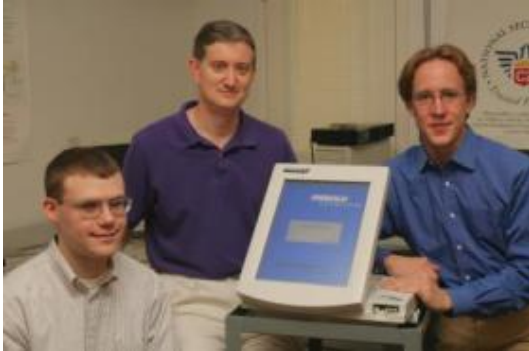


Researchers reveal 'extremely serious' vulnerabilities in e-voting machines



Edward Felten (center), director of the Center for Information Technology Policy, has coauthored a paper with graduate students Ariel Feldman (left) and Alex Halderman on a demonstration vote-stealing software that highlights security vulnerabilities in electronic voting machines. Credit: John Jameson, Princeton University

In a paper published on the Web today, a group of Princeton computer scientists said they created demonstration vote-stealing software that can be installed within a minute on a common electronic voting machine. The software can fraudulently change vote counts without being detected.

"We have created and analyzed the code in the spirit of helping to guide public officials so that they can make wise decisions about how to secure elections," said Edward Felten, the director of the Center for Information Technology Policy, a new center at Princeton University that addresses crucial issues at the intersection of society and computer technology.

The paper appears on the Web site for the Center for Information Technology Policy (<http://itpolicy.princeton.edu/voting/>).

The researchers obtained the machine, a Diebold AccuVote-TS, from a private party in May. They spent the summer analyzing the machine and developing the vote-stealing demonstration.

"We found that the machine is vulnerable to a number of extremely serious attacks that undermine the accuracy and credibility of the vote counts it produces," wrote Felten and his co-authors, graduate students Ariel Feldman and Alex Halderman.

In a 10-minute video on their Web site, the researchers demonstrate how the vote-stealing software works. The video shows the software sabotaging a mock presidential election between George Washington and Benedict Arnold. Arnold is reported as the winner even though Washington gets more votes. (The video is edited from a longer continuously shot video; the long single-shot version will be available for downloading from the center's site as well.)

The researchers also demonstrate how the machines "are susceptible to computer viruses that can spread themselves automatically and invisibly from machine to machine during normal pre- and post-election activity."

Felten said that policy-makers should be concerned about malicious software infecting the Diebold AccuVote-TS and machines like it, from Diebold and other companies. "We studied these machines because they were available to us," the researchers wrote in their Web posting. "If we had gotten access to another kind of machine, we probably would have studied it instead."

Felten said, "There is reason for concern about other machines as well, even though our paper doesn't directly evaluate them. Jurisdictions using these machines should think seriously about finding a backup system in time for the November elections."

Felten, a professor of computer science and public affairs who is known for his groundbreaking work in computer security, said that some of the problems discussed in the paper cannot be fixed without completely redesigning the machine.

Other problems can be fixed by addressing software or electronic procedures. "But time is short before the next election," he said.

According to the researchers' paper, the Diebold machine they examined and another newer version are scheduled to be used in 357 U.S. counties representing nearly 10 percent of all registered voters. About half those counties, including all Maryland and Georgia, will use the exact machine examined by Felten's group.

Felten said that, out of security concerns, the Diebold machine infected with the vote-stealing software has been kept under lock and key in a secret location.

"Unfortunately election fraud has a rich history from ballot stuffing to dead people voting," he said. "We want to make sure this doesn't fall into the wrong hands. We also want to make sure that policy-makers stay a step ahead of those who might create similar software with ill intent."

Source: Princeton University

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