Questions linger in US on high-tech voting

March 11 2012, by Rob Lever

A series of problems with electronic voting machines has raised fresh questions about election technology as newer computerized systems gain ground for the 2012 US election.

As many as 25 percent of Americans are expected to use paperless electronic voting machines in the upcoming November elections, according to the Verified Voting Foundation, but confidence has been eroded by incidents showing vulnerabilities.

The foundation, which seeks more reliable election systems, contends that voting machines in 11 states are all-electronic, with no paper systems for recounts, and that many other jurisdictions have some of these systems in place.

Last year, Microsoft Research published a paper describing vulnerabilities to what had been described as "fully verifiable" direct recording electronic (DRE) systems in which a hacker can "undetectably alter large numbers of votes."

Separately, scientists at Argonne National Laboratory described a way to tamper with certain electronic voting machines by inserting a $10 component along with a $15 radio frequency device to alter vote results.

Pamela Smith of the Verified Voting Foundation said these incidents highlight the fact "that you can have insider challenges as well as outsider hacks. It points out that you have to be able to check the system."

Election security and technology has been an issue in the United States since the 2000 president election marred by "hanging chads" in Florida that muddled the result.

US laws enacted since then encourage the use of new technology including touch-screen ballots. But some critics say these can be vulnerable to hackers and that some lack a "paper trail" which could allow a recount in case of machine failure.

"We still have a number of states which do not have what I call resilient recountable systems," Smith said.

"If they do have problems they may not be able to recover from them. So we would like states to move to recoverable systems where they could do a recount if there were a problem."

Last September, researchers led by Roger Johnston at the Argonne lab were able to change votes on the a ballot machine using about $25 worth of equipment, by inserting a device to manipulate touch screens by remote control

"We believe these 'man in the middle attacks' are possible on a wide variety of voting machines," with little technical expertise, Johnston said.

In October, Microsoft Research released a paper describing a so-called "trash attack" which it said could be "effective against the majority of fully verifiable election systems."

It is known as a trash attack because it would allow a corrupt elections worker, for example, see a voter dumping a receipt on the way out from a polling station, and then modify the vote without detection, and with no way to verify the original vote. Microsoft also offered a technical fix for this weakness.

Dan Wallach, a Rice University computer scientist, said little has changed since reports about vulnerabilities in voting machines began around 2007.

"Anybody trying to compromise them could have read all the public reports in 2007 and now, five years later, they've had lots of time to engineer attacks," Wallach said.

Wallach said it is not clear if any elections have been compromised by computer intrusions: "We don't know. If they were doing it and were doing it skillfully, we'd never know."

Other countries have faced similar issues. The Netherlands scrapped electronic voting several years ago after a high-profile hacking incident. Ireland also abandoned the use of Dutch-made voting machines. Controversies have arisen over security of voting machines in India and several other countries.

Richard Soudriette, president of the Colorado-based Center for Diplomacy and Democracy, said it was "unfortunate that electronic voting systems have taken on such a negative connotation."

"I think it is entirely possible to build trustworthy and verifiable systems. But there has been so much negative publicity about electronic voting, I don't think it's going to make a revival."

Charles Stewart, a political scientist at the Massachusetts Institute of Technology and faculty member of the Voting Technology Project of MIT and the California Institute of Technology, said he is "more comfortable than most people" with the new systems, while acknowledging that any system can be vulnerable.

"I trust my computer scientist friends when they tell me all the ways you

can hack into the machines," he said. "But I've yet to see an election hacked."

Stewart that if the 2012 presidential race is a runaway, few will notice any flaws in vote technology. But if it is a tight race, "I can easily imagine in a state like Ohio or Florida or Pennsylvania, if there are one or two counties where things go wrong, that could raise this issue again."

(c) 2012 AFP

Citation: Questions linger in US on high-tech voting (2012, March 11) retrieved 30 April 2024 from https://phys.org/news/2012-03-linger-high-tech-voting.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.