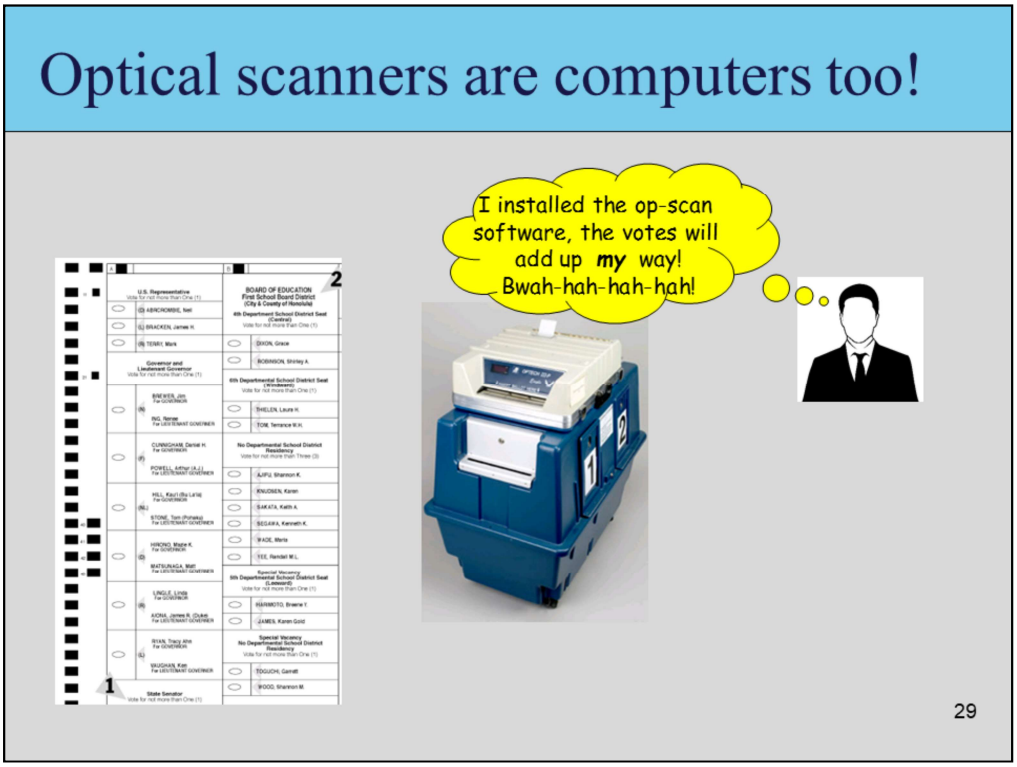
(used in most states)

Voter marks op-scan ballot

Voter feeds ballot to scanner

28

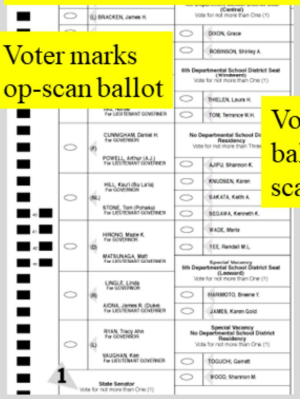
Here's a better idea: Voters mark their choices on a paper ballot, and feed the ballot into an optical-scan computer that counts it accurately.



Well, that is, the op-scan computer counts it accurately *if the computer has not been reprogrammed to cheat!* So, why is that any better than a touchscreen DRE?

Voter-Verified Paper Ballot

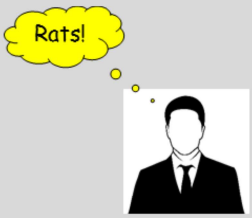
"Voter Verified" means:
The voter sees the actual votes, on the *ballot of record that will be used for recounts*, without any computer in the way.



