The New York Times Magazine

The New York Times Magazine https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html

The Myth of the Hacker-Proof Voting Machine

By Kim Zetter
Feb. 21, 2018

In 2011, the election board in Pennsylvania's Venango County — a largely rural county in the northwest part of the state — asked David A. Eckhardt, a computer science professor at Carnegie Mellon University, to examine its voting systems. In municipal and state primaries that year, a few voters had reported problems with machines "flipping" votes; that is, when these voters touched the screen to choose a candidate, the screen showed a different candidate selected. Errors like this are especially troubling in counties like Venango, which uses touch-screen voting machines that have no backup paper trail; once a voter casts a digital ballot, if the machine misrecords the vote because of error or maliciousness, there's little chance the mistake will be detected.

Eckhardt and his colleagues concluded that the problem with the machines, made by Election Systems & Software (ES&S), was likely a simple calibration error. But the experts were alarmed by something else they discovered. Examining the election-management computer at the county's office — the machine used to tally official election results and, in many counties, to program voting machines — they found that remote-access software had been installed on it.

Remote-access software is a type of program that system administrators use to access and control computers remotely over the internet or over an organization's internal network. Election systems are supposed to be air-gapped — disconnected from the internet and from other machines that might be connected to the internet. The presence of the software suggested this wasn't the case with the Venango machine, which made the system vulnerable to hackers. Anyone who gained remote access to the system could use the software to take control of the machine. Logs showed the software was installed two years earlier and used multiple times, most notably for 80 minutes on November 1, 2010, the night before a federal election.

The software, it turns out, was being used not by a hacker but by an authorized county contractor working from home. Still, the arrangement meant anyone who might gain control of the contractor's home computer could use it to access and gain control of the county's election system.

It was just another example of something that Eckhardt and other experts had suspected for many years: that many critical election systems in the United States are poorly secured and protected against malicious attacks.

In the 15 years since electronic voting machines were first adopted by many states, numerous reports by computer scientists have shown nearly every make and model to be vulnerable to hacking. The systems were not initially designed with robust security in mind, and even where security features were included, experts have found them to be poorly implemented with glaring holes.

But for as long as experts have warned about security problems, voting machine makers and election officials have denied that the machines can be remotely hacked. The reason, they say, is that the systems are not connected to the internet — an assurance the public has largely accepted. This defense was never more loudly expressed than in 2016, when the government disclosed that Russian hackers were probing American voter-registration systems and had breached at least one of them. Concerned that hacking fears could make the public less likely to vote, the United States Election Assistance Commission and state election officials rushed to assert that there was no need to worry about the votes because voting machines themselves were isolated from the internet.

The reality, as the incident in Venango County makes clear, is far more complicated.

Venango removed the remote-access software and isolated its system after Eckhardt and colleagues pointed out the security risk. But it's likely that the software is still installed on other election systems around the country. ES&S has in the past sometimes sold its election-management system with remote-access software preinstalled, according to one official; and where it wasn't preloaded, the company advised officials to install it so ES&S technicians could remotely access the systems via modem, as Venango County's contractor did, to troubleshoot and provide maintenance. An ES&S contract with Michigan from 2006 describes how the company's tech support workers used remote-access software called pcAnywhere to access customer election systems. And a report from Allegheny County, Pennsylvania, that same year describes pcAnywhere on that county's election-management system on June 2 when ES&S representatives spent hours trying to reconcile vote discrepancies in a local district race that took place during a May 16th primary. An Allegheny County election official told me that remote-access software came pre-installed on their ES&S election-management system.

(In a statement, ES&S said, "None of the employees who reviewed this response, including long-tenured employees, has any knowledge that our voting systems have ever been sold with remote-access software.")

Installing remote-access software and modems on systems that program voting machines and tally final results is a serious security issue and one that election officials are beginning to understand, as evidenced by Venango's response to Eckhardt's warning. But there's an even more fundamental way that many voting machines themselves are being connected to the internet and put at risk of hacking, and there's no sign that election officials at the state or federal level are aware the risk exists.

