GlobalResearch
Center for Research on Globalization

“Stolen Elections”: How “Easy-to-Hack Voting Machines” Endanger Democracy

Seven Minutes Per Machine to Steal an Election

By Alan Gilbert
Global Research, November 01, 2016
Who What Why 31 October 2016

Region: USA
In-depth Report: U.S. Elections

This article was first published by WhoWhatWhy

Since the “Help America Vote Act” in 2002, tallying votes in our elections has become dependent on machines that sometimes leave no paper trail. Manufacturers have “proprietary” programs and will not let any public officials or independent experts examine them.

On a cold winter day in 2007, Andrew Appel, a Princeton computer professor and election specialist, changed the outcome on one of these machines in seven minutes. He proved something that should alarm everyone: in effect, it took seven minutes per machine to steal an election.

Andrew Appel and a Sequoia AVC Advantage voting machine. Photo credit: Andrew Appel / Princeton

In testimony to a House of Representatives Technology Committee on September 28, 2016, which is now suddenly paying attention because of the fear of “Russian” hacking, Appel noted:

> Installing new software in a voting machine is not really much different from installing new software in any other kind of computer. Installing new software is how you hack a voting machine to cheat. In 2009, in the courtroom of the Superior Court of New Jersey, I demonstrated how to hack a voting machine. I wrote a vote-stealing computer program that shifts votes from one candidate to another.Installing that vote-stealing program in a voting machine takes seven minutes, per machine, with a screwdriver.

Machines were initially adopted for vote counting over a century ago,because they promised speed and convenience. They can tally results more quickly than a more reliable and re-checkable hand count.

From the beginning, there were ways to corrupt non-computerized machines, Appel said. One such ploy was the "pencil shaving trick." Putting shavings on the lever of an opposition party would choke off counting ballots until the shavings came loose and fell free.

While this left a tell-tale discrepancy between the counted results and the number of voters who signed in at that polling place to vote, the scam worked if no one checked.

Latest Computers *Easier* to Hack

You might think the advent of computerized voting machines, starting around 2002, would have made it harder to corrupt vote counting. In fact, even the latest generation of such machines are much easier to hack without leaving a trace.

These machines are big money-makers for private corporations, which lobbied legislators about their supposed advantages. But they also pose a serious threat to the integrity of our elections.

DRE Direct-Recording Electronic or "touchscreen" voting machines that leave no paper trail will be mainly used by voters in 14 states, according to the Brennan Center,. Those states include Georgia, and Pennsylvania — which are in play this year. Even large regions of Ohio, Virginia, North Carolina and many other states still use them. Among the brand names are Shouptronic, AVC Advantage, AccuVote OS, Optech-III Eagle.

Most of these machines are over 10 years old, and the local authorities have no manuals for maintenance and repair. Claiming a lack of funds, state legislatures have refused to replace them.

In 14 states, either computer error or Appel-like reprogramming could distort results. Without a paper trail, the only way to check the tally is through "initial" exit polling conducted throughout the full span of voting hours and ending when the polls close.

Voting machines: Danaher Shouptronic 1242, Sequoia (Dominion) AVC Advantage, Premier/Diebold (Dominion)
AccuVote OS and Optech IIIP-Eagle. Photo credit: Verified Voting

Touchscreen machines were widely used in Ohio in the 2004 Kerry-Bush election, the only one of 154 American contests that year in which initial exit polling, which is ordinarily reliable, was markedly out of sync with the officially announced total. Those who know about computers have long been skeptical of this result.

As Appel has demonstrated, tt takes no super-hacking skills to alter voting counts: "I did this in a secure facility and I'm confident my program has not leaked out to affect real elections, but really the software I built was not rocket science — any computer programmer could write the same code. Once it's installed, it could steal elections without detection for years to come."

But if computer experts can hack every variety of touchscreen machine, what about foreign governments or domestic organizations?

"Other computer scientists have demonstrated similar hacks on many models of machine," Appel added. "This is not just one glitch in one manufacturer's machine, it's the very nature of computers."

In late July and early August, columns by Hiawatha Bray in the *Boston Globe,* and Zeynep Tufekci of *The New York Times* questioned for the first time whether voting in American elections is secure from such hacking — with suspicion directed, though without evidence, primarily at Russia. Suddenly, the disorganization and lack of transparency of American vote counting had become a National Security Issue.

In late September, the US House of Representatives Subcommittee on Information Technology held hearings on "Cybersecurity: Ensuring the Integrity of the Ballot Box."

Weighing in on the issue, President Barack Obama pointed out that most American elections are local or state, done under diverse procedures and laws, and involving a large number of voters. Even if particular computers, or a system of computers connected to the Internet, could be hacked from the outside, it would be hard for a foreign or domestic outlaw to falsify

the results of a national election.

On the surface, this is a heartening thought. But consider a close election like 2004. A targeted hack — say, altering one candidate's vote by an algorithm that kicks in as precincts increase in size — might alter the outcome in certain key counties in a swing state

In addition, voter registration lists are centralized and kept on the Internet. During the Arizona and New York primaries, many Democrats, often younger ones, reported that their registration was changed without their knowledge. They were listed as a Republican or Independent or with no year of registration indicated; as a result, they couldn't vote in their party's primary.

This turned out to have been done by election officials "by accident," and perhaps also by hackers via Internet access.