Voter marks op-scan ballot

Voter feeds ballot to scanner

Paper ballot drops into ballot box



Ballots can be recounted by hand

30

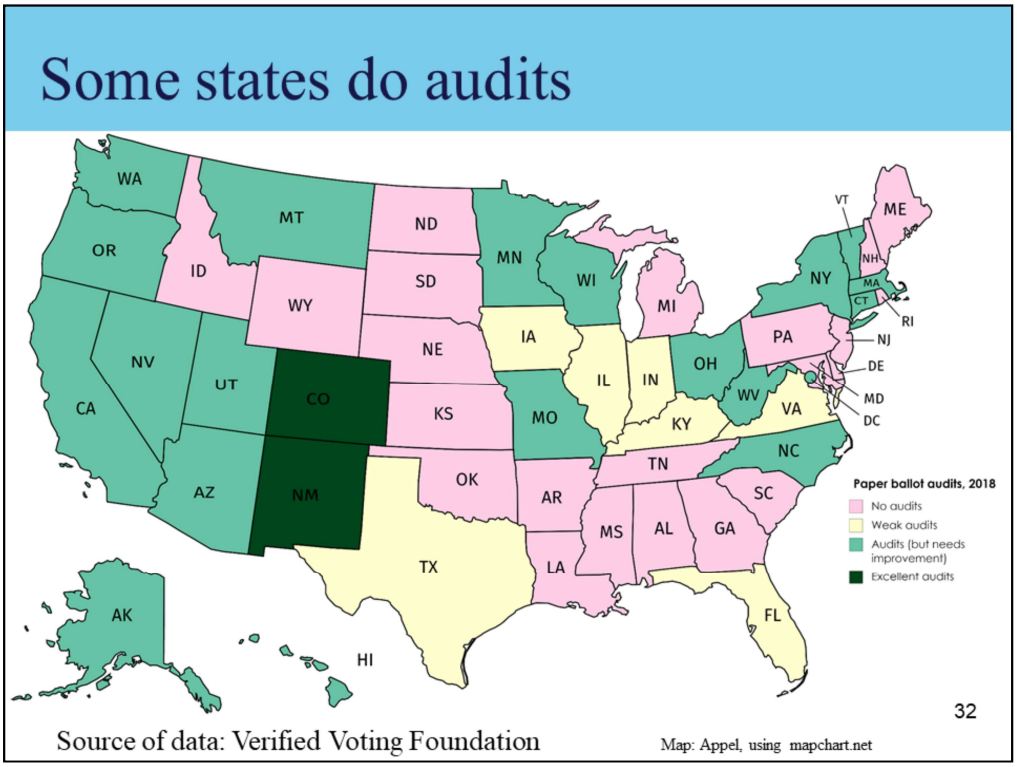
Here's why: You can recount the paper ballot *that the voter actually marked* by hand, in the presence of witnesses from both parties, without any computer "interpreting" the ballot to you.

Random audits

- If you have to recount the ballots by hand, what's the point of having a computer?
- Solution: Recount a random sample of precincts!
  - If there's widespread computer fraud in many precincts, recounting paper ballots in just a few precincts will find evidence of a discrepancy
  - Besides "recount a random sample of the ballot boxes," there are other cost-effective methods for making "risk-limiting audits" a standard part of all elections prior to certification of final results.

31

These audits help protect *not only* against cheating inside the voting computer. They also protect against accidental miscalibration, accidental mistakes in the layout of the Ballot Definition File, and so on.



A few states do random audits, but unfortunately,

1. Not very many states do it (just the ones shown here in light green and dark green)
2. Even in most of the states that do audits, the audits are inadequate. They don't audit enough percentage of the ballot boxes to catch fraud (if it were to occur); or they do the audits *after the results are officially certified,* when it's too late; or they don't audit the actual paper ballots, which means that a cheating computer could still fool them.

Audits are the best way to protect against computerized election theft, but they have to be done well in order to provide protection. Colorado and New Mexico have models that other states should emulate.