On election nights, many polling places around the country transmit voting results to their county election offices via modems embedded in or

connected to their voting machines. Election officials and vendors insist that the modem transmissions are safe because the connections go over phone lines and not the internet. But as security experts point out, many of the modems are cellular, which use radio signals to send calls and data to cell towers and routers belonging to mobile carriers — Verizon, Sprint, AT&T. These routers are technically part of the internet. Even when analog (landline) modems are used instead of cellular ones, the calls still likely pass through routers, because phone companies have replaced much of their analog switching equipment in recent years with digital systems.

Because of this, attackers could theoretically intercept unofficial results as they're transmitted on election night — or, worse, use the modem connections to reach back into election machines at either end and install malware or alter election software and official results.

"Almost any phone call, whether on a cellular network or a so-called landline, goes through a part of the internet," says Andrew Appel, a computer-science professor at Princeton University and longtime voting-machine security expert. "It may be a part that's supposedly behind the walls of some phone provider," Appel added. But, he said, "if the security of the phone provider is not perfect — and nobody's security is perfect — then that phone call can be interfered with like any other transmission on the internet."

How could someone pull this off? To subvert machines via their modem connection, an attacker could set up a device known as an IMSI-catcher (or stingray, as they're also called) near precincts or county election offices to intercept and alter vote tallies as they're transmitted. IMSI-catchers — which law enforcement, militaries and spies use — impersonate legitimate cell towers and trick phones and other devices in their vicinity into connecting to them instead of legitimate towers.

Alternatively, a hacker could subvert telecom routers to intercept and alter election results as they pass through telecom equipment. Like any other digital device, telecom routers have vulnerabilities, and they have become a prime target in recent years for nation-state hackers from Russia and other countries. In 2012, hackers from Britain's GCHQ spy agency targeted routers belonging to the Belgian telecom Belgacom to intercept mobile traffic passing through them.

In either scenario, experts say, attackers could also potentially use an IMSI-catcher or subverted telecom router to hack back into election systems and alter software to affect election outcomes.

The Election Assistance Commission, which oversees testing and certification of voting machines and advises states to isolate election systems from the internet, has said modems aren't a problem. "The caution about not permitting network access does not apply to the use of modems on election night to transmit *unofficial* polling place results to the central office," the commission's election guidelines state. "The technical expertise required to intercept and alter a telephone communication without detection is extremely complex. Therefore, it is unlikely that anyone will be able to intercept and alter these results without detection."

The document doesn't address the risk of someone hacking into voting machines via the modem, but vendors insist that the machines have protections to prevent this. Election officials also assert that routine procedures they perform would detect if someone altered transmitted votes or machine software. Experts, however, say the procedures are inadequate to detect altered software, and that vendor claims about security can't be trusted, because of their long history of implementing security poorly. Federal labs responsible for certifying voting equipment don't test the vulnerability of the modems to hacking, so there's no independent verification of vendor claims.

"What I've seen in the past 10 years is that the vendors have absolutely fumbled every single attempt in security," says Jacob D. Stauffer, vice president of operations for Coherent Cyber, who has conducted voting-machine security assessments for California's secretary of state for a decade. In a report Stauffer and colleagues published last year about their recent assessment of ES&S machines, they found the voting machines and election-management systems to be rife with security problems.

With Russia expected to intensify efforts to influence American elections this year and beyond, American election security has never been in sharper relief. But experts say that blindness to the risks posed by modems puts the integrity of American elections in grave danger.

"The incorrect assertion that voting machines or voting systems can't be hacked by remote attackers because they are 'not connected to the internet' is not just wrong, it's damaging," says Susan Greenhalgh, a spokeswoman for the National Election Defense Coalition, an elections integrity group. "This oft-repeated myth instills a false sense of security that is inhibiting officials and lawmakers from urgently requiring that all voting systems use paper ballots and that all elections be robustly audited."

