wired.com

America’s Electronic Voting Machines Are Scarily Easy Targets

Author: Brian Barrett. Brian Barrett Security

A voter uses an electronic voting machine in Philadelphia, April 26 2016. Andrew Harrer/Bloomberg/Getty Images

This week, GOP presidential candidate Donald Trump openly speculated that this election would be “rigged.” Last month, Russia decided to take an active role in our election. There’s no basis for questioning the results of a vote that’s still months away. But the interference and aspersions do merit a fresh look at the woeful state of our outdated, insecure electronic voting machines.

We’ve previously discussed the sad state of electronic voting machines in America, but it’s worth a closer look as we approach election day itself, and within the context of increased cyber-hostilities between the US and Russia. Besides, by now states

have had plenty of warning since a damning report by the Brennan Center for Justice about our voting machine vulnerabilities came out last September. Surely matters must have improved since then.

Well, not exactly. In fact, not really at all.

Rise of the Machines

Most people remember the vote-counting debacle of the 2000 election, the dangling chads that resulted in the Supreme Court breaking a Bush-Gore deadlock. What people may not remember is the resulting Help America Vote Act (HAVA), passed in 2002, which among other objectives worked to phase out the use of the punchcard voting systems that had caused millions of ballots to be tossed.

In many cases, those dated machines were replaced with electronic voting systems. The intentions were pure. The consequences were a technological train wreck.

“People weren’t thinking about voting system security or all the additional challenges that come with electronic voting systems,” says the Brennan Center’s Lawrence Norden. “Moving to electronic voting systems solved a lot of problems, but created a lot of new ones.”

The list of those problems is what you’d expect from any computer or, more specifically, any computer that’s a decade or older. Most of these machines are running Windows XP, for which Microsoft hasn’t released a security patch since April 2014. Though there’s no evidence of direct voting machine interference to date, researchers have demonstrated that many of them are susceptible to malware or, equally if not more alarming, a well-timed denial of service attack.

“When people think that people think about doing something major

to impact our election results at the voting machine, they think they'd try to switch results," says Norden, referring to potential software tampering. "But you can do a lot less than that and do a lot of damage… If you have machines not working, or working slowly, that could create lots of problems too, preventing people from voting at all."

The extent of vulnerability isn't just hypothetical; late last summer, Virginia decertified thousands of insecure WinVote machines. As one security researcher described it, "anyone within a half mile could have modified every vote, undetected" without "any technical expertise." The vendor had gone out of business years prior.

The WinVote systems are an extreme case, but not an isolated one. Other voting machine models have potentially vulnerable wireless components; Virginia's just the only one where a test proved how bad the situation was.

The worst part about the current state of voting machines is that they don't even require outside interference to undo an election. "They're all computers. They run on tens of thousands of lines of code," says Norden. "It's impossible to have a perfectly secure, perfectly reliable computer."

That's true, but in fairness, most computers aren't quite this imperfect, either.

A Good Kind of Audit

So electronic voting machines aren't ideal. The good news is, it's entirely possible to mitigate any potential harm they might cause, either by malice or mistake.

First, it's important to realize that electronic voting machines aren't as commonplace as one might assume. Three-quarters of the country will vote on a paper ballot this fall, says Pamela Smith,

president of Verified Voting, a group that promotes best practices at the polls. Only five states—Delaware, Georgia, Louisiana, South Carolina, and New Jersey—use “direct recording electronic” (DRE) machines exclusively. But lots of other states use electronic machines in some capacity. Verified Voting also has a handy map of who votes using what equipment, which lets you drill down both to specific counties and machine brands, so you can see what’s in use at your polling station.

More than half of the states conduct post-election auditing, by checking vote totals against paper records, to ensure that the votes are accurate. Both Smith and Norden agree that this sort of auditing is the single best way to guarantee confidence in election results, as does MIT computer scientist Ronald Rivest, who has written extensively [PDF] on voting machine issues.

The problem is that not every state does post-election audits. And even some that require them by law, namely Pennsylvania and Kentucky, don’t actually use voter-verifiable paper trails, meaning they have no way to complete an audit. And progress toward more and better auditing is slow; Maryland just put an auditable system in place this year, Smith says, and will pilot it during the fall election. Over a dozen states still have no audit procedure at all.

The problem with putting these auditing systems in place is the same one keeping more reliable voting machines from the booths in the first place: a lack of money and political will. There’s new voting equipment out there that’s much more secure than the machines states purchased in bulk a decade or more ago, but only a handful of states and municipalities—Rhode Island, DC, and parts of Wisconsin among them—have upgraded in the past year.

“The money’s not there right now,” says Norden. “We interviewed election officials who told us what they were hearing from their state legislators and others who would be funding this type of equipment, and they say come back to us after there’s some kind of crisis.”

Which, if they wait long enough, is exactly what they're going to get.

Rigging the Vote

For what it's worth, electronic voting machines have been this hackable in previous elections as well, and there's no indication—even in Virginia—that there's ever been any interference.

This year feels different though, in no small measure because of Russia's alleged responsibility for the DNC hack. If Putin would go so far as release those emails, would he pursue a direct assault on our vulnerable voting machines as well?

The short answer? *Nyet*.

"Putin's not very nice, but he's not stupid," says Ryan Maness, a visiting fellow at Northeastern University who specializes in international cyber conflict and Russian foreign policy. "If they were going to mess with the voting machines and the vote-counting software, they wouldn't have done the DNC hack."

Maness argues that the DNC hack and subsequent email release has put a spotlight on Russia. The blowback from such direct interference in a United States election would be too severe. Besides, Maness says, Putin's main objective was likely to embarrass Hillary Clinton, rather than elevate Trump. And he's certainly achieved that much already.

But even if Maness is wrong, the even better news is that the three states that will likely decide the election—Florida, Ohio, and Pennsylvania—have voting machines that are in relatively good shape. Florida has an audit requirement in place, while Ohio not only conducts audits, Smith says, it has an "automatic recount provision," where close races trigger a manual recount without requiring a candidate to request one. "Pennsylvania is of the most

concern” among those three, says Smith, “based on the fact they have so many paperless DREs in use.” Even there, though, election officials will actively deploy paper ballots in the event that those machines fail.

Still, unlikelihood that Russia would tamper with our voting machines hasn’t lifted the sense of unease around the election. When Donald Trump suggests the election might be “rigged,” he’s referring to a host of potential disruptions, from the times and dates of scheduled debates to whatever else he might bend to his narrative. In November, should he lose, he’ll find the voting machines to be an easy target.

That suspicion is the real danger of electronic voting systems, and especially of those that can’t be easily or effectively audited. If you can’t guarantee that there was no tampering—which not every state can—it might not matter if any actually took place. In the wrong hands, the doubt itself is damaging enough.