PHYS.ORG

Hacking the election: security flaws need fixing, researchers say

October 10 2017, by Rob Lever

A report says there is no way to know if votes have been manipulated with paperless machines which have no paper ballots to be recounted

Hackers could have easily infiltrated US voting machines in 2016 and are likely to try again in light of vulnerabilities in electronic polling systems, a group of researchers said Tuesday.

A report with detailed findings from a July hacker conference which demonstrated how voting machines could be manipulated concluded that numerous vulnerabilities exist, posing a national security threat.

The researchers analyzed the results of the "voting village" hacking contest at the DefCon gathering of hackers in Las Vegas this year, which showed how ballot machines could be compromised within minutes.

"These machines were pretty easy to hack," said Jeff Moss, the DefCon founder who presented the report at the Atlantic Council in Washington.

"The problem is not going away. It's only going to accelerate."

The report said the DefCon hack was just the tip of the iceberg—with potential weaknesses in voter databases, tabulating software and other parts of the system.

The researchers said most voting machines examined included at least some foreign-manufactured parts, raising the possibility that malware could be introduced even before the devices are delivered.

"This discovery means that a hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line," the report said.

"With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility."

Researchers say their latest analysis of electronic voting machines highlights vulnerabilities which couldleave systems open to hackers

No certainty on 2016

Harri Hursti, a researcher with Nordic Innovation Labs and a co-author of the report, said it's impossible to say with certainty if votes were tampered with in 2016 because many systems "don't have the capacity" to be audited.

The report said five US states operate entirely on paperless systems which have no paper trail to be reviewed and another nine states are partially paperless.

"The only way to know is if the hacker tells you," he said, adding that "it can be done without leaving tracks."

Douglas Lute, former US ambassador to NATO who presented the report, said in a forward to the report that the findings highlight "a serious national security issue that strikes at the core of our democracy."

Although some researchers in the past have shown individual machines could be breached, this report suggests a range of vulnerabilities across a range of hardware, software and databases.

"What the report shows is that if relative rookies can hack a voting system so quickly, it is difficult to deny that a nefarious actor -- like Russia -- with unlimited time and resources, could not do much greater damage," said University of Chicago cybersecurity instructor Jake Braun, another co-author.

The threat becomes all the more grave "when you consider they could hack an entire line of voting machines, remotely and all at once via the supply chain," he added.

In presenting the findings, the researchers said members of the DefCon hacker community would work with academics and security researchers in a new coalition aimed at improving election security.

Citation: Hacking the election: security flaws need fixing, researchers say (2017, October 10) retrieved 24 April 2024 from https://phys.org/news/2017-10-hacking-election-flaws.html