Cryptographic voting debuts

November 13 2009, by Larry Hardesty

In last week's municipal election in Takoma Park, Maryland, voters voted by exposing three-digit numerical codes printed on their ballots in invisible ink. By later verifying the codes online, they could help minimize the possibility of election fraud. Photo: Alex Rivest

(PhysOrg.com) -- Last week, in Takoma Park, Md., a new cryptographic voting system that could ensure accurate vote counts was used for the first time in a real election. MIT's Ron Rivest, the Viterbi Professor of Electrical Engineering and Computer Science, helped develop the system and says he's quite pleased with how the technology worked. Takoma Park's city clerk, Jessie Carpenter, agrees that the trial "went very well."

To minimize the disruption of existing voting procedures, the system, called Scantegrity II, was designed to work with ordinary optical-scan voting technology. Optical-scan voting — which has become the dominant technology in the United States since the 2000 presidential election — usually requires the voter to fill in bubbles printed on a ballot next to candidates' names. With Scantegrity II, the voter instead uses a special pen to expose a code printed inside the bubble in invisible ink. Thereafter, the ballot is fed into an ordinary optical reader, which simply determines which bubbles have been darkened.

Any voter who'd later like to confirm her vote can simply jot down the code that's in the exposed bubble, along with the ballot's serial number, and take that information home. (In the Takoma Park election, voters could record their codes on cards stacked in the voting booths, which were printed with the names of the contested offices — mayor and city councilor.) The voter can then look up that serial number on the election commission's website and confirm that it's correlated with the code inside the bubble she marked. Although on the website, the code is never associated with the candidate's name, Scantegrity ensures that if just 2 percent of voters confirm their codes, it's statistically almost impossible for vote tampering to go undetected.

The key to the system is that before the election, the election commission prepares a set of tables that, taken together, link the ballot codes and the candidates' names; but that link can't be deduced from any one table by itself. Then the commission publicly releases a set of digital signatures that cryptographically describe all the entries in the tables without actually revealing them. That way, the tables can't be tampered with after the ballots are cast, but neither do they reveal any information that ballot stuffers could use before the election.

After the election, the election commission releases some of the information contained in the tables — including the codes exposed on all

the recorded ballots — along with encryption keys that verify its authenticity. The partially revealed tables conceal enough information to preserve voter anonymity: There's no way to figure out which ballot went for which candidate. But they reveal enough information that anyone interested in performing an audit can ferret out fraud.

Going into the Takoma Park trial, the crucial question was whether 2 percent of voters would bother to write down their codes and check them online. According to Poorvi Vora, a member of the Scantegrity team at George Washington University, 1,722 votes were cast and 66 people checked their codes — almost 4 percent.

Carpenter says that she would have liked that number to be higher. But "that's not the fault of the Scantegrity system," she says. "We needed to have done more education of the voters."

Another question was whether the decoder pens would hold up over the course of the day. "The smudging issue was one we were slightly concerned about," Rivest says. "You know, if you take a highlighter and you run it over newspaper, it will collect the black ink." Poll workers, he says, were instructed to check the decoder pens occasionally to make sure they were in good working order. But "the ink seemed to be lasting fine," Rivest says, and "smudging wasn't much of an issue."

Carpenter adds that a very small number of voters refused to use the decoder pens, instead pulling out their own ink pens and filling in the bubbles. But since the Scantegrity system requires no modification to the optical scanners, that kind of improvised procedural change didn't affect the final tally.

"I was a little bit afraid that we'd have a lot of invalid ballots," Carpenter says. "But we didn't. We had some, but I don't think it was high compared to any other ballot-marking system." Rivest confirms that,

according to the Scantegrity team's research, the fraction of invalid ballots was consistent with that seen in conventional optical-scan voting.

"I don't think the system slowed us down at all," Carpenter adds. Slightly after 5 p.m., she says, a large wave of voters hit the polls, and the wait got up to about 15 minutes, she says. But Carpenter believes that the sudden surge was the result of a story on a local National Public Radio affiliate describing the Scantegrity trial. "I think we got a little publicity boost that made people come out who might otherwise not have come out," she says. "We just had tremendous lines once that story hit, and I can't believe it was coincidence."

When Takoma Park decided to use the Scantegrity system, "we certainly took notice of that," says Matthew Masterson of the U.S. Election Assistance Commission, which oversees voting technologies and procedures in the United States. "The National Institute of Standards and Technology, who's our partner in developing the standards, just held a conference on end-to-end cryptographic systems [like Scantegrity II], and we've started the process of looking at systems like that and how to test them." Masterson adds that "anytime a jurisdiction takes a look at new technology like that —the cryptographic end-to end system in this case — that's a great conversation for voters and election officials to be having. And in that sense, it's very positive for democracy."

Provided by Massachusetts Institute of Technology (news : web)