Electronic Voting Machine Information Sheet

Sequoia Voting Systems — AVC Edge

Name / Model: AVC / Edge[1]
Vendor: Sequoia Voting Systems, Inc.
Voter-Verifiable Paper Trail Capability: Yes.[2]



Brief Description: The Sequoia AVC Edge is a touch screen direct-recording electronic (DRE) voting machine. It is a multilingual voting system activated by a smart card that records votes on internal flash memory. Voters insert a "smart-card" into the machine and then make their choices by touching an area on a computer screen, much in the same way that modern ATMs work. The votes are then recorded to internal electronic flash memory. When polls close, the votes for a particular machine are written to a "PCMCIA card" which are removed from the system and either physically transported to election headquarters or their contents transmitted via computer network.

Checking the Voter-Verifiable Paper Trail: The Edge's optional voter-verifiable paper-trail printer is called the VeriVote. The VeriVote printer is a cash-register type printer and is located to the left of the touch screen. Where the VeriVote is available, voters should be encouraged to check the printout to make sure it correctly reflects their choices, before they cast their ballot. Jurisdictions using the Edge *without* the VeriVote attachment include: District of Columbia, Louisiana (early voting), Indian River and Palm Beach Counties, FL (mainly for accessible voting), York County, PA, Salem County, NJ, Arapahoe County, CO, and a number of jurisdictions in Virginia.

Detailed Voting Process: When the voter enters the precinct, he or she is given a "smart-card" by a poll worker after confirming the voter is registered. A "smart-card" is a card the size and shape of a credit-card which contains a computer chip, some memory and possibly basic data such as the voter's political party. The voter then takes the smartcard to a voting machine and inserts the smart-card into the yellow slot visible in the middle

[1] See: http://www.sequoiavote.com/productguide.php?product=AVC%20Edge
[2] When equipped with a VeriVote printer.

Electronic Voting Machine Information Sheet

Sequoia Voting Systems — AVC Edge

picture above. The first screen presented to the voter is one that allows him or her to choose the ballot language. After using the touchscreen to vote, 1) the record of the vote is directly recorded electronically to two flash memory cards and 2) the voter's smart card is reset to ensure that the voter can only vote once. The AVC Edge may also be equipped in some precincts to print a voter-verifiable paper audit trail using the VeriVote printer. In this case, the voter will inspect the printout that is displayed underneath glass. If the paper accurately reflects the vote, the voter indicates so using the touchscreen and casts the vote; the printed paper is withdrawn into the machine to protect privacy. If the paper is incorrect, the voter may mark it as spoiled and change his or her vote using the touchscreen interface. After the vote is cast, the smart-card pops out of the machine and the voter returns it to a poll worker.

When the polls close, a poll worker or election official inserts a different-type of smart card, an administrator card, into each voting machine and puts the machine into a postelection mode where it will no longer record votes. At this point, the machine writes the votes from its internal memory to flash memory on a "PCMCIA card." The PCMCIA card is merely a removable form of flash memory. A printed tape of all votes cast or vote totals for the voting machine can also be printed out at this time depending on local procedure and regulations**.**

The PCMCIA cards are removed from each machine and either taken to a central tabulation facility or to remote tabulation facilities. At the tabulation facility the votes are copied from the PCMCIA cards and into a central computer database where precincts are combined to result in an aggregate vote. The votes may also be transmitted to the central tabulation facility via a closed "Intranet", the Internet or modem. The PCMCIA cards and possible any printouts from the voting machines can then become part of the official record of the election.

Things to Look Out For

- Security Seals. Ideally, the Edge's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: http://www.flickr.com/photos/joebeone/2247733620/ . Seals should be logged to maintain chain of custody of sensitive materials.
- Memory Cards and Physical Access. The internal (cryptographic) keys used to protect the Edge from software modification are hard-coded into the software. This means that physical access to a single Edge or Edge memory card could jeopardize the security of all Edge machines with a given hard-coded key. With this key, an attacker could forge a software update cartridge and upload software of her own design. Memory cards and physical access to Edge machines are

sensitive and care should be exercised in terms of allowing unsupervised access to memory cards or Edge DRE units.

- Poor Provisional Ballot Notification. If a jurisdiction is using its Edges to allow electronic provisional votes, the only indication that a voter is casting a provisional vote with a provisional vote smartcard is the words "Provisional Voter" on the VVPAT tape. We are uncertain if there is any indication of provisional ballot status on Edge machines that do not use the VeriVote VVPAT attachment.
- Forging and Duplication of Voter Cards. With knowledge of the hard-coded key used with Voter Cards, it is possible to forge valid Voter Cards. Also, between the time a voter's Voter Card is activated by the pollworker and used, it can be duplicated and used to vote multiple times, without any knowledge of the hard-coded key. Smartcard duplication equipment can be hidden easily on a voter's person. To protect against duplicate voting, be on the watch out for some sounds that might indicate duplicate voting: 1) each time a Voter Card is ejected from the Edge, it makes a loud click sound; 2) also, if the Edge is equipped with the VeriVote VVPAT printer, printing out of the VVPAT record will also be noticeably loud each time a vote is cast.

Past Problems

August 2007: *California.* Following an expert top-to-bottom review of voting systems which finds critical security vulnerabilities in the Edge, the Secretary of State disallows the machine's use as a primary voting system.[3]

March 2006: *Florida.* Touch screen voting machines malfunction, switch votes on the screen. One candidate watched his vote for himself switch to his opponent.[4] Group calls for audit of March 7 elections. Members say the results are "highly suspect" after an elections staffer was given the code to a computer server.[5]

November 2004: *Washington*. Voters in at least four polling precincts in Snohomish County said they have encountered problems with the Sequoia electronic voting machines. When they touched the screen to vote for a candidate, an indicator showed

[3] Sequoia Voting Systems, Withdrawal of Approval/Conditional Reapproval, Secretary of State of California,October 25, 2007, http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia_102507.pdf
[4] Id.
[5] Id.

they had selected the opposing candidate. It took at least four attempts before the indicator showed the correct candidate.[6]

October 2004: *New Mexico.* Votes change on the screen and are resistant to voter's attempt to vote for their choice.[7]

September 2004: *Florida.* High percentages of undervotes in the primary election present the county with an unanswerable question since the paperless machines provide no method of doing an audit.[8]

References:

Blaze, M., Cordero, A., Engle, S., Karlof, C., Sastry, N., Sherr, M., et al. (2007). Source Code Review of the Sequoia Voting System. California Secretary of State. Retrieved January 29, 2008, from http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf.

"DRE Security Assessment, Volume 1, Computerized Voting Systems, Summary of Findings and Recommendations," InfoSENTRY, 21 Nov. 2003. See: http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf

"Direct Recording Electronic (DRE) Technical Security Assessment Report," Compuware Corporation, 21 Nov. 2003. See: http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

[6] Id.
[7] Id.
[8] See http://www.votersunite.org/info/Sequoiainthenews.pdf