Will State Prevent Election Cyber Attacks?

Cybersecurity experts warn Wisconsin’s system is vulnerable. What are state officials doing about it?

By Grigor Atanesian, Wisconsin Center for Investigative Journalism - Sep 17th, 2018 03:06 pm

Get a daily rundown of the top stories on Urban Milwaukee

A private vendor inadvertently introduces malware into voting machines he is servicing. A hacker hijacks the cellular modem used to transmit unofficial Election Day results. An email address is compromised, giving bad actors the same access to voting software as a local elections official.

These are some of the potential vulnerabilities of Wisconsin’s election system described by cybersecurity experts.

State officials insist they are on top of the problem and that Wisconsin’s elections infrastructure is secure because, among other safeguards, voting machines are not connected to the internet and each vote is backed by a paper ballot to verify results.

In July, the Wisconsin Center for Investigative Journalism reported that Russian hackers have targeted websites of the Democratic Party of Wisconsin, the state Department of Workforce Development and municipalities including Ashland, Bayfield and Washburn. Elections in this swing state are administered by 1,853 municipal clerks, 72 county clerks and the Wisconsin Elections Commission.
Top cybersecurity experts from the United States, Canada and Russia interviewed by the Center said that some practices and hardware components could make voting in Wisconsin open to a few types of malicious attacks, and that Russian actors have a record of these specific actions.

Brad Pamperin talks with Deborah Hermsen, an election chief-in-training, during voting at the village hall in Little Chute, Wis., for a special election in the 1st Senate District on June 12, 2018. The village had retired an older style of voting machine for the newer DS200 scanner and tabulator. Officials also were using a new ExpressVote machine for electronic voting.

State officials insist that Wisconsin’s elections infrastructure is secure because, among other safeguards, voting machines are not connected to the internet and each vote is backed by a paper ballot to verify results.

And it is not just Wisconsin — this is a nationwide threat, the National Academy of Sciences, Engineering and Medicine stated in its newly released report, Securing the Vote.

“With respect to foreign threats, the challenge is compounded by the great asymmetry between the capabilities and resources available to local jurisdictions in the United States and those of foreign intelligence services,” according to the report.

Wisconsin Elections Commission spokesman Reid Magney said
the agency has been doing “almost everything they recommend” in the report for several years except for a specific type of post-election audit, which will be discussed at a Sept. 25 meeting.

“In short, we’re way ahead of the curve in election security and ought to get some credit for that,” Magney said.

Private companies, which supply the hardware and software for voting, are increasingly the focus of federal lawmakers, security experts and election integrity advocates.

Former longtime Legislative Audit Bureau manager Karen McKim, a coordinator for the Madison-based grassroots group Wisconsin Election Integrity, said many Wisconsin elections officials do not realize “how very much is completely outside their control.”

“They really, truly, do believe that if they keep the individual voting machines unconnected from the internet and do pre-election testing, that the software is safe,” said McKim, whose group advocates for measures to secure Wisconsin’s elections. “You cannot really blame them for that, because for both state and local election officials, the vendors are pretty much their sole source of information on voting-machine security.”

Voting machines are certified by the state. But there are no federal standards for security, operation or hiring processes at companies that provide hardware and software for voting. The state does not scrutinize the security practices of such private vendors.

“While (outsourcing pre-election programming) may introduce a vulnerability, the more important question is whether that
vulnerability is acceptable,” Magney said. “And that depends on the exact details of the security mitigations involved.”

Dane County Clerk Scott McDonell said large counties in Wisconsin such as his “typically code their own elections,” but “the small ones are outsourcing.”

“If I were being paranoid,” he added, “I would worry about the outsourced ones.”

Dane County Clerk Scott McDonell says his county programs all of its voting machines but that many smaller counties use private vendors. “If I were being paranoid,” McDonell says, “I would worry about the outsourced ones.” Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

Cybersecurity expert Luke McNamar confirmed that private vendors can be a vulnerability. McNamara is a senior analyst at the California-based FireEye cybersecurity firm, which investigated the breach of Illinois’ voter registration database that happened before the 2016 election.

He said governments need to make sure the vendors they work with “are using proper security and safeguarding their own software, data and systems that they’re deploying out to the
state level.

“If the actors are able to compromise the software or even the hardware that is being utilized by a vendor,” McNamara added, “that can have an effect down the road when a state uses this system for an election.”

According a leaked National Security Agency report, data stolen from a private vendor by Russian intelligence operatives was used to probe local government systems in 2016. The vendor was later identified as VR Systems, a Tallahassee-based vendor working with most Florida counties.