Note: some states (IN, PA, NJ) have statutes requiring audits, but most of their voters use unauditable paperless DREs, so in practice they don't do ballot audits.

Conclusion: hackability of voting computers

Computers connected to the Internet, *even indirectly,* can be vulnerable to hacking.

Election officials should use good security practices to make their computers *less vulnerable,* but there is no way to make them *invulnerable.*

Therefore we should run our elections in a way that can detect and correct for computer hacking, without having to put all our trust in computers.

That way is: Voter-Verified Paper Ballots, counted by computer, audited by direct inspection (independent of hackable computers), of a statistically appropriate random sample.

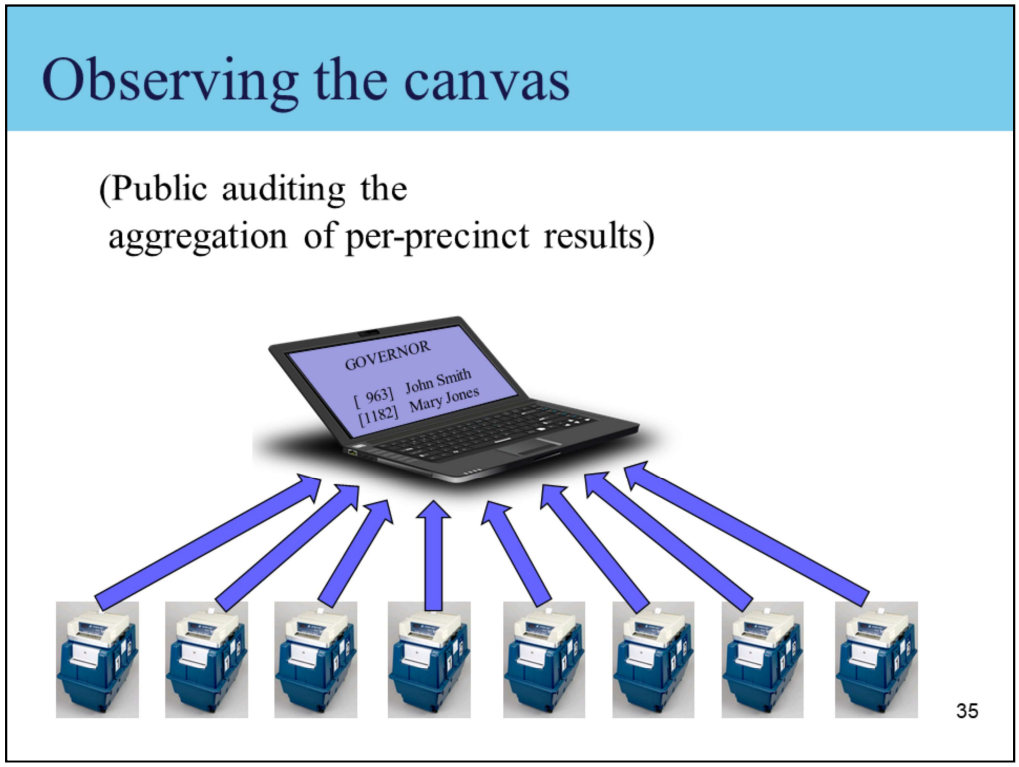
33

Can voters trust op-scan + audits?

