DEFCON: Professional Hackers Breached Dozens Of Voting Machines Within Minutes

The utter lack of security on voting systems around the world shatters the illusion of tamper-free elections. Technocrats who build these technologies have no sense of building in security from the start, and could care less about patching them up after they have been hacked. White-hat hackers busted in to many machines within minutes of starting. Un-hackable voting machine is an oxymoron. TN Editor

Professional hackers were invited to break into dozens of voting machines and election software at this year's annual DEFCON cybersecurity conference. And they successfully hacked every single one of the 30 machines acquired by the conference.

The challenge was held at DEF CON's "Voting Village," where hackers took turns breaching ten sample voting machines and voter registration

systems, Politico reported.

Carten Schurman, a professor of computer science at the University of Copenhagen in Denmark, was able to break into one voting machine in minutes.

“I could have done this in 2004, or 2008, or 2012,” Schurman told Politico. With access to the voting machine, Schurman had the the power not only to see all the votes cast on the machine, but also to manipulate the results.

DEF CON’s hacking exercise came as the US grapples with the fallout from Russia’s interference in the 2016 election, which included attempts to tamper with voting systems.

Bloomberg reported in June that election systems in as many as 39 states could have been attacked by Russian state actors, though voting tallies are not believed to have been altered or manipulated in any way.

“In Illinois, investigators found evidence that cyber intruders tried to delete or alter voter data,” Bloomberg said. “The hackers accessed software designed to be used by poll workers on Election Day, and in at least one state accessed a campaign finance database.”

The report was bolstered by a leaked NSA document published by The Intercept in June detailing how hackers connected to Russian military intelligence had attempted to breach US voting systems days before the election.

At DEFCON, an intern named Anne-Marie Hwang was able to gain administrative access to a voting machine by simply using a generic key like the ones poll workers are given, plugging in a keyboard to the machine, and hitting control-alt-delete, Politico reported.

Read full story here…