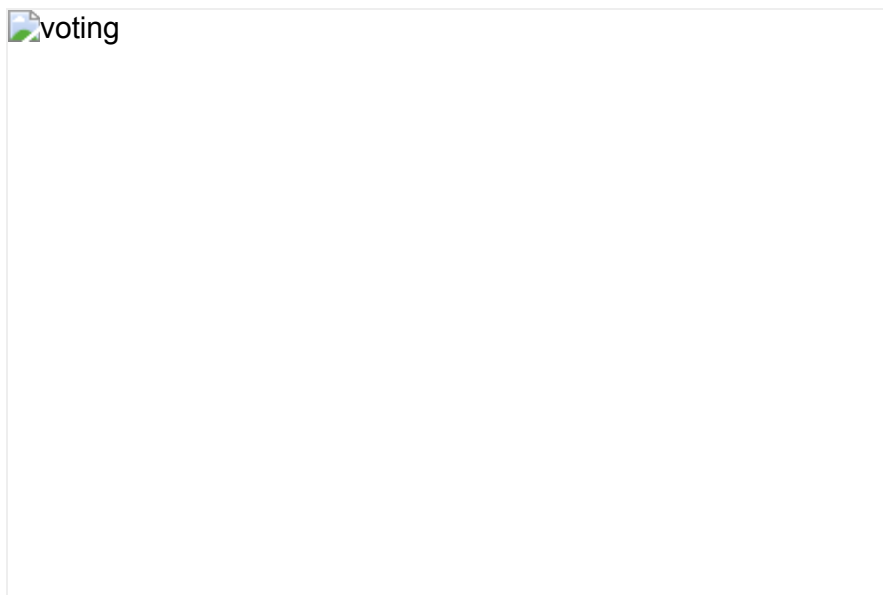


DEF CON hackers dossier on US voting machine security is just as grim as feared

Good thing Congress has been so forceful in improving security

By [Shaun Nichols](#) in [San Francisco](#) 26  [Reg comments](#) [SHARE](#) ▼



Hackers probing America's electronic voting systems have painted an astonishing picture of the state of US election security, less than six weeks before the November midterms.

The full [50-page report \[PDF\]](#), released Thursday during a presentation in Washington DC, was put together by the organizers of the DEF CON hacking conference's Voting Village. It recaps [the findings](#) of that village, during which attendees uncovered ways resourceful miscreants could compromise electoral computer systems and change vote tallies.

In short, the dossier outlines shortcomings in the electronic voting systems many US districts will use later this year for the midterm elections. The report focuses on vulnerabilities exploitable by scumbags with physical access to the hardware.

"The problems outlined in this report are not simply election administration flaws that need to be fixed for efficiency's sake, but rather serious risks to our critical infrastructure and thus national security," the report stated. "As our nation's security is the responsibility of the federal government, Congress needs to codify basic security standards like those developed by local election officials."

Criminally easy to hack

Researchers found that many of the systems tested were riddled with basic security blunders committed by their manufacturers, such as using default passwords and neglecting to install locks or tamper-proof seals on casings. These could be exploited by miscreants to do anything from add additional votes to create and stuff the ballot with entirely new candidates. It would require the crooks to get their hands on the machines long enough to meddle with the hardware.

Some electronic ballot boxes use smart cards loaded with Java-written software, which executes once inserted into the computer. Each citizen is given a card, which they slide in the machine when they go to vote. Unfortunately, it is possible to reprogram your card yourself so that when inserted, you can vote multiple times. If the card reader has wireless NFC support, you can hold your NFC

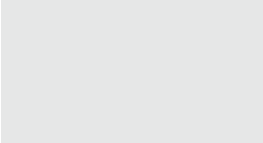
smartphone up to the voting machine, and potentially cast a ballot many times over.

"Due to a lack of security mechanisms in the smart card implementation, researchers in the Voting Village demonstrated that it is possible to create a voter activation card, which after activating the election machine to cast a ballot can automatically reset itself and allow a malicious voter to cast a second (or more) unauthorized ballots," the report read.

"Alternatively, an attacker can use his or her mobile phone to reprogram the smart card wirelessly."

Separately, a ballot-counting ES&S M650 machine raised a few eyebrows: it had poor physical security, and is intended to be networked to a county clerk's computer to report the results of scanning citizens' voting slips.

The DEF CON village was not without its share of controversy. Voting machine maker ES&S [condemned the conference's workshops and contests](#) as a security threat, while the organizers noted that the results of the gathering were limited because hackers were only being able to access publicly obtainable machines – typically decommissioned devices bought on eBay – leading some wondering how much damage a hacker could deal to today's in-production voting systems.



Ultimately, however, the researchers believe that the findings from the event show that there are more than enough holes to warrant a larger effort

ople voting
good old
r

by US Congress to get national security standards in place for electoral computer systems.

"While many local election officials have worked tirelessly to advocate for Congress to act and fund robust security practices, it's not enough. National security leaders must also remind Congress daily of the gravity of this threat and national security implications," the report stated.

"It is the responsibility of both current and former national security leaders to ensure Congress does not myopically view these issues as election administration issues but rather the critical national security issues they are. Disclosing vulnerabilities does not seem to be enough to get them fixed, even years later."

Hopefully, the dossiers' authors – Matt Blaze, University of Pennsylvania; Jake Braun, University of Chicago; Harri Hursti, Nordic Innovation Labs; David Jefferson, Verified Voting; Margaret MacAlpine, Nordic Innovation Labs; and Jeff Moss, DEF CON founder – aren't hoping to get that any time soon. Despite the repeated calls to improve election security ahead of the midterms, Congress has [steadfastly refused](#) to take any significant action. ®