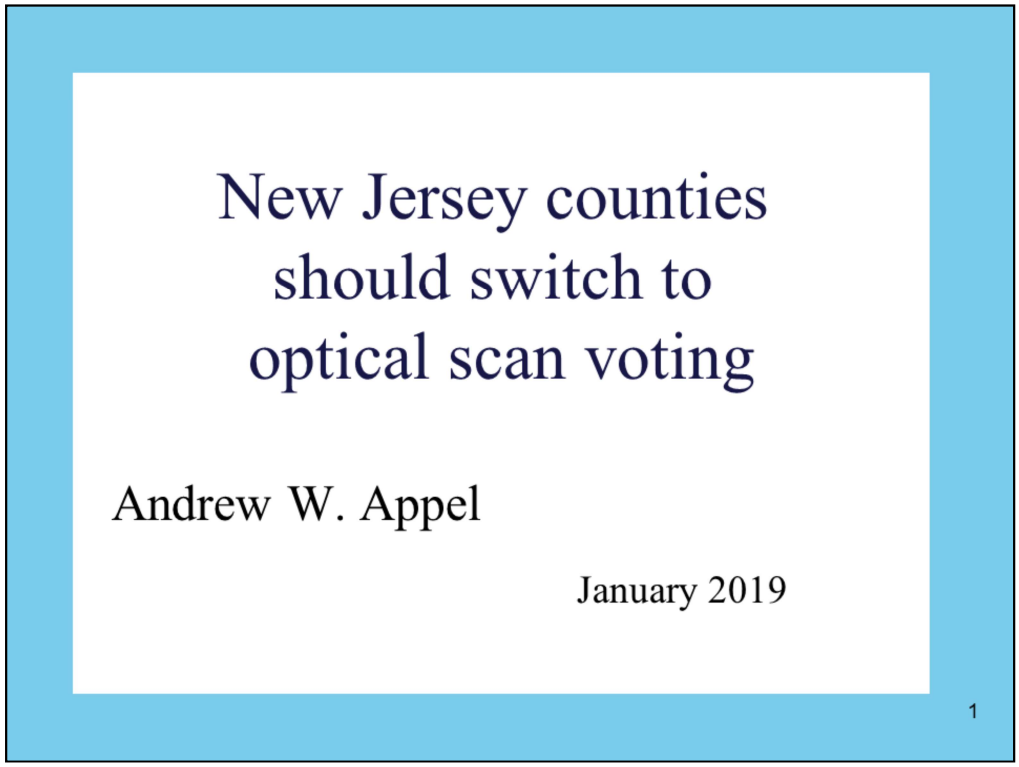


Almost all NJ's counties use paperless DRE (direct-recording electronic, "touchscreen") voting machines. Because these voting computers have no paper trail that could detect and correct computer hacking, New Jersey's counties should switch now to a more trustworthy voting method used by most states: precinct-count optical scan voting.

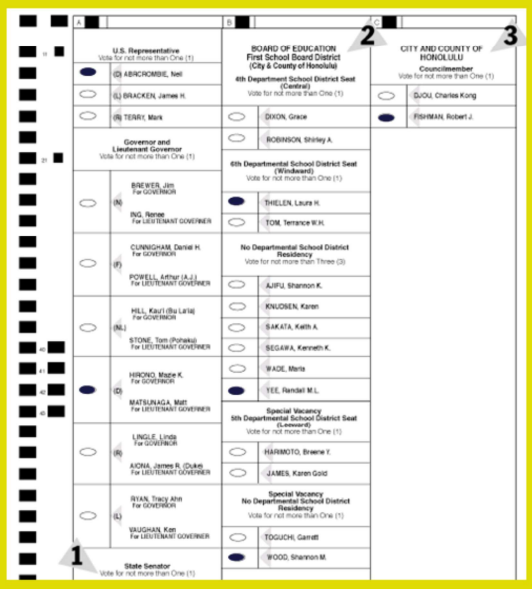
By background, I am a computer scientist with expertise in computer security and formal verification of software. But for the last 16 years I have also studied, and written about, elections and voting technology.

Andrew W. Appel

Professor of Computer Science

Princeton University

Precinct-count optical-scan



2

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.

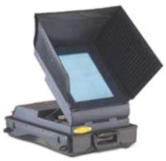
Touch screens:

Direct-Recording Electronic

Shouptronic, 1980

Sequoia, 1987

Votronic, 1991



Sequoia, 2000

Diebold, 2002

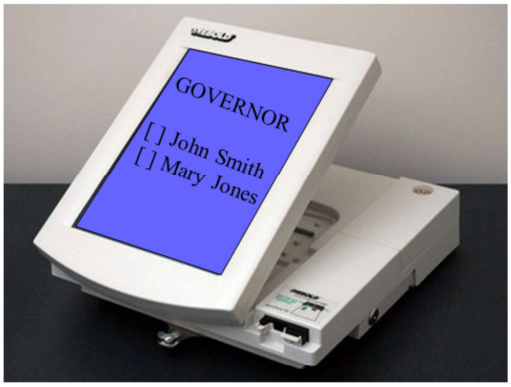
3

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.