Bones to Pick with Bipartisan Watchdogs

Now elections are watched over by bipartisan committees in which Appel has some confidence. At least, he points out, such supervision does not depend on a single powerful party or leader:

> When we elect our government officials, sometimes we are voting for or against the very person or political party who is in office right now, running that very election! How can we trust that this person is running the election fairly? The answer is, we organize our elections so we don't have to trust any single person or party.
>
> That's why, when you go to the polls in most places, there are typically two poll-workers there, often (by law) from different political parties; and there are poll-watchers, representing the parties to make sure everything is done right. That's why recounts are done in the presence of witnesses from both parties. We run our elections transparently so the parties can watch each other, and the result is that even the losing candidate can trust that the election was run fairly.

But there are two problems here. So-called bipartisanship means that third parties, such as the Green Party and the Libertarian Party, are by definition excluded.

In addition, many aspects of the process end up in the hands of a single individual. Chief Clerk of Elections Diane Haslett-Rudiano arbitrarily stripped 123,000 people from the Brooklyn voter rolls in this year's New York Democratic primary. She was later fired by the Board of Elections — after the.election was over.

Systemic Weak Points

But Appel is even more worried about a systemic weak point in the electoral process.

> Voting machines are often delivered to polling places several days before the election — to elementary schools, churches, firehouses. In these locations anyone could gain access to a voting machine for 10 minutes. Between elections the machines are routinely opened up for maintenance by county employees or private contractors. Let's assume they have the utmost integrity, but still, in the US we try to run our elections so that we can trust the election

results without relying on any one individual.

The Necessity of Recountable Paper Ballots

The only sure way to run a fair election, Appel says, is to use and keep paper ballots. In 2009, Germany adopted a system in which an initial exit poll is announced immediately after voting closes — this determines a range of plausible results within a margin of error — and then paper ballots are counted by hand. They have, since that time, had no major controversies about electoral fairness.

Appel testified that newer, optical screen voting machines can be equally secure if paper ballots are kept and checked. Premier Optical Scan with Automark is used, in parts of California, Colorado, and since 2008, under Secretary of State Jennifer Brunner, in parts of Ohio. Often, these involve entering your vote, and leaving a record, which you see in the machine, on a paper tape, of how your ballot was cast.

But there are two striking problems with even these somewhat better machines. First, in 2014, the Environmental Protection Agency discovered that Volkswagens had an internal computer program which had long passed US emission tests, but polluted forty times more on the road. The cars were able to recognize when they were being tested (and had to keep the emission controls switched on) and when they were on the road and could pollute at will without fear of being caught. As Barbara Simons of Verified Voting aptly put it, we do not want "VW-style elections."

Appel's mantra is: "any computer can be hacked."

Separating paper ballots physically from a computerized tape and keeping them in a different location, many computer experts believe, would provide further insurance against hacking even on optical scan machines.

Second, challenging the results, particularly in a presidential election and even starting from an automatic recount, as Al Gore did in Florida in 2000, is very difficult. It would take a long time to recount the votes, even if the party in power were not trying to sabotage it…

So the most important thing, as in Germany, is to get each election right in the first place. Why, we might ask, have officials sold public elections and the equal right to vote — again, the most important public feature of our democracy — to private, profit-making corporations? Once again, these corporations, claiming their programs are "proprietary" secrets, do not allow any independent check of how they operate.

A few states like New Mexico have adopted, Appel says, a model procedure for close or controversial elections:

*Immediately conduct a random recount of part of the paper ballots.

*If there is an error, do a full recount.

*Do not certify an election until both are done."

Appel and nine other experts, including Lawrence Norden from the Democracy Program of the Brennan Center at the New York University Law School and John McCarthy of the Verified

Voting Foundation, offered 10 suggestions for securing existing machines and registration lists. For instance, they underline that "without voter-verified paper ballots, effective audits are impossible; they recommend checking samples from the voting system with hand counts of matched sets of paper ballots, recruiting technical experts to help with such tests, and publicizing the results, before certification of the election.

They also recommend a new, detailed ballot accounting by each polling center and reconciliation with the number of those who signed in to vote there. Still, to put these procedures into practice would probably require sustained pressure from the voting public.

Moreover, anyone familiar with vote counting in precincts across the country knows that many computer checking and security measures these experts recommend are far too sophisticated for most poll-watchers to implement before the November 8 election. Further, all Secretaries of State, who are often unabashed political partisans, would have to have good intentions — an assumption hard to reconcile with the actions ofKenneth Blackwell in Ohio in 2004 or Katherine Harris in Florida in 2000.

In contrast, consider the record of Dana Debeauvoir, election clerk in Travis County which includes the University of Texas (Austin). She has worked with critics and computer experts, to propose a new type of encryption plus a paper record (it will not be ready, unfortunately, until the 2020 election).

A federal law requiring oversight of elections by politically independent or neutral state officials would vastly improve the security of the American electoral process. But Appel is not optimistic about the prospect of Congressionally mandated reforms. For the upcoming election, some of the recommended measures will be in place in some jurisdictions across the country.

After this election, however, with a strong democratic push from below, it might be possible to outlaw the highly insecure DREs (*touch-screen* machines), provide adequate funding as well as training for election officials nationwide, and ensure an independent paper trail on *optical scan* machines.

In fact, it might even be possible to go to a paper ballot backed up by an initial exit poll. In contrast to this November 8 — when, at best, only the large scale of the election makes likely a trustworthy result — such reforms would ensure that our elections are, both in appearance and in reality, fair.

Articles by: Alan Gilbert