Why the "But our voting systems are not connected to the internet, so they're secure" defense is completely wrong.

AIR GAPS (*Explanation by Free & Fair, http://freeandfair.us/articles/air-gaps/*)

Q: Is disconnecting from the internet enough to keep a voting system safe from hacking?

A: No. Just about anything you plug into a computer can breach an air gap. All of these items are examples of potentially compromised hardware, available for sale on the dark net or to foreign intelligence agencies.

Excerpts from articles (but read articles for full and additional explanations):

One possibility is that attackers could infiltrate what are called election-management systems. These are small networks of computers operated by the state or the county government or sometimes an outside vendor where the ballot design is prepared.

There's a programming process by which the design of the ballot—the races and candidates, and the rules for counting the votes—gets produced, and then gets copied to every individual voting machine. Election officials usually copy it on memory cards or USB sticks for the election machines. That provides a route by which malicious code could spread from the centralized programming system to many voting machines in the field. Then the attack code runs on the individual voting machines, and it's just another piece of software. It has access to all of the same data that the voting machine does, including all of the electronic records of people's votes.

So how do you infiltrate the company or state agency that programs the ballot design? You can infiltrate their computers, which are connected to the internet. Then you can spread malicious code to voting machines over a very large area. It creates a tremendously concentrated target for attack.

> ***SCIENTIFIC AMERICAN: "The Vulnerabilities of Our Voting Machines"***
> *https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/*

Voting machines are not supposed to be connected to the internet, providing an air gap between the machines and hackers. Halderman said that that practice is good, but explained that there are other ways machines can be hacked.

"This is something that election officials really, really, really like to tell you," Halderman said. "And thank goodness that's true. It would be really dumb if we plugged our voting machines directly into the internet and gave them public IP addresses."

But voting machines do need to be programmed with new ballots for each new election. In many cases that process is done using external memory cards processed on a separate computer, sometimes by an outsourced third party. A determined attacker could spearphish the individuals responsible for programming the ballots and infect their devices with malware that could change vote counts, thus leaping across the air gap, Halderman explained.

Halderman said there's little visibility into how officials or third parties manage the ballot programming process and whether they use cybersecurity best practices, such as air gapping.

"I should certainly hope that they do, but there's no way to confirm that," he said.

> ***CyberScoop:*** ***"Air gapping voting machines isn't enough, says one election security expert"*** *https://www.cyberscoop.com/election-hacking-voting-machines-alex-halderman/*

Relying on the security of the air gap is a mistake, Wallach explained in his address to the House Committee on Space, Science & Technology. An "air gap" is a physical and communication disconnect between one machine and the next created by a lack of internet, WiFi, or other networking connection. "The Stuxnet malware, for example, was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the internet," Wallach noted. "We don't know exactly how the Stuxnet malware got in, but it did nonetheless."

Unfortunately, Wallach says that the security of supposedly air-gapped systems is a great deal flimsier than it's sold as being. "When you dig down, [many vendors] often have election management systems connected to the Internet, albeit behind firewalls, VPNs, or other such devices. It's incorrect to call such systems 'never connected.'" Wallach also noted that certification requirements are such that all elections management systems run on unpatched, obsolete operating systems (usually Windows 2000 or XP), which are subject to a variety of vulnerabilities that have been well-known for years.

But because air-gapped voting machines run on ballot and tabulation software centrally programmed elsewhere, the air gap is a moot point.

"These are small businesses with little to no operational security oversight on the part of the government," Bernhard explained. "So any breach would be hard to detect. Moreover, it's likely that ballots are programmed by computers that are in some way connected to the Internet."

> ***Think Progress:*** ***" How easy would it be to rig the next election?"*** *https://thinkprogress.org/how-easy-would-it-be-to-rig-the-next-election-819326cbbbd/*

The Princeton group has no shortage of things that keep them up at night. Among possible targets, foreign hackers could attack the state and county computers that aggregate the precinct totals on election night—machines that are technically supposed to remain non-networked, but that Appel thinks are likely connected to the Internet, even accidentally, from time to time.

They could attack digitized voter registration databases—an increasingly utilized tool, especially in Ohio, where their problems are mounting—erasing voters' names from the polls (a measure that would either cause voters to walk away, or overload the provisional ballot system).

They could infect software at the point of development, writing malicious ballot definition files that companies distribute, or do the same on a software patch.

They could FedEx false software to a county clerk's office and, with the right letterhead and convincing cover letter, get it installed. If a county clerk has the wrong laptop connected to the Internet at the wrong time, that could be a wide enough entry window for an attack**.**

"No county clerk anywhere in the United States has the ability to defend themselves against advanced persistent threats," Wallach tells me, using the parlance of industry for highly motivated hackers who "lay low and stick around for a while." Wallach painted an unseemly picture, in which a seasoned cyber warrior overseas squared off against a septuagenarian volunteer. "In the same way," continues Wallach, "you would not expect your local police department to be able to repel a foreign military power."

> ***POLITICO MAGAZINE: "How to Hack an Election in 7 Minutes"***
> *https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144*

For many years voting machine vendors have claimed that voting machines were air gapped — not connected to the internet — and were thus unhackable. Kim Zetter debunked that idea in *The New York Times* in February.

An attacker who managed to break into a voting machine vendor employee's work email, because the employee used the same password as on a breached site, could leverage that to gain access to the voting machines themselves. And if voting machine vendors install remote access software on voting machines, factory backdoors that vendor employees use to remotely access the machines for maintenance, troubleshooting or election setup purposes, this turns voting machine vendor employees into targets.

Hack the vendor, hack the voting machine.

> ***CSO: "Want to hack a voting machine? Hack the voting machine vendor first." How password reuse and third-party breaches leave voting machine vendors vulnerable to attack.***
> *https://www.csoonline.com/article/3267625/security/want-to-hack-a-voting-machine-hack-the-voting-machine-vendor-first.html*