The biggest election systems vendors, including those working in Wisconsin, have refused to answer security-related questions and ignored invitations to testify before the U.S. Senate.

The Green Party’s presidential candidate, Jill Stein, who won the right to evaluate the source code for Wisconsin’s voting machines, is advocating for public ownership of voting systems and technologies related to them.

“It’s outrageous that our election systems are owned by private corporations that claim a proprietary interest in keeping critical information secret from the public,” Stein campaign spokesman Dave Schwab wrote in an email to the Center.

Computer scientist J. Alex Halderman, who was part of the team that pushed for the 2016 recount of the presidential vote in Wisconsin, told the U.S. Senate Intelligence Committee that private vendors can make elections systems vulnerable.

“A small number of election technology vendors and support contractors service the systems used by many local governments,” Halderman, director of the University of Michigan’s Center for Computer Security and Society, testified in 2017. “Attackers could target one or a few of these companies and spread malicious code to election equipment that serves millions of voters.”

Wisconsin election integrity activists have sought transparency
from Command Central LLC, a Minnesota-based vendor that has provided voting machine programming to more than half of Wisconsin’s 72 counties. In a 2011 email interview with local activists, a company representative said it serviced “3,000 pieces of equipment” in 46 Wisconsin counties.

The Center asked Command Central several questions, including the number of governments it currently serves in Wisconsin, what technology it uses to exchange files with clerks and whether there are any full-time security personnel in the company.

“We do not disclose information to the press (or the public) about internal and external procedures with our customers or the specifics of our internal security settings/applications,” Command Central President Chad Trice wrote in response.

Companies sue over software review

Two corporations that supply most of the voting machines in Wisconsin, Election Systems & Software of Omaha, Nebraska; and Dominion Voting Systems of Denver, are suing the state Elections Commission and the Stein campaign in Dane County Circuit Court in Madison over the Stein campaign’s plans to evaluate the source code.

State law explicitly allows such an examination in the event of a recount. Green Party candidate Stein paid for the 2016 presidential recount in Wisconsin, which confirmed Donald Trump as the winner.
Scanner and tabulator machines are seen during a public test of election equipment in Madison, Wis., on Aug. 6. The machines are not connected to the internet, but send the results via a one-way modem to the Dane County Clerk's Office. A scanned version of each ballot is stored on a USB memory card. Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

The voting machine companies are seeking to block the Elections Commission and the Stein campaign from publicizing “in any media or public forum whatsoever any information or materials or any opinions, conclusions, or comments concerning the review.”

Schwab said Wisconsin was wise to create the legal mechanism to allow for independent examination of the software.

“The source code for voting software has never before been examined,” he said. “Given the evidence of breaches in systems surrounding the vote, the public deserves an examination of our voting systems themselves to know whether other breaches might have occurred.”

In their motion, the vendors questioned the impartiality of the Stein campaign, calling it “subjective and biased.” The companies insist that any public comment would jeopardize “highly confidential, proprietary and trade secret information.”
Removable memory devices debated

Another potential vulnerability is the use of removable devices to transfer programming to the voting machines. The issue of removable devices came up at the Dane County Circuit Court hearing about the 2016 presidential recount. Then-Wisconsin Elections Commission Administrator Michael Haas confirmed at the time that “most often, the equipment is programmed by a private vendor for each election” at the vendors’ offices and then that programming is passed onto municipalities by “removable media” inserted in voting machines.

Certified Municipal Clerk Thomas Lund heads up a public test of election equipment in Madison, Wis., ahead of the Aug. 14, primary. A group of paid staff and volunteers test all the voting machines by running ballots with all voting scenarios for that ballot, and for each candidate, through the machines and making sure they tally them correctly. Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

Haas also testified that the commission does not know if the vendors connect their computers to the internet, and there are no requirements not to. But, according to the commission, any problems with the voting machines would be identified pre-election.
“State law requires municipal clerks to publicly test voting equipment for logic and accuracy before each election. Voting equipment memory devices are secured in the machines with tamper-evident seals,” the commission said.

However, if such a device contains malicious software, it can infect even voting machines not connected to the internet, said Alexis Dorais-Joncas of the cybersecurity firm ESET, who investigated just such an attack by Russian intelligence-associated hackers in 2014.

Any device, including a removable memory device, that touches both a computer connected to the internet and an unconnected machine creates an opening for malicious code to penetrate the system, agreed Dmitry Volkov, chief technology officer for the company Group-IB based in Moscow.

