Compliance Toolkit

Electronic voting: Moving beyond the ballot box

- Tags:
- electronic voting,
- ballot box

Declan McCullagh CNET News.com
Published: 08 Jun 2004 16:20 BST

Encrypted receipts

The leading contenders so far, independently created by Chaum and mathematician Andrew Neff, represent two variants of a voting technology that uses encrypted printed receipts to solve many of the problems that have bedevilled existing hardware. These prototypes work in the lab. But one obstacle may be whether notoriously conservative voting officials can be convinced to try something new.

The idea of having computerised voting machines produce paper receipts, providing a physical record that can be audited, is believed among voting experts to be a useful safeguard against fraud. But some counties that have already installed printerless, computerised voting systems oppose any requirement that they add new equipment to provide paper receipts of any kind.

Other proposals for providing paper receipts in computerised voting systems include attaching printers to voting machines that spit out a hard copy of votes recorded below a glass barrier. Once voters reviewed the receipts and confirmed that they were accurate, the receipts would be placed in a secure box. If a recount were required, voting officials would open the boxes and proceed to tally up the results by hand.

Critics of this type of receipt argue that the end product is little better than a punch card ballot, subject to many of the same kinds of miscount problems that plagued the Florida election in 2000. Encrypted systems like Chaum's, on the other hand, would not be vulnerable to many of those flaws, because only the records that were tampered with would be subject to verification in a recount. In addition, tampering could be detected the moment a voter left the polling station.

Chaum, who declines to give his age for privacy reasons, boasts a dazzling resume as one of the brightest computer scientists of the 1980s, whose ideas led to the creation of anonymous remailers, privacy-protecting Web browsing techniques and secure electronic cash. He returned to the topic of secure voting four years ago and came up with his crucial innovation -- encrypted receipts on plain paper -- in late 2003. Chaum owns patents covering the use of the technology. After the Florida recount debacle, "I decided that maybe there was a chance that these systems would be used," Chaum says. "But I needed to find a way to make them practical."

Chaum's insight was to invoke the logic of cryptography to prove that votes can't be changed after the voter leaves the polling booth. For each voter, his machine prints bar code-like dots on two strips of paper that, when combined under the carefully angled lens of a custom viewfinder, reveal the name of the candidate in plain English. The voter can keep only one encrypted strip as a receipt for use in post-election auditing -- but without its mate, an individual strip will not reveal which candidate was

chosen.

For cryptographers, the inherent beauty of such a system is that it safeguards privacy and security -- and doesn't require voters to trust the government or untested software on a voting machine. "The next real issue is, 'When can I buy it?'" says Chaum, who created a company called Votegrity to develop and sell the hardware. "That's why we have to aggressively push forward with the company at this stage to make it an option." He is looking for investors and a chief executive to bring his system to market.

This isn't the first time that Chaum has launched a start-up with a clever idea and a sheaf of patents. A decade ago, he founded the pioneering DigiCash company, but it ended up filing for Chapter 11 bankruptcy protection in 1998. Chaum says voting systems are an easier sell because digital cash wasn't attractive until many people were using it -- a catch-22 that ultimately doomed the plan.

Injecting encryption into elections, central to both the Chaum and Neff systems, began receiving serious attention after a group of top scientists convened a small workshop in Tomales Bay, California, nine months after the Florida recount. At the 26 and 27 May conference sponsored by Rutgers University's DIMACS computer science centre this year, experts in the field seemed ready to accept that the Chaum and Neff systems were secure enough to be used in a real-world election.

"It's an important step forward," Moti Young, a professor of computer science at Columbia University, says of Chaum's design. "I don't see any bugs. It's technically very sound."

Poorvi Vora, an assistant professor of computer science at George Washington University, is also enthusiastic. Vora and her graduate students wrote their own software, based on Chaum's two-strip concept, and demonstrated it at the Rutgers conference. Instead of using a custom viewfinder, they printed on transparencies that can be laid on top of each other on an overhead projector.

But not everyone in the e-voting community is so enthusiastic about the Chaum and Neff systems. Rebecca Mercuri, who wrote her Ph.D. dissertation on electronic vote tabulation, says she remains sceptical.

"I can read the math," Mercuri says. "I am holding the bar very very high...I will continue to serve as a sceptic. I have not been convinced yet. It does not exist in the form where people can use it yet."

TALKBACK

Post a comment

1 comment

If the final vision is one where citizens can vote... Kikki Bona Sijabat