

E-Voting machines face decertification

- by Tom Courbat

State security/hack teams expose numerous ways to manipulate Sequoia E-Voting Machines used in Riverside and San Bernardino Counties.



Late Friday afternoon, July 27 2007, Secretary of State (SOS) Debra Bowen announced that in just five short weeks, security teams were able to *“bypass both physical and software security in every [E-voting] system they tested,”* [emphasis added]. California state law requires the SOS to review voting systems and withdraw approval if found to be unacceptable. The SOS has the option of attaching additional conditions to a certification that could mitigate potential vulnerabilities.

Public hearing, then final decision

In a press interview the afternoon of the 27th, Ms. Bowen stated that “a decision regarding every system tested WILL be made by August 3rd.” State law requires that the SOS provide any certification changes no later than six months before a statewide election. In this case, that is the upcoming presidential primary elections, to be held in California on February 5, 2008. A public hearing was scheduled for July 30th for input from the public and the vendors to assist the SOS in making final recommendations regarding the fate of E-voting systems in California.

Seven easy pieces

The report detailed seven attack scenarios that were successful in breaking into the Sequoia Edge II DRE touchscreen machines, the Central Tabulator (which tallies all the voting cartridges from the 3,700 machines currently in Riverside County), and the new, new Sequoia scanning machines for which the county is right now considering paying out millions of dollars.

The report was particularly critical of the “paper trails” printed by the new machines. It outlined a number of ways in which the paper trails gave a false sense of security to the voter, assuming the voter even checked the paper trail against how he/she actually voted. Most studies show that less than one in five voters even checks the results, allowing the machines to easily print results that are not reflective of how the voter voted.

Insiders to blame 95% of time

Computer-voting scientist Harri Hursti, who addressed the Riverside County Board of Supervisors’ hand-picked “Blue Ribbon” Elections Review Committee in March, reported that “typically 95% of computer fraud is committed by insiders.” That makes sense, since they have the most knowledge of the system and often 24/7 unfettered access, and in Riverside County, in a warehouse of 3,700 machines with no video monitoring. It is a situation ripe for internal attack.

Election rigging examples

One example of vote tampering would be where "...the Edge system returns a vote count of 5,400 but only 5,000 people showed up to vote," the report quoted. Since it would "...not be possible to tell which votes are the ones added and which are legitimate ones... it should be considered an effective attack that will affect the outcome of an election."

Another example is forging update cartridges, since the password used to protect the updating process from abuse is stored on the cartridge itself, according to the report. In other words, as many votes as desired could be transferred from Candidate A to Candidate B without leaving a trace.

It runs on Windows, just like your computer

One of the reports issued, entitled "Security Evaluation of the Sequoia Voting System Public Report" reported that the software responsible for the management of the election process (including programming, configuring, tabulating and reporting the results) is a program called WinEDS. Win EDS is composed of two Windows programs running on a Windows XP operating system. Windows has been notorious for its vulnerability to viruses and Trojan horses that can modify the outcome of any election, and "...WinEDS...therefore inherits the vulnerabilities associated with that operating system."

Upgrading to a "functionally identical" system for \$15 million

The same report stated that the AVC Edge Model I and II "are for all intents and purposes functionally identical...[and] are capable of being controlled by the same system firmware image". Yet Riverside County, against recommendations of local Election Integrity advocates, chose to "upgrade" their Model Is for Model IIs in February 2006 for "only" \$15 million (less a \$2 million "trade-in" allowance).

Tricking the machines to report any result desired

Other concerns were that the "Logic and Accuracy" testing was a non-starter, as it was easy to create malicious firmware that could count accurately during the L&A test, and then introduce errors during the actual voting procedure. In fact, the report went on to state "There is no way to determine which version of the firmware is running on an Edge device" and thus"...there is no secure, hardware-based mechanism to ensure that no corrupted firmware gets loaded and executed...the Edge firmware is stored on a flash memory card and can be easily overwritten."

A final example, and there are many more, was the case of "sleepovers" wherein voting machines would be delivered days or a week or more in advance of an election to a polling place and then not properly guarded, giving easy access to anyone who wished to install malicious code and change election outcomes. Changing just one memory card on one DRE touchscreen can then infect the central computer and change thousands of votes, without leaving a trace.

Official findings confirm worst predictions of Election Integrity advocates

For those who have been following the concerns with E-voting, there were few surprises, but activists breathed a collective sigh of relief at seeing the shortcomings they have been warning of for years finally confirmed by an official state study, conducted through the University of California.