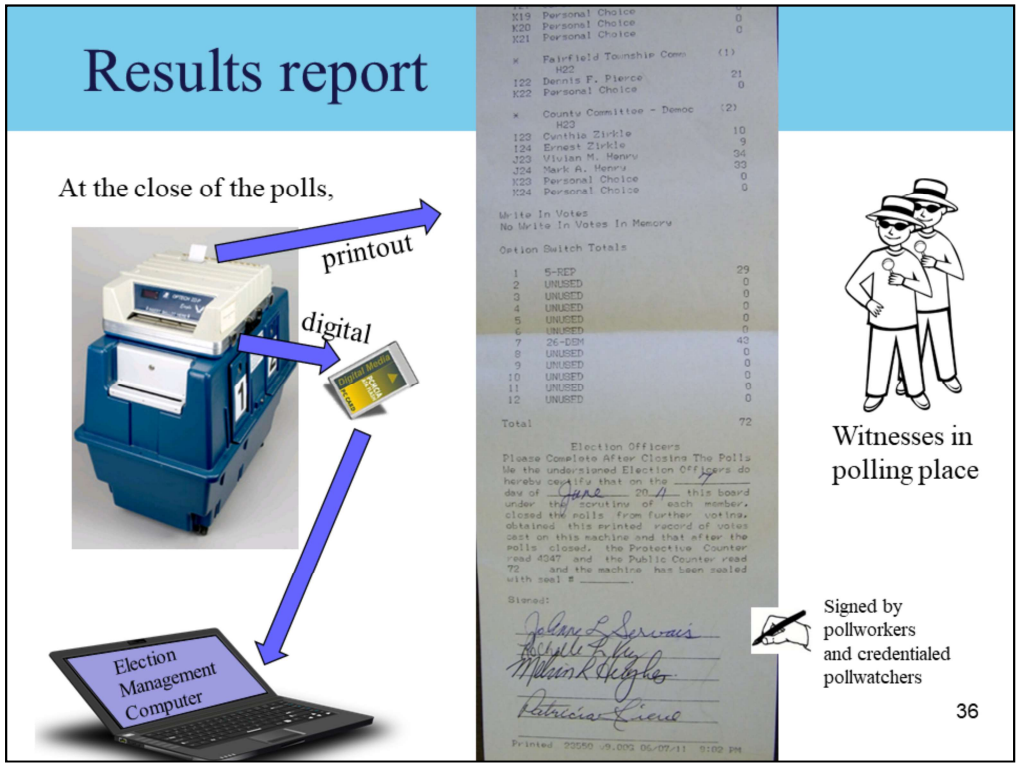
- Voters can see what they wrote on the ballot, and
- deposit the ballot directly into the scanner/ballot-box
- Integrity of the ballot box at the polling place and until the audit/recount is an important chain-of-custody issue, addressed via witnesses and seals.*
- Audits should be performed immediately after polling, before election results are certified.
- Written procedures for audits should be published, so voters, candidates, parties, experts can understand them.
- The audit itself (like a recount) should be performed in public.

*Don't put *too much* faith in tamper-evident seals; they're hackable too!
Security Seals on Voting Machines: A Case Study, by Andrew W. Appel. *ACM Transactions on Information and System Security* vol. 14, no. 2, pages 18:1--18:29, September 2011.

