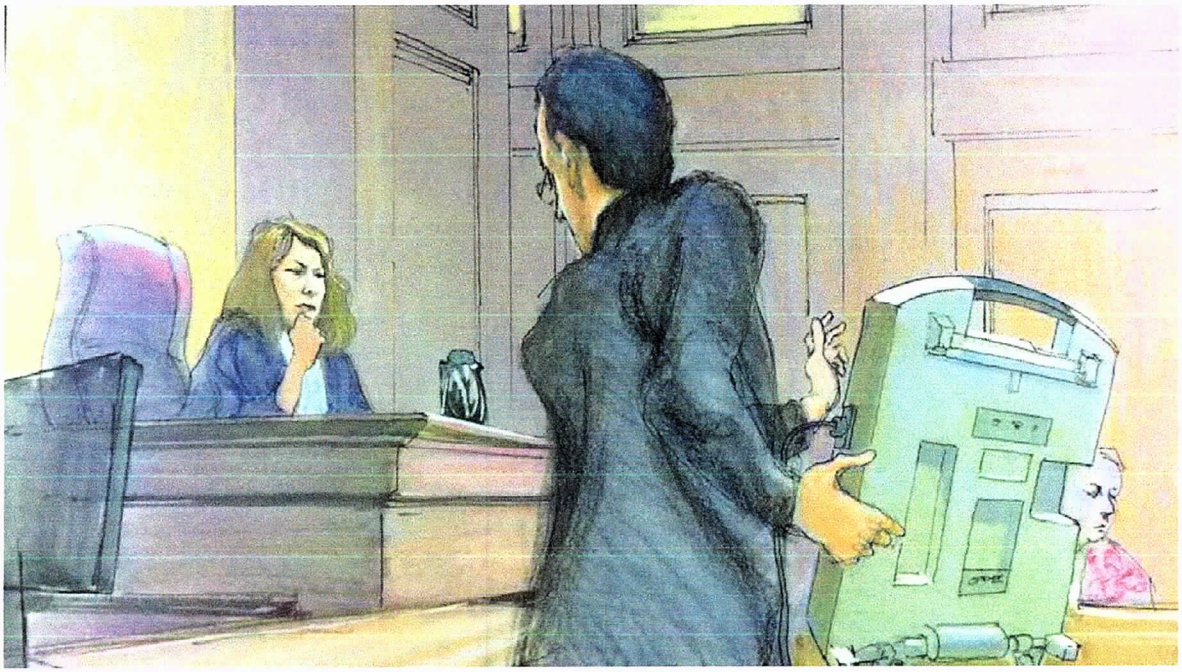
POLITICS

Expert shows how to tamper with Georgia voting machine in security trial

Election officials say vulnerabilities are merely speculative



U.S. District Judge Amy Totenberg listens as Alex Halderman, a University of Michigan computer science professor, shows how a voting machine could be hacked during a 2018 hearing. Halderman gave a similar demonstration Thursday in a trial before Totenberg to determine whether Georgia's voting system is vulnerable to manipulation or...

More

By Mark Niesse

Jan 22, 2024

Huddled around a voting machine in a federal courtroom, a small crowd watched as expert witness Alex Halderman demonstrated how someone could meddle with a Georgia election within seconds.

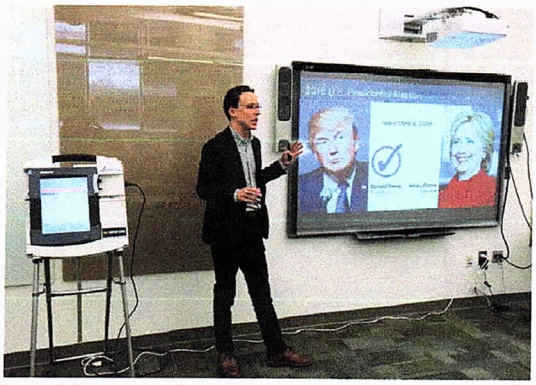
Halderman, a University of Michigan computer scientist, changed results of a hypothetical referendum on Sunday alcohol sales. He flipped the winner in a theoretical election between

President George Washington and Benedict Arnold, the Revolutionary War general who defected to the British. He rigged the machine to print out as many ballots as he wanted.

All he needed was a pen to reach a button inside the touchscreen, a fake $10 voter card he had programmed, or a $100 USB device that he plugged into a cord connected to a printer, rewriting the touchscreen's code.