More than 350,000 voting machines are used in the United States today, according to an estimate by Verified Voting, a nonprofit that tracks voting equipment use and policy. The machines fall primarily into two categories — direct-recording electronic machines and optical-scan systems. With DREs, voters touch a screen or button or turn a dial to make their selections, and the ballots and votes are entirely digital; some DREs are outfitted with printers to produce a voter-verifiable paper trail. With optical-scan machines, which many states have purchased in recent years to replace their DREs, voters make their selections on a full-size paper ballot, which gets fed into an optical scanner and can be used after an election to verify the digital results. (Hybrid machines are also available which combine touch-screen voting with a scannable paper ballot.)

With both kinds of voting systems, digital votes are stored on memory cards or flash drives that are collected from machines after an election and are supposed to be used for official results. But many machines also have embedded or externally connected modems to transmit unofficial results rapidly on election night.

The top voting machine maker in the country, ES&S, distributes modems or modeming capability with many of its DRE and optical-scan machines. (Some states, including California and New York, require voting machine makers to not only remove communication devices from their systems but also eliminate communications capability from their software for security.) About 35,000 of ES&S's newest precinct-based optical scanner, the DS200, are used in 31 states and the District of Columbia and can be outfitted with either analog or cellular modems to transmit results. Maryland, Maine, Rhode Island and the District of Columbia use only DS200 machines statewide (though they also use two other systems specifically for

disabled voters and absentee ballots); Florida and Wisconsin use the DS200s in dozens of counties, and other states use them to lesser degrees. ES&S's earlier model M100 optical scanners, which also can be equipped with modems, have long been used in Michigan — a critical swing state in the 2016 presidential election — though the state is upgrading to DS200 machines this year, as well as machines made by Dominion Voting Systems. Dominion's machines use external serial-port modems that are connected to machines after an election ends.

Not every polling place with embedded modems uses them to transmit results. Richard Rydecki, Wisconsin's state elections supervisor, says counties in his state decide individually whether to transmit election results. Fred Woodhams, spokesman from the Michigan Department of State, said the same is true in his state. But even if a precinct doesn't use its modems, having them embedded in voting machines is still a risk, experts say.

"If it is available for use" by an attacker, says Stauffer, "it can be used."

ES&S insists that its security measures would prevent hackers exploiting or interfering with modem transmissions. According to a one-page document the company provided, the voting machines digitally sign voting results before transmitting them via modem and encrypt them in transit using SFTP — secure file transfer protocol. The election-management systems that receive results then check the signature to authenticate the data transmission. This theoretically means results couldn't be swapped out and replaced with different ones. That is, unless an attacker can obtain ES&S's signing key.

These keys, explains noted cryptographer and computer-security expert Matt Blaze, "need to be stored in the machine, and if they're stored in the machine and under control of the software, any compromise of that software could be used potentially to extract" them. Blaze, who teaches at the University of Pennsylvania, says that ES&S machines he examined for Ohio's secretary of state a decade ago had a number of security problems, including with key security.

As for using the modems to hack into machines and compromise their software, ES&S says its modems are configured to only initiate calls, not receive them, and can make calls only after an election ends, preventing anyone from dialing in or having them dial out at other times. The company also says results are not sent directly to the election-management systems but to a data communications server that operates as a DMZ, or "demilitarized zone," separated from the internet and the election-management system by firewalls. The election-management system accesses the DMZ to collect the results.

ES&S advises election officials to configure the external firewall that protects the DMZ to only accept connections from IP addresses assigned to the voting machines. And election officials in Rhode Island, which uses ES&S's DS200 machines with modems, told me that the modems only transmit for about a minute, which wouldn't be sufficient to hack into voting machines or results servers.