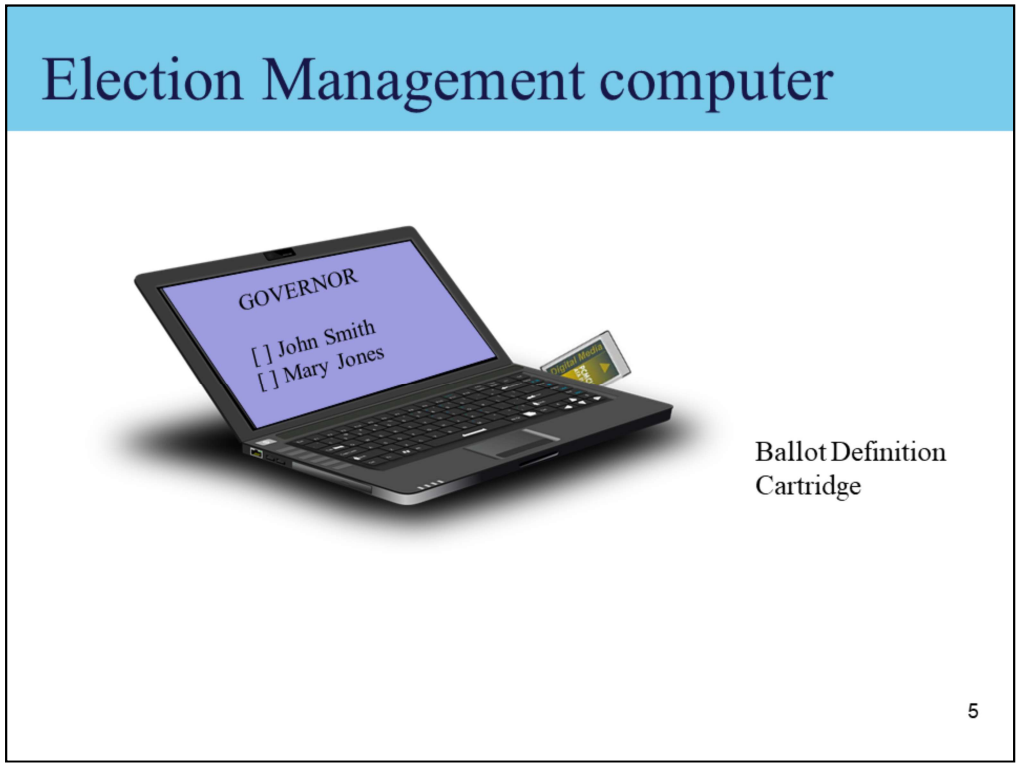
Ballot definition files



4

Now I'm going to talk about the *security* of voting machines.

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.



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

6

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.

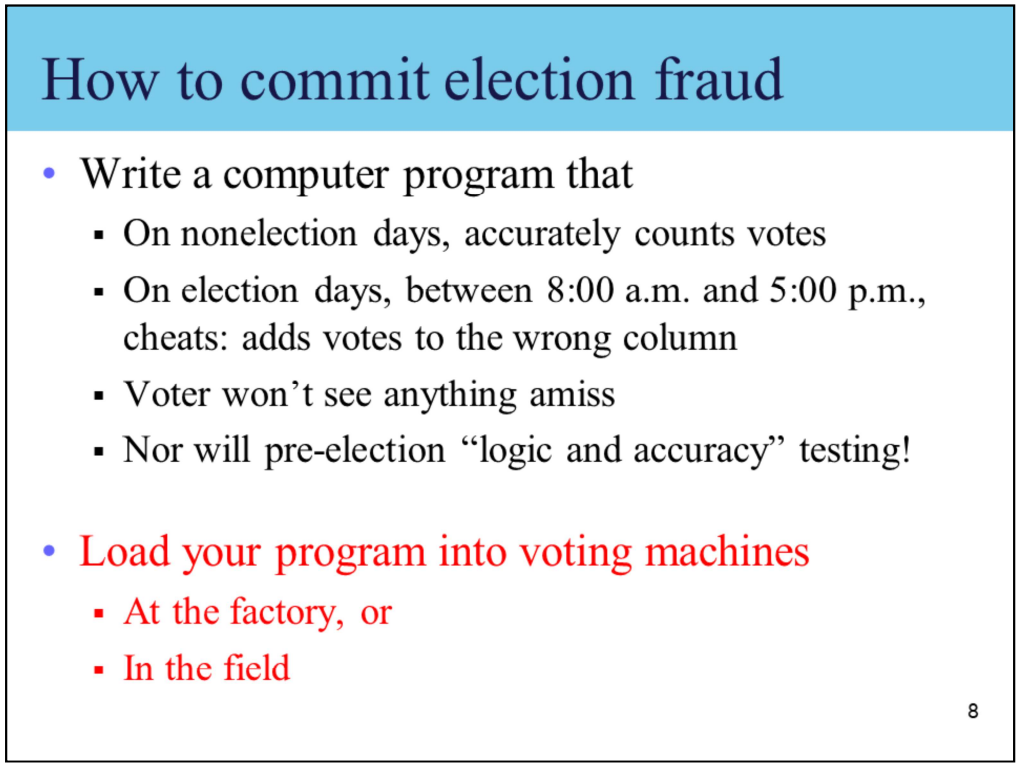
Fundamental flaw of voting computers:

Whoever programs the computer,

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

7

'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.

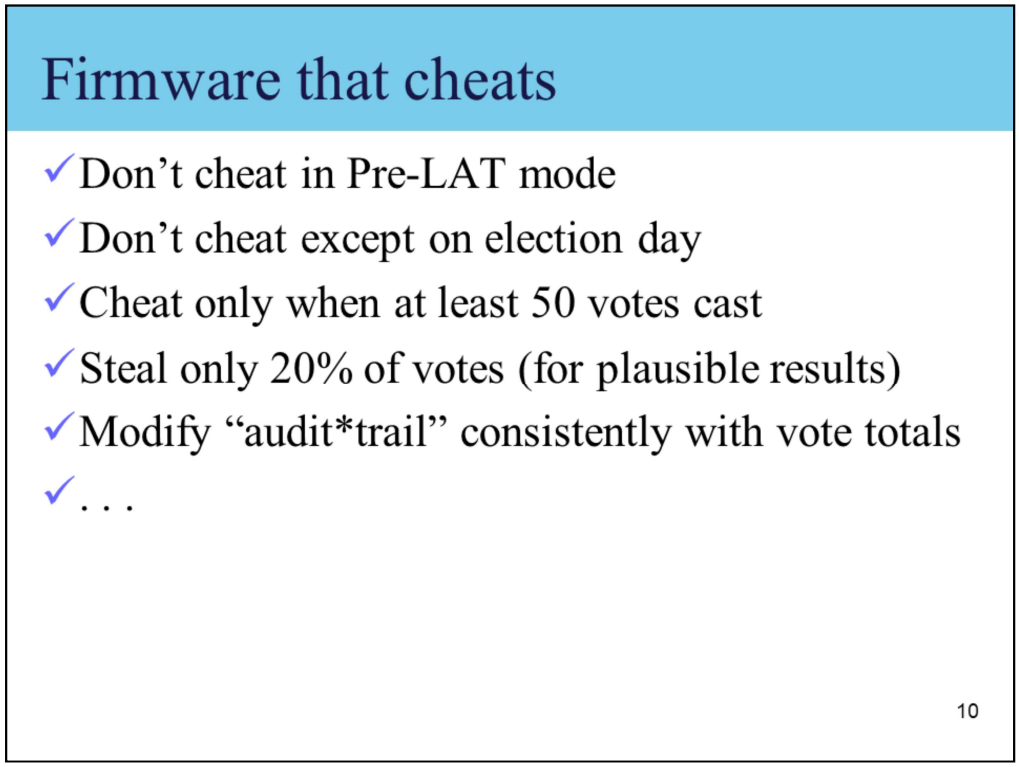
Here's how to install a vote-stealing program into one of NJ's AVC Advantage voting machines