USB memory sticks are seen during a public test of election equipment in Madison, Wis., on Aug. 6. The scanner and tabulator machines used for voting are not connected to the internet, but send the results via a one-way modem to the county clerk’s office. A scanned version of each ballot is stored on a USB memory card. Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

Volkov is a member of the Advisory Group on Internet Security for Europol, the European Union’s law enforcement agency. Group-IB provides cybersecurity services to banks and
corporations in the United States, Russia and a number of European and Asian countries.

“Any software has a vendor. (The vendor) is most likely not air-gapped (disconnected from the internet). So it’s just easier to target the vendor and penetrate its systems” than to hack voting machines, Volkov said.

Volkov said software vendors can be attacked through codes that open a “backdoor,” giving unsanctioned access to computer systems and devices.

“You can also add a malicious code in the update that will be delivered (to customers) after all tests are conducted,” Volkov said. “(If) a vendor has access (to an election system) through a secure channel, if you hack the vendor, you can gain an access through this secure channel.”

Harri Hursti, a New York-based computer scientist and co-founder of the Voting Machine Hacking Village at the annual DEFCON hacker conference, agreed. He testified at the congressional briefing on election cybersecurity in July and has completed studies for the United States and European governments.

“It is hard to make the claim that anything using any kind of USB devices can be air-gapped,” Hursti told the Center. “USB memory cards are mini-computers, and we have known for years how to reprogram those to carry malicious content over air gaps and extract confidential information.”

Top Russians hackers have a record of penetrating offline systems through such devices, according to research by Dorais-Joncas and Thomas Dupuy. They work for the Montreal-based research and development center of ESET, a Slovakian internet security firm.

The pair for years has been investigating Sednit — also known as Fancy Bear — a Russian hacking group that allegedly stole email correspondence from the Hillary Clinton campaign and the Democratic National Committee. That hack has been linked
in an indictment by Special Counsel Robert Mueller to the General Staff of the Russian Armed Forces, better known as the GRU.

Dorais-Joncas and Dupuy told the Center that Sednit first hacked such a “not connected to the internet” system in 2014. The group is capable of penetrating a system through memory sticks or USB drives, Dorais-Juncas said.

“Sednit used unique tools that we’ve never seen with other groups, specifically designed to infect and control” such systems, he told the Center.

Modems vulnerable?

Experts said another potential vulnerability is associated with the use of modems in voting machines across Wisconsin to transmit unofficial Election Day results.

Those modems may be transmitting results over the internet, Haas, the former Elections Commission administrator, acknowledged in 2016 testimony. Haas was responding to questions posed as part of the legal battle over Wisconsin’s presidential recount.

“Some of the newer equipment does have modems that operate using wireless internet,” Haas said. “And so after the polls close … that instantaneous transaction would be conducted over the internet.”
Reid Magney of the Wisconsin Elections Commission says the state already employs many of the strategies outlined in a recent National Academy of Sciences report, Securing the Vote. “We’re way ahead of the curve in election security and ought to get some credit for that,” Magney says. He is seen here on Wisconsin Public Television’s Here and Now show in March 2018. Photo courtesy of Wisconsin Public Television.

But Magney rejected those security concerns. He said the devices “do not accept any incoming connections. The user keys in a specific phone number to dial out. While misdials or interceptions may be possible … the receiving computer also has a firewall, and accepts authenticated transmissions for a very short period of time.”

Vendors and elections commission officials say proper safeguards, such as malware detection and encryption, are in place. Magney said the transmissions are made “only after all the votes have been tabulated.”

Magney noted that the new National Academy of Sciences report does not mention modems as a potential vulnerability.

However, computer scientists say that existing defense measures can be overrun. According to The New Yorker, such concerns have prompted four states — New York, Maryland, Virginia and Alabama — to prohibit the use of machines with modems to transmit election results.
Cellular connection adds vulnerability

Another practice criticized by the computer scientists is the use of cellular technology to transmit unofficial election results. Cellular networks’ security liabilities were detailed in a 2017 U.S. Department of Homeland Security Study on Mobile Device Security.

The DHS report called for enhanced protections when governments use cellular technology, which can open “an avenue to attack back-end systems containing data on millions of Americans in addition to sensitive information relevant to government functions.” In 2017, Homeland Security officials designated election systems as critical infrastructure in need of enhanced protection.

A voting sign is seen at Olbrich Gardens in Madison, Wis., on Feb. 20, 2018. Dane County Clerk Scott McDonell said large counties in Wisconsin such as his “typically code their own elections,” but “the small ones are outsourcing.” Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

At the Center’s request, the list of cellular modems in use in Wisconsin election systems was reviewed by Bart Stidham, chief executive officer of NAND Technologies. The company
specializes in mobile and cellular security, and Stidham has conducted cellular network security analysis for the Department of Homeland Security and commercial clients.