34

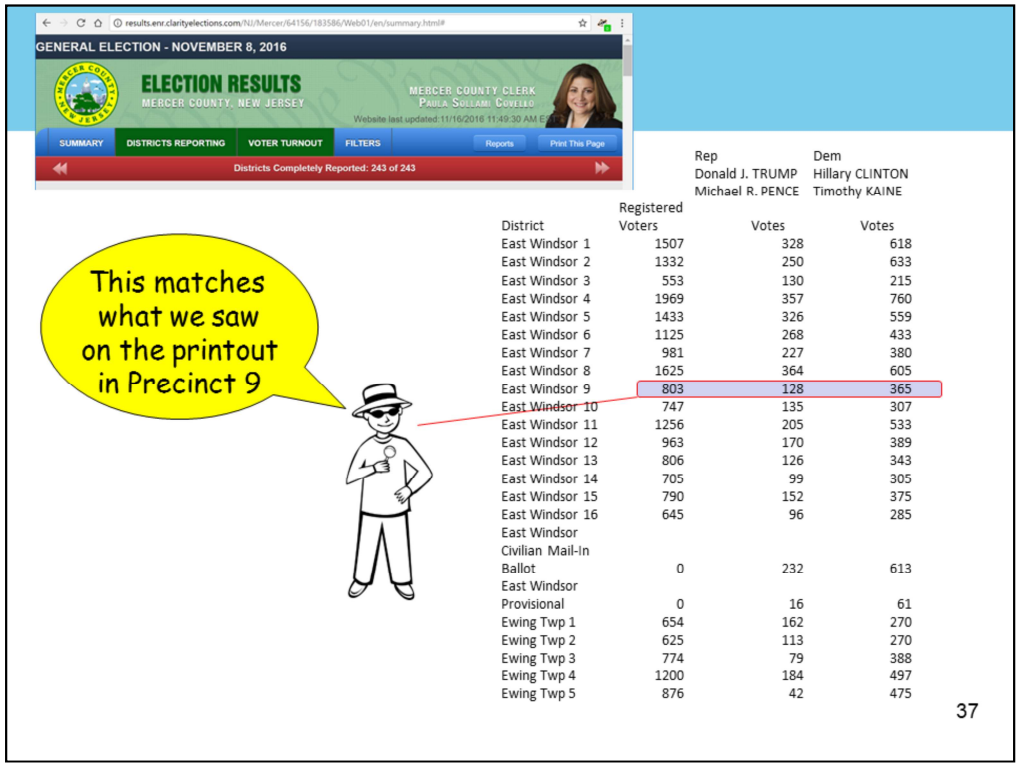


Up to now, I've been talking about cyberfraud that happens *inside the voting machine.* Now let me turn to a different phase of the election. The *canvass* is the procedure of getting the results from every polling place, and adding them up. Can we trust the canvass? What if there's a cheating computer program in the Election Management System computer (the laptop computer shown here) that adds up the votes from all the precincts?

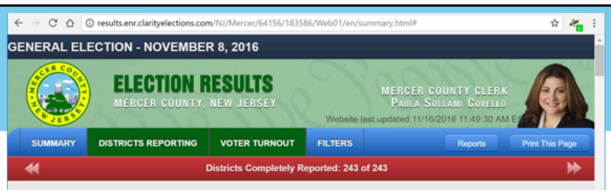


In the polling place, at the close of the polls, the voting computer writes its results—how many votes each candidate got—in two ways: to a removable memory cartridge, and printed on a cash-register tape. Shown here is an actual "Results Report" printout from an election in New Jersey. This printout is made in the presence of witnesses—poll workers hired by the county, poll watchers representing the political parties, and any members of the public who want to watch the process. Anyone is allowed to see the numbers, and copy them down into their own notebook.

Then, if the political party is well organized, their poll watchers will bring those numbers from every precinct back to the candidates' "victory party," and compare with the official returns.



Here are some official returns posted on the internet by the County Clerk in my county, right after the 2016 presidential election. The witnesses in the polling places can compare the numbers with what they saw on the results-report tapes.



District	Registered Voters	Rep Donald J. TRUMP Michael R. PENCE Votes	Dem Hillary CLINTON Timothy KAINE Votes
East Windsor 1	1507	328	618
East Windsor 2	1332	250	633
East Windsor 3	553	130	215
East Windsor 4	1969	357	760
East Windsor 5	1433	326	559
East Windsor 6	1125	268	433
East Windsor 7	981	227	380
East Windsor 8	1625	364	605
East Windsor 9	803	128	365
East Windsor 10	747	135	307
East Windsor 11	1256	205	533
East Windsor 12	963	170	389
East Windsor 13	806	126	343
East Windsor 14	705	99	305
East Windsor 15	790	152	375
East Windsor 16	645	96	285
East Windsor Civilian Mail-In Ballot	0	232	613
East Windsor Provisional	0	16	61
Ewing Twp 1	654	162	270
Ewing Twp 2	625	113	270
Ewing Twp 3	774	79	388
Ewing Twp 4	1200	184	497
Ewing Twp 5	876	42	475

38

How well does this work?