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

9

In 2008 I demonstrated (for a case in the Superior Court of New Jersey) how easy it is to write a vote-stealing program and install it in one of New Jersey's voting machines. It takes about 7 minutes to open up the machine, unscrew the motherboard cover, replace one chip (where I'm pointing with the screwdriver), and replace the screws.

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.



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!

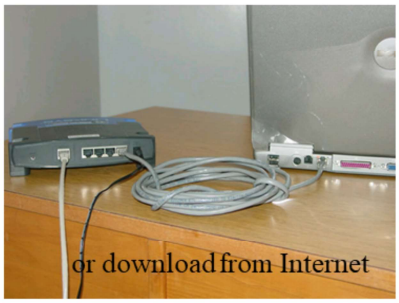
By the way, the Ballot Definition File has each candidate listed with his/her party affiliation (Democrat or Republican). So if you want to steal votes generically in favor of one party or the other, it's easy to program that up. Once you install that program in the voting computer, it will steal votes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

On more "modern" voting computers,

How do you replace the software?

Load it from CD-ROM,

or USB

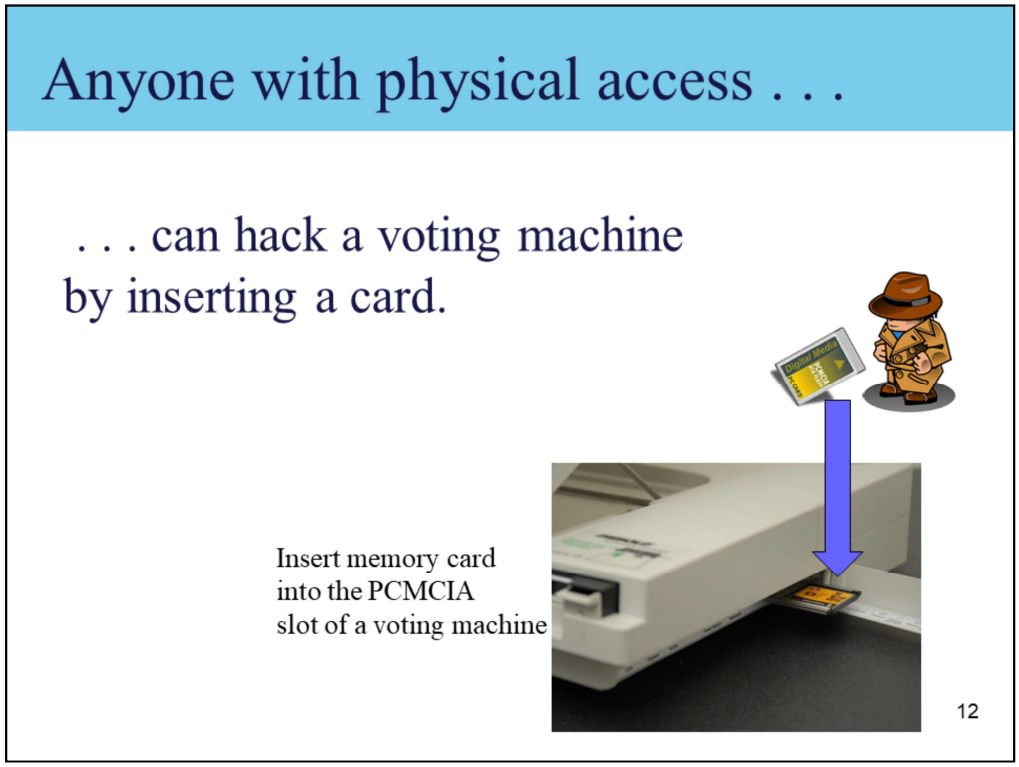


or download from Internet

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

11

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.