But Stauffer and others say none of this would prevent a skilled hacker from penetrating the machines via their modems. Although overwriting the machine's firmware, or voting software, would be difficult to do in just a minute, Stauffer says installing malware on the underlying operating system would not. An attacker might be able to do this directly through the modem to the voting machine, or infect the election-management system on the other end and install malware that gets passed to voting machines when officials program future elections. In either case, the malware could disable modem controls on the voting machines and make the devices secretly dial out to whatever number an attacker wants whenever he wants, while also altering system logs to erase evidence of these calls. This would let an attacker connect to the machines before or during an election to install malicious voting software that subverts results.

In such a scenario, the demilitarized zone concept, which ES&S says protects the election-management system, could actually become a liability, since it's trusted by the election-management systems that communicate with it, says J. Alex Halderman, professor of computer science and engineering at the University of Michigan. Halderman calls the DMZ a "very risky setup in an election context, given that an attacker who infiltrates the EMS can tamper with election results or spread malware to voting machines."

The firewalls surrounding the DMZ can have their own vulnerabilities, and Halderman points out that if an attacker can send corrupt data through the firewall to the DMZ, then he can exploit vulnerabilities in the election-management system when the two communicate. This isn't speculation, Halderman insists: A study done in 2007 for Ohio found multiple vulnerabilities in ES&S's Unity election management system that would let an attacker send it malformed election data in order to run malicious code on the system. "The fact that these election management systems are networked at all should be alarming to anyone who understands election cybersecurity," Halderman says.

A secure voting machine should prevent untrusted or unsigned software from being installed on it. But last year when Stauffer and colleagues examined an optical-scan machine that ES&S submitted to California for testing and certification, they discovered the system wasn't authenticating code during installation or wasn't doing it properly. They were able to modify legitimate ES&S election software and reinstall it on the machine unsigned. Although they conducted their test with physical access to the machines, because California machines don't have embedded modems, Stauffer says an adversary with remote access through the modem would theoretically be able to do the same. Their rogue modification was designed to erase all election data from the machine at the close of an election. A "capable-enough adversary," says Stauffer, might potentially go much further, with an update that would "make a candidate more favorable than the other."

Douglas W. Jones, a computer-science professor at the University of Iowa, has examined multiple voting systems for state and local election officials over the years. "Nothing I know about the machines would defend against" an attack where a hacker altered voting software.. "So this is a vulnerability that should be taken quite seriously."

Even if ES&S were to prevent someone from loading unsigned voting software, an attacker could still install malware on a voting or election-management machine via the modem connection, according to experts, if the underlying operating system software had unpatched security vulnerabilities. In fact, many voting machines across the country run on years-old unpatched Windows and Linux operating systems, partly because counties don't have the staff to maintain the systems and have long believed that the systems are secure, and partly because (due to long delays in getting new or altered versions of voting machines certified) voting machine vendors often sell systems without the latest patches installed.

The operating systems on the election-management systems ES&S submitted to California for testing and certification last year were missing dozens of critical security patches, including one for the vulnerability the WannaCry ransomware used to spread among Windows machines. Two optical-scan machines ES&S submitted for certification had nine unpatched security vulnerabilities between them — all classified by the security industry as critical.

Just last month, Cisco, which makes the model of firewall used with ES&S election-management systems, announced a critical vulnerability in its devices that would let a remote hacker take full control of the firewalls and get at the systems they protect. News reports last week indicated hackers are already attempting to exploit vulnerable Cisco firewalls in the wild.

ES&S says it's working with customers to patch their firewalls, but if they use the firewalls "according to recommended procedures," they can mitigate the vulnerability. Those procedures include configuring the firewalls to only accept connections from known and trusted IP addresses "and shutting off the system when not in use."

Jones says the better solution is for states to seriously reassess their use of modems if they want to protect upcoming elections, particularly because hackers wouldn't need to successfully alter voting machine software to have a detrimental effect; they could just leave behind evidence that they got in.

"This is an extraordinarily powerful tool if all you want to do is simply discredit democracy," Jones says. "All you have to do is create the appearance of something having happened, even if it hasn't happened."