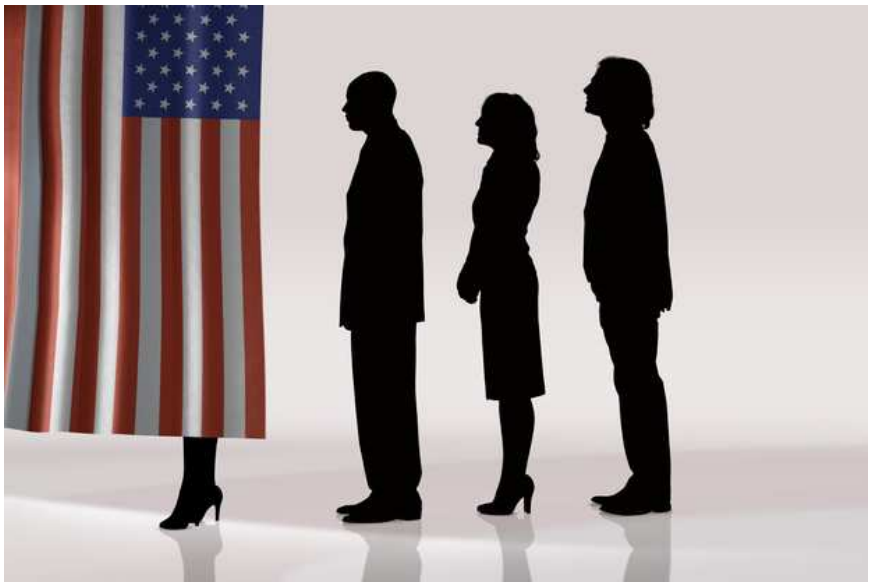
infoworld.com

Voting machines are still too easy to hack

Roger A. Grimes



Credit: Thinkstock

InfoWorld | Sep 6, 2016

People have trouble prioritizing risk. For example, you often hear about the threat of voter fraud, when all evidence suggests that the risks of such fraud are inconsequential. In truth, hacked voting machines are much more likely to affect an election's outcome.

Why would an election fraudster try to herd a flock of criminal participants to the polls when one mildly talented hacker could cause far more trouble?

On a state-by-state level, most presidential elections are decided by many thousands of votes. For example, in 2012, Barack Obama beat Mitt Romney by more than 166,000 votes in the swing state of Ohio. Even in the 2000 election, the closest presidential contest

ever, what sort of Houdini could have marshaled the miscreants necessary to cast a few hundred fake votes to tip the balance without getting caught? A hack of a single voting machine could accomplish the same objective.

The good news is that voting machines are not connected to the internet, so physical access is required to hack them. The bad news: If you can get to them, they're easy to hack.

Voting machines are dinosaurs

America's voting machines include both old mechanical devices and voting computers, which tend to run old operating systems on unsupported, out-of-warranty laptops and servers. Today, approximately 70 percent of U.S. voting sites use a voting computer.

It's amazing how many voting computers still run Microsoft Windows XP, though Microsoft hasn't supported it or offered critical security patches for years. According to the Brennan Center for Justice at New York University School of Law, 43 of our 50 states have voting computers that are at least 10 years old; 14 of those 43 states use voting computers that are 15 years old or more.

Most of the people in charge of protecting, configuring, updating, deploying, and supporting these devices lack the experience or troubleshooting skills of today's average teenager. Few understand the security risks involved with the computers they manage.

All voting computers can be hacked

Most voting computer manufacturers (there are at least 15 vendors) believe white hat hacking is a menace. Proactive bug bounty programs do not exist. Only a few states require independent vulnerability audits.

Every independently audited voting computer has been shown to contain numerous, basic, easy-to-exploit vulnerabilities. A fresh report from the Institute for Critical Infrastructure Technology puts it succinctly: "Voter machines, technically, are so riddled with vulnerabilities that even an upstart script kiddie could wreak havoc." In 2012, white hat hacker Roger Johnston explained to Popular

Science how a voting computer's votes could be changed for less than $10 worth of RadioShack hardware.

Well, at least such hacks require physical access. No one would consider connecting voting computers to the internet and making them exponentially more vulnerable. Right?

The internet voting peril

Wrong. Thirty-plus states and the District of Columbia already allow some votes to be submitted across the internet. More states want to experiment with internet voting. It's simply a matter of time.

Scores of companies are lobbying for internet voting, including Simply Voting, which touts "flawless elections made simple." Granted, I'm confident any system is hackable, but at least this vendor seems to understand some of the risks.

I don't have to think long and hard to imagine a broad, client-side, man-in-the-middle attack, which could flip votes without the vendor or the voter being able to detect it. Sophisticated malware able to accomplish similar tasks, in the form of banking Trojans, has been around for more than a decade.

Keep the vote safe

I know of no independent computer security researcher with voting machine expertise who will tell you that computerized-voting is safe as it stands -- or recommends moving to internet-based voting. Read Bruce Schneier's latest NSFW rant to get his take on the topic.

Lots of other organizations, such Verified Voting, are working hard to safeguard our current computerized voting experience. Verified Voting even lets you find out which voting computer or machine your voting precinct uses.

All voting computer experts agree that verified paper audit systems must be maintained to audit and spot-check a voter's intent. Unfortunately, one quarter of our states don't require paper trails -- and only 26 require post-election auditing verification.

Why is stealing elections so hard?

Hacking an electronic voting computer isn't hard, but rigging an election is, mainly because physical access is necessary. Each physical hack adds to the risk of discovery, and you'd need to hit enough machines in the right places without detection to shift an election's outcome.

Consider the 2000 presidential election. The incredibly tight outcome in Florida could not have been predicted. To swing any election, hackers would need to know who's going to the poll and how many votes would be necessary to offset the early, military, and absentee ballots (which often aren't counted until after the election). That can't be done with any level of accuracy.

In today's world of ultrapolarized politics, where each side accuses the other of "rigging" elections, keeping our elections reliable and tamper-free is paramount. But I don't think "election observers" and voter IDs will do it. Instead, we need paper trial auditing -- and we need to keep voting off the internet.

Roger A. Grimes — Columnist

An InfoWorld security columnist since 2005, Roger Grimes holds more than 40 computer certifications and has authored eight books on computer security.