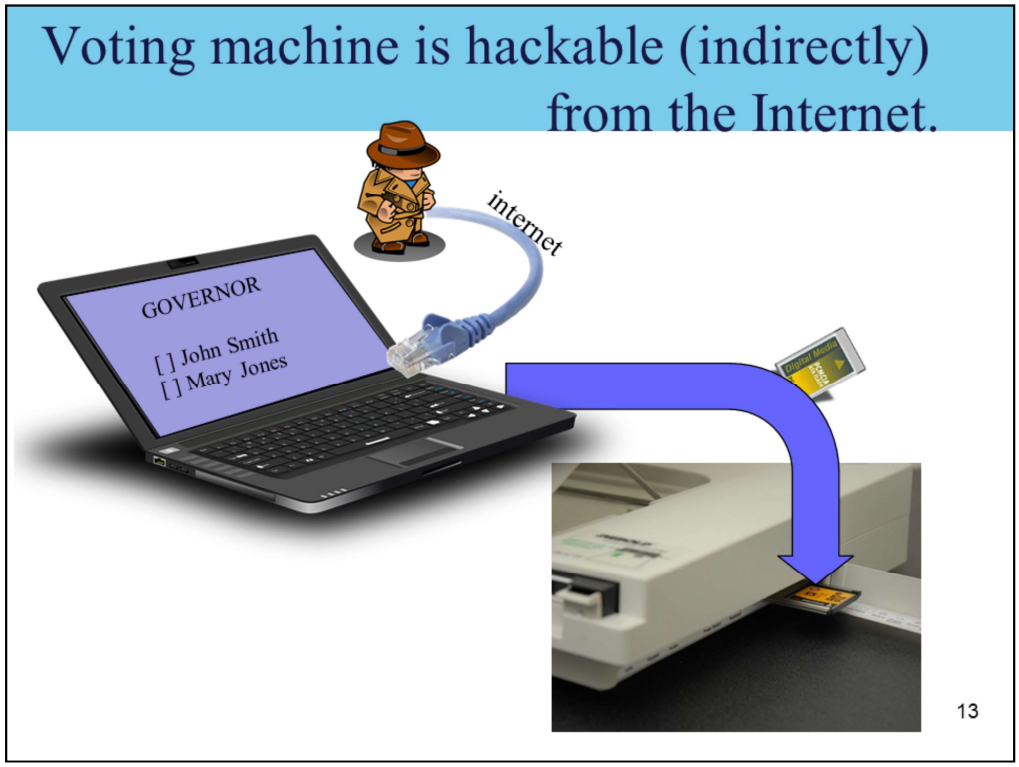
And therefore, if you can get unobserved access to a voting machine for just a minute or so, you can install vote-stealing software into it.

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.

New Jersey's AVC Advantage computers cannot have a new vote-counting program installed from removable media (except as regarding their "audio kit"); but hackers can still switch candidates around on the Ballot Definition file and make them correspond to the wrong locations on the screen.

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.

14

And therefore,

Don't use paperless touch-screen voting computers!

They are a *fatally flawed* technology.

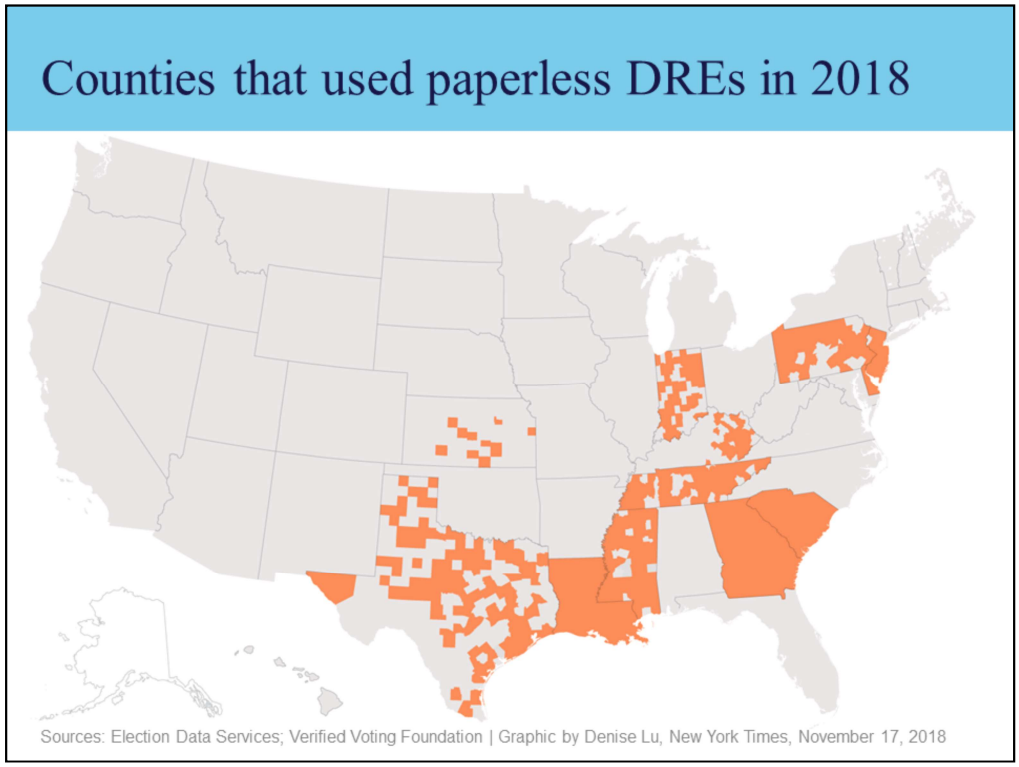
And actually, everybody knows this now:

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.

15



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.

Of these states, several of them are in the process of switching to paper ballots: Pennsylvania, Delaware, Georgia, …

Precinct-count optical scan voting

(used in most states)

