The New York Times
nytimes.com

May 12, 2006

New Fears of Security Risks In Electronic Voting Systems

By MONICA DAVEY; GRETCHEN RUETHLING CONTRIBUTED REPORTING FROM CHICAGO FOR THIS ARTICLE, AND JOHN SCHWARTZ FROM NEW YORK.

With primary election dates fast approaching in many states, officials in Pennsylvania and California issued urgent directives in recent days about a potential security risk in their Diebold Election Systems touch-screen voting machines, while other states with similar equipment hurried to assess the seriousness of the problem.

"It's the most severe security flaw ever discovered in a voting system," said Michael I. Shamos, a professor of computer science at Carnegie Mellon University who is an examiner of electronic voting systems for Pennsylvania, where the primary is to take place on Tuesday.

Officials from Diebold and from elections' offices in numerous states minimized the significance of the risk and emphasized that there were no signs that any touch-screen machines had been tampered with. But computer scientists said the problem might allow someone to tamper with a machine's software, some saying they preferred not to discuss the flaw at all for fear of offering a roadmap to a hacker.

"This is the barn door being wide open, while people were arguing over the lock on the front door," said Douglas W. Jones, a professor of computer science at the University of Iowa, a state where the primary is June 6.

The latest concern about the touch-screen machines was only the newest chapter in an emerging political and legal fight around the country over voting machines. While some voting officials defend the ease of touch-screens (similar to A.T.M.'s), some advocacy groups argue that optical scan machines, using paper ballots, are far more secure.

The wave of high-tech voting machines was prompted by the 2000 election in Florida, which spotlighted the problems of old-fashioned punch card ballots. But the machines that soon followed have spurred division. Here in Chicago, where voters used both touch-screen and optical-scan systems in a March primary, it took officials a week to tally all the votes because of technical problems and human errors, touching off a flurry of criticism over the Sequoia Voting Systems equipment.

In Maryland this spring, the State House of Delegates passed a bill that would have scrapped touch-screen machines, but the Senate last month took no action on the bill, effectively killing the idea.

This week, Voter Action, a nonprofit group, assisted voters in Arizona in filing for a legal injunction to try to block the state from buying touch-screen electronic voting systems. The suit is among several the group says it has pursued, in states including California, New York and New Mexico.

The new concerns about Diebold's equipment were discovered by Harri Hursti, a Finnish computer expert who was working at the request of Black Box Voting Inc., a nonprofit group that has been critical of electronic voting in the past. The group issued a report on the findings on Thursday.

Computer scientists who have studied the vulnerability say the flaw might allow someone with brief access to a voting machine and with knowledge of computer code to tamper with the machine's software, and even,

potentially, to spread malicious code to other parts of the voting system.

As word of Mr. Hursti's findings spread, Diebold issued a warning to recipients of thousands of its machines, saying that it had found a "theoretical security vulnerability" that "could potentially allow unauthorized software to be loaded onto the system."

The company's letter went on: "The probability for exploiting this vulnerability to install unauthorized software that could affect an election is considered low."

David Bear, a spokesman for Diebold Election Systems, said the potential risk existed because the company's technicians had intentionally built the machines in such a way that election officials would be able to update their systems in years ahead.

"For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software," he said. "I don't believe these evil elections people exist."

Still, he said, the company will in the coming months solve the vulnerability, but not before most primary elections occur.

In places where the machines are used, most election officials said they were not worried.

"We're prepared for those types of problems," said Deborah Hench, the registrar of voters in San Joaquin County, Calif. "There are always activists that are anti-electronic voting, and they're constantly trying to put pressure on us to change our system."

Aviel Rubin, a professor of computer science at Johns Hopkins University, did the first in-depth analysis of the security flaws in the source code for Diebold touch-screen machines in 2003. After studying the latest problem, he said: "I almost had a heart attack. The implications of this are pretty astounding."