Works well when...

- Assignment of voters to precincts is clear
- Spreadsheet from county clerk *is meant to match* polling-place results tapes

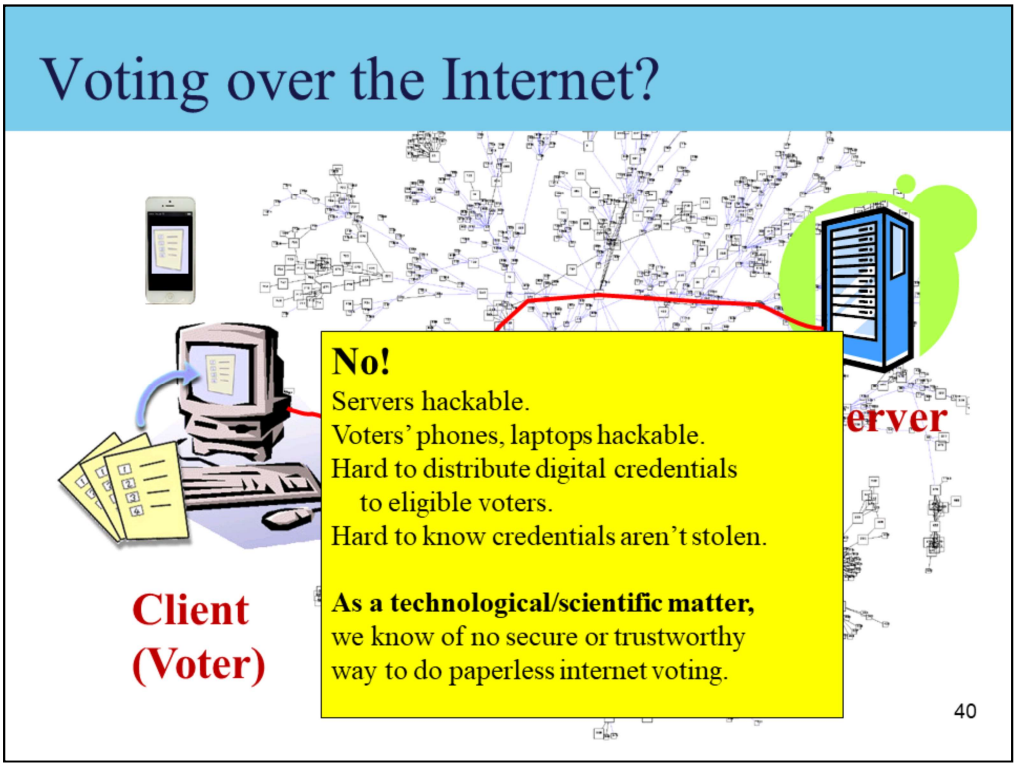
Complicated when...

- Early voting,
- vote centers,
- absentee voting,

makes the correspondence of results tapes to spreadsheet entries difficult to understand

Election administrators should find ways to improve the accountability/transparency of canvassing/aggregation.

39



Some people ask, isn't voting-in-person obsolete? Shouldn't we vote via the Internet, from our smartphones, like we do everything else in life?

The answer is no! Computer scientists don't know of any way to make Internet voting secure and trustworthy. There's some excellent research along these lines, but no results yet that solve the whole problem. For more information, see:

"Internet Voting? Really?" 21-minute TEDx talk by Andrew Appel, https://www.youtube.com/watch?v=abQCqIbBBeM

"If I can shop and bank online, why can't I vote online?" by David Jefferson, 2011, https://electionlawblog.org/wp-content/uploads/jefferson-onlinevoting.pdf

Conclusion

Members of the public should be empowered to observe, verify, and (therefore) trust,

- what's recorded on their own ballot,
- adding the ballots in each precinct,
- adding up the precincts

The way to do this is

- voter-verified paper ballots
- random audits before results are certified
- transparency in reporting

41