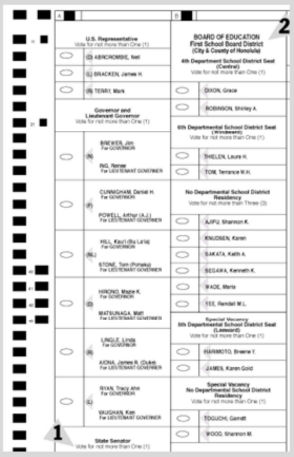
Voter marks op-scan ballot

Voter feeds ballot to scanner

17

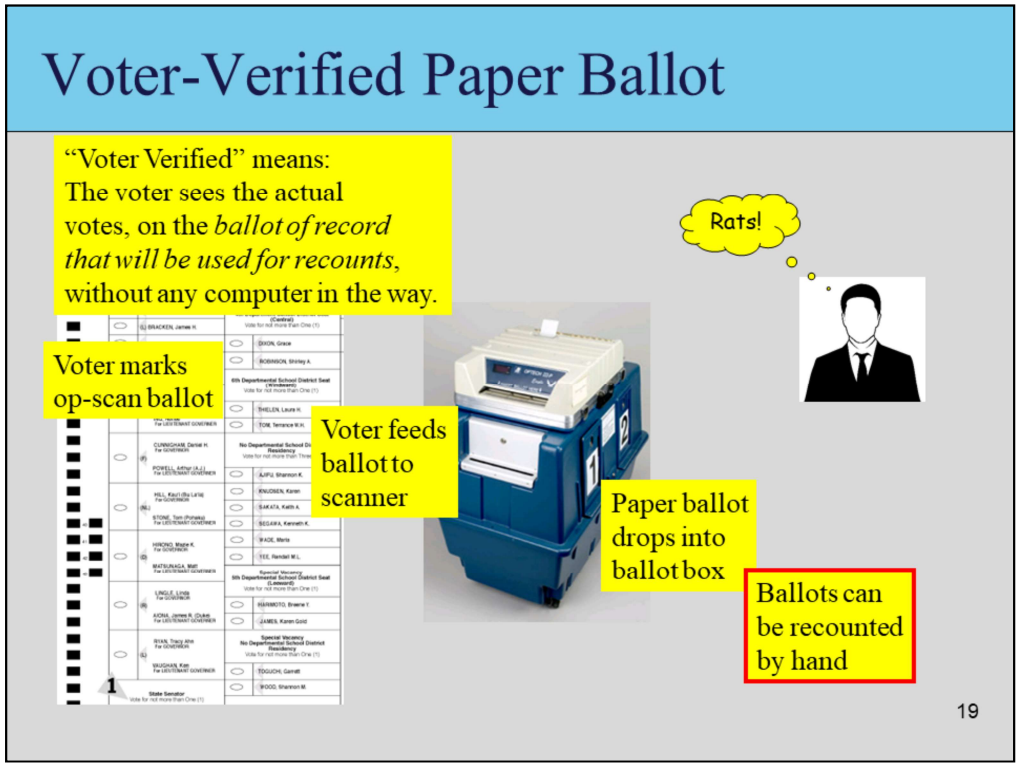
In precinct-count optical scan voting, voters mark their choices on a paper ballot, and feed the ballot into an optical-scan computer that counts it accurately.

Optical scanners are computers too!



18

Well, that is, the op-scan computer counts it accurately *if the computer has not been reprogrammed to cheat!* That is, any voting machine, including an optical scanner, can be hacked. So, why is that any better than a touchscreen DRE?



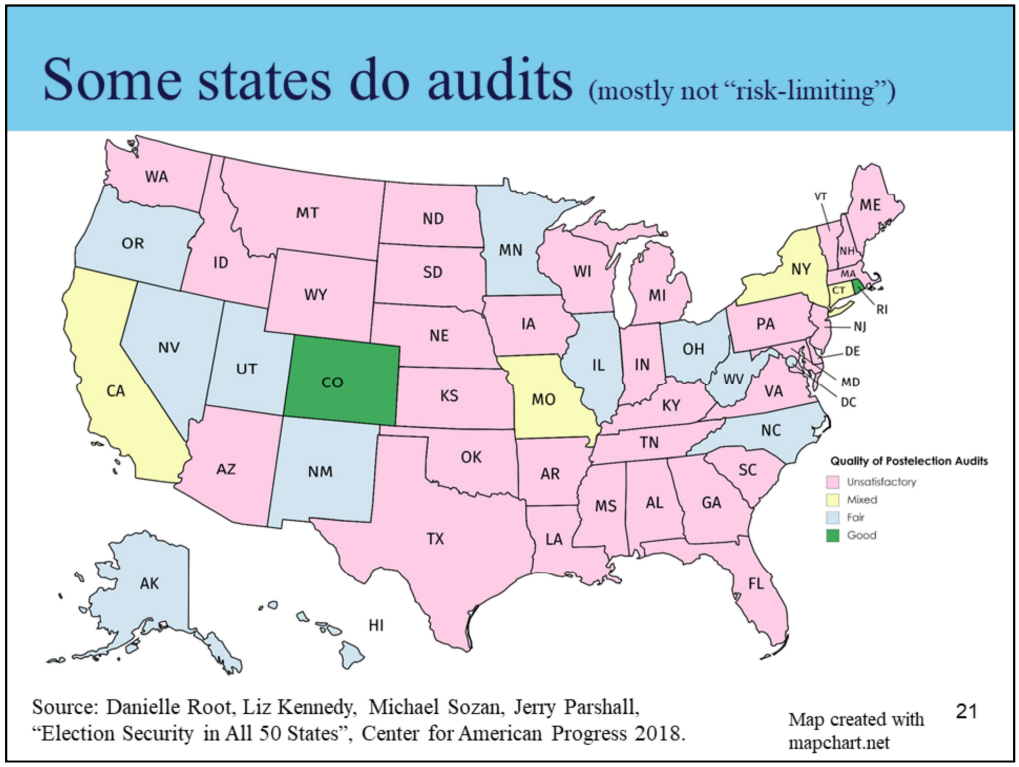
Here's why: You can recount the paper ballot *that the voter actually marked* by hand, in the presence of witnesses from both parties, without any computer "interpreting" the ballot to you.

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.

20

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.



According to a recent study by the National Academy of Sciences,

States should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots. States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. ***Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible***.

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.*

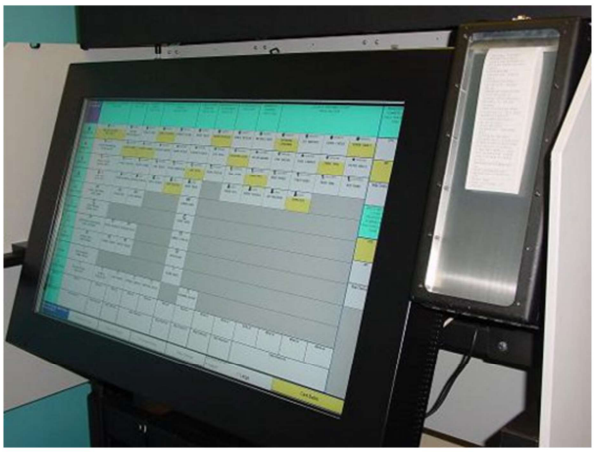
Therefore we should run our elections in a way that can detect and correct for computer hacking, without having to put all our trust in computers.

