

Review finds potential flaws in voting systems

Flaws that leave electronic voting machines vulnerable to security attacks were discovered by University of California researchers as part of an unprecedented "Top-to-Bottom Review" of the systems commissioned by California Secretary of State Debra Bowen.

The review, begun May 31, was designed to restore the public's confidence in the integrity of the electoral process and to ensure that California voters are being asked to cast their ballots on machines that are secure, accurate, reliable and accessible. Bowen released key findings of the "Red Team" part of the review on July 27. Other sections of the review dealing with source code, voting system documentation and accessibility are to be made public later.

The red teams were able to compromise the physical and software security of all three systems tested. The researchers noted, however, that protecting the security of the voting process entails more than ensuring the security of the voting machines.

"Our task was to analyze the machines, but those machines are just one piece of what makes an election secure," said Matt Bishop, professor of computer science at UC Davis, who led the Red Team review. "In my 30 years in this field, I've never seen a system that was perfectly secure, but proper policies and procedures can substantially improve the security of systems. Paper ballots aren't perfect, either, but we've been working with them longer so we know more about how to control the weaknesses in a paper-based system."

Bishop will testify today, Monday, July 30, at a public hearing on the review at the Secretary of State's office in Sacramento.

The three electronic voting systems examined were made by Diebold Elections Systems, Sequoia Voting Systems and Hart InterCivic, respectively. The voting systems are used in 43 of the 58 counties in California by 9 million of the state's 15.7 million registered voters.

The researchers said that many of the security problems they encountered were fairly similar across the three systems.

"The problem with the systems should have been detected early in their development," said Bishop. "There are ways to develop and implement systems that resist compromise much better than the systems we examined. Many of these safeguards are taught in undergraduate and graduate computer security courses, but it was clear they were not used effectively in the electronic voting systems we evaluated."

The Red Team testers were able to bypass the machines' tamper-resistant seals and locks, physically gaining access to the memory cards that store the votes. Such a vulnerability could potentially be exploited on Election Day, the researchers said.

"In many cases, this could be done in less than a minute, and in a way that would not necessarily be noticed by poll workers, particularly if there are privacy shields and curtains blocking their view of the voter," said Bishop.

Once inside the machine, the researchers noted that an individual could then switch out the memory cards. Such a breach might be detected if procedures are in place to compare the memory cards with the votes stored in the machine's internal memory and with the paper trail that is required in California, the

researchers said.

While the Red Team benefited from the work by the source code team, led by David Wagner, associate professor of computer science at UC Berkeley, the researchers emphasized that knowledge of a voting system's source code, while helpful, is not critical to breaking down its security barriers.

"Keeping the source code and other system information secret provides a false sense of security for the systems," said Bishop. "We really only had five weeks to try to penetrate the machines' defenses, but people intent on breaking through the security would spend as much time as necessary to find holes to exploit."

The review also notes that all systems are vulnerable to tampering by people who have access to the machines when votes are tabulated. However, this requires a high level of access, and most counties have careful controls over the people who have access to voting equipment.

Another problem is the potential for the sabotage of machines before an election. Technical glitches in electronic voting machines can take hours to fix, leading to long lines and potentially disenfranchised voters who might be unable to wait, the researchers said.

The 42 members of the UC Davis and UC Berkeley research teams included internationally recognized experts in computer science, computer security, electronic voting, law and public policy. Team members included faculty, post-doctoral scholars, graduate students, and other experts from UC Santa Barbara, Princeton University and other universities, as well as experts from industry, including Consilium, LLC.

Other components of the project include a review of electronic voting system documentation to determine whether those materials are complete and consistent, and an evaluation of system accessibility for voters with disabilities and with special language requirements. The entire report is available online at http://www.sos.ca.gov/elections/elections_vsr.htm.

Source: University of California - Davis

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.