Stidham stated that “most of the cellular modems listed are commodity consumer devices. They are not designed for use in critical infrastructure. Many have features that are not appropriate for use in such an environment, including unsecured firmware updating and unvetted supply chains.”

But Magney said the federal government “is still parsing out what that (critical infrastructure) designation means” when it comes to elections and voting equipment. He added that Wisconsin does “not have the technical capacity or expertise to complete the type of software testing and analysis that is done at the federal level.”

Some of these cellular wireless modems rely on public cellular networks. A variety of voting machines in Wisconsin have such modems. The DS200, an Election Systems & Software-manufactured machine that is in wide use in the state, is equipped with modems running on AT&T, Sprint or Verizon public networks, according to a document from the Elections Commission.

Volkov said the data that run through public mobile networks are vulnerable. “Will malicious actors be looking for vulnerabilities? They will. Think of a modem as any other device that connects you to a public network. If you are on a public network, you can be reached.”

Hursti agreed: “Cellular modems are mini-computers which
communicate with cellular networks, but more importantly, cellular networks have not even offered for a decade the equivalent of dial-up connection. Ninety-nine percent of the time, the reality is, a cellular modem passes the traffic into the mobile carrier's Internet Protocol (IP) network.”

“Yes, that is how cellular modems work,” Magney, the Elections Commission spokesman said. “They connect to the IP network, and to the internet. Then they create an authenticated and encrypted channel through that network.”

Magney downplayed the concerns, noting that only unofficial results from Election Day are transmitted this way. Those are backed up by a printed paper tape, which is used to verify the results.

“Some voting equipment is not equipped with modems and some is,” he said. “Voting equipment with a modem connects to a central computer after the polls close and transmits encrypted, unofficial results. The official results from that voting equipment is the printed paper tape with the totals for each candidate, and that is what the County Board of Canvassers uses to certify the results of an election.

“The paper tape, memory devices, ballots and other documentation is transported to the clerk's office in containers with numbered security tags and chain of custody logs.”

In February, two Princeton University computer science professors, Andrew Appel and Kyle Jamieson, published a blog describing possible scenarios to hack particular modems used in DS200 paper ballot tabulators, including erecting fake cellphone towers near voting locations.

“So, in summary: phone calls are not unconnected to the internet; the hacking of phone calls is easy (police departments with Stingray devices do it all the time); and even between the cell-towers (or land-line stations), your calls go over parts of the internet,” the pair wrote. “If your state laws, or a court with jurisdiction, say not to connect your voting machines to the internet, then you probably shouldn’t use telephone modems
either.”

A public test of election equipment was conducted in Madison, Wis., ahead of the Aug. 14, 2018 primary. A group of paid staff and volunteers test all the voting machines by running ballots with all voting scenarios for that ballot, and for each candidate, through the machines and making sure they tally them correctly. Photo by Coburn Dukehart / Wisconsin Center for Investigative Journalism.

Hursti also raised the concern of caller ID spoofing, in which a call appears to be coming from a particular number but in fact is coming from another number. According to the Federal Trade Commission, “it can be nearly impossible to tell whether the caller ID information is real.”

Magney dismissed potential vulnerability related to the caller ID spoofing.

“Spoofing caller ID does not enter into it,” he said, because the machines make only outgoing calls.

Election officials reiterate that only unofficial results are transmitted via cellular systems, which means that in case of an attack, the final, certified results would not be tampered with.

But even discrepancies between initially reported unofficial results and the outcome of the election may achieve Russia’s
goal of sowing discord, according to FireEye’s McNamara.

He is among those cautioning against becoming too focused on the vulnerabilities of America’s vote-tallying systems. McNamara said the Kremlin’s goal may be simpler: “Attacking the confidence of electoral process itself.”

Grigor Atanesian, a native of St. Petersburg, Russia, is an Edmund S. Muskie fellow at the Wisconsin Center for Investigative Journalism. He studies investigative reporting at the University of Missouri School of Journalism via a Fulbright grant. The nonprofit Center (www.WisconsinWatch.org) collaborates with Wisconsin Public Radio, Wisconsin Public Television, other news media and the UW-Madison School of Journalism and Mass Communication. All works created, published, posted or disseminated by the Center do not necessarily reflect the views or opinions of UW-Madison or any of its affiliates. The Center’s coverage of democracy issues is supported by The Joyce Foundation.