That way is: **voter-marked paper ballots, counted by computer,** audited by direct inspection (independent of hackable computers), of a statistically appropriate random sample.

22

What about a VVPB printer?

15 years ago, we thought that a "voter verified paper ballot" printer, attached to a direct-recording electronic (touchscreen) voting machine, was a good idea.



(This model is used in Warren County, New Jersey)

It's better than a DRE *without* a VVPB, because the VVPBs are auditable and recountable; but the consensus now is that optical-scan is better.

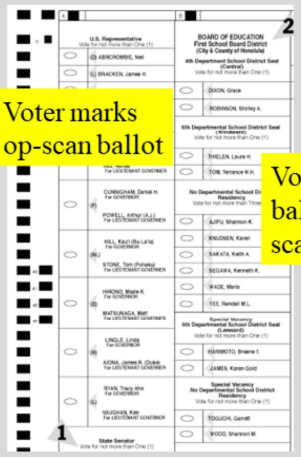
23

The reason is that most voters don't actually pay attention to the paper slip (shown here at upper right), so we can't be at all sure that what's marked on the paper corresponds to what the voter chose.

In contrast, if the voter marks an op-scan ballot with a pen, then we have better assurance that the computer can't cheat in what it writes on the ballot.

New Jersey counties should adopt optical-scan voting

(It works well in at least 37 other states!)



Voter marks op-scan ballot

Voter feeds ballot to scanner

Paper ballot drops into ballot box

Ballots can be recounted by hand

24

This is the standard method now in most of the United States.

Optical-scan can be used in NJ now

ES&S model DS200

Dominion model ICP320

25

Here are just two of the several optical-scan voting machines that would be reasonable to purchase. They are not perfectly secure; no voting machine is! That's why we need audits. However, they are competent machines; New York State switched from lever machines to these machines in 2010 (some counties use one, some use the other) without much fuss.

Ballot marking device (BMD)

Need one of these in each polling place (not in each *precinct!)*,
to accommodate voters not able to mark an optical-scan ballot using a pen. 26

Federal law requires a "voting system equipped for individuals with disabilities at each polling place" (Help America Vote Act, 2002).

When optical-scan voting is used, this "accessible voting system" usually takes the form of a Ballot-Marking Device (BMD), which can produce a paper ballot that can be counted by the optical scanner.

Available from several vendors

EAC certified BMDs, PCOS, and CCOS equipment

	Ballot Marking Device	Precinct OpScan	Central OpScan
ClearBallot	ClearAccess	ClearCast	ClearCount
Dominion	ICX BMD	ICP	ICC
ES&S	ExpressVote 1.0	DS200	DS450,DS480
Hart	Verity TouchWriter	Verity Scan	Verity Central
Unisyn	OVI, FVT	OVO	OCS

Source of information:
Brian J. Hancock, Director, Testing and Certification,
U.S. Election Assistance Commission
October 2017
[updated information from EAC web site, January 2019

27

Organization of polling place

Sign the pollbook, receive a ballot

Mark the ballot with a pen

Insert the ballot into the scanner

28

What I recommend

Sign the pollbook, receive a ballot

Mark the ballot with a pen

Insert the ballot into the scanner

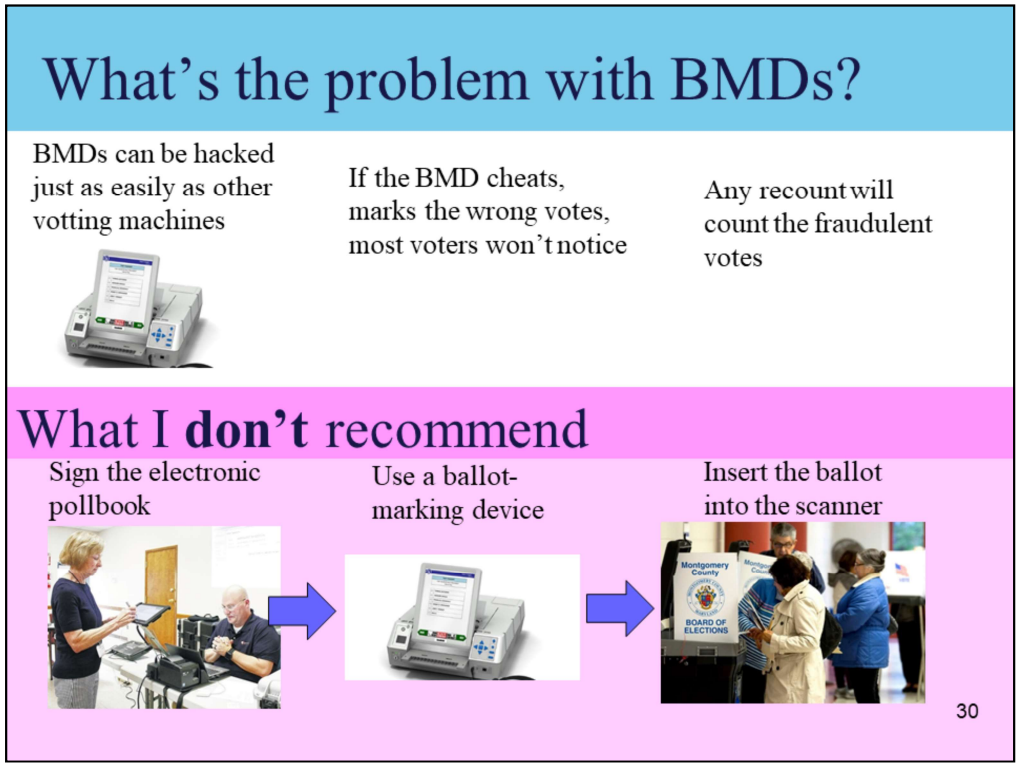
What I **don't** recommend

Sign the electronic pollbook

Use a ballot-marking device

Insert the ballot into the scanner

29



There's a danger to Ballot-Marking Devices (BMDs): if the BMD is hacked (as it can be, it's got a computer in it) then the selections the voter makes on the touchscreen might be deliberately misrecorded on the paper ballot.