Halderman delivered his presentation during an election security trial evaluating whether Georgia's voting system is vulnerable to manipulation or programming errors. All in-person voters in Georgia make their choices on touchscreens that print out paper ballots.

Election officials countered Halderman's testimony with assurances that real-world elections in Georgia have never been hacked and security precautions prevent the possibility of interference.



University of Michigan computer science professor Alex Halderman demonstrates how to hack Georgia's previous voting equipment during a presentation at Georgia Tech in 2018. Curtis Compton/ccompton@ajc.com

"All of these things worry me — just how easy these machines would be to tamper with. It's so far from a secure system," Halderman testified Thursday. "There are all kinds of politically motivated actors that would be eager to affect results."

Under questioning from attorneys defending Georgia's Dominion voting equipment, Halderman said there's no evidence that the vulnerabilities he showed have ever been exploited in an actual election.

Through eight days of the trial, attorneys for the liberal-leaning Georgia voters and activists who are plaintiffs in the case have tried to convince U.S. District Judge Amy Totenberg that she should order the state to prohibit further use of the voting touchscreens as the 2024 elections approach. Voters would instead fill out paper ballots by hand.

Testimony in the case included evidence about the January 2021 breach in Coffee County, when tech experts hired by supporters of Donald Trump copied Georgia's election software, then distributed it to conspiracy theorists across the country. The plaintiffs have also sought to prove that the secretary of state's office hasn't done enough to protect election security and voters' rights.

But State Election Board member Matt Mashburn told the judge that hacking would be difficult to pull off during an election.

"There are serious potentialities. Now, how practical they are to put in place is a different question," Mashburn said Wednesday, according to a court transcript.

Flaws in voting machines would be difficult to exploit at more than one voting machine at a time, minimizing the potential danger, he said.

"I just didn't think it was realistic," Mashburn said. "Is it something you've got to change the whole system for? ... I just don't believe that is very likely. It is possible, but it is not very likely."

Halderman testified that he discovered vulnerabilities after he was given access to a Fulton County touchscreen, called a ballot-marking device, as an expert witness in the case. He reported his findings to the U.S. Cybersecurity and Infrastructure Agency, which validated the technology weaknesses in June 2022.

Credit: arvin.temkar@ajc.com

State Election Board member Matt Mashburn, during testimony in an election security case, questioned the practicality of a demonstration on how to hack Georgia's voting machines. "How practical they are to put in place is a different question," Mashburn said. (Arvin Temkar /...

More

Election officials have said Georgia's voting equipment is secured by locks and seals, poll workers overseeing precincts, preelection testing and audits of paper ballots.

Halderman said a wrongdoer, hidden behind a privacy screen at a voting precinct, wouldn't necessarily be caught by election workers. Changing a touchscreen's programming would take seconds or minutes but potentially create "chaos" in a major election, when it would be difficult to determine which ballots were legitimate, he said.

It isn't necessary to open up a voting machine or remove security seals to gain "superuser" access to a touchscreen and change its programming, Halderman testified. Any voter could bring a forged voter card, pen or USB drive loaded with malicious code to a voting machine.

In one of Halderman's hacks, the text on the ballot would reflect the candidate the voter picked, but the computer QR code counted by a ballot scanner would count the opposite choice. Georgia lawmakers are considering legislation that would remove QR codes from ballots.

The vulnerabilities Halderman showed in court would only affect one voting machine at a time, but he also testified that many more votes could be changed if someone gained access to election management servers overseen by state and county election officials.

Attorneys for Secretary of State Brad Raffensperger, the defendant in the case, contend that the mere possibility of election tinkering doesn't amount to a violation of voting rights protected by the U.S. Constitution, such as free speech and equal protection rights.

"Plaintiffs have failed to produce a single shred of evidence to substantiate the supposed 'risks' they fear," a court filing by the defendants states. "There is no evidence that their ballots or any

ballots cast using a BMD (ballot-marking device) were not accurately counted or that any vote has been changed.... Weighing risk is a political and not judicial decision."

Witnesses for the defendants this week will attempt to dispute the plaintiffs' allegations with testimony from Georgia election officials and cybersecurity experts.

The case will be decided by Totenberg, who was appointed by President Barack Obama, in the weeks after the trial concludes.

About the Author

Mark Niesse

Mark Niesse covers voting rights and elections for The Atlanta Journal-Constitution. He also reports on the

Back to Top