

## Panel: E-voting vulnerable

By Anne Broache

[http://news.com.com/Panel+E-voting+vulnerable/2100-1028\\_3-5891237.html](http://news.com.com/Panel+E-voting+vulnerable/2100-1028_3-5891237.html)

Story last modified Fri Oct 07 16:01:21 PDT 2005

### **GAITHERSBURG, Md.--Overlooked bugs and malicious code pose a plausible threat to software on electronic voting machines, a panel of election experts said Friday.**

At a conference held by the National Institute of Standards and Technology, part of the U.S. Commerce Department, election officials, computer scientists and academics weighed in on steps that should be taken before, during and after elections to protect the voting systems against software-related problems. Voting has gone increasingly electronic during the past couple of election cycles, but the devices remain without national, uniform security standards.

Keeping electronics systems safe is not just about fending off hackers, members of the panel said.

"All of you running voting systems now are assuredly running software that has bugs in it--presumably in most cases not malicious--but software is buggy," Ron Rivest, a professor at the Massachusetts Institute of Technology, told the audience, composed largely of election officials from various parts of the country.

It's those bugs, the panel suggested, that are probably most likely to blame for irregularities in election outcomes. The problem can be quelled to an extent, the panel said, by insisting on a meticulous, higher-quality approach to software development, by certifying all products, and by openly disclosing the source code used.

The openness of voting systems is fundamental to a democratic system, said Michael Shamos, a Carnegie Mellon University computer science professor who has been a longtime election equipment certifier for Pennsylvania.

"If you spend three hours with a voting system, you can figure out how it works and you can replicate it yourself," Shamos said. "I think we need disclosure."

But the idea of exposing the code to outside eyes--not a new one--has spawned criticism from software industry groups such as the Information Technology Association of America, which say they worry it could breed election fraud.

Being able to account for the software's point of origin is also critically important, said Paul Craft, chief of voting systems certification for the state of Florida. He and others said problems have arisen when election workers didn't install the appropriate certified software on the machines in the first place.

The question that remained was just how realistic a threat malicious, deliberate attacks are--and how difficult they'd be to detect.

Shamos of Carnegie Mellon said he, for one, would bet money that no one, even an "omniscient hacker," could create software that "alters the outcome of an election, but does it in such a clever way that no amount of testing either before, after or during the election can reveal it."

He suggested that a tactic known as "parallel testing" could help detect irregularities. Using that method, select voting machines are discreetly "cordoned off" on election day and used only by a special team of people who pose as normal voters. The testers know in advance what the vote totals are supposed to be for those test machines, and the mock voters' behavior is videotaped, so if the ballot numbers don't match up, the testers know there's something wrong with the software.

Others disagreed with Shamos' reasoning. "It's another fence an adversary would have to jump over, but if he knew about it ahead of time, he could use measures to defeat parallel testing," Rivest said.

Some panelists imagined scenarios in which attackers posing as voters could slip corrupted "smart cards" into electronic voting machines that rely on such media or use a "signal"--say, a series of touch screen presses--that would trigger the

software to swap votes to another candidate.

They also expressed concern that, if voting machines were hooked up to wireless signals, someone could sit outside the warehouse where the machines were stored--or simply use a PDA inside the polling place--to transmit malicious software to the voting machines.

The solution? Design the systems with as few additional frills as possible.

"I don't know if I'm going out on a limb on this, but wireless and voting do not mix," Shamos said, drawing applause from the audience.

Copyright ©1995-2006 CNET Networks, Inc. All rights reserved.