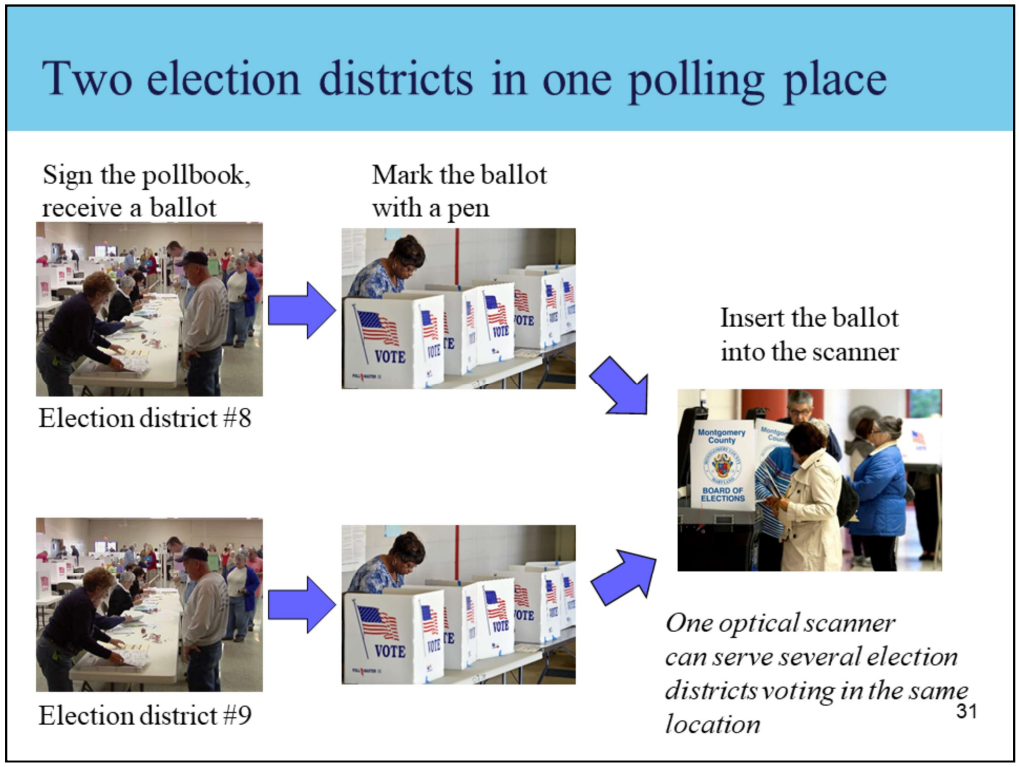
And unfortunately, most voters don't carefully inspect their paper ballot: A 2018 scientific study of real voters in a real polling place found that,

Half the voters don't look at the BMD-printed ballot *at all.*

Half the voters look at the BMD, but only for an *average of 4 seconds.*

Therefore, the BMD-marked ballot is not necessarily a reliable indication of voter intent, is not necessarily *voter verified.*

Therefore, most experts now recommend that voters should mark their ballots by hand, with a pen.



Two or three election districts ("precincts") are often colocated in the same polling place. When using DREs or all-in-one touchscreens, we still need 2 voting machines per precinct. Why is that? First, the voter spends some time at the machine interacting with the ballot, and we want to avoid long lines. Second, if one machine stops working the other machine is available for voters.

When using optical-scan voting, the voter marks the ballot at a low-tech cardboard privacy booth. Each precinct can have several privacy booths. Then the voter brings the marked ballot to the optical scanner, and feeds it in. The voter interacts with the machine for only about 20 seconds. Therefore, optical scanner can easily serve three or four election districts (colocated in the same place).

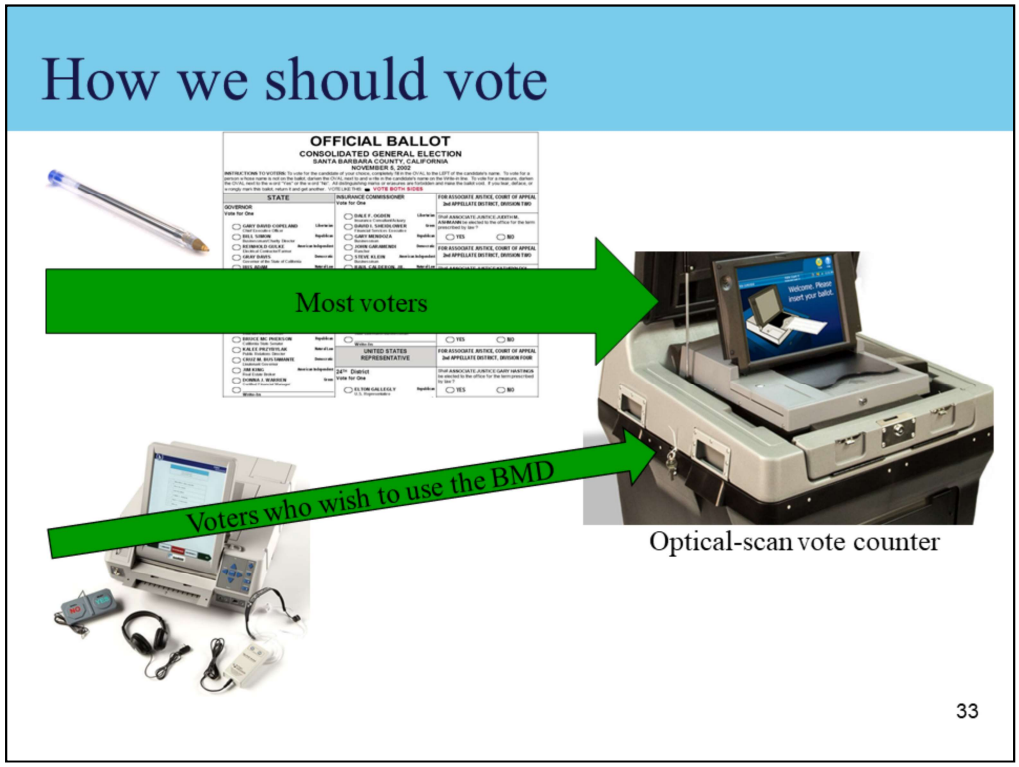
Furthermore, we don't need a backup voting machine if the optical-scanner jams (or otherwise stops working). Voters can deposit their ballots into a secure ballot box for counting later.

All-in-one machines: **not recommended**

Some machines combine a touch-screen BMD and an optical scanner into the same paper path.

That means that, if it's hacked, it can print votes onto the ballot paper *after* the voter sees the paper. This severely reduces the voter verifiability of the ballot. Do not use these machines in elections!

32



The BMD is still necessary to accommodate voters with disabilities.

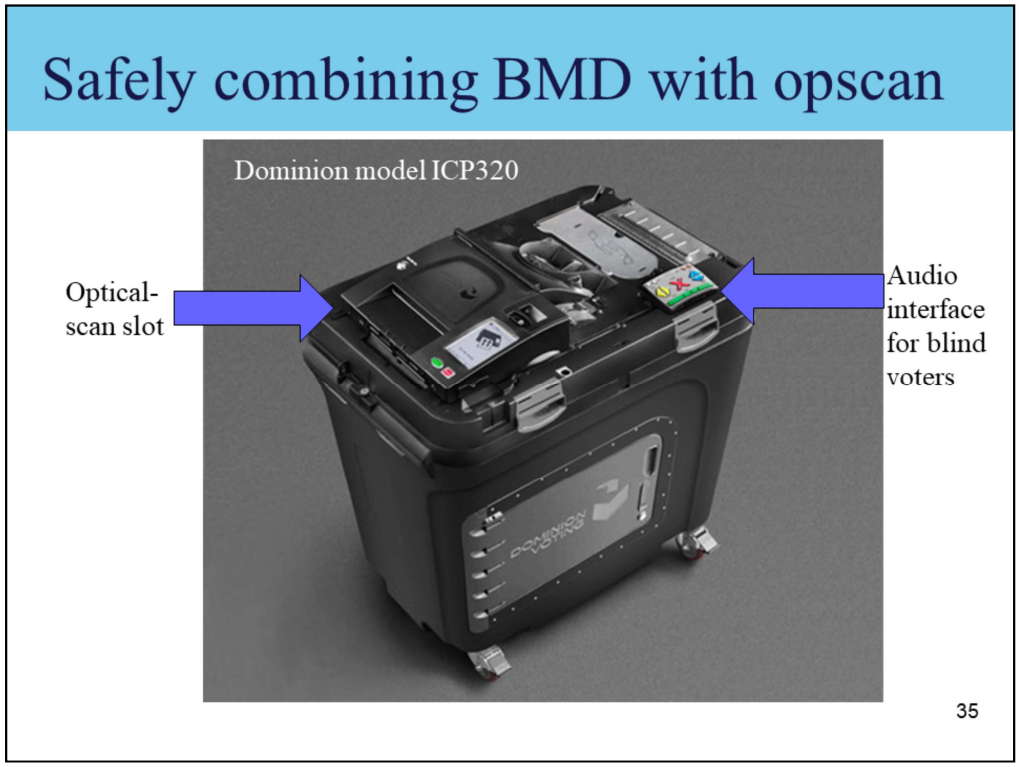
Cost estimates (for New Jersey)

- If using all-in-one touchscreens:
  For each 800 registered voters, 2 voting machines

- If using hand-marked paper ballots + optical scan:
  For each 2400 registered voters, 1 op-scan + 1 BMD

*Other states, with long multipage ballots, may need more equipment per voter; these estimates are specific to New Jersey elections.
** This assume 50% turnout, so 2400 registered voters is 1200 actual voters.

34



In December 2018, I observed this machine in using during a bond referendum election in Princeton, NJ. It has an interesting feature: On one side there is the slot for voters to feed their ballots in; on the other side is a ballot-marking interface that can be used by disabled voters. One of these optical scanners can serve a polling place with up to 1200 voters (2400 registered voters) *without needing a separate BMD for use by disabled voters.*

Earlier I explained that one should not use all-in-one machines that can mark votes after the last time the voter verifies what's on the paper. This machine does *not* have a vote-printer in the same paper-path as the vote-scanner. Therefore, there is no voter-verifiability problem with this machine.

I am told that Dominion is offering this machine in New Jersey at $4000 per unit.

Cost estimates (for one county)

Essex County, NJ

550 election districts, combined into

308 polling places.

Need one optical scanner per polling place: $4000 each

Optical-scanners cost: $308 \times \$4000 = \$1.23$ million

-or-

If you buy an optical scanner for which a separate BMD is needed:

$308 \times (4000+5000) = \$2.77$ million

-or-

Touchscreens cost: $550 \times 2 \times \$5000 = \$5.5$ million

36

Conclusion

Safest way to vote

Hand-marked paper ballot, precinct-count optical scan

(touchscreens are not recommended because, if hacked, they can mark fraudulent votes, and voters won't notice)

Cheapest way to vote

Hand-marked paper ballot, precinct-count optical scan

(touchscreens cost much more)

37